

IBM Spectrum Protect  
8.1.12

テープ・ソリューションのガイド



## 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、[225 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 (製品番号 5725-W98、5725-W99、5725-X15) のバージョン 8、リリース 1、モディフィケーション 12、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。

© Copyright International Business Machines Corporation 1993, 2021.

# 目次

<b>本書について.....</b>	<b>vii</b>
本書の対象読者.....	vii
資料.....	vii
<b>新機能.....</b>	<b>ix</b>
<b>第 1 部計画.....</b>	<b>1</b>
テープ計画の要件.....	2
テープ・ベースのソリューションのシステム要件.....	3
ハードウェア要件.....	3
ソフトウェア要件.....	6
計画ワークシート.....	8
ディスク・ストレージの計画.....	12
ストレージ・アレイの計画.....	12
磁気テープ・ストレージの計画.....	14
サポートされるテープ装置およびライブラリー.....	14
サポートされるテープ装置構成.....	15
ストレージ装置間でのデータ移動.....	15
ライブラリー共有.....	16
LAN フリー・データ移動 (LAN-free data movement).....	16
単一ライブラリーでの混合装置タイプ.....	17
磁気テープ・ストレージ装置の定義.....	19
ストレージ・プール階層の計画.....	20
オフサイト・データ・ストレージ.....	23
セキュリティの計画.....	24
管理者役割の計画.....	24
セキュア通信の計画.....	25
暗号化データのストレージの計画.....	25
ファイアウォール・アクセスの計画.....	26
<b>第 2 部実装.....</b>	<b>29</b>
システムのセットアップ.....	30
ストレージ・ハードウェアの構成.....	30
サーバー・オペレーティング・システムのインストール.....	31
AIX システムへのインストール.....	31
Linux システムへのインストール.....	33
Windows システムへのインストール.....	37
マルチパス入出力の構成.....	38
AIX システム.....	38
Linux システム.....	39
Windows システム.....	40
サーバーのユーザー ID の作成.....	41
サーバーのファイル・システムの準備.....	41
AIX システム.....	42
Linux システム.....	43
Windows システム.....	44
サーバーおよび Operations Center のインストール.....	45
AIX および Linux システムへのインストール.....	45
グラフィカル・ウィザード用の前提条件 RPM ファイルのインストール.....	46
Windows システムへのインストール.....	46

サーバーおよび Operations Center の構成.....	47
サーバー・インスタンスの構成.....	47
バックアップ/アーカイブ・クライアントのインストール.....	48
サーバーのオプションの設定.....	49
セキュリティの概念.....	50
トランスポート層セキュリティを使用したセキュア通信の構成.....	52
Operations Center の構成.....	53
Operations Center とハブ・サーバーの間の通信の保護.....	54
製品ライセンスの登録.....	55
ビジネスに合わせたデータ保存ルールの定義.....	56
サーバー保守アクティビティのスケジュールの定義.....	56
バックアップ・メディアの移動.....	61
保存セット・データの磁気テープ・ストレージとの間での移動.....	67
クライアント・スケジュールの定義.....	75
サーバーのテープ装置の接続.....	75
ユーザーのシステムへの自動ライブラリー装置の接続.....	75
ライブラリー・モードの設定.....	76
テープ・デバイス・ドライバーの選択.....	76
IBM テープ・デバイス・ドライバー.....	76
IBM Spectrum Protect テープ・デバイス・ドライバー.....	77
テープ装置の特殊ファイル名.....	78
テープ・デバイス・ドライバーのインストールと構成.....	79
IBM テープ装置用の IBM デバイス・ドライバーのインストールと構成.....	79
AIX システム.....	83
Linux システム.....	86
Windows システム.....	89
サーバーで使用するライブラリーの構成.....	90
テープ装置の定義.....	92
ライブラリーおよびドライブの定義.....	92
テープ装置クラスの定義.....	94
ライブラリー共用の構成.....	101
例: AIX および Linux サーバーのライブラリー共有.....	102
例: Windows サーバーのライブラリー共有.....	103
ストレージ・プール階層のセットアップ.....	106
アプリケーションおよびシステムの保護.....	108
クライアントの追加.....	108
クライアント・ソフトウェアの選択およびインストールの計画.....	109
クライアント・データのバックアップおよびアーカイブに関するルールの指定.....	110
バックアップおよびアーカイブの操作のスケジュール.....	114
クライアントの登録.....	115
クライアントのインストールおよび構成.....	116
LAN フリー・データ移動の構成.....	120
LAN フリー構成の妥当性検査.....	121
暗号化方式.....	122
磁気テープ・ドライブの暗号化の構成.....	124
磁気テープ・ストレージ操作の制御.....	125
IBM Spectrum Protect によるボリュームの満たし方.....	125
テープ・ボリュームの見積容量の指定.....	126
テープ・メディアの記録形式の指定.....	126
ライブラリー・オブジェクトと装置クラスとの関連付け.....	127
テープ装置のメディア・マウント操作の制御.....	127
同時にマウントされるボリュームの数の制御.....	127
ボリュームのマウント保存期間の制御.....	128
サーバーがドライブを待つ時間の制御.....	129
操作の優先使用.....	129
マウント・ポイントの優先権.....	129
ボリューム・アクセスの優先権.....	130
SAN 上の装置変更の影響.....	131

装置情報の表示.....	131
Write-once, read-many テープ・メディア .....	132
WORM 対応ドライブ.....	132
WORM メディアのチェックイン .....	132
WORM メディアに対する制約事項.....	133
WORM メディアのマウント障害.....	133
WORM メディアの再ラベル付け.....	133
ライブラリーからの専用 WORM ボリュームの除去.....	133
DLT WORM ボリュームの作成.....	133
短いまたは通常の 3592 WORM テープのサポート .....	134
WORM パラメーター設定の装置クラスの照会.....	134
装置の問題のトラブルシューティング .....	134
実装の完了.....	135
<b>第 3 部モニター.....</b>	<b>137</b>
日次チェックリスト.....	137
定期的なチェックリスト.....	147
ハードウェア・エラーに関するテープ・アラート・メッセージのモニター .....	154
メディアの非互換性によるエラーの防止.....	154
クリーナー・カートリッジでの操作.....	155
ライセンス準拠の検証.....	156
E メール・レポートを使用したシステム状況のトラッキング.....	157
<b>第 4 部管理 .....</b>	<b>159</b>
Operations Center の管理.....	159
クライアントの操作の管理.....	159
クライアント・エラー・ログのエラーの評価.....	159
クライアント・アクセプターの停止および再始動.....	160
パスワードの再設定.....	161
クライアント・アップグレードの管理.....	162
クライアント・ノードの廃止.....	163
ストレージ・スペースを解放するためのデータの非活動化.....	165
データ・ストレージの管理.....	166
インベントリー容量の管理.....	166
スケジュール済み活動のチューニング .....	168
クライアント・ファイルのコロケーションの使用可能化による操作の最適化.....	169
操作に対するコロケーションの影響.....	170
コロケーションが有効にされたボリュームの選択.....	172
コロケーションが無効にされたボリュームの選択.....	174
コロケーション設定.....	175
コピー・ストレージ・プールのコロケーション.....	175
保存ストレージ・プールのコロケーション.....	176
コロケーションの計画と使用可能化.....	177
テープ装置の管理.....	179
取り外し可能メディアの準備.....	179
テープ・ボリュームのラベル付け.....	179
ライブラリーへのストレージ・ボリュームのチェックイン.....	181
ボリューム・インベントリーの管理.....	186
ボリュームへのアクセスの制御.....	187
テープの再利用.....	187
スクラッチ・ボリュームの提供の維持.....	189
WORM メディアを含むライブラリーにおけるボリューム提供の維持.....	190
自動ライブラリー内のボリューム・インベントリーの管理.....	190
部分的に書き込まれているボリューム.....	194
共有ライブラリーの操作.....	194
サーバーによるボリューム要求.....	196
磁気テープ・ドライブの管理.....	198

ドライブの更新.....	198
テープ装置のオフラインでの使用.....	199
テープに対する読み取り/書き込み操作中のデータ検証.....	199
サポートされるドライブ.....	200
論理ブロック保護の有効化および無効化.....	201
ボリュームに対する読み取り/書き込み操作.....	202
テープ・ライブラリー内でのストレージ・プール管理.....	202
磁気テープ・ドライブのクリーニング.....	203
磁気テープ・ドライブのクリーニング方法.....	203
自動ライブラリーでドライブ・クリーニングを行うためのサーバーの構成.....	204
ドライブ・クリーニングに関連するエラーの解決.....	206
磁気テープ・ドライブの置換.....	207
磁気テープ・ドライブの削除.....	207
ドライブを同じタイプの別のドライブと置換.....	208
アップグレードされたドライブへのデータのマイグレーション.....	208
サーバーの保護.....	209
管理者の管理.....	209
パスワード要件の変更.....	210
システムでのサーバーの保護.....	211
サーバーへのユーザー・アクセスの制限.....	211
サーバーの停止および始動.....	212
サーバーの停止.....	212
保守または再構成のタスクのためのサーバーの始動.....	213
サーバーのアップグレード計画.....	214
障害に対する準備.....	215
DRM を使用した災害に対する準備と災害からのリカバリー.....	215
災害時回復計画ファイル.....	215
サーバーおよびクライアントのデータのリカバリー.....	218
リカバリー・ドリル.....	219
データベースのリストア.....	220
<b>付録 A アクセシビリティ .....</b>	<b>223</b>
<b>特記事項.....</b>	<b>225</b>
<b>用語集.....</b>	<b>229</b>
<b>索引.....</b>	<b>231</b>

## 本書について

---

本書は、IBM Spectrum Protect ベスト・プラクティスを使用するデータ保護ソリューションの計画、実装、モニター、および操作に関する情報を提供します。

## 本書の対象読者

---

本書は、IBM Spectrum Protect の管理者として登録されている方を対象としています。IBM Spectrum Protect は、一人の管理者が管理することもできますが、複数の担当者が管理責任を分担することもできます。

サーバーが置かれているオペレーティング・システムおよびクライアント /サーバー環境に必要な通信プロトコルを理解している必要があります。また、お客様の所属する組織でのストレージ管理業務 (ワークステーション・ファイルの現行のバックアップ方法およびストレージ装置の使用方法など) についても理解している必要があります。

## 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、およびその他の IBM® のストレージ管理製品が含まれています。

IBM 製品の資料については、[IBM Knowledge Center](#) を参照してください。





## このリリースの新機能

---

このリリースの IBM Spectrum Protect では、新機能および更新が導入されました。

このリリースの新機能および更新情報のリストについては、以下のトピックを参照してください。

- [サーバー・コンポーネントの新機能](#)
- [クライアント・コンポーネントの新機能](#)

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。



# 第1部 テープ・ベースのデータ保護ソリューションの計画

ディスクからディスク、さらにディスクからテープへのバックアップ操作やディスクからテープへのバックアップ操作などのデータ保護ソリューションを計画し、ストレージを最適化します。

## 計画ロードマップ

1 ページの図1のアーキテクチャー・レイアウトを参照して、ダイアグラムの後に示されたロードマップ・タスクを実行することで、テープ・ソリューションを計画します。

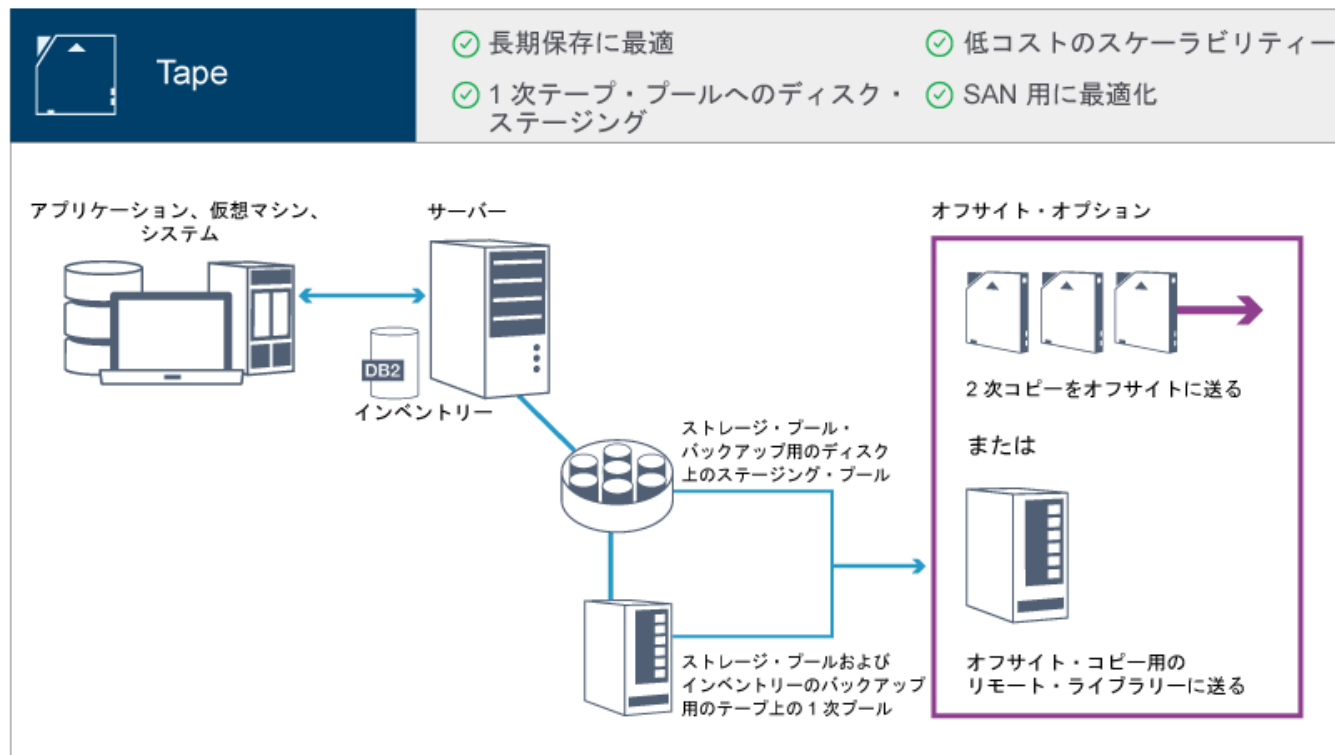


図1. テープ・ソリューション

このデータ保護構成では、サーバーは、ディスク・ストレージと磁気テープ・ストレージの両方のハードウェアを使用します。ストレージ・プール・ステージングが使用され、クライアント・データは、最初にディスク・ストレージ・プールに保管された後、磁気テープ・ストレージ・プールにマイグレーションされます。災害復旧のために、テープ・ボリュームをオフサイトに保管することができます。オフサイト・オプションには、クーリエによるオフサイトへの2次コピーの物理的な移動や、オフサイトのリモート・ライブラリーへのコピーの電子ボルト収容などがあります。

### ヒント:

- ここで説明されているソリューションでは、データはディスク・ストレージ・プールから磁気テープ・ストレージにマイグレーションされます。一方、データをマイグレーションする代わりに、IBM Spectrum Protect バージョン 8.1.8 で導入された「テープへの層化 (tiering-to-tape)」機能を使用できます。この機能を使用すると、ディスクのディレクトリー・コンテナ・ストレージ・プールから磁気テープ・ストレージにデータを自動的に層化できます。すべてのデータを指定の経過時間しきい値に基づいて層化すること、または非アクティブ・データのみを経過時間しきい値に基づいて層化することを指定できます。磁気テープ・ストレージへのデータの層化について詳しくは、[クラウドまたは磁気テープ・ストレージへのデータの層化](#)を参照してください。
- 説明されているソリューションには、ノード複製は含まれません。ノード複製を使用してディスク間でストレージ・プールをバックアップしたい場合は、データがディスクからテープにマイグレーションされ

る前に、複製操作が完了している必要があります。また、ノード複製を使用して、ローカル・テープ装置上のストレージ・プールをローカル・テープ装置上のコピー・ストレージ・プールにバックアップすることもできます。

テープ・ベースのソリューションを計画するには、以下のタスクを実行します。

1. ハードウェアおよびソフトウェアのシステム要件を満たします。
2. 計画ワークシートにご使用のシステム構成の値を記録します。
3. ディスク・ストレージを計画します。
4. 磁気テープ・ストレージを計画します。
5. セキュリティを計画します。

## テープ計画の要件

テープ・ソリューションを実装する前に、システム要件についての一般ガイドラインを確認してください。データをディスクまたはテープのどちらにバックアップするか、あるいはその両方を組み合わせるかを決定します。

### ネットワーク帯域幅

ネットワーク操作には、クライアントとサーバーの間で予想されるデータ転送、およびクロスサイト・リストア操作 (これらは災害復旧に必要) に十分な帯域幅が必要です。サーバーとディスク装置およびテープ装置の間のデータ転送には、ストレージ・エリア・ネットワーク (SAN) を使用してください。詳細については、[3 ページの『ハードウェア要件』](#)を参照してください。

### データ・マイグレーション

すべてのデータをディスクからテープに毎日マイグレーションします。ディスク・ベースのストレージ・プールに対して FILE 装置クラスを指定します。マイグレーションをスケジュールして、処理が行われるタイミングを制御します。マイグレーションしきい値に基づく自動マイグレーションが行われないようにするには、**DEFINE STGPOOL** コマンドの発行時に **HIGHMIG** パラメーターに値 100 を指定し、**LOWMIG** パラメーターに 0 を指定します。リストア操作のためにテープ・ドライブの少なくとも 20% を使用可能な状態で保持する必要があります。使用可能なテープ・ドライブの最大 80% を使用し、スループット・パフォーマンスを向上させるには、**MIGPROCESS** パラメーターを指定します。

マイグレーションするデータのタイプに基づいて、以下の情報を検討してください。

- ・大容量のオブジェクト (データベースなど) を使用するクライアントのデータのバックアップには、テープを使用します。

**ヒント:** テープへの書き込みに適したデータベースのサイズについては、テープ・ドライブの製造元のガイダンスを確認してください。

- ・小さいオブジェクトを使用するクライアントのデータのバックアップには、ディスクを使用します。
- ・データを直接テープにバックアップするには、LAN フリー・データ移動を使用します。詳細については、[120 ページの『LAN フリー・データ移動の構成』](#)を参照してください。
- ・仮想マシンはテープにバックアップしないでください。テープ・ベースのストレージ・プールにマイグレーションしない別個のディスク・ベースのストレージ・プールを使用します。仮想マシンのサポートについて詳しくは、[and IBM Tivoli Storage Manager \(TSM\) guest support for Virtual Machines and Virtualization](#) を参照してください。

### ストレージ・プールのキャパシティー

2 日間のクライアント・バックアップと 20% のバッファーに対応するのに十分なストレージ・プール容量を維持します。十分なストレージ・プール・スペースを確保するために、数日間にわたるフルバックアップをスケジュールしなければならない場合があります。

### 磁気テープ・ドライブ

製造元の仕様書を確認し、磁気テープ・ドライブの容量を見積もります。バックアップ操作およびマイグレーション操作に必要なスペース量を判別します。磁気テープ・ドライブの 20% をリストア操作用に予約します。

## 関連情報

[MIGRATE STGPOOL \(ストレージ・プールの次のストレージ・プールへのマイグレーション\)](#)

# テープ・ベースのソリューションのシステム要件

1 時間当たりのデータ取り込み速度が 14 TB であるテープ・ベースのストレージ・ソリューションのハードウェア要件とソフトウェア要件が示されています。

情報を確認して、ご使用のストレージ環境のハードウェア要件とソフトウェア要件を判別してください。ご使用のシステム・サイズに基づいて調整を行うことが必要な場合があります。

## ハードウェア要件

IBM Spectrum Protect ソリューションのハードウェア要件は、システム・サイズに基づきます。ご使用の環境の最適なパフォーマンスを確保するために、リストされているものと同等またはそれよりも高性能のコンポーネントを選択してください。

ディスク装置の計画について詳しくは、[ディスク・ストレージの計画](#)を参照してください。

テープ装置の計画について詳しくは、[磁気テープ・ストレージの計画](#)を参照してください。

以下の表に、サーバーおよびストレージの最小ハードウェア要件を示します。ローカル区画 (LPAR) または作業区画 (WPAR) を使用している場合は、区画サイズを考慮に入れてネットワーク要件を調整してください。表内の数値は、データ取り込み速度 (1 時間当たり 14 TB) に基づいています。

ハードウェア・コンポーネント	システム要件
サーバー・プロセッサ	<div><div>AIX</div>8 プロセッサ・コア、3.42 GHz 以上。 例えば、POWER8® プロセッサ・ベースのサーバーを使用します。</div> <div><div>Linux</div><div>Windows</div>16 プロセッサ・コア、2.0 GHz 以上。 例えば、Intel Xeon プロセッサを使用します。</div>
サーバー・メモリー	64 GB RAM。
ネットワーク	以下のサイジングでは、1 時間当たり約 14 TB のデータを管理します。 <ul style="list-style-type: none"><li>10 Gb イーサネット (最小 4 ポート)</li><li>8 Gb ファイバー・チャネル・アダプター (最小 4 ポート)</li></ul> ポートの数は、磁気テープ・ストレージに対するディスク・ストレージ・プールへのデータ取り込みのパーセンテージによって決まります。 テープとディスクのデータには、それぞれ別のファイバー・チャネル・アダプターを使用します。

ハードウェア・コンポーネント	システム要件
ストレージ	<p><b>ディスク</b></p> <p>ディスクに書き込むデータの量に基づいて、必要なディスクの数を指定します。</p> <p>ストレージ・エリア・ネットワーク (SAN) の順次入出力 (I/O) スループットは、前の行のネットワークの I/O スループットと一致していることを確認します。</p> <p>例えば、4 時間の時間枠で 10 TB のデータをバックアップする必要がある場合、スループットは約 700 MB/秒になります。この場合、サーバーでは、最小 700 MB/秒のスループットをサポートするフロントエンド・ネットワーク (クライアントからサーバーへのパス) が必要です。バックエンド SAN (サーバーからストレージ装置へのパス) も、最小 700 MB/秒のスループットをサポートする必要があります。</p> <p>必要なディスク速度を計算するには、以下の数式を使用します。</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <math display="block">\frac{(\text{Total amount of daily data ingestion} - \text{amount of daily data ingestion directly to tape})}{(\text{Number of hours for daily client backup operations})} = \text{Megabytes of data ingestion to disk per hour}</math> </div> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <math display="block">(\text{Megabytes of data ingestion to disk per hour}) \div (3600 \text{ seconds per hour}) = \text{Megabytes of data ingestion per second that must be supported by the disk technology}</math> </div> <p><b>テープ</b></p> <p>ビジネス要件に最適なテープ・テクノロジーを選択します。例えば、IBM Linear Tape-Open (LTO) または IBM TS1150 磁気テープ・ドライブを使用します。クライアント・バックアップ操作およびマイグレーション用に十分なマウント・ポイントがあることを確認します。磁気テープ・ストレージの計画について詳しくは、<a href="#">磁気テープ・ストレージの計画</a>を参照してください。サポートされるテープ装置のリストについては、<a href="#">IBM Support Portal for IBM Spectrum Protect</a>を参照してください。</p> <p><b>ヒント:</b> データ移動を最適化するには、LAN フリー・データ移動を使用します。</p>
SAN 入出力アダプター	<p>ディスクとテープの入出力を分離します。アダプターの選択について詳しくは、Brocade ハードウェア製品および IBM Storwize® ストレージ・ソリューションの資料を参照してください。</p> <p><b>ディスク</b></p> <p>少なくとも 2 つのアダプターを使用します。</p> <p><b>テープ</b></p> <p>少なくとも 2 つのアダプターを使用します。</p>

## Operations Center のスペース所要量の見積もり

上記の表には、Operations Center のハードウェア要件が含まれています。ただし、Operations Center が管理対象クライアントのレコードを保持するために使用するデータベースおよびアーカイブ・ログのスペース (インベントリー) を除きます。

Operations Center を IBM Spectrum Protect サーバーと同じシステムにインストールする予定がない場合は、システム要件を個別に見積もることができます。Operations Center のシステム要件を計算するには、[技術情報 1641684](#) のシステム要件の計算機能を参照してください。

IBM Spectrum Protect サーバー上での Operations Center の管理は、ハブ・サーバーおよびすべてのスポーク・サーバーの両方にデータベース操作の追加スペースが必要なワークロードです。ハブ・サーバーが 1 つ以上のスポーク・サーバーをモニターしている場合、ハブ・サーバー上で必要なアーカイブ・ログ用の

スペース量が大きくなります。ご使用の IBM Spectrum Protect サーバーに必要なスペース量を見積もるには、以下のガイドラインを参照してください。

### Operations Center のデータベース・スペース

Operations Center は、そのサーバー上でモニターされている 1000 個のクライアントごとに約 4.4 GB のデータベース・スペースを使用します。この計算は、構成内のハブ・サーバーとスポーク・サーバーの両方に適用されます。

例えば、2000 クライアントを持つハブ・サーバーで、それぞれ 1000 クライアントを持つ 3 つのスポーク・サーバーの管理も行うものとします。この構成には、4 つのサーバー全体で合計 5000 個のクライアントがあります。スポーク・サーバーごとに、4.4 GB のデータベース・スペースが必要です。スポーク・サーバーが IBM Spectrum Protect バージョン 8.1.2 以降である場合、ハブ・サーバーには、その 2000 個のクライアントのみをモニターするために 8.8 GB のデータベース・スペースが必要です。

$$(4.4 \text{ GB} \times 2) = 8.8 \text{ GB}$$

### 管理対象データのデータベース・スペース

管理対象データは、保護されているデータの量 (保存されているすべてのバージョンのデータの量を含む) です。

- 永久差分バックアップを実行するクライアント・タイプの場合、以下の数式を使用して、管理対象データの合計を見積もることができます。

$$\text{Front-end} + (\text{front-end} \times \text{change rate} \times (\text{retention} - 1))$$

例えば、100 TB のフロントエンド・データをバックアップして、30 日の保存期間を使用し、変化率が 5% である場合、次の式を使用して管理対象データの合計を計算します。

$$100 \text{ TB} + (100 \text{ TB} \times 0.05 \times (30-1)) = 245 \text{ TB total managed data}$$

- フルバックアップを毎日実行するクライアント・タイプの場合、以下の数式を使用して、管理対象データの合計を見積もることができます。

$$\text{Front-end} \times \text{retention} \times (1 + \text{change rate})$$

例えば、10 TB のフロントエンド・データをバックアップして、30 日の保存期間を使用し、変化率が 3% である場合、次の式を使用して管理対象データの合計を計算します。

$$10 \text{ TB} \times 30 \times (1 + .03) = 309 \text{ TB total managed data}$$

非構造化データ、平均オブジェクト・サイズ: 4 MB

構造化データ、平均オブジェクト・サイズ: 128 MB

非構造化データ、オブジェクト数 =

$$(245 \text{ TB} \times 1024 \times 1024) / 4 \text{ MB} = 64225280$$

構造化データ、オブジェクト数 =

$$(309 \text{ TB} \times 1024 \times 1024) / 128 \text{ MB} = 2531328$$

オブジェクトの総数: 66756608

管理対象データのコスト (オブジェクト当たり 1 KB) =

$$(66756608 \text{ KB}) / (1024 \times 1024) = 63.66 \text{ GB}$$

データベース・システムが 100% 容量にならないように、20% の追加スペースを計画します:

$$\text{Database total physical storage requirements} = (\text{managed data space} + \text{Operations Center space}) \times (1.20)$$

この例では、次の数字を使用してスペースを計算します。

$$(66.33 \text{ GB} + 8.4 \text{ GB}) \times 1.20 = 76.41 \text{ GB}$$

## アーカイブ・ログ・スペース

Operations Center は、そのサーバーでモニターされている 1000 個のクライアントごとに、サーバー当たり 24 時間で約 18 GB のアーカイブ・ログ・スペースを使用します。さらに、スポーク・サーバー上でモニターされている 1000 個のクライアントごとに、ハブ・サーバー上で追加のアーカイブ・ログ・スペースが使用されます。V8.1.2 以降のスポーク・サーバーの場合、モニターされている 1000 個のクライアントごとに 24 時間当たり 1.2 GB のアーカイブ・ログ・スペースがハブ・サーバー上で追加されます。

例えば、2000 クライアントを持つハブ・サーバーで、それぞれ 1000 クライアントを持つ 3 つのスポーク・サーバーの管理も行うものとします。この構成には、4 つのサーバー全体で合計 5000 個のクライアントがあります。次の数式を使用して、ハブ・サーバーのアーカイブ・ログ・スペースを計算することができます。

$$((18 \text{ GB} \times 2) + (1.2 \text{ GB} \times 3)) = 39.6 \text{ GB of archive log space}$$

これらの見積もりは、デフォルトの状況収集間隔である 5 分に基づいています。収集間隔を 5 分毎から 3 分毎に減らすと、スペース要件は以下のように増加します。以下の例は、V8.1.2 以降のスポーク・サーバーがモニターされている構成で、収集間隔を 3 分ごとに 1 回に設定した場合のログ・スペース要件の増加の概算を示しています。

- ハブ・サーバー: 39.6 GB から 66 GB の範囲
- 各スポーク・サーバー: 18 GB から 30 GB の範囲

サーバー操作に影響を及ぼさずに Operations Center をサポートできるように、アーカイブ・ログ・スペースを割り振ります。

## ソフトウェア要件

IBM Spectrum Protect のテープ・ベースソリューションの資料には、IBM AIX®、Linux®、および Microsoft Windows の各オペレーティング・システムのインストール・タスクおよび構成タスクが記載されています。リストされている最小ソフトウェア要件を満たす必要があります。

### AIX システム

ソフトウェアのタイプ	最小ソフトウェア要件
オペレーティング・システム	IBM AIX 7.1 オペレーティング・システム要件の詳細については、IBM Spectrum Protect のインストール情報を参照してください。
Gunzip ユーティリティ	IBM Spectrum Protect サーバーをインストールまたはアップグレードする場合は、事前にシステムで gunzip ユーティリティが使用可能になっている必要があります。gunzip ユーティリティがインストールされ、gunzip ユーティリティへのパスが PATH 環境変数で設定されていることを確認してください。



ソフトウェアのタイプ	最小ソフトウェア要件
ファイル・システム・タイプ	<p>JFS2 ファイル・システム</p> <p>AIX システムでは、大量のファイル・システム・データをキャッシュに入れることができます。これにより、サーバーおよび IBM Db2® プロセスに必要なメモリーを削減することができます。AIX サーバーでのページングを回避するには、JFS2 ファイル・システムの場合、rbrw マウント・オプションを使用します。ファイル・システム・キャッシュに使用されるメモリーが減り、IBM Spectrum Protect が使用できるメモリーが増えます。</p> <p>IBM Spectrum Protect データベース、ログ、またはストレージ・プール・ボリュームを含むファイル・システムでは、ファイル・システム・マウント・オプション、並行入出力 (CIO)、および直接入出力 (DIO) を使用しないでください。これらのオプションを使用すると、多くのサーバー操作のパフォーマンスが低下する可能性があります。IBM Spectrum Protect および Db2 は、DIO を使用することが有益である場合には引き続き DIO を使用することができますが、IBM Spectrum Protect では、マウント・オプションを使用してこれらの技法の利点を選択的に活用する必要はありません。</p>
その他のソフトウェア	Korn シェル (ksh)

## Linux システム

ソフトウェアのタイプ	最小ソフトウェア要件
オペレーティング・システム	Red Hat® Enterprise Linux 7 (x86_64)
ライブラリー	<p>IBM Spectrum Protect システムに インストールされている GNU C ライブラリー バージョン 2.3.3-98.38 以降。</p> <p>Red Hat Enterprise Linux Servers:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (32 ビットと 64 ビットのパッケージが必要です)</li> <li>• numactl.x86_64</li> </ul>
ファイル・システム・タイプ	<p>データベース関連のファイル・システムは、ext3 または ext4 を使用してフォーマット設定します。</p> <p>ストレージ・プール関連のファイル・システムの場合は、XFS を使用してください。</p>
その他のソフトウェア	Korn シェル (ksh)

## Windows システム

ソフトウェアのタイプ	最小ソフトウェア要件
オペレーティング・システム	Microsoft Windows Server 2012 R2 (64 ビット) または Windows Server 2016
ファイル・システム・タイプ	NTFS

ソフトウェアのタイプ	最小ソフトウェア要件
その他のソフトウェア	<p>Windows 2012 R2 または Windows 2016 (.NET Framework 3.5 がインストールされて有効になっている)</p> <p>以下のユーザー・アカウント制御ポリシーを無効にする必要があります。</p> <ul style="list-style-type: none"> <li>ユーザー・アカウント制御: 組み込みの Administrator アカウントに対する管理者承認モード</li> <li>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</li> </ul>

## 計画ワークシート

計画ワークシートを使用して、システムのセットアップに使用する値を記録し、IBM Spectrum Protect サーバーを構成します。ワークシートにリストされているデフォルト値を使用してください。

各ワークシートは、デフォルト値を使用することによって、システム構成のさまざまな部分を準備する上で役立ちます。

### サーバー・システムの事前構成

事前構成ワークシートを使用して、システムのセットアップ時に IBM Spectrum Protect のファイル・システムを構成するときに作成するファイル・システムとディレクトリーを計画します。サーバー用に作成するすべてのディレクトリーは空でなければなりません。

### サーバー構成

サーバーの構成時に、構成ワークシートを使用します。特に記述されている場合を除き、大半の項目でデフォルト値が推奨されます。

表 1. サーバー・システムの事前構成のワークシート				
項目	デフォルト値	値	最小ディレクトリー・サイズ	詳細情報
サーバーとの通信用の TCP/IP ポート・アドレス	1500		適用されない。	オペレーティング・システムをインストールして構成するときに、このポートを使用できることを確認してください。  ポート番号は、1024 から 32767 の範囲内の番号にすることができます。
サーバー・インスタンスのディレクトリー	<div>Linux   AIX</div> /home/tsminst1/ tsminst1 <div>Windows</div> C:\%tsminst1		<div>AIX</div> 50 GB. <div>Linux   Windows</div> 25 GB.	サーバー・インスタンス・ディレクトリーの値をデフォルトから変更する場合は、 <a href="#">10 ページの表 2</a> の Db2 インスタンス所有者の値も変更してください。

表 1. サーバー・システムの事前構成のワークシート (続き)				
項目	デフォルト値	値	最小ディレクトリー・サイズ	詳細情報
サーバー・インストールのディレクトリー	<ul style="list-style-type: none"> <li><b>Linux</b>   <b>AIX</b> /</li> <li><b>Windows</b> C:</li> </ul>		<b>AIX</b> ディレクトリーに必要な使用可能スペース: 5 GB。  <b>Linux</b>   <b>Windows</b> ディレクトリーに必要な最小スペース: 30 GB	
サーバー・インストールのディレクトリー	/usr		<b>AIX</b> ディレクトリーに必要な使用可能スペース: 5 GB。	
サーバー・インストールのディレクトリー	<b>AIX</b> /var		<b>AIX</b> ディレクトリーに必要な使用可能スペース: 5 GB。	
サーバー・インストールのディレクトリー	<b>AIX</b> /tmp		<b>AIX</b> ディレクトリーに必要な使用可能スペース: 5 GB。	
サーバー・インストールのディレクトリー	<b>AIX</b> /opt		<b>AIX</b> ディレクトリーに必要な使用可能スペース: 10 GB。	
活動ログのディレクトリー	<b>Linux</b>   <b>AIX</b> / tsminst1/TSMalog  <b>Windows</b> C:¥tsminst1¥TSMalog		128 GB.	サーバーの初期構成時に活動ログを作成する場合、サイズを 128 GB に設定します。
アーカイブ・ログのディレクトリー	<b>Linux</b>   <b>AIX</b> / tsminst1/ TSMarchlog  <b>Windows</b> C:¥tsminst1¥TSMarchlog		3 TB.	
データベースのディレクトリー	<b>Linux</b>   <b>AIX</b> / /tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03  <b>Windows</b> C:¥tsminst1¥TSMdbspace00 C:¥tsminst1¥TSMdbspace01 C:¥tsminst1¥TSMdbspace02 C:¥tsminst1¥TSMdbspace03		スペース所要量の計算方法については、3 ページの『ハードウェア要件』を参照してください。	データベース用に 4 個のファイル・システムを作成します。

表 1. サーバー・システムの事前構成のワークシート (続き)				
項目	デフォルト値	値	最小ディレクトリー・サイズ	詳細情報
ストレージのディレクトリー	<div>Linux   AIX</div> /tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ... <div>Windows</div> C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		以下の計算を使用して、すべてのディレクトリーの最小合計容量を判別します。  <div>             日次              percentage of              ingested              data that is              written              to disk + 20% =              Minimum total              capacity           </div>	テープ装置ごとに少なくとも1つのディレクトリーを定義する方法が推奨されます。

表 2. IBM Spectrum Protect 構成のワークシート			
項目	デフォルト値	値	詳細情報
Db2 インスタンス所有者	tsminst1		8 ページの表 1 でサーバー・インスタンス・ディレクトリーの値をデフォルトから変更した場合、Db2 インスタンス所有者の値も変更してください。
Db2 インスタンス所有者のパスワード	<div>Linux   AIX</div> passw0rd <div>Windows</div> pAssW0rd		デフォルトとは異なるインスタンス所有者のパスワードを選択します。この値を安全な場所に必ず記録してください。
Db2 インスタンス所有者の 1 次グループ	<div>Linux   AIX</div> tsmsrvrs		
サーバー名	サーバー名のデフォルト値は、システムのホスト名です。		
サーバー・パスワード	passw0rd		デフォルトとは異なるサーバー・パスワードの値を選択します。この値を安全な場所に必ず記録してください。
管理者 ID: サーバー・インスタンスのユーザー ID	admin		
管理者 ID のパスワード	passw0rd		デフォルトとは異なる管理者パスワードの値を選択します。この値を安全な場所に必ず記録してください。

表 2. IBM Spectrum Protect 構成のワークシート (続き)			
項目	デフォルト値	値	詳細情報
スケジュールの開始時刻	23:00		<p>デフォルトのスケジュールの開始時刻に、クライアント・ワークロード・フェーズが開始します。これは主に、クライアントのバックアップとアーカイブのアクティビティです。クライアント・ワークロード・フェーズの間、サーバー・リソースはクライアント操作をサポートします。通常、これらの操作は、毎晩のスケジュール・ウィンドウ中に実行されます。</p> <p>サーバー保守操作のスケジュールは、クライアント・バックアップ・ウィンドウの 10 時間後に開始するように定義されます。</p> <p>このガイドでは、クライアント・バックアップ操作を開始する推奨時刻は 23:00 です。</p>

表 3. 磁気テープ構成のワークシート			
項目	デフォルト値	値	詳細情報
ロボット装置ファイル	<p>IBM テープ・デバイス・ドライバーを使用する IBM 装置:</p> <ul style="list-style-type: none"> <li>• <b>AIX</b> /dev/smcX</li> <li>• <b>Linux</b> /dev/IBMchangerX</li> <li>• <b>Windows</b> ChangerX</li> </ul> <p>IBM Spectrum Protect デバイス・ドライバーを使用する IBM 以外の装置:</p> <ul style="list-style-type: none"> <li>• <b>AIX</b> /dev/lbX</li> <li>• <b>Linux</b> /dev/tsm SCSI/lbX</li> <li>• <b>Windows</b> lbA.B.C.D</li> </ul>		<p>ライブラリー装置ファイルを手動で定義するには、以下のコマンドを使用します。</p> <ul style="list-style-type: none"> <li>• <b>DEFINE LIBRARY</b></li> <li>• <b>DEFINE DRIVE</b></li> <li>• <b>DEFINE PATH</b></li> </ul> <p>SCSI の場合、<b>PERFORM LIBACTION</b> コマンドを使用して、単一ライブラリーのすべてのドライブおよびそのパスを 1 つのステップで定義することができます。このコマンドを使用してすべてのドライブおよびパスを定義するには、<b>SANDISCOVERY</b> オプションがサポートされて有効にされている必要があります。</p>

表 3. 磁気テープ構成のワークシート (続き)			
項目	デフォルト値	値	詳細情報
磁気テープ・ドライブ	<p>IBM テープ・デバイス・ドライバを使用する IBM 装置:</p> <ul style="list-style-type: none"> <li>• <b>AIX</b> /dev/rmtX</li> <li>• <b>Linux</b> /dev/IBMtapeX</li> <li>• <b>Windows</b> TapeX</li> </ul> <p>IBM Spectrum Protect デバイス・ドライバを使用する IBM 以外の装置:</p> <ul style="list-style-type: none"> <li>• <b>AIX</b> /dev/mtX</li> <li>• <b>Linux</b> /dev/tmscsi/mtX</li> <li>• <b>Windows</b> mtA.B.C.D</li> </ul>		

## ディスク・ストレージの計画

IBM Spectrum Protect コンポーネントに最も効率的なストレージ・テクノロジーを選択し、効率的なサーバー・パフォーマンスと操作を確保します。

ストレージ・ハードウェア装置は、IBM Spectrum Protect での効果的な使用法を決定するさまざまな容量とパフォーマンスの特性を備えています。適切なストレージ・ハードウェアの選択とソリューション用のセットアップに関する一般的なガイダンスとして、以下のガイドラインを確認してください。

### データベース、活動ログ、およびアーカイブ・ログ

- IBM Spectrum Protect データベースおよび活動ログには、ソリッド・ステート・ディスク (SSD) または高速 15,000 rpm ディスクを使用します。
- データベース用のアレイを作成する場合は、RAID レベル 5 を使用してください。
- アーカイブ・ログおよびデータベース・バックアップ・ストレージには別個のディスクを使用します。

### ストレージ・プール

大容量ディスク・タイプを使用している場合は、二重ドライブ障害に対する保護を追加するために、ストレージ・プール・アレイに RAID レベル 6 を使用してください。

## ストレージ・アレイの計画

IBM Spectrum Protect システムのサイズに応じて、RAID アレイおよびボリュームを計画し、ディスク・ストレージの構成を準備します。

IBM Spectrum Protect サーバー・ストレージ・コンポーネントのいずれか (サーバー・データベースやストレージ・プールなど) に適したサイズおよびパフォーマンス 特性を持つストレージ・アレイを設計します。ストレージ計画アクティビティでは、ドライブ・タイプ、RAID レベル、ドライブの数、スペア・ドライブの数などを考慮に入れる必要があります。ソリューション構成では、ストレージ・グループには内部ストレージ RAID アレイが含まれています。ストレージ・グループは、システムに対して論理ボリュームとして提示される複数の物理ディスクで構成されます。ディスク・ストレージ・システムを構成する際、ストレージ・グループ、つまりデータ・ストレージ・プールを作成してから、グループ内にストレージ・アレイを作成します。

ストレージ・グループからボリューム、つまり LUN を作成します。ストレージ・グループは、どのディスクがボリュームを構成するストレージを提供するかを定義します。ボリュームを作成する際、それらを完全に割り振ってください。データベース・ボリュームおよびアクティブ・ログ・ボリュームの保持には、高速なディスク・タイプが使用されます。ストレージ・プール・ボリューム、アーカイブ・ログ、およびデータベース・バックアップ・ボリュームには、低速なディスク・タイプを使用することができます。より小さいディスク・ストレージ・プールを使用してデータをステージングする場合、データの取り込みおよびマイグレーションを行うための日次ワークロード・パフォーマンスを管理するために、より高速なディスクを使用する必要がある場合があります。

13 ページの表 4 および 13 ページの表 5 に、ストレージ・グループおよびボリューム構成のレイアウト要件を示します。

表 4. ストレージ・グループ構成のコンポーネント	
コンポーネント	詳細
サーバー・ストレージ要件	サーバーによるストレージの使用法
ディスク・タイプ	ストレージ要件に合わせて使用されるディスク・タイプのサイズと速度
ディスク数	ストレージ要件に必要な各ディスク・タイプの数
ホット・スペア容量	ディスク障害の発生時に引き継ぐスペアとして予約されるディスクの数。
RAID レベル	論理ストレージに使用される RAID アレイのレベル RAID レベルは、アレイによって提供される冗長性のタイプを定義します (例えば、5 または 6)。
RAID アレイの数	作成する RAID アレイの数
RAID アレイ当たりの DDM	各 RAID アレイで使用されるディスク・ドライブ・モジュール (DDM) の数
RAID アレイ当たりの使用可能サイズ	冗長性のために失われるスペースを考慮した結果、各 RAID アレイ内でデータ・ストレージに使用できるサイズ
合計使用可能サイズ	RAID アレイ内のデータ・ストレージに使用できる合計サイズ: 数量 x 使用可能サイズ
推奨されるストレージ・グループ名およびアレイ名	MDisk および MDisk グループに使用するのに推奨される名前
使用量	物理ディスクの一部を使用するサーバー・コンポーネント

表 5. ボリューム構成のコンポーネント	
コンポーネント	詳細
サーバー・ストレージ要件	物理ディスクを使用するための要件
ボリューム名	特定のボリュームに指定される固有の名前
ストレージ・グループ	ボリュームを作成するためのスペースが含まれているストレージ・グループの名前
サイズ	各ボリュームのサイズ
対象のサーバー・マウント・ポイント	ボリュームがマウントされるサーバー・システム上のディレクトリー
数量	特定の要件に対応して作成されるボリュームの数。同じ要件に対応して作成されるボリュームごとに同じ命名標準を使用してください。
使用量	物理ディスクの一部を使用するサーバー・コンポーネント

## 例

ストレージ・グループおよびボリュームの構成例は、[ストレージ・アレイの計画ワークシートの例](#)で参照できます。例には、さまざまなサーバー・サイズについてストレージを計画する方法が示されています。構成例では、ディスクとストレージ・グループとの間に1対1のマッピングが存在します。例をダウンロードし、ワークシートを編集して、サーバーのストレージ構成を計画することができます。

## 磁気テープ・ストレージの計画

---

どのテープ装置を使用するか、およびどのように構成するかを決定します。システム・パフォーマンスを最適化するには、高速の大容量テープ装置を使用することを計画します。ビジネス要件を満たすのに十分な磁気テープ・ドライブを準備します。

## サポートされるテープ装置およびライブラリー

---

サーバーは、様々なテープ装置およびライブラリーを使用することができます。ビジネス要件を満たすテープ装置およびライブラリーを選択してください。

サポートされる装置および有効な装置クラス・フォーマットのリストについては、ご使用のオペレーティング・システムの Web サイトを参照してください。

- **Windows | AIX** [AIX および Windows でサポートされるデバイス](#)
- **Linux** [Linux でサポートされるデバイス](#)

ストレージ装置およびストレージ・オブジェクトについて詳しくは、[ストレージ装置のタイプ](#)を参照してください。

IBM Spectrum Protect に対して定義された各装置は、1つの装置クラスに関連付けられます。デバイス・クラスでは、デバイス・タイプおよびメディア管理情報(記録形式、見積容量、およびラベル接頭部など)が指定されます。

装置タイプは、同じメディア特性を共用する装置のグループのメンバーとして装置を識別します。例えば、LTO 装置タイプは、すべての世代の LTO 磁気テープ・ドライブに適用されます。

磁気テープ・ドライブの装置クラスではライブラリーも指定する必要があります。物理ライブラリーは、類似したメディア・マウント要件を共用する1つ以上のドライブの集合です。すなわち、ドライブはオペレーターによっても、自動マウント機構によっても、マウントすることができます。

ライブラリー・オブジェクト定義は、ライブラリー・タイプ、およびそのライブラリー・タイプに関連付けられているその他の特性を指定します。

以下の表は、IBM Spectrum Protect バージョン 8.1.6 テープ・ソリューションで推奨されるライブラリー・タイプをリストしています。



表 6. IBM Spectrum Protect 8.1.6 テープ・ソリューションのライブラリー・タイプ

ライブラリー・タイプ	説明	詳細情報
SCSI	<p>SCSI ライブラリーは SCSI インターフェースを使用して制御され、SCSI ケーブル接続を使用してサーバーのホストに直接接続されるか、または Storage Area Network によって接続されます。ロボットなどの機構によって自動的にテープ・ボリュームのマウントおよび取り外しが行われます。</p> <p>SCSI ライブラリーに異なるドライブ・タイプを作成する場合、異なるタイプのドライブ間で分割できない複数の論理ライブラリーを作成します。SCSI ライブラリーでは、異なるテクノロジーのドライブを混用することができます (LTO Ultrium ドライブと Digital Linear Tape (DLT) ドライブなど)。例えば次のとおりです。</p> <ul style="list-style-type: none"> <li>• Oracle StorageTek L700 ライブラリー</li> <li>• IBM 3592 磁気テープ装置</li> </ul>	<p>90 ページの『サーバーで使用するライブラリーの構成』</p> <p>制約事項は、異なる世代のメディアおよびドライブを混用する場合に適用されます。詳細については、以下を参照してください。</p> <ul style="list-style-type: none"> <li>• 98 ページの『単一ライブラリー内での複数世代の 3592 ドライブおよびメディアの混用』</li> <li>• 95 ページの『単一のライブラリー内における LTO ドライブとメディアの混合』</li> </ul>
共有	<p>共有ライブラリーは、SCSI で表される論理ライブラリーです。ライブラリーは、ライブラリー・マネージャーとして構成された IBM Spectrum Protect サーバーによって制御されます。</p> <p>SHARED ライブラリー・タイプを使用する IBM Spectrum Protect サーバーは、ライブラリー・マネージャー・サーバーに対するライブラリー・クライアントになります。共有ライブラリーはライブラリー・マネージャーを参照します。</p>	

## サポートされるテープ装置構成

ローカル・エリア・ネットワーク (LAN) およびストレージ・エリア・ネットワーク (SAN) に関する情報を確認します。データ移動を最適化するには、LAN フリー・データ移動を構成することを計画します。さらに、ライブラリー共有を使用するかどうかを検討します。

ビジネス要件を満たす装置構成を選択してください。

## LAN ベースおよび LAN フリーのデータ移動

ローカル・エリア・ネットワーク (LAN) に接続されたクライアントとストレージ装置の間で、あるいはストレージ・エリア・ネットワーク (SAN) に接続されたストレージ装置にデータを移動することができます。これは、LAN フリー・データ移動と呼ばれます。

標準的な LAN 構成では、1 つ以上のテープ・ライブラリーが単一の IBM Spectrum Protect サーバーに関連付けられます。LAN フリー・データ移動により、LAN の帯域幅が他の用途に使用できるようになり、IBM Spectrum Protect サーバー上の負荷が減少します。

LAN 構成では、クライアント・データ、E メール、端末接続、アプリケーション・プログラム、および装置制御情報はすべて、同じネットワークで処理される必要があります。装置制御情報、およびクライアントのバックアップ・データとリストア・データが LAN 全体を流れます。

SAN は、システム・パフォーマンスを向上させる専用ストレージ・ネットワークです。

SAN で IBM Spectrum Protect を使用することで、以下の機能を利用できます。

- 複数の IBM Spectrum Protect サーバーの間でストレージ装置を共有する。

**制約事項:** GENERICTAPE 装置タイプを持つストレージ装置は、サーバー間で共有することができません。

- ・クライアント・システムでストレージ・エージェントを構成することによって、IBM Spectrum Protect クライアント・データをストレージ装置に直接移動する (LAN フリー・データ移動)。

SAN では、IBM Spectrum Protect サーバーでサポートされている磁気テープ・ドライブおよびライブラリー (ほとんどの SCSI テープ装置が含まれます) を共有することができます。

IBM Spectrum Protect サーバーが SCSI テープを共有する場合、1つのサーバー (ライブラリー・マネージャー) がその装置を所有して制御します。ストレージ・エージェントと、このライブラリーを共有するその他の IBM Spectrum Protect サーバーは、ライブラリー・クライアントです。ライブラリー・クライアントは、ライブラリー・マネージャーからドライブやメディアなどの共有ライブラリー・リソースを要求しますが、それらのリソースを独立して使用します。ライブラリー・マネージャーは、これらのリソースへのアクセスを調整します。ライブラリー・クライアントとして定義されている IBM Spectrum Protect サーバーは、サーバー間通信を使用してライブラリー・マネージャーに接続し、装置サービスを要求します。データは、SAN を介して各サーバーとストレージ装置との間を移動します。

**要件:** IBM Spectrum Protect サーバーと共有されるライブラリー・マネージャー・サーバーを定義する場合は、**SANDISCOVERY** オプションを ON に設定する必要があります。デフォルトで、このオプションは OFF に設定されています。

IBM Spectrum Protect サーバーは、自動ライブラリーを共用する場合に以下のフィーチャーを使用します。

#### ボリューム・インベントリーの分割

共有ライブラリー内のメディア・ボリュームのインベントリーは、サーバー間で分割されています。1つのサーバーが特定のボリュームを所有するか、またはボリュームが グローバル・スクラッチ・プールに入るかのどちらかです。いずれのサーバーもスクラッチ・プールを所有しません。

#### 逐次ドライブ・アクセス

各磁気テープ・ドライブには、一時点で1つのサーバーのみがアクセスします。ドライブ・アクセスは逐次化されます。IBM Spectrum Protect は、ドライブ・アクセスを制御して、サーバーが他のサーバーのボリュームをマウント解除したり、他のサーバーがそれらのボリュームをマウントするドライブに書き込んだりすることがないようにします。

#### 逐次マウント・アクセス

ライブラリーのオートチェンジャーは、一時点で1つのマウント操作またはマウント解除操作を行います。ライブラリー・マネージャーがすべてのマウント操作を行って、この逐次化を可能にします。

## ライブラリー共有

ライブラリー共有を構成することで、テープ・ソリューションの効率を最適化することができます。ライブラリー共有により、複数の IBM Spectrum Protect サーバーが、ストレージ・エリア・ネットワーク (SAN) 上の同じテープ・ライブラリーとドライブを使用して、バックアップおよびリカバリーのパフォーマンスとテープ・ハードウェアの使用効率を改善することができます。

IBM Spectrum Protect サーバーがライブラリーを共有する場合、1つのサーバーがライブラリー・マネージャーとしてセットアップされて、マウントや取り外しなどのライブラリー操作を制御します。ライブラリー・マネージャーはまた、ボリューム所有権とライブラリー・インベントリーの制御も行います。その他のサーバーはライブラリー・クライアントとしてセットアップされ、サーバー間通信を使用してライブラリー・マネージャーに連絡し、リソースを要求します。

ライブラリー・クライアントは、ライブラリー・マネージャー・サーバーと同じバージョンかそれより前のバージョンでなければなりません。ライブラリー・マネージャーは、それより後のバージョンのライブラリー・クライアントをサポートできません。詳しくは、[Storage-agent and library-client compatibility with an IBM Spectrum Protect server](#) を参照してください。

## LAN フリー・データ移動 (LAN-free data movement)

IBM Spectrum Protect を使用することで、クライアントは、ストレージ・エージェントを介して SAN 上のテープ・ライブラリーに直接データをバックアップしたり、テープ・ライブラリーから直接データをリストアしたりできるようになります。このタイプのデータ移動は、LAN フリー・データ移動とも呼ばれます。

**制約事項:** Centera ストレージ装置を LAN フリー操作のターゲットにすることはできません。

17 ページの図 2 は、クライアントがテープに直接アクセスしてデータの読み取りまたは書き込みを行っている SAN 構成を示しています。

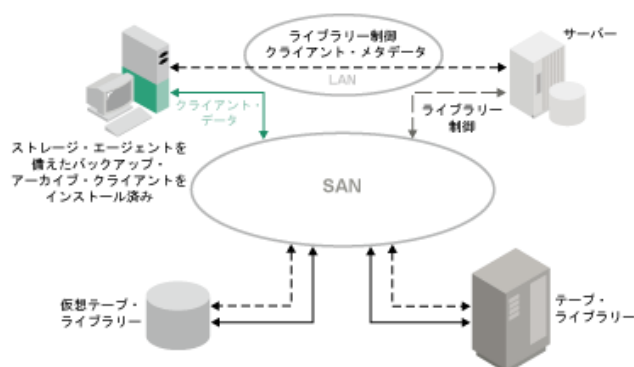


図 2. LAN フリー・データ移動 (LAN-free data movement)

LAN フリー・データ移動の場合、そのクライアント・システムにストレージ・エージェントをインストールしておく必要があります。サーバーは、データベースおよび回復ログを保守し、ライブラリー・マネージャーとして機能して装置操作を制御します。クライアントのストレージ・エージェントは、SAN 上の装置へのデータ転送を処理します。このインプリメンテーションにより、クライアント・データ移動に使用されるはずだった LAN における帯域幅が解放されます。

## 単一ライブラリーでの混合装置タイプ

IBM Spectrum Protect では、異なる装置タイプ用の異なるメディアを自動ライブラリーで識別できる場合、単一の自動ライブラリー内での複数の異なる装置タイプの混用をサポートします。構成プロセスを簡素化するためには、ライブラリーでの異なる装置タイプの混用を計画しないでください。装置タイプを混用する必要がある場合は、制限事項を確認してください。

この機能を持つライブラリーは、標準で混合ドライブを備えたモデルか、または混合ドライブの追加をサポートするモデルです。詳しくは、製造元の資料を参照してください。IBM Spectrum Protect 上でテストされた、装置タイプが混在するライブラリーの詳細については、ご使用のオペレーティング・システムに関する以下の情報を参照してください。

- [AIX、HP-UX、Solaris、および Windows の IBM Spectrum Protect サポート対象デバイス](#)

## • Linux の IBM Spectrum Protect サポート対象デバイス

例えば、LTO Ultrium ドライブおよび IBM TS1100 ドライブを単一のライブラリーで IBM Spectrum Protect サーバーに対して定義することができます。

## ライブラリーでの異なるメディア世代

IBM Spectrum Protect サーバーは、自動ライブラリー内での装置タイプの混用を許可しますが、通常は、同じタイプでも異なる世代のドライブの混用はサポートされません。新しいドライブは古いメディア・フォーマットに書き込むことができず、古いドライブは新しいフォーマットを読み取ることができません。LTO Ultrium ドライブは、このルールの例外です。

この新しいドライブ・テクノロジーにおいて、古い世代のドライブでフォーマットされたメディアに対して書き込みができない場合は、サーバー操作に関する問題を回避するために、その古いメディアには読み取り専用のマークを付ける必要があります。また、古いドライブをライブラリーから除去するか、古いドライブの定義をサーバーから除去する必要があります。例えば、IBM Spectrum Protect サーバーは、Oracle StorageTek 9940A ドライブと 9940B ドライブを単一ライブラリー内で他の装置タイプと組み合わせて使用することをサポートしません。

一般的に、IBM Spectrum Protect は、LTO Ultrium ドライブおよびメディアの世代の混用をサポートしません。ただし、以下の混用はサポートされます。

- LTO Ultrium 第 3 世代 (LTO-3) と LTO Ultrium 第 4 世代 (LTO-4)
- LTO Ultrium 第 4 世代 (LTO-4) と LTO Ultrium 第 5 世代 (LTO-5)
- LTO Ultrium 第 5 世代 (LTO-5) と LTO Ultrium 第 6 世代 (LTO-6)
- LTO Ultrium 第 6 世代 (LTO-6) と LTO Ultrium 第 7 世代 (LTO-7)
- LTO-8 磁気テープ装置を使用したライブラリー、または LTO-8 と LTO-7 の磁気テープ装置を混合して使用したライブラリーの LTO Ultrium 第 7 世代 (LTO-7) メディアと LTO Ultrium 第 8 世代 (LTO-8 および LTO-M8) メディア

サーバーがこれらの混用をサポートするのは、異なるドライブが異なるメディアの読み取りおよび書き込みができるためです。すべてのドライブを第 4 世代 (あるいは第 5、6、7、または 8 世代) にアップグレードする予定の場合、すべての既存の LTO Ultrium ドライブ定義およびそれらに関連付けられたパスを削除する必要があります。その後、新規の第 4 世代 (あるいは第 5 世代、第 6 世代、第 7 世代、または第 8 世代) のドライブおよびパスを定義することができます。

### LTO Ultrium テープ・ドライブおよびメディアの混用に適用される制約時効

- LTO-5 ドライブ LTO-3 メディアでは読み取りしかできません。LTO-3 を LTO-5 のドライブおよびメディアと単一ライブラリーで混合使用する場合、LTO-3 メディアに読み取り専用のマークを付ける必要があります。すべての LTO-3 スクラッチ・ボリュームをチェックアウトする必要があります。
- LTO-6 ドライブ LTO-4 メディアでは読み取りしかできません。LTO-4 を LTO-6 のドライブおよびメディアと単一ライブラリーで混合使用する場合、LTO-4 メディアに読み取り専用のマークを付ける必要があります。すべての LTO-4 スクラッチ・ボリュームをチェックアウトする必要があります。
- LTO-7 ドライブ LTO-5 メディアでは読み取りしかできません。LTO-5 を LTO-7 のドライブおよびメディアと単一ライブラリーで混合使用する場合、LTO-5 メディアに読み取り専用のマークを付ける必要があります。すべての LTO-5 スクラッチ・ボリュームをチェックアウトする必要があります。
- LTO-8 ドライブは LTO-6 メディアを読み取ることができません。単一のライブラリーで LTO-6 と LTO-8 のドライブとメディアを混合使用する場合、そのライブラリーは 2 つのライブラリーに分割する必要があります。1 つのライブラリーには LTO-8 のドライブとメディアのみだけを入れて、他方のライブラリーに LTO-6 のドライブとメディアを入れます。

### ライブラリー内での LTO Ultrium テープ・ドライブの世代の混用に適用される制約事項

磁気テープ・ドライブより前の世代のテープ・カートリッジを使用する必要があります。後の世代の磁気テープ・ドライブは、前の世代のテープ・カートリッジへのデータの読み取りおよび書き込みが可能です。例えば、ライブラリーに LTO-7 および LTO-6 磁気テープ・ドライブがある場合、LTO-6 テープ・カートリッジを使用する必要があります。LTO-7 および LTO-6 のどちらの磁気テープ・ドライブも、LTO-6 テープ・カートリッジへのデータの読み取りおよび書き込みが可能です。



## ライブラリー内での LTO Ultrium テープ・カートリッジの世代の混用に適用される制約事項

磁気テープ・ドライブと同じ世代または1つ前の世代のテープ・カートリッジを使用する必要があります。例えば、ライブラリーに LTO-7 磁気テープ・ドライブがある場合、LTO-7 テープ・カートリッジを使用するか、LTO-7 と LTO-6 のテープ・カートリッジを混用することができます。このライブラリーに LTO-7、LTO-6、および LTO-5 のテープ・カートリッジがある場合、LTO-5 テープ・カートリッジのアクセス・モードを READONLY に変更する必要があります。

LTO Ultrium の世代を混合する場合のその他の考慮事項については、95 ページの『LTO 装置クラスの定義』を参照してください。

IBM Spectrum Protect を使用する場合、3592、TS1130、TS1140、TS1150 およびそれ以降の世代のドライブを混用することはできません。3つの特殊構成のいずれかを使用してください。詳細については、98 ページの『3592 装置クラスの定義』を参照してください。

ライブラリー内のボリュームを暗号化する予定である場合は、ライブラリーのメディアの世代を混合させないようにしてください。

## 混合メディアおよびストレージ・プール

ストレージ・プール内でメディア・フォーマットを混用しないことで、テープ・ソリューションの効率を最適化することができます。フォーマットを混用せずに、固有のメディア・フォーマットごとに、独自の装置クラスを使用して別個のストレージ・プールにマップします。この制限は、LTO フォーマットにも適用されます。

異なるタイプの複数のストレージ・プールおよびその装置クラスは、18 ページの『ライブラリーでの異なるメディア世代』で説明したように、サポートする同じライブラリーを指すことができます。

以下のステップに従えば、同じストレージ・プール内で新しい世代のメディア・タイプにマイグレーションできます。

1. ライブラリー内のすべての古いドライブを新しい世代のドライブに置き換えます。ドライブは混合状態にする必要があります。
2. 新しいドライブがそれらのテープを古いフォーマットで追加できない場合は、古いフォーマットの既存のボリュームに読み取り専用のマークを付けます。新しいドライブが既存のメディアにその古いフォーマットで書き込める場合は、これは不要ですが、ステップ 1 は必要です。読み取りは行われるが書き込みは行わない異なるドライブ世代が、同一ライブラリー内で互換性を保持する必要がある場合は、それぞれに別個のストレージ・プールを使用します。

## 磁気テープ・ストレージ装置の定義


IBM Spectrum Protect サーバーがテープ装置を使用できるようにするには、事前にオペレーティング・システムおよびサーバーに対して装置を構成する必要があります。計画プロセスの一環として、磁気テープ・ストレージ装置の定義を判別します。


**ヒント：PERFORM LIBACTION** コマンドを使用すると、SCSI ライブラリー・タイプおよび VTL ライブラリー・タイプに装置を追加するときのプロセスを簡素化することができます。

19 ページの表 7 は、さまざまな装置タイプの定義を要約しています。

表 7. ストレージ装置の定義					
装置	装置タイプ	定義			
		ライブラリー	ドライブ	パス	装置クラス
磁気ディスク	DISK	—	—	—	Yes <sup>1</sup>
	FILE <sup>2</sup>	—	—	—	Yes
	<div>Windows AIX</div> CENTERA	—	—	—	Yes
	<div>Linux</div> CENTERA <sup>3</sup>				

表 7. ストレージ装置の定義 (続き)

装置	装置タイプ	定義			
		ライブラリ	ドライブ	パス	装置クラス
テープ	3590 3592 DLT LTO NAS VOLSAFE  GENERICTAPE ECARTRIDGE <sup>4</sup>	Yes	Yes	Yes	Yes
取り外し可能メディア (ファイル・システム)	REMOVABLEFILE	Yes	Yes	Yes	Yes

1. DISK 装置クラスはインストール時に存在し、変更できません。
2. ストレージ・エージェントとの共用には、FILE ライブラリー、ドライブ、およびパスが必要です。
3.  CENTERA 装置タイプは、Linux x86\_64 システムでのみ使用可能です。
4. ECARTRIDGE 装置タイプは、Oracle StorageTek カートリッジテープ装置 (9840 や T10000 ドライブなど) 用です。

## ストレージ・プール階層の計画

データが毎日ディスクからテープに確実にマイグレーションされるように、ストレージ・プール階層を計画します。マイグレーションは、ディスク装置上のスペースを解放し、長期保管のためにデータをテープに移動します。このようにして、テープ・ストレージのスケラビリティ、コスト効率、およびセキュリティ機能を活用することができます。

### 始める前に

ストレージ・プール階層は、データのフローを管理するのに役立ちます。データ・フローを理解するには、[21 ページの図 3](#) を参照してください。

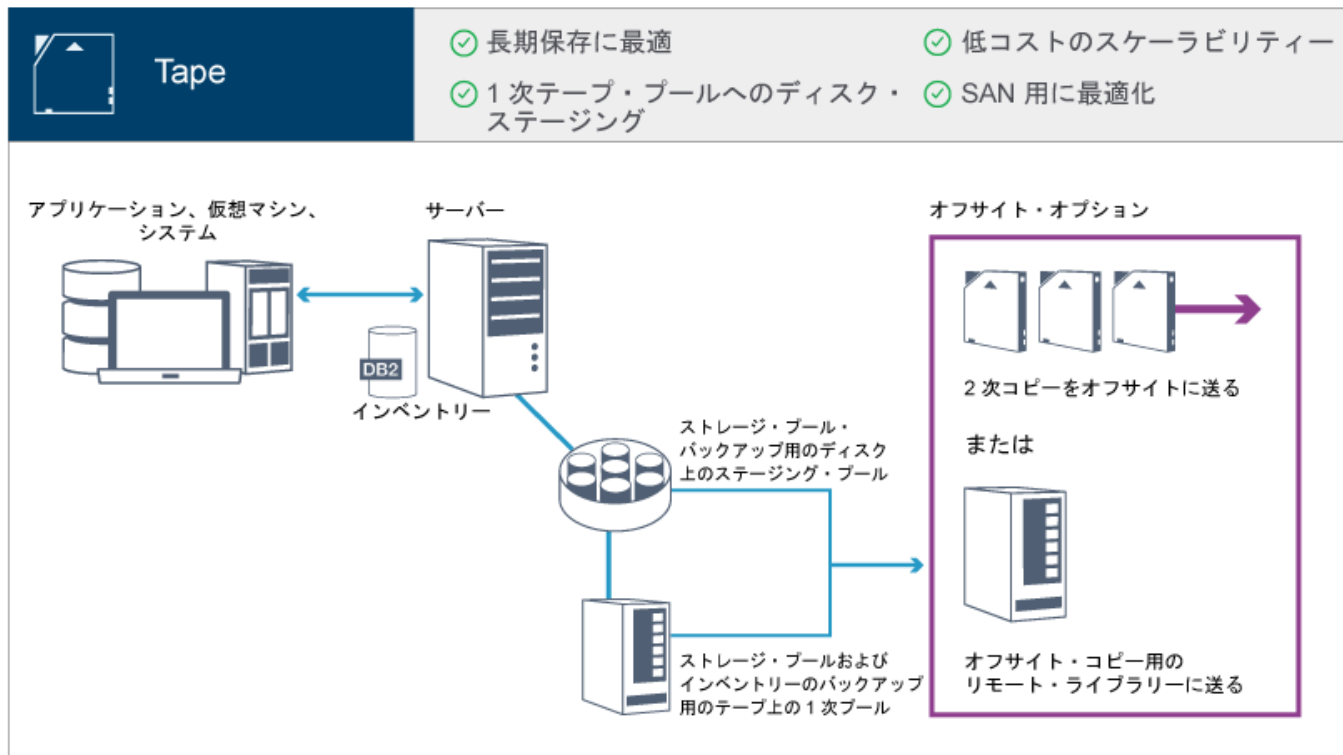


図 3. テープ・ソリューション

以下のステップは、図の番号に対応しています。

1. サーバーは、クライアント (アプリケーション、仮想マシン、またはシステム) からデータを受け取り、そのデータを 1 次ストレージ・プールに保管します。クライアント・タイプに応じて、データはディスクまたはテープ上の 1 次ストレージ・プールに保管されます。
2. ディスクおよびテープ上のデータは、テープ上のコピー・ストレージ・プールにバックアップされます。
3. ディスク上の 1 次ストレージ・プール内のデータは、テープ上の 1 次ストレージ・プールに毎日マイグレーションされます。
4. テープ上のコピー・ストレージ・プールからのデータは、長期保存および災害復旧をサポートするためにオフサイトに移動されます。

## 手順

ストレージ・プール階層を計画するには、以下の質問に答えてください。

- a. どのクライアントがディスクにデータをバックアップする必要があるか、およびどのクライアントがテープにデータをバックアップする必要があるか。
  - 大容量のオブジェクト (データベースなど) をホストするクライアントについては、テープにバックアップする方法が推奨されます。
  - その他のすべてのクライアントについては、ディスクにバックアップする方法が推奨されます。
  - 仮想マシン (VM) クライアントは、ディスクまたはテープにバックアップすることができます。VM クライアントについては、テープにマイグレーションされない独立したディスク・ストレージ・プールにバックアップする方法が推奨されます。VM クライアントをテープにマイグレーションする必要がある場合は、VMware 制御ファイルを保持するための小さいディスク・ストレージ・プールを作成してください。この小さいディスク・ストレージ・プールは、テープへのマイグレーションを許可することができません。テープへの VM クライアントのバックアップについて詳しくは、[磁気テープ・メディアのガイドラインおよび IBM Tivoli Storage Manager \(TSM\) guest support for Virtual Machines and Virtualization](#) を参照してください。

**ヒント:**多くのクライアントが単一のストレージ・プールにデータをバックアップする必要がある場合は、ディスク上のストレージ・プールを使用することを検討してください。多くのマウント・ポイントが指定できるためです。**REGISTER NODE** コマンドで **MAXNUMMP** パラメーターの最大値 999 を指定することができます。

- b. ディスク・ベースのディスク・ストレージ・プールの容量を指定する場合の考慮事項は何か。

少なくとも、1日のバックアップ操作で生じるデータを保管するのに十分な容量を計画してください。2日間のバックアップ操作に相当するデータを保管するのに十分な容量に20%のバッファを追加した容量を計画する方法が推奨されます。

- c. ディスク・ベースのディスク・ストレージ・プールに装置クラスを指定する場合の考慮事項は何か。

**FILE** 装置クラスを指定する方法が推奨されます。**MOUNTLIMIT** パラメーターを 4000 に設定します。また、ノードに十分に多い数のマウント・ポイントがあることを確認します。これは、**REGISTER NODE** コマンドで **MAXNUMMP** パラメーターを使用することで指定できます。

- d. ディスク・ストレージ・プールに対してデータ重複排除を指定する必要があるか。

いいえ。データがテープにマイグレーションされる前にディスクに保管されるのは1日のみであるためです。

- e. マイグレーションしきい値に基づいてデータの自動マイグレーションを指定する必要があるか。

いいえ。代わりに、**MIGRATE STGPOOL** コマンドを使用して日次マイグレーションをスケジュールすることを計画します。(マイグレーションしきい値に基づく自動マイグレーションが行われないようにするには、**DEFINE STGPOOL** コマンドの発行時に **HIGHMIG** パラメーターに値 100 を指定し、**LOWMIG** パラメーターに 0 を指定します。)

- f. マイグレーション遅延を指定する必要があるか。

ディスクからテープへの日次マイグレーションを指定し、マイグレーション遅延を指定しない(これには追加の計画が必要)方法が推奨されます。マイグレーション遅延について詳しくは、[ストレージ・プール階層内のファイルのマイグレーション](#)を参照してください。

- g. テープ・ドライブの数を計算する方法

- i) 製造元を資料を参照して、ドライブのネイティブ・データ転送速度を判別します。ご使用のストレージ環境の持続データ転送速度の見積もりを取得するには、ネイティブ・データ転送速度から30%を減算します。
- ii) サーバーによるデータ取り込みの必要な速度を計算します。次に、単一テープ装置の持続データ転送速度でその数値を除算します。その結果が、データ取り込みをサポートするためのドライブの最小数です。
- iii) データをテープにバックアップするクライアント(複数セッションを使用するクライアントを含む)に必要なマウント・ポイントの数を計算します。マウント・ポイントは、バックアップ・ウィンドウ全体に分散させることができます。この際、クライアントが大容量のオブジェクトをバックアップする可能性があり、そのバックアップでウィンドウの大半を使用する場合があることを留意してください。
- iv) 保守タスク(ディスクからテープへのマイグレーションやテープ間のマイグレーションなど)に必要なパフォーマンス要件およびマウント・ポイントを計算します。データをテープにバックアップすることで、マイグレーション・プロセスを回避することはできますが、テープ間のコピーを作成することで、テープ・ドライブの所要量が2倍になります。
- v) 必要になる可能性がある追加ドライブの数を計算します。例えば、以下のような場合です。
  - ・ テープ・ドライブで誤動作が発生した場合、その問題が使用可能なマウント・ポイントの数や取り込み速度に影響します。スペア・ドライブの提供を検討します。例えば、通常の操作で5つのテープ・ドライブが必要な場合は、2つのスペア・ドライブを提供することを検討します。
  - ・ リストア操作およびリトリブ操作では、その操作と同時にデータ取り込みや保守操作を実行する予定の場合に、追加の磁気テープ・ドライブが必要になることがあります。必要な場合は、追加の磁気テープ・ドライブを提供し、リストア操作やリトリブ操作を開始したときにそれらのドライブが使用されないようにする必要があります。

- h. リストア操作を最適化するために使用可能な代替方法は何か。



コロケーションを使用して、システム・パフォーマンスを向上させ、データ編成を最適化することができます。コロケーションにより、大容量データをリストアしなければならない時にアクセスする必要があるボリュームの数を削減できます。

- ・ディスク・ベースのストレージ・プールの場合、ノードごとにコロケーションを使用する方法が推奨されます。サーバーは、ノードのデータを可能な限り少ないボリュームに保管します。
- ・テープ・ベースのストレージ・プールの場合、グループごとにコロケーションを使用する方法が推奨されます。グループごとのコロケーションにより、未使用のテープ容量が削減されます。これによって、より多くのデータを個々のテープ上でコロケーションできるようになります。

コロケーションについて詳しくは、[169 ページの『クライアント・ファイルのコロケーションの使用可能化による操作の最適化』](#)を参照してください。

経験豊富なシステム管理者である場合、リストア操作を最適化するための追加アクションを計画することもできます。[クライアントのリストア操作の最適化](#)、[ファイル・バックアップ技法](#)、および [MOVE NODEDATA \(順次アクセス・ストレージ・プールでのノード別のデータの移動\)](#)を参照してください。

## オフサイト・データ・ストレージ

データ・リカバリーを容易にするため、および災害復旧戦略の一環として、テープ・コピーをオフサイトに保管します。

災害復旧管理機能 (DRM) 機能を使用して、災害後に自動的にサーバーをリストアし、クライアント・データをリカバリーするために必要な情報、スクリプト、および手順を含む災害時回復計画を構成し、自動的に生成します。災害復旧戦略として以下のいずれかのオフサイト・データ・ストレージ・オプションを選択し、テープ・コピーを保護します。

### 単一の実動サイトからオフサイト・ボールドへの収容

ストレージ・ボリューム (テープ・カートリッジやメディア・ボリュームなど) は、オフサイト・コロケーションのボールドに収容されます。クーリエは、データをオフサイトのストレージ設備からリカバリー・サイトに移送します。災害が発生すると、ハードウェアと IBM Spectrum Protect サーバーがリストアされた後、ボリュームは実動サイトに返送されます。

### リカバリー・サイトを使用したオフサイト・ボールドへの収容

クーリエは、ストレージ・ボリュームを実動サイトからオフサイトのストレージ設備に移動します。専用のリカバリー・サイトを持つことで、単一の実動サイトと比較してリカバリー時間を削減することができます。ただし、このオプションを使用すると、維持が必要なハードウェアとソフトウェアの数が増加するため、災害復旧のコストが増加します。例えば、リカバリー・サイトには、互換性のある磁気テープ装置と IBM Spectrum Protect サーバー・ソフトウェアが必要です。実動サイトをリカバリーする前に、リカバリー・サイトのハードウェアとソフトウェアをセットアップして実行する必要があります。

### 電子的ボールド収容

災害復旧戦略として電子ボールドを使用するには、リカバリー・サイトで IBM Spectrum Protect サーバーが稼働している必要があります。重要データは、電子的に実動サイトからリカバリー・サイトのボールドに収容されます。重要データ以外のデータのオフサイト・ボールドへの収容には、DRM も使用されます。電子的ボールド収容では、従来のクーリエ方式よりもより速く頻繁に重要データがオフサイトに移動されます。重要データは既にリカバリー・サイトに保管されているため、リカバリー時間が削減されます。ただし、リカバリー・サイトが継続的に稼働するため、災害復旧戦略のコストは、オフサイト・ボールド収容より高額になります。

### 関連概念

[DRM を使用した災害に対する準備と災害からのリカバリー](#)

IBM Spectrum Protect は、災害時にご使用のサーバーおよびクライアントのデータをリカバリーするための災害復旧管理機能 (DRM) 機能を提供します。

## セキュリティの計画

アクセスと認証の制御を備えた IBM Spectrum Protect ソリューションでシステムのセキュリティを保護する計画を立て、データおよびパスワード送信の暗号化を検討します。

## 管理者役割の計画

IBM Spectrum Protect ソリューションにアクセスできる管理者に割り当てる権限レベルを定義します。

管理者には以下のいずれかのレベルの権限を割り当てることができます。

### システム

システム権限を持つ管理者は、最高レベルの権限を持っています。このレベルの権限を持つ管理者は、どのタスクでも実行できます。すべてのポリシー・ドメインとストレージ・プールを管理でき、その他の管理者に権限を付与することができます。

### ポリシー

ポリシー権限を持つ管理者は、ポリシー管理に関連するすべてのタスクを管理できます。この特権を無制限にしたり、特定のポリシー・ドメインに制限したりすることができます。

### ストレージ

ストレージ権限を持つ管理者は、サーバー用のストレージ・リソースを割り振り、制御することができます。

### オペレーター

オペレーター権限を持つ管理者は、サーバーの即時操作と、テープ・ライブラリーやドライブなどのストレージ・メディアの可用性を制御できます。

24 ページの表 8 のシナリオでは、管理者がタスクを実行できるようにさまざまなレベルの権限を割り当てる理由を例を挙げて示します。

表 8. 管理者役割のシナリオ	
シナリオ	セットアップする管理者 ID のタイプ
小規模な会社の管理者は、サーバーを管理し、すべてのサーバー・アクティビティを担当します。	<ul style="list-style-type: none"><li>システム権限: 1 つの管理者 ID</li></ul>
複数のサーバーの管理者は、システム全体の管理も行います。その他の何人かの管理者が、それぞれのストレージ・プールを管理します。	<ul style="list-style-type: none"><li>すべてのサーバーに対するシステム権限: システム全体の管理者用に 1 つの管理者 ID</li><li>指定されたストレージ・プールに対するストレージ権限: その他の各管理者に 1 つの管理者 ID</li></ul>
管理者が 2 つのサーバーを管理します。他のユーザーが管理タスクを補助します。2 人のアシスタントが、重要なシステムがバックアップされていることの確認の補助を担当します。各アシスタントは、1 台の IBM Spectrum Protect サーバーのスケジュール済みバックアップのモニターを担当しています。	<ul style="list-style-type: none"><li>両方のサーバーに対するシステム権限: 2 つの管理者 ID</li><li>オペレーター権限: 各ユーザーが担当するサーバーへのアクセス権を持つアシスタント用に 2 つの管理者 ID</li></ul>

### 関連タスク

#### 管理者の管理

システム権限を持つ管理者は、IBM Spectrum Protect サーバーを使用するすべてのタスク (他の管理者への権限レベルの割り当てを含む) を実行することができます。一部のタスクを実行するには、1 つ以上の権限レベルを割り当てられることによって権限を付与される必要があります。

# セキュア通信の計画

IBM Spectrum Protect ソリューション・コンポーネント間の通信を保護するための計画。

企業の運営に適用される規制要件とビジネス要件に基づいて、データに必要な保護のレベルを判別します。

パスワードとデータ転送に関して高水準のセキュリティがビジネスで要求される場合は、Transport Layer Security (TLS) プロトコルまたは Secure Sockets Layer (SSL) プロトコルを使用したセキュア通信の実装を計画します。

TLS および SSL は、サーバーとクライアントとの間にセキュア通信を提供しますが、システム・パフォーマンスに影響を及ぼす可能性があります。システム・パフォーマンスを向上させるには、オブジェクト・データを暗号化しない状態で、認証用に TLS を使用します。サーバーが TLS を使用するのにはセッション全体か、認証に対してだけかを指定するには、クライアントとサーバー間の通信の場合は SSL クライアント・オプションを参照し、サーバー間通信の場合は **UPDATE SERVER=SSL** パラメーターを参照してください。

V8.1.2 以降、TLS は認証用にデフォルトで使用されます。セッション全体の暗号化に TLS を使用する場合は、必要な場合のみセッションにプロトコルを使用し、ネットワーク・トラフィックの増加を管理するために、サーバーにプロセッサ・リソースを追加してください。その他のオプションを試すこともできます。例えば、ルーターやスイッチのような一部のネットワーキング装置が TLS 機能または SSL 機能を提供します。

TLS および SSL を使用して、可能な各種通信パスの一部またはすべてを保護することができます。例えば、次のものがあります。

- Operations Center: ブラウザーからハブ、ハブからスポーク
- クライアントからサーバー
- サーバーからサーバー: ノード複製

## 関連タスク

トランスポート層セキュリティを使用したセキュア通信の構成

ご使用の環境のデータを暗号化し、通信を保護するには、Secure Sockets Layer (SSL) または Transport Layer Security (TLS) を IBM Spectrum Protect サーバーおよびバックアップ/アーカイブ・クライアントで有効にします。SSL 証明書は、サーバーとクライアントの間の通信要求を検証するために使用されます。

# 暗号化データのストレージの計画

企業で保管データを暗号化する必要があるかどうかを判別して、ニーズに最も適した方式を選択します。

表 9. データ暗号化方式の選択		
ビジネス要件	暗号化方式	追加情報
クライアント・レベルでデータを保護します。	IBM Spectrum Protect クライアント暗号化	包含/除外リストを使用して、ファイル・レベルでデータを暗号化できます。この方法では、どのデータを暗号化するかについて高度な制御を維持することができます。クライアントで追加のコンピューティング・リソースが必要になり、バックアップ・プロセスやリストア・プロセスのパフォーマンスに影響する可能性があります。この方式について詳しくは、 <a href="#">IBM Spectrum Protect クライアントの暗号化</a> を参照してください。

表 9. データ暗号化方式の選択 (続き)

ビジネス要件	暗号化方式	追加情報
磁気テープ・ドライブ上のストレージ・プール・ボリューム内のデータを保護します。	アプリケーション方式	アプリケーション方式を使用する場合、IBM Spectrum Protect が暗号鍵を管理して、ストレージ・プール・ボリューム内のデータを保護します。暗号鍵がサーバー・データベースに保管されるため、データベース・バックアップをより慎重に保護する必要があります。データベース・バックアップへのアクセスと一致する暗号鍵がなければ、データをリストアすることはできません。この方法を使用して、データベース・バックアップ、エクスポートされたデータ、およびバックアップ・セットを暗号化することはできません。アプリケーション方式について詳しくは、 <a href="#">122 ページの『テープ暗号化方式』</a> を参照してください。
磁気テープ・ドライブ上のデータを保護します。	ライブラリー方式	ライブラリー方式を使用する場合、ライブラリーが暗号鍵を管理します。ストレージ・プール内のデータと磁気テープ・ドライブ上のその他のデータの両方を暗号化することができます。バーコード・シリアル番号を使用して、どのボリュームを暗号化するかを制御できます。ライブラリー方式について詳しくは、 <a href="#">122 ページの『テープ暗号化方式』</a> を参照してください。
磁気テープ・ドライブ上のデータを保護します。	システム方式	システム方式を使用する場合、デバイス・ドライバーまたは AIX オペレーティング・システムが暗号化を管理します。この暗号化方式は、AIX オペレーティング・システムでのみ使用可能です。ストレージ・プール内のデータと磁気テープ・ドライブ上のその他のデータの両方を暗号化することができます。システム方式について詳しくは、 <a href="#">122 ページの『テープ暗号化方式』</a> を参照してください。

## ファイアウォール・アクセスの計画

設定されているファイアウォールと、IBM Spectrum Protect ソリューションを機能させるために開く必要のあるポートを決定します。

26 ページの表 10 では、サーバー、クライアント、および Operations Center で使用されるポートについて説明します。

表 10. サーバー、クライアント、および Operations Center によって使用されるポート

項目	デフォルト	方向	説明
基本ポート (TCP <code>PORT</code> )	1500	アウトバウンド/インバウンド	サーバー・インスタンスには、個別に固有のポートが必要です。代替ポート番号を指定することができます。TCP <code>PORT</code> オプションは、クライアントからの TCP/IP セッションと SSL 対応セッションの両方を listen します。TCP <code>ADMINPORT</code> オプションおよび <b>ADMINONCLIENTPORT</b> オプションを使用して、管理クライアント・トラフィック用のポート値を設定することができます。
SSL 専用ポート (SSLTCP <code>PORT</code> )	デフォルトなし	アウトバウンド/インバウンド	このポートは、ポート上の通信を SSL 対応セッションのみに制限したい場合に使用します。サーバーは、TCP <code>PORT</code> オプションまたは TCP <code>ADMINPORT</code> オプションを使用することで、SSL 通信と非 SSL 通信の両方をサポートすることができます。

表 10. サーバー、クライアント、および Operations Center によって使用されるポート (続き)			
項目	デフォルト	方向	説明
SMB	45	インバウンド/ アウトバウン ド	このポートは、ネイティブ・プロトコルを使用して複数のホストと通信する構成ウィザードによって使用されます。
SSH	22	インバウンド/ アウトバウン ド	このポートは、ネイティブ・プロトコルを使用して複数のホストと通信する構成ウィザードによって使用されます。
SMTP	25	アウトバウン ド	このポートは、サーバーから E メール・アラートを送信するために使用されます。
複製	デフォルトなし	アウトバウン ド/インバウン ド	複製用のアウトバウンド・ポートのポートおよびプロトコルは、複製をセットアップするために使用される <b>DEFINE SERVER</b> コマンドによって設定されます。  複製用のインバウンド・ポートは、 <b>DEFINE SERVER</b> コマンドでソース・サーバー用に指定された TCP ポートおよび SSL ポートです。
クライアント・スケジュール・ポート	クライアント・ポート: 1501	アウトバウン ド	クライアントは、指定されたポートで listen し、サーバーにポート番号を伝えます。サーバーは、サーバーが要求したスケジューリングが使用されている場合にクライアントに接続します。クライアント・オプション・ファイルで代替ポート番号を指定することができます。
長時間実行中のセッション	<b>KEEPALIVE</b> 設定: YES	アウトバウン ド	<b>KEEPALIVE</b> オプションが有効にされている場合、ファイアウォール・ソフトウェアが長時間実行中の非アクティブ接続を閉じないように、クライアント/サーバー・セッション中にキープアライブ・パケットが送信されます。
Operations Center	HTTPS: 11090	インバウン ド	これらのポートは、Operations Center Web ブラウザーに使用されます。代替ポート番号を指定することができます。
クライアント管理サービス・ポート	クライアント・ポート: 9028	インバウン ド	IBM Spectrum Protect クライアント管理サービスを使用する予定の場合、Operations Center からクライアント管理サービス・ポートにアクセスする必要があります。ファイアウォールによって接続が妨げられないことを確認します。クライアント管理サービスは、管理セッションを使用する認証に、クライアント・ノードのサーバーの TCP ポートを使用します。

## 関連情報

IBM Spectrum Protect クライアント管理サービスを使用した診断情報の収集

[ADMINONCLIENTPORT サーバー・オプション](#)

[DEFINE SERVER \(サーバー間の通信のためのサーバー定義\)](#)

[TCPADMINPORT サーバー・オプション](#)

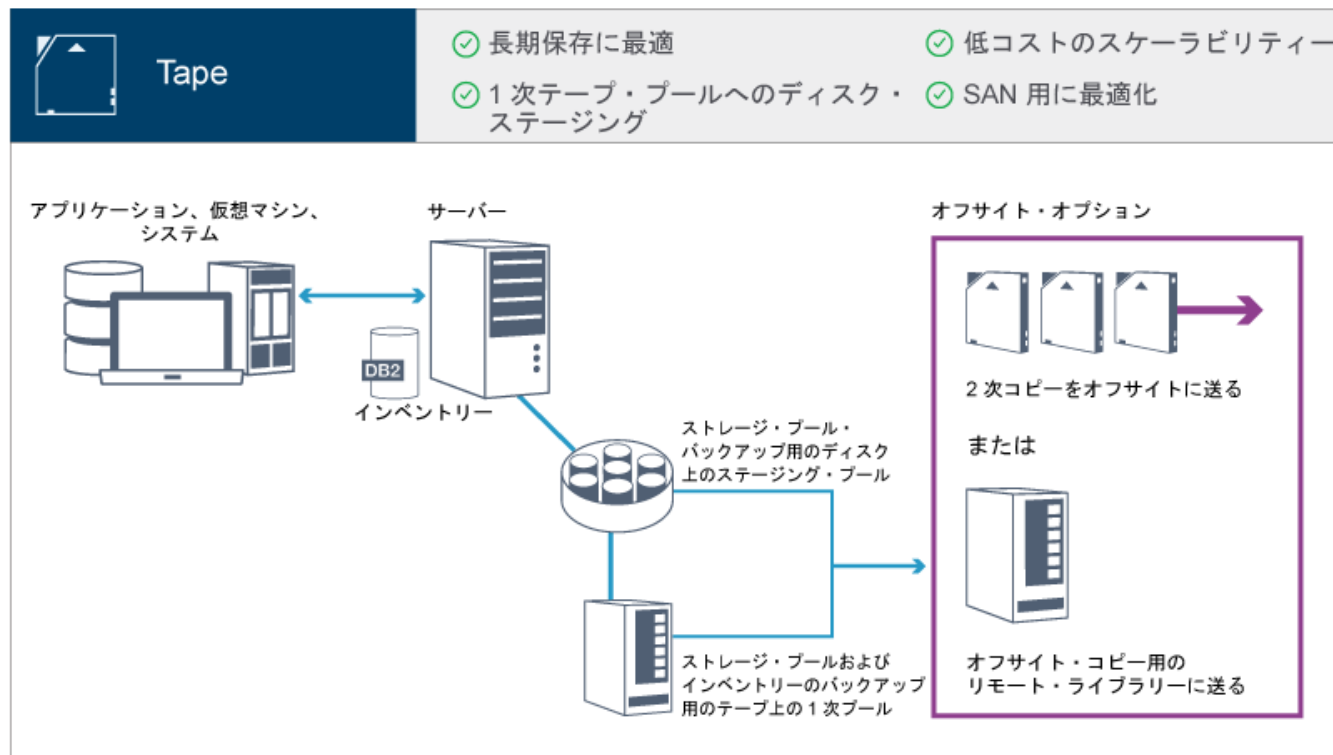
[TCPPOINT サーバー・オプション](#)





## 第2部 テープ・ベースのデータ保護ソリューションの実装

テープ・ベースのソリューションを実装します。このソリューションでは、ディスクからディスク、さらにディスクからテープへのバックアップおよびディスク・ステージングを使用してストレージを最適化します。テープ・ソリューションを実装することで、長期間のデータ保存が可能になり、低コストでのスケーラビリティを実現することができます。



### ヒント:

- ここで説明されているソリューションでは、データはディスク・ストレージ・プールから磁気テープ・ストレージにマイグレーションされます。一方、データをマイグレーションする代わりに、IBM Spectrum Protect バージョン 8.1.8 で導入された「テープへの層化 (tiering-to-tape)」機能を使用できます。この機能を使用すると、ディスクのディレクトリー・コンテナ・ストレージ・プールから磁気テープ・ストレージにデータを自動的に層化できます。すべてのデータを指定の経過時間しきい値に基づいて層化すること、または非アクティブ・データのみを経過時間しきい値に基づいて層化することを指定できます。磁気テープ・ストレージへのデータの層化について詳しくは、[クラウドまたは磁気テープ・ストレージへのデータの層化](#)を参照してください。
- 説明されているソリューションには、ノード複製は含まれません。ノード複製を使用してディスク間でストレージ・プールをバックアップしたい場合は、データがディスクからテープにマイグレーションされる前に、複製操作が完了している必要があります。また、ノード複製を使用して、ローカル・テープ装置上のストレージ・プールをローカル・テープ装置上のコピー・ストレージ・プールにバックアップすることもできます。

### 実装のロードマップ

テープ・ベースのソリューションをセットアップするには、以下のステップが必要です。

1. システムをセットアップします。
2. サーバーおよび Operations Center をインストールします。
3. サーバーおよび Operations Center を構成します。

4. サーバーのテープ装置を接続します。
5. サーバーで使用するテープ・ライブラリーを構成します。
6. ストレージ・プール階層をセットアップします。
7. クライアントをインストールし、構成します。
8. LAN フリー・データ移動を構成します。
9. 暗号化方式を選択し、暗号化を構成します。
10. 磁気テープ・ストレージ操作をセットアップします。
11. 実装を完了します。

## システムのセットアップ

---

システムをセットアップするには、最初にディスク・ストレージ・ハードウェアおよびサーバー・システムを IBM Spectrum Protect 用に構成する必要があります。

### このタスクについて

ヒント：サーバーおよびディスク・ストレージ・システムのセットアップ手順について説明しています。テープ装置のセットアップを開始するには、75 ページの『サーバーのテープ装置の接続』を参照してください。

## ストレージ・ハードウェアの構成

---

ディスク・ストレージを最適化するには、IBM Spectrum Protect を使用したディスク・ストレージのセットアップに関するガイドラインを確認してください。その後、サーバーとディスク・ストレージ・デバイス装置を接続し、他の構成タスクを完了します。

### 始める前に

ディスク・ストレージのセットアップのガイドラインについては、DISK または FILE のストレージ・プールのチェックリストを参照してください。

### 手順

1. 以下のガイドラインに従って、サーバーとストレージ装置の間の接続を提供します。
  - ファイバー・チャネル接続用にスイッチまたは直接接続を使用します。
  - 接続されるポートの数と、必要となる帯域幅の量を検討します。
  - サーバー上のポートの数と、接続されているディスク・システム上のホスト・ポートの数を検討します。
2. サーバー・システム、アダプター、およびオペレーティング・システムのデバイス・ドライバーおよびファームウェアが最新状態かつ推奨レベルであることを確認します。
3. ストレージ・アレイを構成します。最適なパフォーマンスを確保できるように適切に計画したことを確認します。

詳細については、12 ページの『ディスク・ストレージの計画』を参照してください。
4. サーバー・システムが、作成されるディスク・ボリュームにアクセスできる必要があります。次の手順を実行してください。
  - a) システムがファイバー・チャネル・スイッチに接続されている場合、ディスクを認識できるようにサーバーをゾーニングします。
  - b) この特定のサーバーが各ディスクを認識できることをディスク・システムに通知するために、すべてのボリュームをマップします。



5. テープ装置とディスク装置が異なるホスト・バス・アダプター (HBA) ポートを使用する必要があります。SAN を使用して、テープおよびディスクの入出力を制御します。テープとディスクの入出力には、それぞれ別のファイバー・チャネル・ポートを使用します。

### 関連タスク

#### マルチパス入出力の構成

ディスク・ストレージのマルチパスを有効にして構成することができます。詳細な手順については、ハードウェアに付属の資料を参照してください。

## サーバー・オペレーティング・システムのインストール

サーバー・システムにオペレーティング・システムをインストールして、IBM Spectrum Protect サーバー要件を満たしていることを確認します。指示に従ってオペレーティング・システムの設定を調整します。

### AIX システムへのインストール

サーバー・システムに AIX をインストールするには、以下の手順を実行します。

#### 手順

1. 製造元の指示に従い、AIX バージョン 7.1 TL4、SP6 以降をインストールします。
2. オペレーティング・システムのインストール手順に従って、TCP/IP 設定を構成します。
3. /etc/hosts ファイルを開き、以下のアクションを実行します。

- ・ ファイルを更新して、サーバーの IP アドレスとホスト名を組み込みます。例えば次のとおりです。

```
192.0.2.7 server.yourdomain.com server
```

- ・ ファイルにアドレス 127.0.0.1 を持つローカル・ホストの項目が含まれていることを確認します。例えば次のとおりです。

```
127.0.0.1 localhost
```

4. 次のコマンドを発行して、AIX 入出力完了ポートを有効にします。

```
chdev -l iocp0 -P
```

サーバーのパフォーマンスは、Olson タイム・ゾーン定義の影響を受ける可能性があります。

5. パフォーマンスを最適化するには、ご使用のシステムのタイム・ゾーン形式を Olson から POSIX に変更します。タイム・ゾーン設定を更新するには、次のコマンドを形式を使用します。

```
chtz=local_timezone,date/time,date/time
```

例えば、アメリカ山岳標準時を使用するアリゾナ州のツーソンに住んでいる場合、次のコマンドを発行して、POSIX 形式に変更します。

```
chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

6. インスタンス・ユーザーの .profile ファイルに、以下の環境変数が設定されていることを確認します。

```
export MALLOCOPTIONS=multiheap:16
```

これ以降の IBM Spectrum Protect サーバーのバージョンでは、この値はサーバーの開始時に自動的に設定されます。インスタンス・ユーザーが使用不可能な場合、後でインスタンス・ユーザーが使用可能になったときにこのステップを実行します。

7. 完全なアプリケーション・コア・ファイルを作成するようにシステムを設定します。以下のコマンドを発行します。

```
chdev -l sys0 -a fullcore=true -P
```

8. サーバーおよび Operations Center との通信のために、存在する可能性があるすべてのファイアウォールで以下のポートが開いていることを確認します。

- サーバーとの通信の場合は、ポート 1500 を開きます。
- Operations Center とのセキュア通信の場合は、ハブ・サーバー上でポート 11090 を開きます。

デフォルトのポート値を使用していない場合は、使用しているポートが開いていることを確認してください。

9. TCP ハイパフォーマンス機能拡張を有効にします。以下のコマンドを発行します。

```
no -p -o rfc1323=1
```

10. 最適なスループットと信頼性を確保するために、中規模システムの場合は 2 つの 10 Gb イーサネット・ポート、大規模システムの場合は 4 つの 10 Gb イーサネット・ポートを結合してください。System Management Interface Tool (SMIT) を使用して、イーサチャネルを使用してポートを結合します。テストでは以下の設定が使用されました。

mode	8023ad	
auto_recovery	yes	Enable automatic recovery after failover
backup_adapter	NONE	Adapter used when whole channel fails
hash_mode	src_dst_port	Determines how outgoing adapter is chosen
interval	long	Determines interval value for IEEE 802.3ad mode
mode	8023ad	EtherChannel mode of operation
netaddr	0	Address to ping
no_loss_failover	yes	Enable lossless failover after ping failure
num_retries	3	Times to retry ping before failing
retry_time	1	Wait time (in seconds) between pings
use_alt_addr	no	Enable Alternate EtherChannel Address
use_jumbo_frame	no	Enable Gigabit Ethernet Jumbo Frames

11. ユーザー処理リソースの限度 (*ulimits* と呼ばれる) が [32 ページの表 11](#) のガイドラインに従って設定されていることを確認します。*ulimit* 値が正しく設定されていない場合、サーバーが不安定になったり、サーバーが応答できない状態になったりする可能性があります。

表 11. ユーザー限度 ( <i>ulimit</i> ) 値			
ユーザー限度のタイプ	設定	値	値を照会するコマンド
作成されるコア・ファイルの最大サイズ	core	無制限	<code>ulimit -Hc</code>
プロセスのデータ・セグメントの最大サイズ	data	無制限	<code>ulimit -Hd</code>
最大ファイル・サイズ	fsize	無制限	<code>ulimit -Hf</code>
オープン・ファイルの最大数	nofile	65536	<code>ulimit -Hn</code>
最大プロセッサ時間 (秒単位)	cpu	無制限	<code>ulimit -Ht</code>
ユーザー・プロセスの最大数	nproc	16384	<code>ulimit -Hu</code>

ユーザー限度の値を変更する必要がある場合は、ご使用のオペレーティング・システムの資料に記載されている説明に従ってください。

# Linux システムへのインストール

サーバー・システムに Linux x86\_64 をインストールするには、以下の手順を実行します。

## 始める前に

オペレーティング・システムは、内蔵ハード・ディスクにインストールされます。ハードウェア RAID 1 アレイを使用して、内蔵ハード・ディスクを構成します。例えば、小規模システムを構成している場合、2 個の 300 GB 内蔵ディスクが RAID 1 でミラーリングされ、オペレーティング・システム・インストーラーで単一の 300 GB ディスクが使用可能であることが提示されます。

## 手順

1. 製造元の指示に従って、Red Hat Enterprise Linux バージョン 7.8 以降またはバージョン 8.2 以降をインストールします。

サポート対象バージョンの Red Hat Enterprise Linux が含まれるブート可能 DVD を入手し、この DVD からシステムを始動します。インストール・オプションについては、以下のガイダンスを参照してください。以下のリストで項目が記載されていない場合は、デフォルトの選択のまま残します。

- a) DVD を開始した後、メニューから「**Install or upgrade an existing system**」を選択します。
- b) ようこそ画面で、「**Test this media & install Red Hat Enterprise Linux 7.8**」を選択します。
- c) 使用する言語およびキーボード設定を選択します。
- d) ロケーションを選択し、適切なタイム・ゾーンを設定します。
- e) 「**ソフトウェアの選択**」を選択し、次の画面で「**サーバー (GUI を使用)**」を選択します。
- f) インストールの要約ページで、「**インストール先**」をクリックし、以下の項目を確認します。
  - ・ インストール・ターゲットとして 300 GB のローカル・ディスクが選択されている。
  - ・ 「その他のストレージオプション」で、「自動構成のパーティション構成」が選択されている。

「完了」をクリックします。

- g) 「**インストールの開始**」をクリックします。

インストールが開始されたら、root ユーザー・アカウントの root パスワードを設定します。

インストールが完了した後、システムを再始動し、root ユーザーとしてログインします。**df** コマンドを発行して、基本的な区画化を確認します。

例えば、テスト・システムで、初期の区画化によって以下のような結果が生じたとします。

```
[root@tvapp02]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root  50G   3.0G   48G   6% /
devtmpfs        32G     0    32G   0% /dev
tmpfs           32G   92K    32G   1% /dev/shm
tmpfs           32G   8.8M    32G   1% /run
tmpfs           32G     0    32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home 220G   37M   220G   1% /home
/dev/sda1       497M  124M   373M  25% /boot
```

2. オペレーティング・システムのインストール手順に従って、TCP/IP 設定を構成します。

最適なスループットと信頼性を確保するために、複数のネットワーク・ポートを結合することを検討してください。中規模システムの場合は 2 つのポートを、大規模システムの場合は 4 つのポートを結合してください。これは、Link Aggregation Control Protocol (LACP) ネットワーク接続を作成することで実現できます。LACP ネットワーク接続は、複数の従属ポートを結合して単一の論理接続にします。推奨される方法は、結合モード 802.3ad、**miimon** 設定 100、および **xmit\_hash\_policy** 設定 layer3+4 を使用する方法です。

**制約事項:** LACP ネットワーク接続を使用するには、LACP をサポートするネットワーク・スイッチが必要です。

Red Hat Enterprise Linux バージョン 7 での結合ネットワーク接続の構成に関する追加手順については、[Create a Channel Bonding Interface](#) を参照してください。

3. `/etc/hosts` ファイルを開き、以下のアクションを実行します。

- ファイルを更新して、サーバーの IP アドレスとホスト名を組み込みます。例えば次のとおりです。

```
192.0.2.7 server.yourdomain.com server
```

- ファイルにアドレス `127.0.0.1` を持つローカル・ホストの項目が含まれていることを確認します。例えば次のとおりです。

```
127.0.0.1 localhost
```

4. サーバーのインストールに必要なコンポーネントをインストールします。以下のステップを実行して、Yellowdog Updater Modified (YUM) リポジトリを作成し、前提条件パッケージをインストールします。

- a) Red Hat Enterprise Linux のインストール DVD をシステム・ディレクトリーにマウントします。例えば、`/mnt` ディレクトリーにマウントするには、次のコマンドを発行します。

```
mount -t iso9660 -o ro /dev/cdrom /mnt
```

- b) **mount** コマンドを発行して、DVD がマウントされていることを確認します。  
次の例のような出力が表示されるはずです。

```
/dev/sr0 on /mnt type iso9660
```

- c) 次のコマンドを発行して、YUM リポジトリ・ディレクトリーに移動します。

```
cd /etc/yum/repos.d
```

For RHEL 8:

```
cd /etc/yum.repos.d
```

`repos.d` ディレクトリーが存在しない場合は、作成してください。

- d) ディレクトリーの内容をリストします。

```
ls rhel-source.repo
```

- e) **mv** コマンドを発行して、元のリポジトリ・ファイルの名前を変更します。  
例えば次のとおりです。

```
mv rhel-source.repo rhel-source.repo.orig
```

- f) テキスト・エディターを使用して、新しいリポジトリ・ファイルを作成します。  
例えば、`vi` エディターを使用するには、次のコマンドを発行します。

```
vi rhel78_dvd.repo
```

- g) 新しいリポジトリ・ファイルに以下の行を追加します。**baseurl** パラメーターは、ディレクトリーのマウント・ポイントを指定します。

```
[rhel78_dvd]
name=DVD Redhat Enterprise Linux 7.8
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

For RHEL 8:

```
[InstallMedia-BaseOS]
name=Red Hat Enterprise Linux 8.2.0
mediaid=None
metadata_expire=-1
gpgcheck=0
cost=500
enabled=1
baseurl=file:///mnt/BaseOS/
```

```
[InstallMedia-AppStream]
name=Red Hat Enterprise Linux 8.2.0
mediaid=None
metadata_expire=-1
gpgcheck=0
cost=500
enabled=1
baseurl=file:///mnt/AppStream/
```

- h) **yum** コマンドを発行して、追加の前提条件ソフトウェア・パッケージをインストールします。例えば次のとおりです。

```
yum install ksh.x86_64
yum install sysstat
For RHEL 8:
yum install libnsl
```

5. ソフトウェア・インストールが完了すると、以下のステップを実行して、元の YUM リポジトリの値を復元できます。

- a) 次のコマンドを発行して、Red Hat Enterprise Linux のインストール DVD をアンマウントします。

```
umount /mnt
```

- b) 次のコマンドを発行して、YUM リポジトリ・ディレクトリに移動します。

```
cd /etc/yum/repos.d
```

- c) 作成したリポジトリ・ファイルを名前変更します。

```
mv rhel78_dvd.repo rhel78_dvd.repo.orig
```

- d) 元のファイルを元の名前に変更します。

```
mv rhel-source.repo.orig rhel-source.repo
```

6. カーネル・パラメーターの変更が必要かどうかを判別します。次の手順を実行してください。

- a) **sysctl -a** コマンドを使用して、パラメーターの値をリストします。
- b) [35 ページの表 12](#) のガイドラインを使用して結果を分析し、何らかの変更が必要かどうかを判別します。
- c) 変更が必要な場合は、`/etc/sysctl.conf` ファイルでパラメーターを設定します。  
ファイルの変更は、システムの始動時に適用されます。

**ヒント:** 自動的にカーネル・パラメーター設定を調整し、これらの設定を手動で更新する必要性を除去します。Linux では、Db2 データベース・ソフトウェア は、プロセス間通信 (IPC) カーネル・パラメーター値を優先設定に自動的に調整します。カーネル・パラメーター設定について詳しくは、[バージョン 11.5 製品資料](#) で Linux カーネル・パラメーターを検索してください。

表 12. Linux カーネル・パラメーターの最適な設定	
パラメーター	説明
<b>kernel.shmmni</b>	セグメントの最大数。
<b>kernel.shmmax</b>	共有メモリー・セグメントの最大サイズ (バイト)。 このパラメーターは、システム起動時に IBM Spectrum Protect サーバーを自動的に始動する前に設定する必要があります。
<b>kernel.shmall</b>	共有メモリー・ページの最大割り振り (ページ)。

表 12. Linux カーネル・パラメーターの最適な設定 (続き)	
パラメーター	説明
<b>kernel.sem</b> <b>kernel.sem</b> パラメーターには 4 つの値があります。	(SEMMSL) アレイごとの最大セマフォ数。
	(SEMMNS) システムごとの最大セマフォ数。
	(SEMOPM) セマフォ・コールごとの最大操作数。
	(SEMMNI) アレイの最大数。
<b>kernel.msgmni</b>	システム全体のメッセージ・キューの最大数。
<b>kernel.msgmax</b>	メッセージの最大サイズ (バイト)。
<b>kernel.msgmnb</b>	キューのデフォルト最大サイズ (バイト)。
<b>kernel.randomize_va_space</b>	<b>kernel.randomize_va_space</b> パラメーターは、カーネルによるメモリー ASLR の使用を構成します。V7.1 以降のサーバー用に ASLR を使用可能にしてください。Linux ASLR および Db2 の詳細については、 <a href="#">技術情報 1365583</a> を参照してください。
<b>vm.swappiness</b>	<b>vm.swappiness</b> パラメーターは、カーネルが物理的なランダム・アクセス・メモリー (RAM) からアプリケーション・メモリーをスワップできるかどうかを定義します。カーネル・パラメーターについて詳しくは、「 <a href="#">Db2 製品情報</a> 」を参照してください。
<b>vm.overcommit_memory</b>	<b>vm.overcommit_memory</b> パラメーターは、カーネルが割り振りを許可する仮想メモリーの量に影響します。カーネル・パラメーターについて詳しくは、「 <a href="#">Db2 製品情報</a> 」を参照してください。

7. ファイアウォール・ポートを開き、サーバーと通信します。次の手順を実行してください。

- ネットワーク・インターフェースが使用するゾーンを決定します。デフォルトでは、ゾーンはパブリックです。

次のコマンドを発行します。

```
# firewall-cmd --get-active-zones
public
interfaces: ens4f0
```

- サーバーとの通信にデフォルトのポート・アドレスを使用するには、Linux ファイアウォールで TCP/IP ポート 1500 を開きます。

以下のコマンドを発行します。

```
firewall-cmd --zone=public --add-port=1500/tcp --permanent
```

デフォルト以外の値を使用する場合は、1024 から 32767 の範囲の数値を指定することができます。デフォルト以外のポートを開く場合、構成スクリプトの実行時にポートを指定する必要があります。

- このシステムをハブとして使用する予定の場合は、ポート 11090 を開きます。このポートは、セキュア (https) 通信用のデフォルト・ポートです。

以下のコマンドを発行します。

```
firewall-cmd --zone=public --add-port=11090/tcp --permanent
```

- d) 変更を有効にするには、ファイアウォール定義を再ロードします。

以下のコマンドを発行します。

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

8. ユーザー処理リソースの限度 (*ulimits* と呼ばれる) が [37 ページの表 13](#) のガイドラインに従って設定されていることを確認します。*ulimit* 値が正しく設定されていない場合、サーバーが不安定になったり、サーバーが応答できない状態になったりする可能性があります。

表 13. ユーザー限度 ( <i>ulimit</i> ) 値			
ユーザー限度のタイプ	設定	値	値を照会するコマンド
作成されるコア・ファイルの最大サイズ	core	無制限	<code>ulimit -Hc</code>
プロセスのデータ・セグメントの最大サイズ	data	無制限	<code>ulimit -Hd</code>
最大ファイル・サイズ	fsize	無制限	<code>ulimit -Hf</code>
オープン・ファイルの最大数	nofile	65536	<code>ulimit -Hn</code>
最大プロセッサ時間 (秒単位)	cpu	無制限	<code>ulimit -Ht</code>
ユーザー・プロセスの最大数	nproc	16384	<code>ulimit -Hu</code>

ユーザー限度の値を変更する必要がある場合は、ご使用のオペレーティング・システムの資料に記載されている説明に従ってください。

## Windows システムへのインストール

Microsoft Windows Server 2012 Standard Edition をサーバー・システムにインストールして、IBM Spectrum Protect サーバーのインストールと構成のためにシステムを準備します。

### 手順

1. 製造元の指示に従い Windows Server 2016 または 2019 Standard Edition をインストールします。
2. 以下のステップを実行して、Windows アカウント制御ポリシーを変更します。
  - a) `secpol.msc` を実行して、「ローカル セキュリティ ポリシー」エディターを開きます。
  - b) 「ローカル ポリシー」 > 「セキュリティのオプション」をクリックして、以下のユーザー・アカウント制御ポリシーが無効になっていることを確認します。
    - ・ 組み込みの Administrator アカウントに対する管理者承認モード
    - ・ 管理者承認モードですべての管理者を実行する
3. オペレーティング・システムのインストール手順に従って、TCP/IP 設定を構成します。
4. 以下のステップを実行して、Windows の更新を適用し、オプション・フィーチャーを有効にします。
  - a) 最新の Windows Server の更新を適用します。
  - b) 必要な場合は、FC およびイーサネット HBA のデバイス・ドライバーを新規レベルに更新します。
5. IBM Spectrum Protect サーバーとの通信のためにデフォルトの TCP/IP ポート 1500 を開きます。  
例えば、次のコマンドを出します。



```
netsh advfirewall firewall add rule name="Backup server port 1500"  
dir=in action=allow protocol=TCP localport=1500
```

6. Operations Center のハブ・サーバーで、Operations Center とのセキュア (https) 通信用にデフォルトのポートを開きます。

ポート番号は 11090 です。

例えば、次のコマンドを発行します。

```
netsh advfirewall firewall add rule name="Operations Center port 11090"  
dir=in action=allow protocol=TCP localport=11090
```

## マルチパス入出力の構成

ディスク・ストレージのマルチパスを有効にして構成することができます。詳細な手順については、ハードウェアに付属の資料を参照してください。

## AIX システム

ディスク・ストレージ用にマルチパスを有効にして構成するには、以下の手順を実行します。

### 手順

1. ディスク・サブシステム上のホスト定義に使用する必要があるファイバー・チャンネル・ポート・アドレスを判別します。すべてのポートに対して **lscfg** コマンドを発行します。

- 小規模および中規模のシステムでは、以下のコマンドを発行します。

```
lscfg -vps -l fcs0 | grep "Network Address"  
lscfg -vps -l fcs1 | grep "Network Address"
```

- 大規模のシステムでは、以下のコマンドを発行します。

```
lscfg -vps -l fcs0 | grep "Network Address"  
lscfg -vps -l fcs1 | grep "Network Address"  
lscfg -vps -l fcs2 | grep "Network Address"  
lscfg -vps -l fcs3 | grep "Network Address"
```

2. 以下の AIX ファイル・セットがインストールされていることを確認します。

- devices.common.IBM.mpio.rte
- devices.fcp.disk.rte

3. **cfgmgr** コマンドを発行して、AIX でハードウェアを再スキャンし、使用可能なディスクを検出します。例えば次のとおりです。

```
cfgmgr
```

4. 使用可能なディスクをリストするには、次のコマンドを実行します。

```
lsdev -Ccdisk
```

出力は、以下の例のようになります。

```
hdisk0 Available 00-00-00 SAS Disk Drive  
hdisk1 Available 00-00-00 SAS Disk Drive  
hdisk2 Available 01-00-00 SAS Disk Drive  
hdisk3 Available 01-00-00 SAS Disk Drive  
hdisk4 Available 06-01-02 MPIO IBM 2076 FC Disk  
hdisk5 Available 07-01-02 MPIO IBM 2076 FC Disk  
...
```

5. **lsdev** コマンドの出力を使用して、各ディスク装置の装置 ID を識別してリストします。

例えば、装置 ID は hdisk4 のようになります。IBM Spectrum Protect サーバー用にファイル・システムを作成するときに使用するために、装置 ID のリストを保存します。



6. システム内のすべての物理ボリュームに関する詳細情報をリストして、SCSI 装置をディスク・システムの特定のディスク LUN に相互に関連付けます。以下のコマンドを発行します。

```
lspv -u
```

IBM Storwize システムでは、各装置について以下のような情報が表示されます。

```
hdisk4 00f8cf083fd97327 None active
3321360050763008101057800000000000003004214503IBMfc
```

この例で、**60050763008101057800000000000030** は、Storwize 管理インターフェースによって報告されるボリュームの UID です。

ディスク・サイズ (メガバイト単位) を確認してシステムについてリストされた値と比較するには、次のコマンドを発行します。

```
bootinfo -s hdisk4
```

## Linux システム

ディスク・ストレージ用にマルチパスを有効にして構成するには、以下の手順を実行します。

### 手順

1. Linux ホストに対してマルチパスを有効にするには、`/etc/multipath.conf` ファイルを編集します。`multipath.conf` ファイルが存在しない場合は、次のコマンドを発行して作成することができます。

```
mpathconf --enable
```

IBM FlashSystem® ストレージ・システムでのテストのために、`multipath.conf` で以下のパラメーターが設定されています。

```
defaults {
    user_friendly_names no
}

devices {
    device {
        vendor "IBM "
        product "2145"
        path_grouping_policy group_by_prio
        user_friendly_names no
        path_selector "round-robin 0"
        prio "alua"
        path_checker "tur"
        failback "immediate"
        no_path_retry 5
        rr_weight uniform
        rr_min_io_rq "1"
        dev_loss_tmo 120
    }
}
```

2. システムの始動時に開始するようにマルチパス・オプションを設定します。  
以下のコマンドを発行します。

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

3. ディスクがオペレーティング・システムに認識されていてマルチパスによって管理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。

```
multipath -l
```

4. 各装置がリストされていて、期待どおりの数のパスを持っていることを確認します。サイズおよび装置 ID の情報を使用して、リストされているディスクを識別できます。

例えば、以下の出力は、2 TB ディスクが 2 つのパス・グループと 4 つのアクティブ・パスを持っていることを示しています。2 TB のサイズにより、ディスクがプール・ファイル・システムに対応していることを確認します。長い装置 ID 番号の一部 (この例では 12) を使用して、ディスク・システムの管理インターフェースでボリュームを検索します。

```
[root@tapsrv01 code]# multipath -l
36005076802810c50980000000000012 dm-43 IBM,2145
size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|+- policy='round-robin 0' prio=0 status=active
|  |- 2:0:1:18 sdcw 70:64 active undef running
|  |- 4:0:0:18 sdgb 131:112 active undef running
|+- policy='round-robin 0' prio=0 status=enabled
|  |- 1:0:1:18 sdat 66:208 active undef running
|  |- 3:0:0:18 sddy 128:0 active undef running
```

- a) 必要な場合は、LUN ホスト割り当てディスクを訂正して、バスの再スキャンを強制します。  
例えば次のとおりです。

```
echo "- - -" > /sys/class/scsi_host/host0/scan
echo "- - -" > /sys/class/scsi_host/host1/scan
echo "- - -" > /sys/class/scsi_host/host2/scan
```

システムを再始動して、ディスクの LUN ホスト割り当てを再スキャンすることもできます。

- b) **multipath -l** コマンドを再発行して、ディスクをマルチパス入出力に使用できるようになったことを確認します。

## 5. マルチパス出力を使用して、各ディスク装置の装置 ID を識別してリストします。

例えば、2 TB ディスクの装置 ID は 36005076802810c50980000000000012 です。

次のステップで使用するために装置 ID のリストを保存します。

## Windows システム

ディスク・ストレージ用にマルチパスを有効にして構成するには、以下の手順を実行します。

### 手順

1. マルチパス入出力機能がインストールされていることを確認します。必要であれば、追加のベンダー固有のマルチパス・ドライバをインストールします。IBM FlashSystem デバイスには、Microsoft Device Specific Module (MSDSM) を使用してください。インストール手順については、IBM FlashSystem の資料 ([https://www.ibm.com/support/knowledgecenter/STHGuj\\_8.3.1/com.ibm.storwize.v5000.831.doc/svc\\_w2kmpio\\_21oxvp.html](https://www.ibm.com/support/knowledgecenter/STHGuj_8.3.1/com.ibm.storwize.v5000.831.doc/svc_w2kmpio_21oxvp.html)) を参照してください。
2. ディスクがオペレーティング・システムに認識されていてマルチパス入出力によって管理されていることを確認するには、Microsoft Windows Power Shell コマンド・プロンプトを開き、次のコマンドを発行します。

```
mpclaim -e
```

3. mpclaim の出力を調べて、IBM ストレージが MPIO 制御下として報告されていることを確認します。

"Target H/W Identifier"	"Bus Type"	MPIO-ed	ALUA Support
"IBM 2145"	"SAS"	YES	Implicit Only

4. 接続ディスク装置の詳細は、Windows wmic コマンドを使用して入手できます。

```
wmic diskdrive get
```

5. 新規ディスクをオンラインにして、読み取り専用属性をクリアするには、以下のコマンドを使用して diskpart.exe を実行します。各ディスクに対して操作を繰り返します。

```
diskpart
select Disk 1
online disk
```

```
attribute disk clear readonly
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
attribute disk clear readonly
exit
```

## サーバーのユーザー ID の作成

IBM Spectrum Protect サーバー・インスタンスを所有するユーザー ID を作成します。サーバーの初期構成時にサーバー・インスタンスを作成するときに、このユーザー ID を指定します。

### このタスクについて

ユーザー ID には、小文字 (a から z)、数字 (0 から 9)、および下線文字 (\_) のみを使用できます。ユーザー ID とグループ名は、以下のルールに従う必要があります。

- 長さは 8 文字以下でなければなりません。
- ユーザー ID およびグループ名の先頭に *ibm*、*sql*、*sys* または数字は使用できません。
- ユーザー ID およびグループ名を、*user*、*admin*、*guest*、*public*、*local*、または SQL の予約語にすることはできません。

### 手順

1. オペレーティング・システム・コマンドを使用してユーザー ID を作成します。

- **Linux** | **AIX** サーバー・インスタンスを所有するユーザーのホーム・ディレクトリーに、グループおよびユーザー ID を作成します。

例えば、グループ *tsmsrvrs* にパスワード *tsminst1* を持つユーザー ID *tsminst1* を作成するには、管理ユーザー ID から次のコマンドを発行します。

```
AIX mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

```
Linux groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

ログオフした後、システムにログインします。作成したユーザー・アカウントに変更します。telnet のような対話式ログイン・プログラムを使用してください。これを使用すると、パスワードの入力を求めるプロンプトが出され、必要に応じてパスワードを変更できます。

- **Windows** ユーザー ID を作成し、その新規 ID を管理者グループに追加します。例えば、ユーザー ID *tsminst1* を作成するには、次のコマンドを発行します。

```
net user tsminst1 * /add
```

新規ユーザーのパスワードを作成して確認した後、次のコマンドを発行して、そのユーザー ID を管理者グループに追加します。

```
net localgroup Administrators tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. 新規ユーザー ID をログオフします。

## サーバーのファイル・システムの準備

サーバーで使用するために、ディスク・ストレージのファイル・システム構成を完了する必要があります。

## AIX システム

AIX 論理ボリューム・マネージャーを使用して、サーバー用のボリューム・グループ、論理ボリューム、およびファイル・システムを作成する必要があります。

### 手順

1. 使用可能なすべての *hdiskX* ディスクのキュー項目数と最大転送サイズを増やします。各ディスクに対して以下のコマンドを発行します。

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

これらのコマンドをオペレーティング・システム内部ディスク (*hdisk0* など) に対して実行しないでください。

2. IBM Spectrum Protect データベース、活動ログ、アーカイブ・ログ、データベース・バックアップ、およびストレージ・プールのボリューム・グループを作成します。先ほど特定した対応するディスクに装置 ID を指定して、**mkvg** コマンドを発行します。

例えば、装置名 *hdisk4*、*hdisk5*、および *hdisk6* がデータベース・ディスクに対応している場合は、データベース・ボリューム・グループなどにそれらを組み込みます。

**システム・サイズ**: 以下のコマンドは、中規模のシステム構成に基づいています。小規模システムおよび大規模システムでは、必要に応じて構文を調整する必要があります。

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. 論理ボリュームを作成するときに使用する物理ボリューム名と空き物理区画数を決定します。前のステップで作成した各ボリューム・グループに対して **lsvg** を発行します。

例えば次のとおりです。

```
lsvg -p tsmdb
```

出力は次のようになります。*FREE PPs* 列は、物理区画を表しています。

tsmdb:				
PV_NAME	PV STATE	TOTAL PPs	FREE PPs	FREE DISTRIBUTION
hdisk4	active	1631	1631	327..326..326..326..326
hdisk5	active	1631	1631	327..326..326..326..326
hdisk6	active	1631	1631	327..326..326..326..326

4. **mklv** コマンドを使用して、各ボリューム・グループに論理ボリュームを作成します。ボリューム・サイズ、ボリューム・グループ、および装置名は、システムのサイズやディスク構成におけるバリエーションに応じて異なります。

例えば、中規模システムに IBM Spectrum Protect データベース用のボリュームを作成するには、次のコマンドを発行します。

```
mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
```

5. **crfs** コマンドを使用して、各論理ボリューム内のファイル・システムをフォーマットします。

例えば、中規模システム上のデータベース用にファイル・システムをフォーマットするには、次のコマンドを発行します。

```
crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
```

```
crfs -v jfs2 -d tsbdb02 -p rw -a logname=INLINE -a options=rbrw  
-a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
```

6. 次のコマンドを発行して、新しく作成されたすべてのファイル・システムをマウントします。

```
mount -a
```

7. **df** コマンドを発行して、すべてのファイル・システムをリストします。

ファイル・システムが正しい LUN で正しいマウント・ポイントにマウントされていることを確認します。また、使用可能なスペースを確認してください。

以下のコマンド出力例は、使用スペースの量が通常は 1% であることを示しています。

```
tapsrv07> df -g /tsminst1/*  
Filesystem      GB blocks   Free   %Used   Iused   %Iused   Mounted on  
/dev/tsmact00    195.12    194.59    1%      4        1%      /tsminst1/TSMalog
```

8. 41 ページの『サーバーのユーザー ID の作成』で作成したユーザー ID に、サーバーのディレクトリーに対する読み取り/書き込み権限があることを確認します。

## Linux システム

IBM Spectrum Protect サーバーで使用する各ディスク LUN で、ext4 ファイル・システムまたは xfs ファイル・システムをフォーマットする必要があります。

### 手順

1. 前に生成した装置 ID のリストを使用して **mkfs** コマンドを発行し、各ストレージ LUN 装置のファイル・システムを作成してフォーマットします。コマンドで装置 ID を指定します。以下の例を参照してください。  
データベースの場合、ext4 ファイル・システムをフォーマットします。

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
```

ストレージ・プール LUN の場合、xfs ファイル・システムをフォーマットします。

```
mkfs -t xfs /dev/mapper/36005076300810105780000000000002c3
```

異なる装置をいくつ使用しているかに応じて、**mkfs** コマンドを 50 回まで発行できます。

2. ファイル・システム用のマウント・ポイント・ディレクトリーを作成します。

作成する必要があるディレクトリーごとに **mkdir** コマンドを発行します。計画ワークシートに記録したディレクトリー値を使用します。

例えば、デフォルト値を使用してサーバー・インスタンス・ディレクトリーを作成するには、次のコマンドを発行します。

```
mkdir /tsminst1
```

各ファイル・システムに対して **mkdir** コマンドを繰り返します。

3. サーバーの始動時にファイル・システムが自動的にマウントされるように、各ファイル・システム用の項目を **/etc/fstab** ファイルに追加します。

例えば次のとおりです。

```
/dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4  
defaults 0 0
```

4. **mount -a** コマンドを発行して、**/etc/fstab** ファイルに追加したファイル・システムをマウントします。  
5. **df** コマンドを発行して、すべてのファイル・システムをリストします。

ファイル・システムが正しい LUN で正しいマウント・ポイントにマウントされていることを確認します。また、使用可能なスペースを確認してください。

以下の IBM Storwize システムでの例は、使用スペースの量が通常は 1% であることを示しています。

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem                                Size  Used Avail Use% Mounted on
/dev/mapper/36005076300810105780000000000003 134G  188M 132G   1%  /tsminst1/
TSMalog
```

6. 41 ページの『サーバーのユーザー ID の作成』で作成したユーザー ID に、IBM Spectrum Protect サーバーのディレクトリーに対する読み取り/書き込み権限があることを確認します。

## Windows システム

IBM Spectrum Protect サーバーが使用する各ディスク LUN で、New Technology File System (NTFS) ファイル・システムをフォーマットする必要があります。

### 手順

1. ファイル・システム用のマウント・ポイント・ディレクトリーを作成します。

作成する必要があるディレクトリーごとに **md** コマンドを発行します。計画ワークシートに記録したディレクトリー値を使用します。例えば、デフォルト値を使用してサーバー・インスタンス・ディレクトリーを作成するには、次のコマンドを発行します。

```
md c:¥tsminst1
```

各ファイル・システムに対して **md** コマンドを繰り返します。

2. Windows ボリューム マネージャを使用して、サーバー・インスタンス・ディレクトリー下のディレクトリーにマップされる各ディスク LUN 用のボリュームを作成します。

「サーバー マネージャ」 > 「ファイルおよび記憶域サービス」に進み、前のステップで作成された LUN マッピングに対応する各ディスクに対して以下の手順を実行します。

- a) ディスクをオンラインにします。
- b) ディスクを GPT 基本タイプ (デフォルト) に初期化します。
- c) ディスク上のすべてのスペースを占有する単純なボリュームを作成します。NTFS を使用してファイル・システムをフォーマットし、TSMfile00 など、ボリュームの目的に合致するラベルを割り当てます。新規ボリュームをドライブ名に割り当てないでください。代わりに、C:¥tsminst1¥TSMfile00 など、インスタンス・ディレクトリー下のディレクトリーにボリュームをマップします。

**ヒント:** 報告されたディスクのサイズに基づいて、ボリューム・ラベルおよびディレクトリー・マッピング・ラベルを決定します。

3. ファイル・システムが正しい LUN で正しいマウント・ポイントにマウントされていることを確認します。**mountvol** コマンドを発行してすべてのファイル・システムをリストし、出力を確認します。例えば次のとおりです。

```
¥¥?¥Volume{8ffb9678-3216-474c-a021-20e420816a92}¥
C:¥tsminst1¥TSMdbspace00¥
```

4. ディスク構成が完了したら、システムを再始動してください。

### 次のタスク

Windows Explorer を使用して、各ボリュームのフリー・スペースの容量を確認することができます。

# サーバーおよび Operations Center のインストール

IBM Installation Manager グラフィカル・ウィザードを使用して、コンポーネントをインストールします。

## AIX および Linux システムへのインストール

IBM Spectrum Protect サーバーと Operations Center を同じサーバーにインストールします。

### 始める前に

オペレーティング・システムが、必要な言語に設定されていることを確認します。デフォルトで、オペレーティング・システムの言語はインストール・ウィザードの言語です。

### 手順

#### 1. AIX

必要な RPM ファイルがシステムにインストールされていることを確認します。

詳細については、[46 ページの『グラフィカル・ウィザード用の前提条件 RPM ファイルのインストール』](#)を参照してください。

2. インストール・パッケージをダウンロードする前に、製品パッケージからインストール・ファイルを抽出したときにそれらのファイルを保管するの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は、[ダウンロード資料 \(技術情報 588093\)](#) を参照してください。

3. [Passport Advantage®](#) にアクセスし、任意の空のディレクトリーにパッケージ・ファイルをダウンロードします。

4. パッケージに対する実行権限が設定されていることを確認します。必要な場合は、次のコマンドを実行してファイル権限を変更します。

```
chmod a+x package_name.bin
```

5. 次のコマンドを発行して、パッケージを抽出します。

```
./package_name.bin
```

ここで、*package\_name* はダウンロードしたファイルの名前です。

#### 6. AIX

ウィザードが正しく機能するように、以下のコマンドが使用可能であることを確実にします。

```
lsuser
```

デフォルトで、このコマンドは使用可能です。

7. 実行可能ファイルを置いたディレクトリーに変更します。
8. 次のコマンドを発行して、インストール・ウィザードを開始します。

```
./install.sh
```

インストールするパッケージを選択するときには、サーバーと Operations Center の両方を選択します。

### 次のタスク

- インストール処理中にエラーが発生した場合、これらのエラーは、IBM Installation Manager のログ・ディレクトリーに格納されるログ・ファイルに記録されます。

Installation Manager ツールからインストール・ログ・ファイルを表示するには、「ファイル」 > 「ログの表示」をクリックします。Installation Manager ツールからこれらのログ・ファイルを収集するには、「ヘルプ」 > 「問題分析のためのデータのエクスポート」をクリックします。



- サーバーをインストールした後、使用目的に合わせてカスタマイズする前に、[サポート・サイト](#) にアクセスしてください。「**Support and downloads**」をクリックし、適用できる修正があれば適用します。

## AIX グラフィカル・ウィザード用の前提条件 RPM ファイルのインストール

RPM ファイルは、IBM Installation Manager グラフィカル・ウィザードに必要です。

### 手順

1. 以下のファイルがシステムにインストールされていることを確認します。ファイルがインストールされていない場合は、ステップ 2 に進みます。

```
atk-1.12.3-2.aix5.2.ppc.rpm      libpng-1.2.32-2.aix5.2.ppc.rpm
cairo-1.8.8-1.aix5.2.ppc.rpm     libtiff-3.8.2-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm     pango-1.14.5-4.aix5.2.ppc.rpm
fontconfig-2.4.2-1.aix5.2.ppc.rpm  pixman-0.12.0-3.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm  xcursor-1.1.7-3.aix5.2.ppc.rpm
gettext-0.10.40-6.aix5.1.ppc.rpm  xft-2.1.6-5.aix5.1.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm     xrender-0.9.1-3.aix5.2.ppc.rpm
gtk2-2.10.6-4.aix5.2.ppc.rpm      zlib-1.2.3-3.aix5.1.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
```

2. /opt ファイル・システムに少なくとも 150MB のフリー・スペースを確保します。
3. インストール・パッケージを解凍したディレクトリーで、gtk ディレクトリーに移動します。
4. 次のコマンドを発行して、[IBM AIX Toolbox for Linux Applications Web サイト](#) から現行作業ディレクトリーに RPM ファイルをダウンロードします。

```
download-prerequisites.sh
```

5. ダウンロードした RPM ファイルが入っているディレクトリーから、次のコマンドを発行してファイルをインストールします。

```
rpm -Uvh *.rpm
```

## Windows システムへのインストール

IBM Spectrum Protect サーバーと Operations Center を同じサーバーにインストールします。

### 始める前に

以下の前提条件が満たされていることを確認します。

- オペレーティング・システムが、必要な言語に設定されていることを確認します。デフォルトで、オペレーティング・システムの言語はインストール・ウィザードの言語です。
- インストール時に使用するユーザー ID がローカル管理者権限を持つユーザーであることを確認します。

### 手順

1. インストール・パッケージをダウンロードする前に、製品パッケージからインストール・ファイルを抽出したときにそれらのファイルを保管するの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は、[ダウンロード資料 \(技術情報 588095\)](#) を参照してください。
2. [パスポート・アドバンテージ](#) にアクセスし、任意の空のディレクトリーにパッケージ・ファイルをダウンロードします。
3. 実行可能ファイルを置いたディレクトリーに変更します。
4. 実行可能ファイルをダブルクリックして、現行ディレクトリーに抽出します。
5. インストール・ファイルが抽出されたディレクトリーで、install.bat ファイルをダブルクリックして、インストール・ウィザードを開始します。  
インストールするパッケージを選択するときには、サーバーと Operations Center の両方を選択します。



## 次のタスク

- インストール処理中にエラーが発生した場合、これらのエラーは、IBM Installation Manager のログ・ディレクトリに格納されるログ・ファイルに記録されます。

Installation Manager ツールからインストール・ログ・ファイルを表示するには、「**ファイル**」>「**ログの表示**」をクリックします。Installation Manager ツールからこれらのログ・ファイルを収集するには、「**ヘルプ**」>「**問題分析のためのデータのエクスポート**」をクリックします。

- サーバーをインストールした後、使用目的に合わせてカスタマイズする前に、[サポート・サイト](#) にアクセスしてください。「**Support and downloads**」をクリックし、適用できる修正があれば適用します。

## サーバーおよび Operations Center の構成

コンポーネントをインストールした後、IBM Spectrum Protect サーバーおよび Operations Center の構成を実行します。

### サーバー・インスタンスの構成

IBM Spectrum Protect サーバーのインスタンス構成ウィザードを使用して、サーバーの初期構成を完了します。

#### 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。

Linux | AIX

- IBM Spectrum Protect をインストールしたシステムに、X Window System クライアントをインストールしておく必要があります。また、デスクトップで X Window System サーバーを実行している必要もあります。
- システムでセキュア・シェル (SSH) プロトコルが有効にされている必要があります。ポートがデフォルト値の 22 に設定されていること、およびポートがファイアウォールによってブロックされていないことを確認してください。/etc/ssh/ ディレクトリ内の sshd\_config ファイルでパスワード認証を有効にする必要があります。また、localhost 値を使用してシステムに接続するためのアクセス権限が SSH デモン・サービスにあることを確認します。
- SSH プロトコルを使用して、サーバー・インスタンス用に作成したユーザー ID で IBM Spectrum Protect にログインできる必要があります。ウィザードを使用する場合、システムにアクセスするためにこのユーザー ID およびパスワードを指定する必要があります。
- 上記ステップでいずれかの設定を変更した場合は、構成ウィザードを先に進める前にサーバーを再始動してください。

Windows

以下のステップを実行して、リモート・レジストリー・サービスが開始されていることを確認します。

1. 「**スタート**」>「**管理ツール**」>「**サービス**」をクリックします。「**サービス**」ウィンドウで、「**Remote Registry**」を選択します。開始されていない場合は、「**開始**」をクリックします。
2. 次のようにして、ポート 137、139、および 445 がファイアウォールによってブロックされていないことを確認します。
  - a. 「**スタート**」>「**コントロールパネル**」>「**Windows ファイアウォール**」をクリックします。
  - b. 「**詳細設定**」を選択します。
  - c. 「**受信の規則**」を選択します。
  - d. 「**新しい規則**」を選択します。
  - e. TCP ポート 137、139、および 445 のポート規則を作成して、ドメインおよびプライベート・ネットワークで接続できるようにします。

3. 「ローカル セキュリティ ポリシー」 オプションにアクセスして以下のステップを実行し、ユーザー・アカウント制御を構成します。
  - a. 「スタート」 > 「管理ツール」 > 「ローカル セキュリティ ポリシー」をクリックします。「ローカル ポリシー」 > 「セキュリティのオプション」を展開します。
  - b. まだ有効になっていない場合は、「アカウント: Administrator アカウントの状態」 > 「有効」 > 「OK」を選択して、組み込みの管理者アカウントを有効にします。
  - c. まだ無効になっていない場合は、「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」 > 「無効」 > 「OK」を選択して、すべての Windows 管理者に対してユーザー・アカウント制御を無効にします。
  - d. まだ無効になっていない場合は、「ユーザー・アカウント制御: 組み込みの Administrator アカウントに対する管理者承認モード」 > 「無効」 > 「OK」を選択して、組み込み Administrator アカウントに対してユーザー・アカウント制御を無効にします。
4. 上記ステップでいずれかの設定を変更した場合は、構成ウィザードを先に進める前にサーバーを再起動してください。

## このタスクについて

ウィザードは停止と再起動ができますが、サーバーは構成プロセス全体が完了するまでは操作可能になりません。

## 手順

1. ウィザードのローカル・バージョンを開始します。
  - **Linux** | **AIX** /opt/tivoli/tsm/server/bin ディレクトリーで dsmicfgx プログラムを開きます。このウィザードは、root ユーザーとしてのみ実行できます。
  - **Windows** 「スタート」 > 「すべてのプログラム」 > 「IBM Spectrum Protect」 > 「構成ウィザード」とクリックします。
2. 指示に従って構成を完了します。

IBM Spectrum Protect システムのセットアップ時に [8 ページの『計画ワークシート』](#)で記録した情報を使用して、ウィザードでディレクトリーおよびオプションを指定します。

**Linux** | **AIX** 「サーバー情報」ウィンドウで、システムのブート時にインスタンス・ユーザー ID を使用して自動的に始動するように、サーバーを設定します。

**Windows** 構成ウィザードを使用することで、サーバーがリブート時に自動的に開始するように設定されます。

## バックアップ/アーカイブ・クライアントのインストール

ベスト・プラクティスとして、管理コマンド・ライン・クライアントおよびスケジューラーが使用可能になるように、サーバー・システムに IBM Spectrum Protect バックアップ/アーカイブ・クライアントをインストールしてください。

## 手順

- バックアップ/アーカイブ・クライアントをインストールするには、ご使用のオペレーティング・システム用のインストール手順に従います。
  - [UNIX および Linux バックアップ/アーカイブ・クライアントのインストール](#)
  - [Windows クライアントの初回インストール](#)

## サーバーのオプションの設定

IBM Spectrum Protect サーバーと一緒にインストールされたサーバー・オプション・ファイルを参照し、ご使用のシステムに適切な値が設定されていることを確認します。

### 手順

1. サーバー・インスタンス・ディレクトリーに移動して、`dsmserv.opt` ファイルを開きます。
2. 以下の表の値を参照して、システム・サイズに基づいてご使用のサーバー・オプション設定を確認します。

サーバー・オプション	値
<b>ACTIVELOGDIRECTORY</b>	構成中に指定されたディレクトリー・パス
<b>ACTIVELOGSIZE</b>	131072
<b>ARCHLOGCOMPRESS</b>	No
<b>ARCHLOGDIRECTORY</b>	構成中に指定されたディレクトリー・パス
<b>COMMMETHOD</b>	TCPIP
<b>COMMTIMEOUT</b>	3600
<b>DEVCONFIG</b>	devconf.dat
<b>EXPINTERVAL</b>	0
<b>IDLETIMEOUT</b>	60
<b>MAXSESSIONS</b>	500
<b>NUMOPENVOLSALLOWED</b>	20
<b>TCPADMINPORT</b>	1500
<b>TCPPORT</b>	1500
<b>VOLUMEHISTORY</b>	volhist.dat

必要に応じてサーバー・オプションの設定値を更新して、表の値と一致するようにしてください。更新するには、`dsmserv.opt` ファイルを閉じ、管理コマンド・ライン・インターフェースから **SETOPT** コマンドを使用して、オプションを設定します。

例えば、`IDLETIMEOUT` オプションを 60 に更新するには、以下のコマンドを発行します。

```
setopt idletimeout 60
```

3. サーバー、クライアント、および Operations Center のセキュア通信を構成するには、以下の表のオプションを確認してください。

サーバー・オプション	すべてのシステム・サイズ
<b>SSLDISABLELEGACYTLS</b>	YES
<b>SSLFIPSMODE</b>	NO
<b>SSLTCPPORT</b>	SSL ポート番号を指定します。サーバーの TCP/IP 通信ドライバーは、クライアントからの SSL 対応セッションに対する要求をこのポートで待ちます。

サーバー・オプション	すべてのシステム・サイズ
<b>SSLTCPADMINPORT</b>	サーバーがコマンド・ライン管理クライアントからの SSL 対応セッションの要求を待機するポート・アドレスを指定します。
<b>TLS12</b>	YES

オプション値のいずれかを更新する必要がある場合は、以下のガイドラインを使用して、`dsmserve.opt` ファイルを編集します。

- ・オプションを有効にする場合は、その行の先頭にあるアスタリスクを削除します。
- ・各行には、1つのオプションとそのオプションに対して指定された値のみを入力してください。
- ・ファイル内の複数の項目にオプションが出現する場合、サーバーは最後の項目を使用します。

変更を保存してファイルを閉じます。`dsmserve.opt` ファイルを直接編集した場合、変更を有効にするには、サーバーを再始動する必要があります。

## セキュリティの概念

通信プロトコルを使用して、パスワードを保護し、管理者にそれぞれ異なるアクセス・レベルを提供することにより、IBM Spectrum Protect をセキュリティ・リスクから保護できます。

### トランスポート層セキュリティ

Secure Sockets Layer (SSL) またはトランスポート層セキュリティ (TLS) プロトコルを使用すると、トランスポート層セキュリティを提供して、サーバー、クライアント、およびストレージ・エージェント間にセキュア接続を確立できます。サーバー、クライアント、ストレージ・エージェント間でデータを送信する場合は、SSL または TLS を使用してデータを暗号化してください。

**ヒント:** 「SSL」または「SSL の選択」を示す IBM Spectrum Protect 資料はすべて、TLS にも適用されます。

SSL は、サーバー、クライアント、ストレージ・エージェントが使用する IBM Spectrum Protect サーバーとともにインストールされる Global Security Kit (GSKit) によって提供されます。

**制約事項:** IBM Spectrum Protect サーバーで使用する IBM Db2 データベース・インスタンスとの通信に、SSL プロトコルおよび TLS プロトコルを使用しないでください。

SSL を使用可能にする各サーバー、クライアント、またはストレージ・エージェントは、信頼された自己署名証明書を使用するか、認証局 (CA) が署名する固有の証明書を取得する必要があります。独自の証明書を使用するか、CA から証明書を購入することができます。どちらかの証明書をインストールして、IBM Spectrum Protect サーバー、クライアント、またはストレージ・エージェントの鍵データベースに追加する必要があります。証明書は、SSL 通信の要求や開始を行う SSL クライアントやサーバーによって検証されます。一部の CA 証明書は、デフォルトで鍵データベースにプリインストールされています。

SSL は、IBM Spectrum Protect サーバー、クライアント、およびストレージ・エージェントのそれぞれで個別にセットアップされます。

### 権限レベル

各 IBM Spectrum Protect サーバーでは、管理者が実行できるタスクを決定する、それぞれ異なる管理権限レベルを使用できます。

登録後、管理者に 1 つ以上の管理権限レベルを割り当てることによって、権限を付与する必要があります。システム権限を持つ管理者は、サーバーに対してすべてのタスクを実行でき、**GRANT AUTHORITY** コマンドを使用して他の管理者に権限レベルを割り当てることができます。ポリシー権限、ストレージ権限、またはオペレーター権限を持つ管理者は、タスクのサブセットを実行できます。

管理者は、他の管理者 ID の登録、それらへの権限レベルの付与、ID の名前変更、ID の除去、およびサーバーからの ID のロックおよびアンロックを実行できます。

管理者は、root ユーザー ID および非 root ユーザー ID について特定のクライアント・ノードへのアクセスを制御できます。デフォルトでは、非 root ユーザー ID はノード上のデータをバックアップできません。バックアップできるようにノードの設定を変更するには、**UPDATE NODE** コマンドを使用します。

## パスワード

デフォルトで、サーバーはパスワード認証を自動的に使用します。パスワード認証が使用される場合、すべてのユーザーはサーバーにアクセスするときにパスワードを入力する必要があります。

Lightweight Directory Access Protocol (LDAP) を使用して、パスワードの厳格な要件を適用します。詳細については、[パスワードおよびログオン手順の管理 \(V7.1.1\)](#)を参照してください。

表 14. パスワード認証の特性	
特性	詳細情報
大/小文字の区別	大/小文字の区別はありません。
デフォルトのパスワードの有効期限	90 日。 この有効期限間は、管理者 ID またはクライアント・ノードを初めてサーバーに登録した時に開始されます。この期間内にパスワードが変更されていない場合、次にユーザーがサーバーにアクセスするときにパスワードを変更する必要があります。
無効なパスワードの試行回数	すべてのクライアント・ノードに対して、無効パスワードの連続試行回数の制限を設定することができます。この制限を超えると、サーバーはノードをロックします。
デフォルトのパスワード長	8 文字。 管理者は最小長を指定することができます。バージョン 8.1.4 以降、サーバー・パスワードのデフォルトの最小長は 0 から 8 文字に変更されました。

## セッション・セキュリティ

セッション・セキュリティは、IBM Spectrum Protect クライアント・ノード、管理クライアント、およびサーバーの間の通信に使用されるセキュリティのレベルで、**SESSIONSECURITY** パラメーターを使用して設定されます。

**SESSIONSECURITY** パラメーターは、以下のいずれかの値に設定することができます。

- **STRICT** 値は、IBM Spectrum Protect サーバー、ノード、および管理者の間の通信に最大レベルのセキュリティを実施します。
- **TRANSITIONAL** 値は、IBM Spectrum Protect ソフトウェアを V8.1.2 以降に更新する間に、既存の通信プロトコルが使用されることを指定します。これはデフォルトです。  
**SESSIONSECURITY=TRANSITIONAL** を指定した場合、より上位のバージョンの TLS プロトコルが使用されたり、ソフトウェアが V8.1.2 以降に更新されたりすると、より厳しいセキュリティ設定が自動的に実施されます。ノード、管理者、あるいはサーバーが **STRICT** 値の要件を満たすと、セッション・セキュリティは自動的に **STRICT** 値に更新され、エンティティは、旧バージョンのクライアントあるいは以前の TLS プロトコルを使用して認証できなくなります。

**注：**サーバーをアップグレードする前に、バックアップ/アーカイブ・クライアントを V8.1.2 以降に更新する必要はありません。サーバーを V8.1.2 以降にアップグレードした場合でも、ソフトウェアの旧バージョンを使用しているノードと管理者は、エンティティが **STRICT** 値の要件を満たすまで、**TRANSITIONAL** 値を使用して引き続きサーバーと通信します。同様に、IBM Spectrum Protect サーバーをアップグレードする前に、バックアップ/アーカイブ・クライアントを V8.1.2 以降にアップグレードで



きますが、サーバーを最初にアップグレードする必要はありません。サーバーとクライアント間の通信は中断されません。

**SESSIONSECURITY** パラメーター値について詳しくは、以下のコマンドを参照してください。

表 15. SESSIONSECURITY パラメーターの設定に使用されるコマンド	
エンティティ	コマンド
クライアント・ノード	<ul style="list-style-type: none"><li>• REGISTER NODE</li><li>• UPDATE NODE</li></ul>
管理者	<ul style="list-style-type: none"><li>• REGISTER ADMIN</li><li>• UPDATE ADMIN</li></ul>
サーバー	<ul style="list-style-type: none"><li>• DEFINE SERVER</li><li>• UPDATE SERVER</li></ul>

**DSMADMC** コマンド、**DSMC** コマンド、あるいは dsm プログラムを使用して認証する管理者は、V8.1.2 以降を使用して認証を行った後、旧バージョンを使用して認証することができません。管理者の認証の問題を解決するには、以下のヒントを参照してください。

#### ヒント：

- 管理者アカウントがログオンに使用するすべての IBM Spectrum Protect ソフトウェアが V8.1.2 以降にアップグレードされていることを確認します。管理者アカウントが複数のシステムからログオンする場合は、各システム上にサーバーの証明書がインストールされている必要があります。
- 管理者が V8.1.2 以降のソフトウェアまたは V7.1.8 以降のソフトウェアを使用して正常に認証を行った後は、その管理者は V8.1.2 または V7.1.8 より前のバージョンのクライアントやサーバーを使用してサーバーで認証を行えなくなります。管理者コマンドは、どのシステムからでも発行することができます。
- 必要な場合は、V8.1.1 以前のソフトウェアを使用するクライアントおよびサーバーでのみ使用するために、別の管理者アカウントを作成してください。

すべてのノード、管理者、およびサーバーが **STRICT** セッション・セキュリティを使用するようにすることで、IBM Spectrum Protect サーバーとの通信で最高レベルのセキュリティを実施します。**SELECT** コマンドを使用して、どのサーバー、ノード、および管理者が **TRANSITIONAL** セッション・セキュリティを使用しており、**STRICT** セッション・セキュリティを使用するように更新する必要があるかを判別することができます。

#### 関連情報

[通信の保護](#)

## トランスポート層セキュリティを使用したセキュア通信の構成

ご使用の環境のデータを暗号化し、通信を保護するには、Secure Sockets Layer (SSL) または Transport Layer Security (TLS) を IBM Spectrum Protect サーバーおよびバックアップ/アーカイブ・クライアントで有効にします。SSL 証明書は、サーバーとクライアントの間の通信要求を検証するために使用されます。

### このタスクについて

次の図に示すように、サーバーおよびクライアントのオプション・ファイルでオプションを設定し、サーバー上で生成された自己署名証明書をクライアントに転送することで、サーバーとバックアップ/アーカイブ・クライアントの間の安全な通信を手動で構成することができます。あるいは、認証局 (CA) によって署名された固有の証明書を入手して転送することもできます。



SSL または TLS 通信のサーバーおよびクライアントの構成について詳しくは、[SSL を使用してサーバーに接続するためのストレージ・エージェント、サーバー、クライアント、および Operations Center の構成](#)を参照してください。

## Operations Center の構成

Operations Center をインストールした後、以下の構成ステップを実行して、ストレージ環境の管理を開始します。

### 始める前に

初めて Operations Center に接続する場合は、以下の情報を提供する必要があります。

- ハブ・サーバーとして指定するサーバーの接続情報
- そのサーバーに定義される管理者 ID のログイン資格情報

### 手順

1. Secure Sockets Layer (SSL) プロトコルを構成して、Operations Center とハブ・サーバーの間のセキュア通信をセットアップします。

54 ページの『[Operations Center とハブ・サーバーの間の通信の保護](#)』の指示に従ってください。

2. ハブ・サーバーを指定する。

Web ブラウザーで、以下のアドレスを入力します。

```
https://hostname:secure_port/oc
```

ここで、

- *hostname* は、Operations Center がインストールされているコンピューターの名前を表します。
- *secure\_port* は、そのコンピューター上で Operations Center が HTTPS 通信に使用するポート番号を表します。

例えば、ホスト名が `tsm.storage.mylocation.com` で、Operations Center でデフォルトのセキュア・ポート (11090) を使用している場合、アドレスは次のとおりです。

```
https://tsm.storage.mylocation.com:11090/oc
```

初めて Operations Center にログインすると、ウィザードにより、サーバーでシステム権限を持つ新しい管理者をセットアップするための初期構成手順が示されます。

3. オプション: システム状況を要約する日次 E メール・レポートを受け取るには、Operations Center で E メール設定を構成します。

157 ページの『[E メール・レポートを使用したシステム状況のトラッキング](#)』の指示に従ってください。



## Operations Center とハブ・サーバーの間の通信の保護

Operations Center とハブ・サーバー間の通信を保護するために、ハブ・サーバーの Transport Layer Security (TLS) 証明書を Operations Center のトラストストア・ファイルに追加します。

### 始める前に

Operations Center のトラストストア・ファイルは、Operations Center がアクセスできる証明書用のコンテナです。Operations Center のインストール時に、トラストストア・ファイルのパスワードを作成する必要があります。Operations Center とハブ・サーバーの間の通信を保護するには、同じパスワードを使用して、ハブ・サーバーの証明書をトラストストア・ファイルに追加する必要があります。このパスワードを覚えていない場合は、この時点でトラストストア・ファイルを再作成して構成する必要があります。手順については、[Operations Center のトラストストア・ファイルのパスワードの削除と再割り当て](#)を参照してください。

次の図は、ハブ・サーバーと Operations Center の間に Secure Sockets Layer (SSL) 接続をセットアップするためのコンポーネントを示しています。



### このタスクについて

この手順では、自己署名証明書を使用してセキュア通信を実装します。

認証局 (CA) によって署名された証明書を使用する場合は、[CA 署名証明書を使用した Operations Center とハブ・サーバー間の通信の保護](#)の説明に従ってください。

### 手順

自己署名証明書を使用して SSL 通信をセットアップするには、以下の手順を実行します。

1. Operations Center Web サーバーを停止します。
2. Operations Center がインストールされているシステムで、オペレーティング・システムのコマンド・ラインを開き、以下のディレクトリーに移動します。

- **Linux** | **AIX** `installation_dir/ui/jre/bin`
- **Windows** `installation_dir¥ui¥jre¥bin`

ここで、`installation_dir` は、Operations Center がインストールされているディレクトリーを表します。

3. 次のコマンドを発行して、「IBM 鍵管理」ウィンドウを開きます。

```
ikeyman
```

4. 「鍵データベース・ファイル」 > 「オープン」をクリックします。
5. 「参照」をクリックして、以下のディレクトリーに移動します。ここで、`installation_dir` は、Operations Center がインストールされているディレクトリーを表します。
  - **Linux** | **AIX** `installation_dir/ui/Liberty/usr/servers/guiServer`
  - **Windows** `installation_dir¥ui¥Liberty¥usr¥servers¥guiServer`
6. `guiServer` ディレクトリーで、`gui-truststore.jks` ファイルを選択します。
7. 「オープン」をクリックして、「OK」をクリックします。
8. トラストストア・ファイルのパスワードを入力して、「OK」をクリックします。

9. 「IBM 鍵管理」ウィンドウの「**鍵データベースの内容 (Key database content)**」域で、矢印をクリックして、リストから「署名者証明書」を選択します。「追加」をクリックします。
10. 「オープン」ウィンドウで、「参照」をクリックして、インスタンスを作成した管理者によって指定されたハブ・サーバー・インスタンス・ディレクトリーに移動します。例えば次のとおりです。

- **Linux** | **AIX** `home/tsminst1`
- **Windows** `c:\Program Files\Tivoli\TSM\server1`

ディレクトリーには `cert256.arm` 証明書が含まれています。

「オープン」ウィンドウからハブ・サーバー・インスタンス・ディレクトリーにアクセスできない場合は、以下の手順を実行します。

- a) FTP または別のファイル転送方式を使用して、`cert256.arm` ファイルを、ハブ・サーバーのインスタンス・ディレクトリーから、Operations Center がインストールされているコンピューターの以下のディレクトリーにコピーします。

- **Linux** | **AIX** `installation_dir/ui/Liberty/usr/servers/guiServer`
- **Windows** `installation_dir\ui\Liberty\usr\servers\guiServer`

- b) 「オープン」ウィンドウで、`guiServer` ディレクトリーに進みます。

11. SSL 証明書として `cert256.arm` 証明書を選択します。
12. 「オープン」をクリックして、「OK」をクリックします。
13. 証明書のラベルを入力します。例えば、ハブ・サーバーの名前を入力します。
14. 「OK」をクリックします。ハブ・サーバーの SSL 証明書がトラストストア・ファイルに追加され、そのラベルが「IBM 鍵管理」ウィンドウの「**鍵データベースの内容 (Key database content)**」域に表示されます。
15. 「IBM 鍵管理」ウィンドウを閉じます。
16. Operations Center Web サーバーを開始します。

初めて Operations Center に接続する場合、ハブ・サーバーの IP アドレスまたはネットワーク名、およびハブ・サーバーとの通信用のポート番号を指定するようプロンプトが出されます。ADMINONCLIENTPORT サーバー・オプションが IBM Spectrum Protect サーバーに対して有効な場合、TCPADMINPORT サーバー・オプションで指定されているポート番号を入力します。ADMINONCLIENTPORT サーバー・オプションが有効でない場合、TCPPORT サーバー・オプションで指定されているポート番号を入力します。

## 製品ライセンスの登録


IBM Spectrum Protect 製品のライセンスを登録するには、**REGISTER LICENSE** コマンドを使用します。

### このタスクについて

ライセンスは、登録証明書ファイルに保管されていて、これには製品のライセンス情報が入っています。登録証明書ファイルは、インストール・メディアに含まれており、インストール中にサーバー上に配置されます。製品を登録すると、ライセンスは現行ディレクトリー内の NODELOCK ファイルに保管されます。

### 手順

ライセンスが入っている登録証明書ファイルの名前を指定して、ライセンスを登録します。このタスクで Operations Center コマンド・ビルダーを使用するには、以下のステップを実行します。

1. Operations Center を開きます。
2. 設定アイコン  上にカーソルを移動して「コマンド・ビルダー」をクリックし、Operations Center コマンド・ビルダーを開きます。
3. **REGISTER LICENSE** コマンドを発行します。

例えば、IBM Spectrum Protect の基本ライセンスを登録するには、次のコマンドを発行します。

```
register license file=tsmbasic.lic
```

## 次のタスク

登録証明書ファイルが収められたインストール・メディアを保存してください。例えば、以下のいずれかの状態が発生した場合など、ライセンスを再登録する必要がある場合があります。

- サーバーの別のコンピューターへの移動。
- NODELOCK ファイルの破壊。サーバーはライセンス情報を、サーバーを始動するディレクトリー内にある NODELOCK ファイルに保管します。
- **Linux** サーバーがインストールされているサーバーに関連付けられているプロセッサ・チップを変更する場合。

## ビジネスに合わせたデータ保存ルールの定義

データ重複排除用のディレクトリー・コンテナー・ストレージ・プールを作成した後、新規ストレージ・プールを使用するためにデフォルトのサーバー・ポリシーを更新します。このタスクを実行するために、「ストレージ・プールの追加 (Add Storage Pool)」ウィザードが Operations Center で「サービス」ページを開きます。

### 手順

1. Operations Center の「サービス」ページで、STANDARD ドメインを選択して「詳細」をクリックします。
2. ポリシー・ドメインの「要約」ページで、「ポリシー・セット」タブをクリックします。  
「ポリシー・セット」ページには、アクティブ・ポリシー・セットの名前が示され、そのポリシー・セットのすべての管理クラスがリストされます。
3. 「構成」トグルをクリックし、以下の変更を行います。
  - STANDARD 管理クラスのバックアップ宛先をディレクトリー・コンテナー・ストレージ・プールに変更します。
  - 「バックアップ」列の値を「無制限」に変更します。
  - 保存期間を変更します。ビジネス要件に応じて、「追加バックアップの保持」列を 30 日以上に設定します。
4. 変更を保存し、ポリシー・セットが編集不可になるように、再度「構成」トグルをクリックします。
5. 「活動化」をクリックしてポリシー・セットを活動化します。

## サーバー保守アクティビティのスケジュールの定義

Operations Center コマンド・ビルダーで **DEFINE SCHEDULE** コマンドを使用して、各サーバー保守操作のスケジュールを作成します。

### このタスクについて

サーバー保守操作をクライアント・バックアップ操作の後に実行するようにスケジュールします。各操作の開始時刻と期間を組み合わせることで、スケジュールのタイミングを制御することができます。

次の図は、保守操作をどのように計画するかの例を示しています。

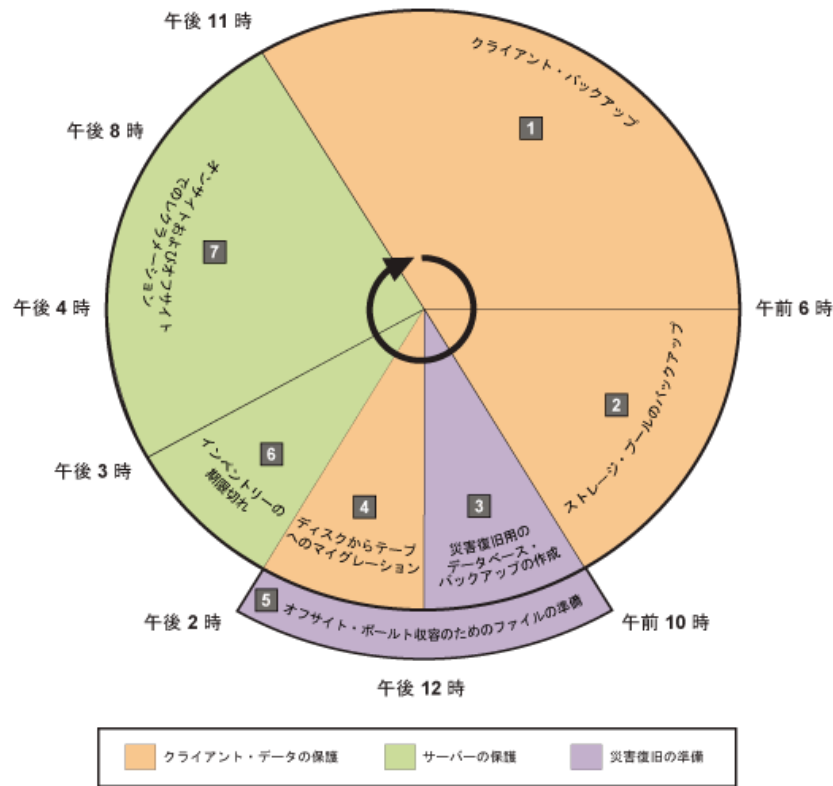


図 4. テープ・ソリューションに関するサーバー操作の日次スケジュール

以下の表は、テープ・ソリューションでクライアント・バックアップ・スケジュールと組み合わせてサーバー保守プロセスをどのようにスケジュールできるかを示しています。

操作	スケジュール
クライアント・バックアップ	午後 11 時に開始されます。
ストレージ・プールのバックアップ	午前 6 時に開始されます。
データベースおよび災害復旧ファイルの処理	<ul style="list-style-type: none"> <li>データベース・バックアップ操作は、午前 10 時またはクライアント・バックアップ操作が開始されてから 11 時間後に開始されます。このプロセスは、完了するまで実行されます。</li> <li>装置構成情報およびボリューム・ヒストリーのバックアップ操作は、午後 5 時またはデータベース・バックアップ操作が開始されてから 7 時間後に開始されます。</li> <li>ボリューム・ヒストリーの削除は、午後 8 時またはデータベース・バックアップ操作が開始されてから 10 時間後に開始されます。</li> </ul>
オフサイト・ボールドのファイルの準備	午前 10 時に、データベースおよび災害復旧ファイルの処理と同時に開始されます。
ディスクからテープへのマイグレーション	午後 12 時またはデータベース・バックアップ操作が開始されてから 2 時間後に開始されます。

操作	スケジュール
インベントリーの有効期限	午後 2 時またはクライアント・バックアップ操作が開始されてから 15 時間後に開始されます。このプロセスは、完了するまで実行されます。
スペース・レクラメーション	午後 3 時またはクライアント・バックアップ操作が開始されてから 16 時間後に開始されます。

## 手順

データベース・バックアップ用に装置クラスを構成した後、**DEFINE SCHEDULE** コマンドを使用して、データベース・バックアップおよびその他の必要な保守操作のスケジュールを作成します。ご使用の環境のサイズに応じて、例に示された各スケジュールの開始時刻を調整する必要があります。

1. データベース・バックアップのスケジュールを作成する前に、バックアップ操作の装置クラスを定義してください。

次のように **DEFINE DEVCLASS** コマンドを使用して、LTOTAPE という名前の装置クラスを作成します。

```
define devclass ltotape devtype=lto library=ltolib
```

2. 自動データベース・バックアップ用の装置クラスを設定します。**SET DBRECOVERY** コマンドを使用して、上記のステップでデータベース・バックアップ用に作成した装置クラスを指定します。  
例えば、装置クラスが LTOTAPE である場合、次のコマンドを発行します。

```
set dbrecovery ltotape
```

3. **DEFINE SCHEDULE** コマンドを使用して、保守操作のスケジュールを作成します。以下の表で、必要な操作とコマンド例を参照してください。

操作	コマンドの例と追加情報
ストレージ・プールをバックアップします。	<p><b>BACKUP STGPOOL</b> コマンドを実行するスケジュールを作成します。</p> <p>例えば、次のコマンドを発行して、PRIMARY_POOL という名前の 1 次ストレージ・プールのバックアップ・スケジュールを作成します。プールは、コピー・ストレージ・プール COPYSTG にバックアップされます。</p> <pre>define schedule BACKUPSTGPOOL type=administrative cmd="backup stgpool primary_pool copystg" active=yes starttime=06:00 period=1</pre>
データベースのバックアップを取ります。	<p><b>BACKUP DB</b> コマンドを実行するスケジュールを作成します。</p> <p>例えば、次のコマンドを発行して、新規の装置クラスを使用するバックアップ・スケジュールを作成します。</p> <pre>define schedule DBBACKUP type=admin cmd="backup db devclass=ltotape type=full numstreams=3 wait=yes compress=yes" active=yes desc="Back up the database." startdate=today starttime=10:00:00 duration=45 durunits=minutes</pre>
ノードを複製します。	<p>オプションで、ノード複製を使用して、データを 2 次サーバーにバックアップすることでクライアント・データを保護します。手順については、<a href="#">別のサーバーへのクライアント・データの複製</a>を参照してください。マイグレーション操作を開始する前に、ノード複製が完了していることを確認してください。</p>

操作	コマンドの例と追加情報
<p>ディスクからテープにデータを毎日マイグレーションします。</p>	<p>ストレージ・プール・マイグレーションのスケジュールを作成します。</p> <p>例えば、ディスク・ストレージ・プールの名前が DISKPOOL で、次のストレージ・プールが TAPEPOOL である場合、次のコマンドを発行して、ストレージ・プール・マイグレーションをスケジュールすることができます。</p> <pre>define schedule stgpool_migration type=administrative cmd="migrate stgpool diskpool lomig=0" active=yes description="migrate disk storagepool to tapepool" startdate=today starttime=12:00 duration=2 durunits=hours period=1 perunits=days</pre> <p>スループットを最大化するために、以下のステップを実行して、ファイルのマイグレーションに使用する並列処理の数を指定することができます。</p> <p>a. 磁気テープ・ストレージ・プールの場合、コロケーションが有効にされていることを確認します。コロケーションが有効にされているかどうかを確認するには、<b>QUERY STGPOOL</b> コマンドを実行します。 COLLOCATE フィールドに値 GROUP、NODE、または FILESPACE が指定されていることを確認します。値 GROUP、NODE、または FILESPACE が指定されていない場合、<b>UPDATE STGPOOL</b> コマンドを使用して、システム構成に応じて COLLOCATE=GROUP、COLLOCATE=NODE、または COLLOCATE=FILESPACE を指定します。</p> <p>b. ディスク・ストレージ・プールの場合、<b>DEFINE STGPOOL</b> コマンドまたは <b>UPDATE STGPOOL</b> コマンドを使用して、<b>MIGPROCESS</b> パラメーターの値を指定します。例えば、12 個の磁気テープ・ドライブがある場合、MIGPROCESS=10 を指定します。この場合、最大 10 個の磁気テープ・ドライブがマイグレーション・プロセスに使用されます。2 つのドライブは他のタスク (リストア操作、データベース・バックアップ操作、クライアント・バックアップ操作など) 用に確保されます。</p>
<p>オフサイト・ボールド収容のためのファイルを準備します。</p>	<p>a. <a href="#">61 ページの『バックアップ・メディアの移動』</a>の手順に従って、テープ・ボリュームをオフサイトに移動します。</p> <p>b. ソース・サーバー上で <b>PREPARE</b> コマンドを発行して、災害時回復計画ファイルを作成します。</p> <pre>prepare</pre> <p>c. 災害復旧に必要なすべてのボリュームが復旧計画ファイルに含まれている必要があります。詳細については、<a href="#">215 ページの『DRM を使用した災害に対する準備と災害からのリカバリー』</a>を参照してください。</p>
<p>装置構成情報をバックアップします。</p>	<p>次のように、<b>BACKUP DEVCONFIG</b> コマンドを実行するスケジュールを作成します。</p> <pre>define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Backup the device configuration file." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>



操作	コマンドの例と追加情報
ボリューム・履歴をバックアップします。	<p>次のように、<b>BACKUP VOLHISTORY</b> コマンドを実行するスケジュールを作成します。</p> <pre>define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Back up the volume history." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>
不要になった古いバージョンのデータベース・バックアップを削除します。	<p>次のように、<b>DELETE VOLHISTORY</b> コマンドを実行するスケジュールを作成します。</p> <pre>define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Remove old database backups." startdate=today starttime=20:00:00 duration=45 durunits=minutes</pre>
許可された保存期間を超えたオブジェクトを削除します。	<p><b>EXPIRE INVENTORY</b> コマンドを実行するスケジュールを作成します。</p> <p>構成するシステム・サイズに基づいて、ご使用のシステムに対して指定したプロセッサ・コアの数と等しくなるように <b>RESOURCE</b> パラメーターを設定します。</p> <p>例えば、<b>EXPINVENTORY</b> という名前のスケジュールを作成するには、以下のコマンドを実行します。</p> <pre>define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=8 duration=120" active=yes desc="Remove expired objects." startdate=today starttime=14:00:00 duration=1 durunits=hours</pre>
スペースをレクラメーション処理します。	<p><b>RECLAIM STGPOOL</b> コマンドを実行するスケジュールを作成します。</p> <p>例えば、<b>RECLAIM</b> という名前のスケジュールを作成するには、以下のコマンドを実行します。</p> <pre>define schedule RECLAIM type=admin cmd="reclaim stgpool tapepool duration=60" startdate=today starttime=15:00:00 duration=5 durunits=hours</pre> <p><b>ヒント：</b>スループットを最大化するために、スペースのレクラメーション処理に使用する並列処理の数を指定することができます。</p> <p><b>RECLAIMPROCESS</b> パラメーターの値を指定して <b>UPDATE STGPOOL</b> コマンドを使用することで、磁気テープ・ストレージ・プールを更新します。例えば、12 個の磁気テープ・ドライブがある場合、<b>RECLAIMPROCESS=5</b> を指定します。レクラメーション・プロセスごとに 2 つのドライブが使用されるため、レクラメーションに使用できるドライブの総数は 10 です。2 つのドライブは、バックアップ操作に確保されます。</p>

## 次のタスク

サーバー保守タスクのスケジュールを作成した後、以下のステップを実行することで、そのスケジュールを Operations Center で表示できます。

1. Operations Center のメニュー・バーで、「サーバー」にカーソルを移動します。
2. 「保守」をクリックします。

## 関連情報

[UPDATE STGPOOL \(ストレージ・プールの更新\)](#)

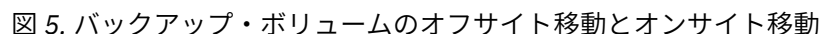


### DEFINE STGPOOL (ストレージ・プール内のボリュームの定義)

災害からリカバリーするには、データベース・バックアップ・ボリューム、コピー・ストレージ・プール・ボリューム、および追加ファイルが必要です。災害に備えて常に準備をしておくために、日常の作業を実行する必要があります。

リモート・ターゲット・サーバー上にオブジェクトをもつ仮想コピー・ストレージ・プールおよびデータベース・バックアップ・ボリュームをすべて表示するには、**QUERY DRMEDIA** コマンドを出します。

災害時回復管理機能 (DRM) により、オフサイト・メディアの移動を追跡することができます。以下の図は、災害復旧操作の一環としてバックアップ・メディアをオフサイトに移動してオンサイトに戻す場合の、一般的な操作のライフサイクルを示します。



DRM は、以下のメディア状態をボリュームに割り当てます。メディア状態は、ボリュームが位置から位置へと移動するにつれてボリューム追跡します。一部のメディア状態はオプションです。組織がボリュームの移動をどの程度細かく追跡するかに応じて、組織がこれらのオプションのメディア状態をスキップする可能性があります。以下のメディア状態が表示されます。

#### **MOUNTABLE**

このボリュームには有効なデータが入っており、オンサイトで、IBM Spectrum Protect サーバーからアクセスできます。

#### **NOTMOUNTABLE**

このボリュームには有効なデータが入っており、オンサイトですが、IBM Spectrum Protect サーバーからはアクセスできません。

#### **COURIER**

このボリュームには有効なデータが入っており、ボールドに転送中です。

#### **VAULT**

このボリュームには有効なデータが入っており、ボールド内にあります。

#### **VAULTRETRIEVE**

このボリュームはオフサイト・ボールドにあり、有効なデータが入っていないので、オンサイトに戻されます。

#### **COURIERRETRIEVE**

このボリュームにはもはや有効なデータが入っていないので、クーリエによって戻されます。

#### **ONSITERETRIEVE**

このボリュームにはもはや有効なデータが入っていないので、オンサイトに戻されます。データベース・バックアップのボリューム・レコード、スクラッチ・コピー・ストレージ・プール・ボリューム、およびスクラッチ活動データ・プール・ボリュームは、データベースから削除されます。専用コピー・ストレージ・プール・ボリュームおよび活動データ・プール・ボリュームの場合、アクセス・モードは、READWRITE に更新されます。

#### **RESTOREONLY**

データの修復を可能にするために、ボリュームをライブラリーにチェックインします。ボリュームは、データ修復のみに使用されます。

## **コピー・ストレージ・プール・ボリュームのオフサイトへの移動**

1 次ストレージ・プールおよびデータベースのバックアップ・コピーを作成した後、バックアップ・メディアをオフサイトに送ることができます。メディアをオフサイトに送るには、そのボリュームを IBM Spectrum Protect に対して使用不可としてマーク付け、それをクーリエに渡します。

### **始める前に**

ストレージ・プールのバックアップ処理が完了している必要があります。この方法では、**MOVE DRMEDIA** コマンドと **BACKUP STGPOOL** コマンドが同時に実行された場合に発生する可能性がある問題を回避できます。

**制約事項:** 保存ボリューム、つまり保存セットのデータが入っているテープ・ボリュームをオフサイトに移動するためには、この手順を使用しないでください。**MOVE RETMEDIA** コマンドを使用するか、Operations Center でメディアの移動操作を行う必要があります。手順については、[67 ページの『保存セット・データの磁気テープ・ストレージとの間での移動』](#)を参照してください。

### **手順**

1. オフサイトに移動するコピー・ストレージ・プールおよびデータベースのバックアップ・ボリュームを識別するには、**QUERY DRMEDIA** コマンドを発行し、**WHERESTATE** パラメーターを指定します。

```
query drmedia * wherestate=mountable
```

2. 次のように **MOVE DRMEDIA** コマンドを発行して、**WHERESTATE** パラメーターを指定し、現行の状態が MOUNTABLE であるボリュームの移動を指示します。

```
move drmedia * wherestate=mountable
```

- a) チェックアウト処理の過程で、SCSI ライブラリーはオペレーターの介入を要求します。次のコマンドを発行して、これらの要求をバイパスし、ライブラリーからカートリッジを排出します。

```
move drmedia * wherestate=mountable remove=no
```

- b) 次のコマンドを発行して、ボリュームのリストにアクセスし、カートリッジを識別してライブラリーから取り出します。

```
query drmedia wherestate=notmountable
```

MOUNTABLE 状態であるすべてのボリュームに対して、DRM は以下のタスクを実行します。

- ボリュームの状態を NOTMOUNTABLE に更新し、**SET DRMNOTMOUNTABLENAME** コマンドを発行した場合、ボリューム・ロケーションを更新します。**SET DRMNOTMOUNTABLENAME** コマンドを発行しない場合、デフォルトのロケーションは NOTMOUNTABLE です。
  - コピー・ストレージ・プール・ボリュームのアクセス・モードを使用不可に更新します。
  - 自動ライブラリーのボリュームをチェックアウトします。
3. オフサイト・ロケーションに転送するために、ボリュームをクーリエに送信し、以下のコマンドを発行します。

```
move drmedia * wherestate=notmountable
```

NOTMOUNTABLE 状態のすべてのボリュームに対して、DRM はボリューム状態を COURIER に更新し、**SET DRMCOURIERNAME** コマンドに従ってボリューム・ロケーションを更新します。**SET** コマンドを発行しなかった場合、デフォルトのロケーションは COURIER です。

**ヒント: MOVE DRMEDIA** コマンドを発行し、**TOSTATE** パラメーター設定を指定して宛先状態を指定することで、ボリューム状態のすべてを経由しなくても済みます。例えば、ボリュームを NOTMOUNTABLE 状態から VAULT 状態に変更するには、次のコマンドを発行します。

```
move drmedia * wherestate=notmountable tostate=vault
```

NOTMOUNTABLE 状態のすべてのボリュームに対して、DRM はボリューム状態を VAULT に更新し、**SET DRMVAULTNAME** コマンドに従ってボリューム・ロケーションを更新します。**SET** コマンドがまだ出されていない場合、デフォルトのロケーションは、VAULT です。

4. ボールト・ロケーションでボリュームの受け入れが確認されたら、**MOVE DRMEDIA** コマンドを発行して COURIER 状態を指定します。

```
move drmedia * wherestate=courier
```

COURIER 状態のすべてのボリュームに対して、DRM はボリューム状態を VAULT に更新し、**SET DRMVAULTNAME** に従ってボリューム・ロケーションを更新します。**SET** コマンドを発行しなかった場合、デフォルトのロケーションは VAULT です。

5. 次のコマンドを発行して、ボールトにある、有効なデータが含まれるボリュームのリストを表示します。

```
query drmedia wherestate=vault
```

## コピー・ストレージ・プール・ボリュームのオンサイトへの移動

災害復旧操作の一環としてバックアップ・メディアをオンサイトに移動することができます。データをリストアするために、ボリュームをオンサイトに戻すことができます。非仮想データベース・バックアップ・ボリュームを期限切れにし、そのボリュームをオンサイトに戻して、再使用したり取り外したりすることもできます。

## 始める前に

**制約事項:** 保存セットのデータが入っているボリュームをオンサイトに戻すためには、この手順を使用しないでください。 **MOVE RETMEDIA** コマンドを使用するか、Operations Center でメディアの移動操作を行う必要があります。手順については、[67 ページの『保存セット・データの磁気テープ・ストレージとの間での移動』](#)を参照してください。

ボリュームを再使用するために戻す場合は、それらのボリュームの有効期限に達していることを確認してください。以下のすべての条件が満たされている場合、データベース・バックアップ・ボリュームを期限切れにすることができます。

- 集合の最後のボリュームの経過日数が、期限切れ値を超えている。期限切れ値は、集合の最後のバックアップ後の経過日数を示します。インストール時の期限切れ値は 60 日です。この値をオーバーライドするには、**SET DRMDBBACKUPEXPIREDAYS** コマンドを発行します。
- 集合内のすべてのボリュームが VAULT 状態である。
- ボリュームが最新のデータベース・バックアップの集合の一部ではない。

満了処理は、**EXPIRE INVENTORY** コマンドを発行して手動で開始するか、サーバー・オプション・ファイルで指定する EXPINTERVAL オプション設定を使用して自動で開始します。

## 手順

ストレージ・プール・ボリュームをオンサイトに移動するには、以下のいずれかのアクションを実行します。

タスク	手順
空のボリュームを再使用または取り外しのためにオンサイトに移動する。	<p>空のストレージ・プール・ボリュームをオンサイトに移動するには、以下の手順を実行します。</p> <p>a. <b>SET DRMDBBACKUPEXPIREDAYS</b> コマンドを発行して、データベース・バックアップの集合の期限が切れるまでの日数を指定します。例えば、日数を 30 に設定するには、次のコマンドを発行します。</p> <pre>set drmdbbackupexpiredays 30</pre> <p><b>ヒント:</b> <b>DEFINE STGPOOL</b> コマンドを発行して、コピー・ストレージ・プール定義の <b>REUSEDELAY</b> パラメーターに同じ値を指定することで、以下が行われるようにします。</p> <ul style="list-style-type: none"><li>• データベースを以前のレベルにリストアすることができる。</li><li>• コピー・ストレージ・プール内のファイルへのデータベース参照を引き続き有効にする。</li></ul> <p>DRM によって管理されているコピー・ストレージ・プールが、異なる <b>REUSEDELAY</b> 値を持っている場合、<b>SET DRMDBBACKUPEXPIREDAYS</b> コマンドを発行し、<b>REUSEDELAY</b> パラメーターを最大値に設定します。</p> <p>b. 有効なデータが含まれなくなり、オンサイトに戻ることができる、オフサイト・ボールドにあるすべてのボリュームを識別します。空のボリュームの場合、サーバーはそのボリュームを自動的に VAULTRETRIEVE メディア状態にします。以下のコマンドを発行します。</p> <pre>query drmedia * wherestate=vaultretrieve</pre>

タスク	手順
	<p>c. コピー・ストレージ・プールを移動するプロセスを開始するには、次のコマンドを発行します。</p> <pre data-bbox="586 275 1097 300">move drmedia * wherestate=vaultretrieve</pre> <p><b>制約事項:</b> コピー・ストレージ・プール・ボリュームは、<b>DEFINE STGPOOL</b> コマンドの <b>REUSEDELAY</b> パラメーターで指定された日数以上 <b>EMPTY</b> 状態である場合、オンサイトに移動することができます。</p> <p>サーバーは、<b>VAULTRETRIEVE</b> 状態であるすべてのボリュームに対して、以下のアクションを実行します。</p> <ul style="list-style-type: none"> <li>• ボリューム状態を <b>COURIERRETRIEVE</b> に変更します。</li> <li>• <b>SET DRMCOURIERNAME</b> コマンドの指定に従って、ボリュームの位置を更新します。</li> </ul> <p><b>ヒント:</b></p> <p><b>MOVE DRMEDIA</b> コマンドを発行して <b>TOSTATE</b> パラメーター設定を指定することによって、ボリュームの宛先を指定することもできます。例えば、ボリュームを <b>VAULTRETRIEVE</b> 状態から <b>ONSITERETRIEVE</b> 状態に移動するには、次のコマンドを発行します。</p> <pre data-bbox="586 858 1390 884">move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve</pre> <p>サーバーは、<b>VAULTRETRIEVE</b> 状態であるすべてのボリュームに対して、以下のアクションを実行します。</p> <ul style="list-style-type: none"> <li>• 再使用または取り外しが可能なオンサイトにボリュームを移動します。</li> <li>• データベース・バックアップ・ボリュームを、ボリューム・ヒストリー・テーブルから削除します。</li> <li>• スクラッチ・コピー・ストレージ・プール・ボリュームのデータベース内のレコードを削除し、専用コピー・ストレージ・プール・ボリュームの場合は、アクセス権限を読み取り/書き込みに更新します。</li> </ul> <p>d. クーリエによってボリュームをオンサイトに戻す場合は、次のコマンドを発行します。</p> <pre data-bbox="586 1325 1122 1350">move drmedia * wherestate=courierretrieve</pre> <p>サーバーは、<b>COURIERRETRIEVE</b> 状態であるすべてのボリュームに対して以下のアクションを実行します。</p> <ul style="list-style-type: none"> <li>• 再使用または後処理が可能なオンサイトにボリュームを移動します。</li> <li>• データベース・バックアップ・ボリュームを、ボリューム・ヒストリー・テーブルから削除します。</li> <li>• スクラッチ・コピー・ストレージ・プール・ボリュームのデータベース内のレコードを削除します。専用コピー・ストレージ・プール・ボリュームの場合は、アクセス権限を読み取り/書き込みに更新します。</li> </ul>
空ではないボリュームをデータ・リストアのためにオンサイトに移動する。	データをリストアするためにストレージ・プール・ボリュームをオンサイトに移動するには、以下のステップを実行します。

タスク	手順
	<p>a. オンサイトに戻したいボリュームを特定します。必要なボリュームをそのオフサイト・ロケーションで見つけるには、<b>QUERY DRMEDIA</b> コマンドを発行し、<b>WHERESTATE</b> パラメーターを指定します。例えば、オフサイト・ボールドにあるすべてのボリュームを表示するには、次のコマンドを発行します。</p> <pre>query drmedia * wherestate=vault</pre> <p>b. ボリュームをオンサイトに移動します。<b>TOSTATE</b> パラメーター設定を指定して <b>MOVE DRMEDIA</b> コマンドを発行し、ボリュームの宛先を指定します。例えば、ボリューム VOL001 をオンサイトに移動するには、次のコマンドを発行します。</p> <pre>move drmedia vol001 wherestate=vault tostate=onsiteretrieve</pre> <p>サーバーは、VAULT 状態であるすべての指定されたボリュームに対して以下のアクションを実行します。</p> <ul style="list-style-type: none"> <li>• データのリストアに使用できるオンサイトにボリュームを移動します。</li> <li>• ボリューム状態を <b>ONSITERETRIEVE</b> に変更します。</li> </ul> <p>c. ボリュームをテープ・ライブラリーにチェックインして、ボリュームをリストア操作でできるようにします。ボリュームを <b>ONSITERETRIEVE</b> 状態から <b>RESTOREONLY</b> 状態に移動するには、<b>CHECKIN LIBVOL</b> コマンドを発行します。例えば、ライブラリーの名前が <b>LIBNAME</b> の場合、次のコマンドを発行します。</p> <pre>checkin libvol libname search=bulk waittime=0 checklabel=barcode status=private</pre> <p><b>ヒント:</b> SCSI ライブラリー内のテープ・ボリュームの場合、サーバーがバーコード・ラベルを読み取るように指定することで、チェックイン時間を短縮することができます。</p> <p>ボリュームが自動化ライブラリーに追加され、ボリュームのメディア状態が <b>RESTOREONLY</b> に変更されます。</p> <p>d. テープ・ボリュームからデータをリストアします。データ修復の完了後、テープ・ボリュームをオフサイト・ボールドに送り返すことができます。オフサイトに移動される他のテープ・ボリュームと一緒にテープ・ボリュームを処理できます。ボリュームのメディア状態はデフォルトで <b>MOUNTABLE</b> に変わります。以下のコマンドを発行します。</p> <pre>move drmedia * wherestate=restoreonly</pre> <p>あるいは、<b>MOVE DRMEDIA</b> コマンドを発行して、<b>TOSTATE</b> パラメーター設定を指定することによって、ボリュームの宛先を指定することもできます。例えば、ボリュームを <b>RESTOREONLY</b> 状態から <b>VAULT</b> 状態に移動するには、次のコマンドを発行します。</p> <pre>move drmedia * wherestate=restoreonly tostate=vault</pre>

## タスクの結果

選択したストレージ・プール・ボリュームはオンサイトに戻され、テープ・ライブラリーにチェックインされます。空のテープ・ボリュームは、スクラッチ状況に戻され、再使用可能になります。空でないボリュームは **RESTOREONLY** 状態になっており、データのリストアに使用できます。

## 保存セット・データの磁気テープ・ストレージとの間での移動

保存セット・データをテープ・ボリュームにコピーして、ボリュームをオンサイト・ライブラリーからオフサイトの磁気テープ・ストレージ・ボールドに移動することができます。ボールドは、長期間の安全な保管を行うために設計されています。保存セットがテープにコピーされ、テープ・ボリュームがテープ・ライブラリーから除去された後、ボリュームのオフサイトとオンサイト間の移動を追跡できます。

1つ以上の保存セットのデータが入っているテープ・ボリュームは、保存ボリュームと呼ばれます。テープ・ボリュームをある場所から別の場所に移動すると、そのボリュームの状態は新しい場所を反映するように変更されるので、ユーザーはその情報を使用してボリュームの物理的な場所を追跡できます。

保存ボリュームのライフサイクルは、以下の主なステージで構成されています。

1. 保存セットをテープ・ボリュームに書き込むプロセスが開始されると、スクラッチ・ボリュームがテープ・ライブラリーのスクラッチ・プールから取得されるか、既存のボリュームが保存プールから選択されます。1つ以上の保存セットのデータがボリュームに書き込まれます。ボリュームが満杯になると、クーリエによってオフサイト・ボールドに運ばれます。
2. リストアする必要があるデータがボリュームに含まれている場合、そのボリュームはボールドから取得され、クーリエによってオンサイトに戻されます。保存セット内のデータがリストアされた後、ボリュームはオフサイト・ボールドに戻されます。
3. 時間の経過とともに、有効期限ポリシーに基づいて保存セットのデータの有効期限が切れる可能性があります。ボリュームにデータを含むすべての保存セットが有効期限に達した場合、ボリュームを再使用のためにオンサイトに戻すことができます。

以下の図は、保存ボリュームをオフサイトに移動してオンサイトに戻す、一般的な操作のライフサイクルを示します。



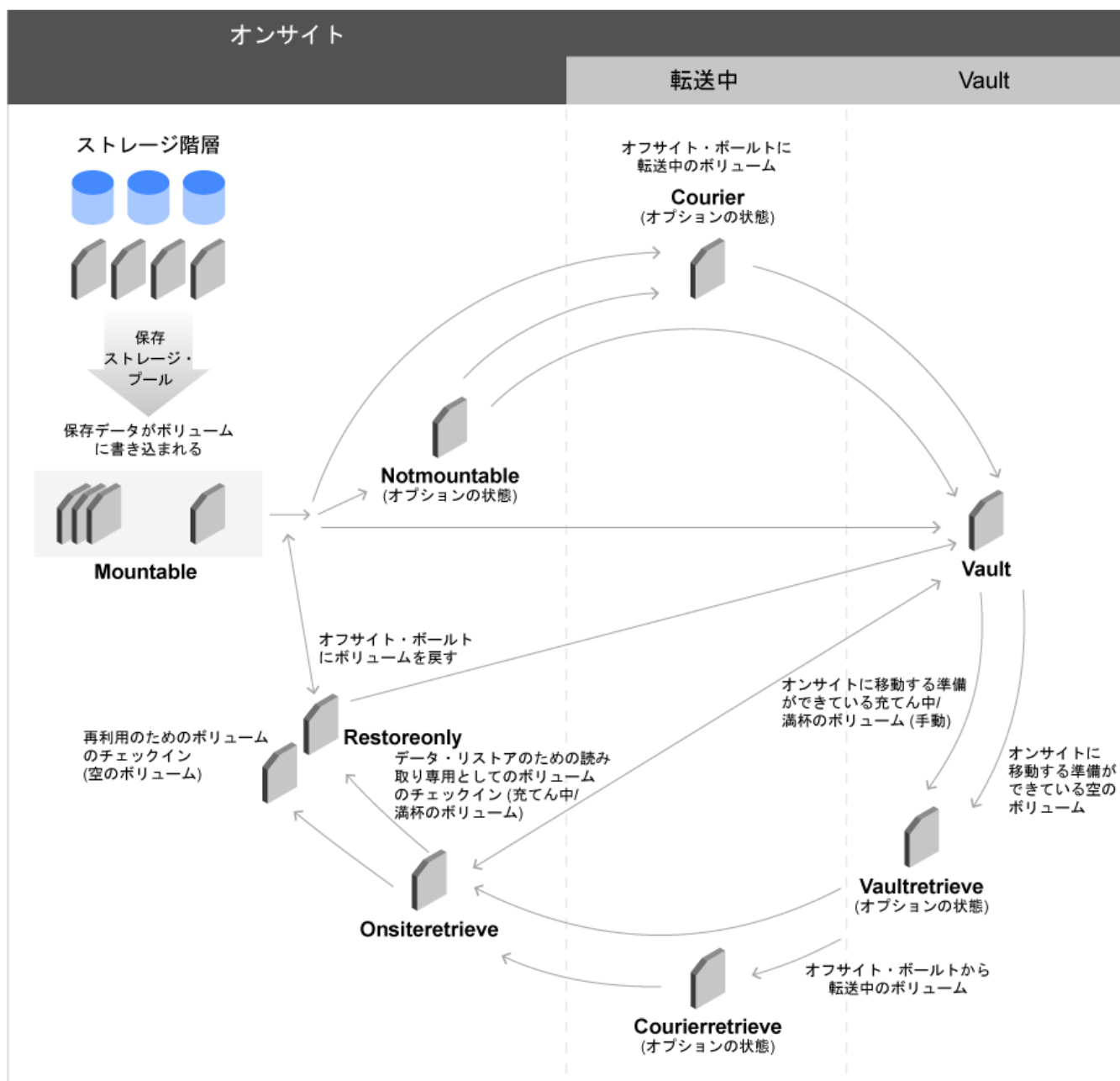


図 6. 保存ボリュームのオフサイト移動とオンサイト移動

ボリュームのメディア状態は、ボリュームがオンサイト・ライブラリーからオフサイト・ポールトに移動してから、データの修復またはテープの再利用のためにオンサイトに戻るときに、現行の位置を識別するのに役立ちます。ボリュームのメディア状態は、ボリュームの物理ロケーションに関連した論理指定です。一部のメディア状態はオプションです。組織がボリュームの移動をどの程度細かく追跡するかに応じて、組織がこれらのオプションのメディア状態をスキップする可能性があります。以下のメディア状態が表示されます。

#### MOUNTABLE

ボリュームはオンサイトで、ライブラリーにチェックインされています。1つ以上の保存セットのデータがボリュームに書き込まれます。

## NOTMOUNTABLE

ボリュームはオンサイトですが、ライブラリーからチェックアウトされていて、オフサイトへの送信準備ができています。

## COURIER

ボリュームはオフサイト・ボールドに転送中です。

## VAULT

ボリュームは、長期保管のためにオフサイト・ボールドにあります。

## VAULTRETRIEVE

ボリュームは、オフサイト・ボールドからいつでもオンサイトに戻すことが可能です。空のボリュームはオンサイトに移して再使用できます。サーバーは、ボリュームに期限切れデータのみが含まれていることを検出し、そのボリュームを自動的に VAULTRETRIEVE メディア状態にします。埋め込み中または満杯のボリュームもデータ修復のためにオンサイトに移すことができますが、このアクションは、**MOVE RETMEDIA** コマンドの **TOSTATE** パラメーター設定を使用して指定する必要があります。

## COURIERRETRIEVE

ボリュームは、オフサイト・ボールドからオンサイトに戻されています。

## ONSITERETRIEVE

ボリュームはオフサイト・ボールドからリトリブされ、オンサイトに戻されています。空でないボリュームはライブラリーにチェックイン可能であり、保存セット・データをボリュームからリストアできます。空のボリュームはチェックインも再使用も可能です。

## RESTOREONLY

保存セットのデータの修復を可能にするために、ボリュームをライブラリーにチェックインします。

## 保存ボリュームのオフサイトへの移動

1 つ以上の保存セットのデータを含む保存ボリュームをオフサイト・ロケーションに送信できます。オフサイト・ボールドは、テープ・ボリュームのセキュア・ストレージを提供して、必要な場合にデータを確実にリストアできるように設計されています。

## 始める前に

**ヒント:** データベース・バックアップ・ボリュームをオフサイトまたはオンサイトに移動する場合に **MOVE DRMEDIA** コマンドを使用しない場合、**MOVE RETMEDIA** コマンドを使用しても同じことを実行できます。詳細については、[62 ページの『コピー・ストレージ・プール・ボリュームのオフサイトへの移動』](#)を参照してください。

- オフサイトに送信する保存セットが作成された後、**BACKUP DB** コマンドを実行して、サーバー・データベース・ボリュームをバックアップします。データベース・バックアップ・ボリュームが保存ボリュームと共にオフサイトに送信されるようにするには、**MOVE RETMEDIA** コマンドで **SOURCE** パラメーターを指定する必要があります。

**制約事項:** データベース・バックアップ・ボリュームをオフサイトに送信するために、Operation Center でメディアの移動操作を使用することはできません。データベース・バックアップ・ボリュームを移動するには、**MOVE RETMEDIA** コマンドを使用します。

保存ボリュームを移動するための Operations Center の使用方法については、Operations Center のオンライン・ヘルプを参照してください。

- コピーしようとする保存セットの状況が「完了」であることを確認してください。この状況は、保存セットがテープに完全にコピーされ、テープ・ボリュームをオフサイト・ボールドに移動できることを示します。この方法では、メディアの移動操作と保存セットのコピー操作が同時に実行された場合に発生する可能性がある問題を回避できます。

## 手順

1. 次のように **QUERY RETMEDIA** コマンドを発行して、オフサイトに移動する保存ストレージ・プールおよびデータベースのバックアップ・ボリュームを識別します。

```
query retmedia * wherestate=mountable
```

2. 現行の状態が MOUNTABLE であるボリュームの移動を開始します。デフォルトでは、空ではないボリュームはすべて組み込まれます。これは、ボリュームが、コピーされる保存セットか、完全にコピーされた保存セットか、どちらに属しているかは関係ありません。次のコマンドを発行します。

```
move retmedia * wherestate=mountable
```

- a) SCSI ライブラリーを使用している場合、チェックアウト処理の過程で SCSI ライブラリーがオペレーターの介入を要求します。次のコマンドを発行して、これらの要求をバイパスし、ライブラリーからカートリッジを排出します。

```
move retmedia * wherestate=mountable remove=no
```

- b) 次のコマンドを発行して、ボリュームのリストを取得し、カートリッジを識別してライブラリーから取り出します。

```
query retmedia wherestate=notmountable
```

MOUNTABLE 状態であるすべてのボリュームでは、**MOVE RETMEDIA** コマンドを発行すると以下のタスクが実行されます。

- ボリュームの状態を NOTMOUNTABLE に更新し、**SET DRMNOTMOUNTABLENAME** コマンドを発行した場合、ボリューム・ロケーションを更新します。**SET DRMNOTMOUNTABLENAME** コマンドを発行しなかった場合、デフォルトのロケーションは NOTMOUNTABLE です。
- ボリューム・アクセス・モードを使用不可に更新します。
- 自動ライブラリーのボリュームをチェックアウトします。

**ヒント:** 組織はボリュームの移動をどの程度細かく追跡するかに応じて、一部のメディア状態をスキップする可能性があります。**MOVE RETMEDIA** コマンドで **TOSTATE** パラメーターを指定して宛先状態を指定することで、さまざまなメディア状態のすべてを経由することを回避できます。例えば、ボリュームを NOTMOUNTABLE 状態から直接 VAULT 状態に変更するには、以下のコマンドを発行します。

```
move retmedia * wherestate=notmountable tostate=vault
```

3. オフサイト・ロケーションに転送するために、ボリュームをクーリエに送信して、次のコマンドを実行します。

```
move retmedia * wherestate=notmountable
```

NOTMOUNTABLE 状態のすべてのボリュームに対して、ボリューム状態は COURIER 状態に更新され、**SET DRMCOURIERNAME** コマンドに従ってボリューム・ロケーションが更新されます。**SET DRMCOURIERNAME** コマンドを発行しなかった場合、デフォルトのロケーションは COURIER です。

4. オフサイト・ボールドに転送中のテープ・ボリュームの移動を追跡します。次のコマンドを発行します。

```
query retmedia * wherestate=courier
```

5. ボールド・ロケーションがボリュームの受け入れを確認した場合、**MOVE RETMEDIA** コマンドを発行して COURIER 状態を指定します。

```
move retmedia * wherestate=courier
```

COURIER 状態のすべてのボリュームに対して、ボリューム状態は VAULT に更新され、**SET DRMVAULTNAME** コマンドに従ってボリューム・ロケーションが更新されます。**SET DRMVAULTNAME** コマンドを発行しなかった場合、デフォルトのロケーションは VAULT です。

NOTMOUNTABLE 状態のすべてのボリュームに対して、**MOVE RETMEDIA** コマンドはボリューム状態を VAULT に更新し、**SET DRMVAULTNAME** に従ってボリューム・ロケーションが更新されます。**SET DRMVAULTNAME** コマンドがまだ出されていない場合、デフォルトのロケーションは、VAULT です。

## タスクの結果

保存ボリュームおよび指定されたデータベース・バックアップ・ボリュームがオフサイトのテープ・ボールドに移動されます。保存セット・データをリストアする必要がある場合、ボリュームはボールドから取得できます。

## 保存ボリュームのオンサイトへの移動

保存セットをリストアする必要がある場合は、保存セット・データが入っているテープ・ボリュームをリストア操作にオンサイトにすることができます。保存ボリュームにデータを含むすべての保存セットの有効期限に達した場合、空のボリュームをオンサイトに戻して再利用することができます。

## 始める前に

空のボリュームを再使用のために戻す場合は、ボリュームにデータが含まれたすべての保存セットが満了日に達していて保存セットが期限切れになっていることを確認してください。**EXPIRE INVENTORY** コマンドを発行して満了処理を手動で開始することも、**DELETE RESET** コマンドを使用して、削除する保存セットにマークを付けることもできます。

**ヒント:** データベース・バックアップ・ボリュームをオフサイトまたはオンサイトに移動する場合に **MOVE DRMEDIA** コマンドを使用しない場合、**MOVE RETMEDIA** コマンドを使用しても同じことを実行できます。詳細については、[62 ページの『コピー・ストレージ・プール・ボリュームのオフサイトへの移動』](#)を参照してください。

## 手順

保存ボリュームをオンサイトに移動するには、以下の手順を実行します。

タスク	手順
<p>再利用するために空のボリュームをオンサイトに移動する。</p>	<p>空の保存ボリュームをオンサイトに移動するには、以下の手順を実行します。</p> <p>a. オンサイトに戻す、オフサイト・ボルトの保存ボリュームを特定します。空のボリュームの場合、サーバーは、ボリュームに期限切れデータのみが含まれていることを検出し、そのボリュームを自動的に VAULTRETRIEVE メディア状態にします。次のコマンドを発行します。</p> <pre data-bbox="591 380 1240 411">query retmedia * wherestate=vaultretrieve volstatus=empty</pre> <p>b. テープ・ボリュームをオンサイトに移動します。<b>TOSTATE</b> パラメーターを指定して <b>MOVE RETMEDIA</b> コマンドを発行し、ボリュームの宛先を指定します。次のコマンドを発行します。</p> <pre data-bbox="591 558 1229 600">move retmedia * wherestate=vaultretrieve volstatus=empty tostate=onsiteretrieve</pre> <p><b>制約事項:</b> 保存ストレージ・プール・ボリュームは、<b>DEFINE STGPOOL</b> コマンドの <b>REUSEDelay</b> パラメーターで指定された日数以上 <b>EMPTY</b> 状態である場合、オンサイトに移動することができます。</p> <p>サーバーは、以下のアクションを実行します。</p> <ul data-bbox="591 800 1455 947" style="list-style-type: none"> <li>• ボリューム状態を <b>ONSITERETRIEVE</b> に変更します</li> <li>• データベース・バックアップ・ボリュームをボリューム・ヒストリー・テーブルから削除します</li> <li>• スクラッチ保存ボリュームのデータベース内のレコードを削除します</li> </ul> <p>c. <b>CHECKIN LIBVOL</b> コマンドを発行してそのボリュームをスクラッチ・ボリュームと指定することで、空のボリュームをテープ・ライブラリーにチェックインし、そのボリュームを再利用することができます。</p> <p><b>ヒント:</b> SCSI ライブラリー内のテープ・ボリュームの場合、サーバーがバーコード・ラベルを読み取るように指定することで、チェックイン時間を短縮することができます。</p> <p>次のコマンドを発行します。</p> <pre data-bbox="591 1241 1107 1283">checkin libvol libname search=bulk waittime=0 checklabel=barcode status=scratch</pre>

タスク	手順
空ではないボリュームをデータ・リストアのためにオンサイトに移動する。	<p>データ・リストアのために保存ボリュームをオンサイトに移動するには、以下のステップを実行します。</p> <p>a. リストアする保存セット・データが含まれているボリュームを特定します。</p> <ul style="list-style-type: none"> <li>各保存セットによって使用されるボリュームを特定するには、次のコマンドを発行します。</li> </ul> <pre>query retset listvolumes=yes</pre> <ul style="list-style-type: none"> <li>保存ボリュームにデータを持つ保存セットを特定するには、次のコマンドを発行します。</li> </ul> <pre>query volume listretsets=yes</pre> <p>b. <b>QUERY RETMEDIA</b> コマンドを発行し、<b>WHERESTATE</b> パラメーターを指定することにより、必要なボリュームをそのオフサイト・ロケーションで見つけます。例えば、オフサイト・ボールドにあるすべてのボリュームを表示するには、次のコマンドを発行します。</p> <pre>query retmedia * wherestate=vault</pre> <p>c. 必要なボリュームをオンサイトに移動します。<b>TOSTATE</b> パラメーターを指定して <b>MOVE RETMEDIA</b> コマンドを発行し、ボリュームの宛先を指定します。例えば、ボリューム VOL001 をオンサイトに移動するには、次のコマンドを発行します。</p> <pre>move retmedia VOL001 wherestate=vault tostate=onsiteretrieve</pre> <p><b>重要:</b> 保存ストレージ・プールのボリュームをレクラメーション処理で使用するにはボリュームが MOUNTABLE 状態でなければなりません。レクラメーション処理では ONSITERETRIEVE 状態または RESTOREONLY 状態にあるボリュームのレクラメーション処理を行いません。<b>MOVE RETMEDIA</b> コマンドを発行し、<b>TOSTATE=ONSITERETRIEVE</b> パラメーターまたは <b>TOSTATE=RESTOREONLY</b> パラメーターを指定して、保存ストレージ・プールのボリュームをオンサイトに戻す場合、ストレージ・レクラメーション処理ではそれらのボリュームをスキップします。</p> <p>d. ボリュームをテープ・ライブラリーにチェックインして、ボリュームをリストア操作でできるようにします。ボリュームをデータ修復のみに使用できるようにするために、そのアクセス・モードは読み取り専用です。ボリュームを ONSITERETRIEVE 状態から RESTOREONLY 状態に移動するには、<b>CHECKIN LIBVOL</b> コマンドを発行します。次のコマンドを発行します。</p> <pre>checkin libvol libname search=bulk waittime=0 checklabel=barcode status=private</pre> <p><b>ヒント:</b> SCSI ライブラリー内のテープ・ボリュームの場合、サーバーがバーコード・ラベルを読み取るように指定することで、チェックイン時間を短縮することができます。</p> <p>ボリュームが自動化ライブラリーに追加され、ボリュームのメディア状態が RESTOREONLY に変更されます。</p>

## タスクの結果

選択した保存ボリュームはオンサイトに戻され、テープ・ライブラリーにチェックインされます。空のテープ・ボリュームは、スクラッチ状況に戻され、再使用可能になります。空でないボリュームは RESTOREONLY 状態になっており、データのリストアに使用できます。

## 次のタスク

データ修復の完了後、テープ・ボリュームをオフサイト・ボールドに送り返すことができます。次のコマンドを発行します。

```
move retmedia * wherestate=restoreonly tostata=vault
```

## 保存ボリュームの移動をモニターするためのアラート・メッセージ

保存ボリュームをオフサイトに送信したり、オンサイトに戻したりする場合、IBM Spectrum Protect サーバーでは、問題を報告し、状況のモニターに役立てるため ANR メッセージの形式でアラートが生成されます。

すべてのメッセージを確認するには、IBM Spectrum Protect エラー・ログを参照してください。メッセージに関する詳しい資料は、「ANR メッセージ」を参照してください。よく発行されるメッセージについては、以下の表に記載されています。

表 16. 保存テープ・ボリュームをオフサイト・ボールドに送信		
アクション	ANR メッセージ	説明
保存セットはテープ・ボリュームにコピーされます。	ANR3852I	この情報メッセージは、保存セットがテープ・ボリュームに正常にコピーされたことを示します。コピー操作の詳細が示されます。保存セットの状態は COMPLETED です。
テープ・ボリュームはテープ・ライブラリーからチェックアウトされます。	ANR6697I	この情報メッセージは、MOUNTABLE 状態のテープ・ボリュームがテープ・ライブラリーから正常にチェックアウトされたことを示します。
テープ・ボリュームはライブラリーからチェックアウトされ、MOUNTABLE 状態から VAULT 状態に移行します。	ANR6683I	この情報メッセージは、保存データが正常に移動して、状況が変更されたことを示します。

表 17. リストア操作に使用するためのテープ・ライブラリーへのテープ・ボリュームのチェックイン		
アクション	ANR メッセージ	説明
データを含む保存ボリュームがオンサイトのテープ・ライブラリーに正常にチェックインされました。	ANR8532I	この情報メッセージは、データを含むボリュームが、オンサイトのテープ・ライブラリーに正常にチェックインされたことを示します。保存ボリュームの場合、ボリュームのメディアの状態は、ONSITERETRIEVE から RESTOREONLY に変更され、そのアクセス・モードは読み取り専用になります。ボリュームの保存セット・データはリストアできるようになりました。  <b>ヒント:</b> このメッセージは、チェックインされているテープ・ボリュームが空の場合、表示されません。
空ではない保存ボリュームをスクラッチ・ボリュームとして、テープ・ライブラリーへチェックインしようと試みています。	ANR8443E	このエラー・メッセージは、データを含む保存ボリュームをテープ・ライブラリーにチェックインできず、SCRATCH の状況が割り当てられないためにトリガーされます。ボリュームはチェックインされず、テープ上のデータは上書きされません。



表 18. 有効期限切れの保存ボリュームのテープ・ライブラリーへのチェックイン

アクション	ANR メッセージ	説明
空の保存ボリュームがオンサイトのテープ・ライブラリーにチェックインされます。	ANR8430I	この情報メッセージは、空のボリュームが、オンサイトのテープ・ライブラリーに正常にチェックインされたことを示します。ボリュームはスクラッチ状況に戻ります。
空の保存ボリュームのオンサイトのテープ・ライブラリーへのチェックインの試みが失敗しました。	ANR8832E	このエラー・メッセージは、空の保存ボリュームをオンサイトのテープ・ライブラリーにチェックインする操作が失敗したことを示します。

## クライアント・スケジュールの定義

Operations Center を使用して、クライアント操作のスケジュールを作成します。

### 手順

1. Operations Center メニュー・バーで、「クライアント」の上にカーソルを移動します。
2. 「スケジュール」をクリックします。
3. 「+ スケジュール」をクリックします。
4. 「スケジュールの作成」ウィザードのステップを実行します。

56 ページの『サーバー保守アクティビティのスケジュールの定義』でスケジュールしたサーバー保守アクティビティに基づいて、22:00 に開始されるようにクライアント・バックアップ・スケジュールを設定します。

## サーバーのテープ装置の接続

サーバーでテープ装置を使用できるようにするには、事前に装置をサーバー・システムに接続し、適切なテープ・デバイス・ドライバ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

システム・パフォーマンスを最適化するには、高速の大容量テープ装置を使用します。ビジネス要件を満たすのに十分な磁気テープ・ドライブを準備します。

テープ装置は専用のホスト・バス・アダプター (HBA) に接続し、ディスクなどの他の装置タイプと共有しないでください。IBM 磁気テープ・ドライブには、HBA および関連ドライバに関する特殊な要件があります。

## ユーザーのシステムへの自動ライブラリー装置の接続

テープにデータを保管するために、自動ライブラリー装置をユーザーのシステムに接続することができます。

### このタスクについて

自動ライブラリー装置を接続する前に、以下の制約事項を検討してください。

- 接続する装置は、専用のホスト・バス・アダプター (HBA) に取り付ける必要がある。
- HBA を他の装置タイプ (ディスクなど) と共有してはならない。
- マルチポート・ファイバー・チャンネル HBA の場合、装置は専用のポートに接続する必要がある。これらのポートを他の装置タイプと共有してはいけない。

- IBM 磁気テープ・ドライブには、HBA および関連ドライバーに関して特殊な要件があります。装置について詳しくは、ご使用のオペレーティング・システムの Web サイトを参照してください。
  - [IBM Spectrum Protect Supported Devices for AIX](#)
  - [IBM Spectrum Protect Supported Devices for Linux and Windows](#)

## 手順

ファイバー・チャネル (FC) アダプターを使用するには、以下の手順で行います。

1. FC アダプターおよび関連ドライバーをインストールする。
2. 接続されたメディア・チェンジャー装置用の適切なデバイス・ドライバーをインストールする。

## 関連概念

### テープ・デバイス・ドライバーの選択

IBM Spectrum Protect とともにテープ装置を使用するには、適切なテープ・デバイス・ドライバーをインストールする必要があります。

## ライブラリー・モードの設定

IBM Spectrum Protect サーバーが SCSI ライブラリーにアクセスできるようにするには、このテープ装置を適切なモードに設定する必要があります。

## このタスクについて

一部のライブラリーにはフロント・パネル・メニューとディスプレイがあり、明示的なオペレーター要求に使用できます。ただし、そのような要求に応答するようにテープ装置を設定しても、通常、装置は IBM Spectrum Protect 要求に応答しません。

一部のライブラリーは、SEQUENTIAL モードにすることができます。このモードでは、ボリュームは順次方式を使用して自動的にドライブにマウントされます。このモードは、IBM Spectrum Protect がテープ装置にアクセスする方式と競合します。システム・デバイス・ドライバー (IBM テープ・デバイス・ドライバーおよび IBM Spectrum Protect テープ・デバイス・ドライバー) は、SEQUENTIAL モードで構成されたライブラリーをライブラリー・チェンジャー装置として検出しません。

## 手順

1. ライブラリー・モードの設定方法を確認するには、ご使用のテープ装置の資料を参照してください。
2. ご使用のテープ装置を適切なモードに設定します。ほとんどのテープ装置では、適切なモードは RANDOM モードと呼ばれます。ご使用のテープ装置に RANDOM モードがない場合は、装置の資料を参照して適切なモードを識別してください。

## テープ・デバイス・ドライバーの選択

IBM Spectrum Protect とともにテープ装置を使用するには、適切なテープ・デバイス・ドライバーをインストールする必要があります。

### 関連資料

#### テープ・デバイス・ドライバーのインストールと構成

IBM Spectrum Protect でテープ装置を使用できるようにするには、事前に正しいテープ・デバイス・ドライバーをインストールする必要があります。

## IBM テープ・デバイス・ドライバー

IBM テープ・デバイス・ドライバーは、ほとんどの IBM ラベル付きテープ装置に使用可能です。

Fix Central の Web サイトから IBM テープ・デバイス・ドライバーをダウンロードできます。

1. Fix Central Web サイト [Fix Central Web サイト](#) にアクセスします。
2. 「製品の選択」をクリックします。

3. 「製品グループ」メニューの「**System Storage**」を選択します。
4. 「**System Storage**」メニューの「**Tape systems**」を選択します。
5. 「**Tape systems**」メニューの「**Tape drivers and software**」を選択します。
6. 「**Tape drivers and software**」メニューの「**Tape device drivers**」を選択します。テープ・ドライバーのほかに、IBM Tape Diagnostic Tool (ITDT) などのツールにアクセスすることもできます。
7. 「**Platform**」メニューで、ご使用のオペレーティング・システムを選択します。

Windows | AIX

IBM テープ・デバイス・ドライバーによってサポートされる装置とオペレーティング・システムのレベルの最新リストについては、IBM Spectrum Protect Supported Devices の Web サイト ([AIX および Windows でサポートされるデバイス](#)) を参照してください。

Linux

IBM テープ・デバイス・ドライバーによってサポートされるテープ装置とオペレーティング・システムのレベルの最新リストについては、IBM Spectrum Protect Supported Devices の Web サイト ([Linux でサポートされるデバイス](#)) を参照してください。

IBM テープ・デバイス・ドライバーは、一部の Linux カーネル・レベルのみをサポートします。サポートされるカーネル・レベルについて詳しくは、[Fix Central Web サイト](#) を参照してください。

## IBM Spectrum Protect テープ・デバイス・ドライバー

IBM Spectrum Protect サーバーは、テープ・デバイス・ドライバーを提供します。

IBM Spectrum Protect テープ・デバイス・ドライバーは、サーバーとともにインストールされます。

AIX

IBM AIX オペレーティング・システムが提供する汎用 SCSI テープ・デバイス・ドライバーを使用して、IBM Spectrum Protect デバイス・ドライバーによってサポートされていないテープ装置を処理することができます。AIX の汎用 SCSI テープ・デバイス・ドライバーが使用されている場合、GENERICTAPE 装置クラスが、**DEFINE DEVCLASS** コマンドで指定された装置タイプに設定されている必要があります。

以下のテープ装置の場合は、IBM Spectrum Protect テープ・デバイス・ドライバーをインストールするか、またはご使用のオペレーティング・システムのネイティブ・デバイス・ドライバーをインストールするかを選択できます。

ECART  
LTO (IBM 以外)

このリストの磁気テープ・ドライブを含む、SCSI 接続されたすべてのライブラリーは、IBM Spectrum Protect チェンジャー・ドライバーを使用する必要があります。

他のハードウェア・ベンダーから入手したテープ・デバイス・ドライバーが GENERICTAPE 装置クラスに関連付けられている場合は、そのデバイス・ドライバーを使用することができます。Write Once Read Many (WORM) 装置クラスでは、汎用デバイス・ドライバーはサポートされません。

Linux

IBM Spectrum Protect パススルー・デバイス・ドライバーを使用することができます。IBM Spectrum Protect パススルー・デバイス・ドライバーを使用するには、カーネルをインストールするために、Linux オペレーティング・システムとともに、Linux SCSI 汎用 (sg) デバイス・ドライバーが必要です。

例えば、以下のテープ装置用に IBM Spectrum Protect パススルー・デバイス・ドライバーをインストールすることができます。

ECART  
LTO (IBM 以外)

リストに含まれている、IBM のラベルが付いていない磁気テープ・ドライブを含むすべての SCSI 接続ライブラリーも、IBM Spectrum Protect パススルー・デバイス・ドライバーを使用する必要があります。

Linux オペレーティング・システムが提供する汎用 SCSI テープ (st) デバイス・ドライバを使用することはできません。したがって、GENERICTAPE 装置タイプは、**DEFINE DEVCLASS** コマンドでサポートされません。

**Windows** IBM Spectrum Protect デバイス・ドライバの代わりに、Windows Hardware Qualification Lab によって認定されたデバイス・ドライバを選択できます。Windows Hardware Qualification Lab 認定のデバイス・ドライバは、IBM 以外のラベルを持つ装置および IBM 以外の磁気テープ・ドライブにのみ使用することができます。Windows Hardware Qualification Lab 認定のデバイス・ドライバの場合、IBM Spectrum Protect SCSI パススルー・デバイス・ドライバまたは Windows テープ・デバイス・ドライバのいずれかを選択できます。SCSI パススルー・デバイス・ドライバを使用する場合、**DEFINE DEVCLASS** コマンドで装置クラスに GENERICTAPE を指定することはできません。Windows テープ・デバイス・ドライバを使用する場合、装置クラスは GENERICTAPE でなければなりません。

## テープ装置の特殊ファイル名

サーバーがテープ、メディア・チェンジャー、または取り外し可能メディア装置を処理するには、テープ装置に特殊なファイル名が必要です。

### AIX

装置が正常に構成されると、論理ファイル名が戻されます。78 ページの表 19 は、ドライブまたはライブラリーに対応する装置の名前 (特殊ファイル名とも呼ばれます) を示します。装置の特殊ファイル名を得るには、**SMIT** オペレーティング・システム・コマンドを使用できます。例では、x は 0 以上の整数を指定します。

表 19. 装置の例

装置	装置の例	論理ファイル名
IBM Spectrum Protect デバイス・ドライバで利用できる磁気テープ・ドライブ。	/dev/mtx	mtx
IBM テープ・デバイス・ドライバで利用できる磁気テープ・ドライブ。	/dev/rmtx	rmtx
IBM AIX の汎用テープ・デバイス・ドライバで利用できる磁気テープ・ドライブ。	/dev/rmtx	rmtx
IBM Spectrum Protect デバイス・ドライバで利用できるライブラリー装置。	/dev/lbx	lbx
IBM テープ・デバイス・ドライバで利用できるライブラリー装置。	/dev/smcx	smcx

### Linux

装置が正常に構成されると、論理ファイル名が戻されます。78 ページの表 20 は、ドライブまたはライブラリーに対応する装置の名前 (特殊ファイル名とも呼ばれます) を示します。例では、x は 0 以上の整数を指定します。

表 20. 装置の例

装置	装置の例	論理ファイル名
IBM Spectrum Protect パススルー・デバイス・ドライバで利用できる磁気テープ・ドライブ。	/dev/tsm SCSI /mtx	mtx
IBM lin_tape デバイス・ドライバで利用できる磁気テープ・ドライブ。	/dev/IBMtape x	IBMtape x
IBM Spectrum Protect パススルー・デバイス・ドライバで利用できるライブラリー装置。	/dev/tsm SCSI /lbx	lbx

表 20. 装置の例 (続き)

装置	装置の例	論理ファイル名
IBM lin_tape デバイス・ドライバで利用できるライブラリー装置。	/dev/IBMchan gerx	IBMchangerx

## Windows

装置が正常に構成されると、論理ファイル名が戻されます。79 ページの表 21 は、ドライブまたはライブラリーに対応する装置の名前 (特殊ファイル名とも呼ばれます) を示します。例では、*a*、*b*、*c*、*d*、および *x* は 0 以上の整数を指定します。ここで、それぞれの意味は、以下のとおりです。

- *a* は、ターゲット ID を指定します。
- *b* は、LUN を指定します。
- *c* は、SCSI バス ID を指定します。
- *d* は、ポート ID を指定します。

表 21. 装置の例

装置	装置の例	変換された装置名
IBM Spectrum Protect デバイス・ドライバによりサポートされている磁気テープ・ドライブ。	mta.b.c.d	mta.b.c.d
IBM Spectrum Protect パススルー・デバイス・ドライバによりサポートされているテープ装置。	mta.b.c.d	mta.b.c.d
IBM デバイス・ドライバによりサポートされている磁気テープ・ドライブ。	Tapex	mta.b.c.d
IBM Spectrum Protect デバイス・ドライバによりサポートされているライブラリー装置。	lb.a.b.c.d	lba.b.c.d
IBM Spectrum Protect パススルー・デバイス・ドライバによりサポートされているライブラリー装置。	lba.b.c.d	lba.b.c.d
IBM デバイス・ドライバによりサポートされているライブラリー装置。	Changerx	lba.b.c.d

## テープ・デバイス・ドライバのインストールと構成

IBM Spectrum Protect でテープ装置を使用できるようにするには、事前に正しいテープ・デバイス・ドライバをインストールする必要があります。

IBM Spectrum Protect は、IBM テープ・デバイス・ドライバがサポートするすべての装置をサポートしています。ただし、IBM Spectrum Protect は、IBM テープ・デバイス・ドライバがサポートするすべてのオペレーティング・システム・レベルをサポートしているわけではありません。

## IBM テープ装置用の IBM デバイス・ドライバのインストールと構成

IBM テープ装置を使用するための IBM テープ・デバイス・ドライバをインストールおよび構成します。

### このタスクについて

IBM テープ・デバイス・ドライバのインストールおよび構成の説明については、[IBM Tape Device Drivers Installation and User's Guide](#) を参照してください。

## AIX

「*IBM Tape Device Drivers Installation and User's Guide*」で示されたインストール手順を完了すると、インストールするデバイス・ドライバに応じて、異なるメッセージが発行されます。IBM 磁気テ



ープ・ドライブまたはライブラリーのデバイス・ドライバーをインストールする場合、以下のメッセージが返されます。

```
rmtx Available
```

または

```
smcx Available
```

x の値をメモします。この値は、IBM テープ・デバイス・ドライバーによって割り当てられます。ご使用の装置の特殊ファイル名を判別するには、以下のいずれかのコマンドを発行します。

- 磁気テープ・ドライブの場合、`ls -l /dev/rmt*`
- テープ・ライブラリーの場合、`ls -l /dev/smc*`

異なる操作特性を示すために、ファイル名の最後に文字が追加されることがありますが、これらの文字は IBM Spectrum Protect には必要ありません。IBM デバイス・ドライバーの場合は、**DEFINE PATH** コマンドの **DEVICE** パラメーターで基本ファイルを使用して、装置をドライブ (`/dev/rmtx`) またはライブラリー (`/dev/smcx`) に割り当てます。

デバイス・ドライバーをインストールした後、System Management Interface Tool (SMIT) を使用して、IBM 以外の磁気テープ・ドライブおよびテープ・ライブラリーを構成することができます。次の手順を実行してください。

1. SMIT プログラムを実行する。
2. 「装置」をクリックします。
3. 「IBM Spectrum Protect 装置」をクリックします。
4. 「ファイバー・チャネル SAN 接続装置」をクリックします。
5. 「IBM Spectrum Protect によってサポートされる装置の検出 (Discover Devices Supported by IBM Spectrum Protect)」をクリックします。ディスカバリー・プロセスが完了するまで待ちます。
6. 「ファイバー・チャネル SAN 接続装置」メニューに戻り、「検出した装置の属性のリスト」をクリックします。

**Linux** 「IBM Tape Device Drivers Installation and User's Guide」で示されたインストール手順を完了すると、インストールするデバイス・ドライバーに応じて、異なるメッセージが発行されます。IBM LTO または 3592 装置のデバイス・ドライバーをインストールする場合は、次のメッセージが返されます。

```
IBMtapex Available
```

または

```
IBMChangerx Available
```

x の値をメモします。この値は、IBM テープ・デバイス・ドライバーによって割り当てられます。ご使用の装置の特殊ファイル名を判別するには、以下のいずれかのコマンドを発行します。

- 磁気テープ・ドライブの場合、`ls -l /dev/IBMtape*`
- テープ・ライブラリーの場合、`ls -l /dev/IBMChange*`

異なる操作特性を示すために、ファイル名の最後に文字が追加されることがありますが、これらの文字は IBM Spectrum Protect には必要ありません。IBM デバイス・ドライバーの場合は、**DEFINE PATH** コマンドの **DEVICE** パラメーターで基本ファイル名を使用して、装置をドライブ (`/dev/IBMtapex`) またはライブラリー (`/dev/IBMChangerx`) に割り当てます。

**制約事項:** このクラスの装置タイプは、**GENERICTAPE** であってはありません。

**Windows** Windows オペレーティング・システムの場合、IBM Spectrum Protect は、以下の 2 つのデバイス・ドライバーを提供します。

## パススルー・デバイス・ドライバー

テープ装置の製造元が SCSI デバイス・ドライバーを提供している場合、IBM Spectrum Protect パススルー・デバイス・ドライバーをインストールします。

## テープ装置の SCSI デバイス・ドライバー

テープ装置の製造元が SCSI デバイス・ドライバーを提供していない場合、テープ装置用に IBM Spectrum Protect SCSI デバイス・ドライバーをインストールします。ドライバー・ファイル名は `tmsmcsi64.sys` です。

IBM テープ・デバイス・ドライバーのインストールおよび構成手順については、「*IBM Tape Device Drivers Installation and User's Guide*」を参照してください。IBM テープ・デバイス・ドライバーをインストールした後、サーバーは、特殊ファイル名 `TapeX` (IBM 磁気テープ・ドライブの場合) または `ChangerY` (IBM メディア・チェンジャーの場合) を指定します。IBM Spectrum Protect SCSI デバイス・ドライバーまたは IBM Spectrum Protect パススルー・デバイス・ドライバーの場合、Windows オペレーティング・システム・コマンド **regedit** を発行して、デバイスの特殊ファイル名およびドライバーを確認することができます。IBM Spectrum Protect サーバーは、Windows オペレーティング・システムで装置を検査するためのユーティリティも提供します。このユーティリティ **tsmdlst** は、サーバー・パッケージと一緒にパッケージ化されています。このユーティリティを使用するには、以下のステップを実行します。

1. ホスト・バス・アダプターのアプリケーション・プログラミング・インターフェース (API) がインストールされていることを確認します。
2. ホスト・システムから装置情報を取得するには、次のように入力します。

```
tsmdlst
```

## 関連概念

### IBM テープ装置でのマルチパス入出力アクセス

マルチパス入出力は、異なるパス (例えば複数のホスト・バス・アダプター (HBA) やスイッチ) を使用して同じ物理装置にアクセスするための技法です。マルチパス技法を使用すると、単一障害点の発生を避けることができます。

## IBM テープ装置でのマルチパス入出力アクセス

マルチパス入出力は、異なるパス (例えば複数のホスト・バス・アダプター (HBA) やスイッチ) を使用して同じ物理装置にアクセスするための技法です。マルチパス技法を使用すると、単一障害点の発生を避けることができます。

IBM テープ・デバイス・ドライバーは、マルチパス・サポート機能を備えているため、1つのパスに障害が発生しても、サーバーは別のパスを使用してストレージ装置上のデータにアクセスすることができます。障害が起きて、別のパスに遷移したことは、稼働中のサーバーまたはストレージ・エージェントによって認識されることはありません。また、IBM テープ・デバイス・ドライバーは、マルチパス入出力を使用して、入出力パフォーマンスを向上させるための動的ロード・バランシングを行うこともできます。

IBM テープ装置の冗長パスを提供するには、以下のいずれかの構成で各装置を接続します。

- マルチポート・ファイバー・チャンネルの複数のポートに接続します。
- オペレーティング・システムで使用できる場合は、SAS ホスト・バス・アダプターに接続します。
- 別の単一のファイバー・チャンネル・ホスト・バス・アダプターに接続します。

マルチパス入出力が有効である場合に、1つのパスで永続エラー (HBA またはケーブルの誤動作など) が起きると、デバイス・ドライバーにより、代替パスへの自動パス・フェイルオーバーが行われます。

IBM テープ・デバイス・ドライバーは、マルチパス入出力が有効になってから、ホスト・システム上の装置のすべてのパスを検出します。1つのパスが基本パスとして指定され、残りのパスは代替パスとなります。1つの装置の代替パスの最大数は 16 です。IBM テープ・デバイス・ドライバーは、それぞれのパスに対して固有の名前を持つ特殊ファイルを作成します。ドライバーがパスの特殊ファイルを作成するには、システム上にパスが存在していなければなりません。パスが存在しないと、ドライバーは特殊ファイルを作成しません。**DEFINE PATH** コマンドを使用して宛先へのパスを指定する場合は、**DEVICE** パラメーターの値として、基本パスに関連付けられているファイルを指定してください。



AIX では、IBM テープ・デバイス・ドライバーがインストールされても、マルチパス入出力が自動的に有効になることはありません。インストール後に、各論理装置ごとに構成する必要があります。マルチパス入出力は、装置が削除されるか、サポートが構成解除されるまで使用可能状態のままです。構成手順については、「[IBM Tape Device Drivers Installation and User's Guide](#)」を参照してください。

特殊ファイルの名前を取得するには、**ls -l** コマンド (例えば、**ls -l /dev/rmt\***) を使用します。基本パスおよび代替パスは、以下の例に示すように、**PRI** および **ALT** で識別されます。

```
rmt0 Available 20-60-01-PRI IBM 3590 Tape Drive and Medium Changer (FCP)
rmt1 Available 30-68-01-ALT IBM 3590 Tape Drive and Medium Changer (FCP)
```

この例では、以下のパスが IBM 3590 磁気テープ・ドライブと関連付けられます。

- 20-60-01-PRI
- 30-68-01-ALT

基本パスに関連付けられている特殊ファイルの名前は **/dev/rmt0** です。**DEFINE PATH** コマンドの **DEVICE** パラメーターの値として、**/dev/rmt0** を指定します。

特定の磁気テープ・ドライブのパスに関する詳細を表示するには、**itdt -f /dev/rmtx path** コマンドを使用することもできます。ここで、**x** は構成済み磁気テープ・ドライブの番号です。特定のメディア・チェンジャーのパスに関する詳細を表示するには、**itdt -f /dev/smcy path** コマンドを使用します。ここで、**y** は構成済みメディア・チェンジャーの番号です。

#### Linux

Linux では、デバイス・ドライバーがインストールされても、メディア・チェンジャーおよび磁気テープ・ドライブに対するマルチパス入出力が自動的に有効になることはありません。マルチパス入出力の構成手順については、「[IBM Tape Device Drivers Installation and User's Guide](#)」を参照してください。

マルチパス入出力が論理装置に対して有効な場合は、その装置が削除されるか、サポートが構成解除されるまで有効なままです。

IBM 磁気テープ・ドライブおよびメディア・チェンジャーの特殊ファイルの名前を表示するには、**ls -l /dev/IBMx** コマンドを使用します。ここで、**x** は装置の索引番号です。磁気テープ・ドライブに対して **cat /proc/scsi/IBMtape** コマンドを入力することもできます。IBMtape ファイルに示されているように、基本パス、および代替パスは、「Primary」および「Alternate」として識別されます。

Number	Model	SN	HBA	F0 Path
0	03592	IBM1234567	qla2xxx	Primary
1	03592	IBM1234567	qla2xxx	Alternate

この磁気テープ・ドライブの基本パスに関連付けられている特殊ファイルの名前は **/dev/IBMtape0** です。この装置に対する **DEFINE PATH** コマンドの **DEVICE** パラメーターの値として、**/dev/IBMtape0** を指定します。

システムに構成されているすべてのメディア・チェンジャーの基本パスに関連付けられた特殊ファイル名を取得するには、**cat /proc/scsi/IBMchanger** コマンドを実行します。以下の例は、IBMchanger ファイルから取ったものです。

Number	Model	SN	HBA	F0 Path
3	03584L22	IBM1002345	qla2xxx	Primary
4	03584L22	IBM1002345	qla2xxx	Alternate

このメディア・チェンジャーの基本パスに関連付けられている特殊ファイルの名前は **/dev/IBMchanger3** です。この装置に対する **DEFINE PATH** コマンドの **DEVICE** パラメーターの値として、**/dev/IBMchanger3** を指定します。

このシステムにある特定の磁気テープ・ドライブのパスに関する詳細を表示するには、**itdt -f /dev/IBMTapex path** コマンドを使用します。ここで、**x** は構成済みテープ装置の番号です。このシステムにある特定のメディア・チェンジャーのパスに関する詳細を表示するには、**itdt -f /dev/IBMchangerx path** コマンドを使用します。ここで、**x** は構成済みメディア・チェンジャーの番号です。

## Windows

Windows では、デバイス・ドライバがインストールされても、メディア・チェンジャーおよび磁気テープ・ドライブに対するマルチパス入出力が自動的に有効になることはありません。マルチパス入出力の構成手順については、「[IBM Tape Device Drivers Installation and User's Guide](#)」を参照してください。マルチパス入出力が構成されている場合、装置には、2つの一致する装置名が異なるロケーションにあります。基本パスおよび代替パスの詳細情報を取得するには、IBM テープ診断ツールを実行して **qrypath** 機能を使用します。出力は、以下の例のようになります。

```
C:\Users\Administrator\Downloads\ITDT> .\itdt.exe qrypath -f ¥¥.¥Tape0
Querying SCSI paths...
Total paths configured..... 2

Alternate Path
Logical Device..... Tape0
Serial Number..... 0000078F7612
SCSI Host ID..... 8
SCSI Channel..... 0
Target ID..... 3
Logical Unit..... 0
Path Enabled..... Yes

Primary Path
Logical Device..... Tape0
Serial Number..... 0000078F7612
SCSI Host ID..... 8
SCSI Channel..... 0
Target ID..... 1
Logical Unit..... 0
Path Enabled..... Yes

Exit with code: 0
```

## AIX

### AIX システムでのテープ・デバイス・ドライバの構成

AIX システムに IBM 以外のテープ・デバイス・ドライバをインストールおよび構成する手順を確認します。

#### このタスクについて

IBM テープ・デバイス・ドライバのインストールおよび構成手順については、「[IBM Tape Device Drivers Installation and User's Guide](#)」を参照してください。

## AIX

### SCSI 装置およびファイバー・チャネル装置

IBM Spectrum Protect 装置定義メニューおよび SMIT のプロンプトにより、SCSI 接続装置およびファイバー・チャネル (FC) 接続装置の両方の管理が可能になります。

IBM Spectrum Protect のメインメニューには、次の 2 つのオプションがあります。

#### SCSI 接続装置

このオプションを使用して、ホストの SCSI アダプターに接続される SCSI 装置を構成します。

#### ファイバー・チャネル・システム・エリア・ネットワーク (SAN) 接続装置

このオプションを使用して、ホストの FC アダプターに接続される装置を構成します。次の属性のいずれかを選択してください。

#### 検出した装置の属性のリスト

現行の ODM データベースに認識される装置の属性をリストします。

- FC ポート ID:

24 ビット FC ポート ID (N(L)\_Port または F(L)\_Port) です。これは、装置が接続される関連トポロジー内で固有のアドレス ID です。スイッチ環境またはファブリック環境では、スイッチにより決定され、上位 2 バイトはゼロ以外の値です。専用アービトレーテッド・ループでは、上位 2 バイトがゼロのアービトレーテッド・ループ物理アドレス (AL\_PA) です。AL\_PA またはポート ID がどのように割り当てられているかを確認するには、FC ベンダーにご相談ください。

- マップされた LUN ID:

FC から SCSI へのブリッジ (コンバーター、ルーター、またはゲートウェイとも呼ばれる) のボックスです。LUN がどのようにマップされるかについては、ブリッジ・ベンダーにご相談ください。LUN マップ ID を変更しないでください。

- **WW 名:**

装置が接続されるポートのワールド・ワイド名。ブリッジまたはネイティブ FC 装置などの FC コンポーネントのベンダーによって割り当てられる、64 ビットの固有 ID です。ポートの WWN を確認するには、FC ベンダーにご相談ください。

- **製品 ID:**

装置の製品 ID。製品 ID を判別するには、装置ベンダーにご相談ください。

### **IBM Spectrum Protect によってサポートされる装置のディスカバー**

このオプションにより、IBM Spectrum Protect でサポートされる FC SAN 上の装置がディスカバーされ、それらが使用可能にされます。既存の SAN 環境に対して装置が追加されるか、または取り外される場合は、このオプションを選択することによって再ディスカバーされます。装置属性の現行値が「検出した装置の属性のリスト」オプションで表示されるように、装置は最初にディスカバーする必要があります。FC SAN 上でサポートされる装置は、磁気テープ・ドライブおよびオートチェンジャーです。IBM Spectrum Protect デバイス・ドライバーでは、ディスクなどのその他の装置タイプはすべて無視されます。

### **定義されたすべての装置の除去**

このオプションにより、ODM データベースでの状態が DEFINED である FC SAN 接続の IBM Spectrum Protect 装置がすべて除去されます。必要に応じて、すべての定義済み装置の除去の後で、「IBM Spectrum Protect でサポートされる装置の検出」オプションを選択して装置を再ディスカバーします。

### **装置の除去**

このオプションにより、ODM データベースでの状態が DEFINED である FC SAN 接続の単一の IBM Spectrum Protect 装置が除去されます。必要に応じて、定義済み装置の除去の後で、「IBM Spectrum Protect でサポートされる装置の検出」オプションを選択して装置を再ディスカバーします。

## **AIX オートチェンジャーの IBM Spectrum Protect デバイス・ドライバーの構成**

IBM 以外のライブラリーのオートチェンジャー用の IBM Spectrum Protect デバイス・ドライバーを構成するには、次の手順を実行します。

### **手順**

SMIT プログラムを実行して、各オートチェンジャーまたはロボットのための デバイス・ドライバーを構成してください。

1. 「装置」を選択する。
2. **IBM Spectrum Protect** 「装置」を選択する。
3. 「ライブラリー/メディア・チェンジャー」を選択する。
4. 「ライブラリー/メディア・チェンジャーの追加」を選択する。
5. 任意の IBM Spectrum Protect サポートのライブラリーに対して IBM Spectrum Protect-SCSI-LB を選択する。
6. 装置を接続する親アダプターを選択する。この番号は、形式 00-0X で示され、X は SCSI アダプター・カードのスロット番号位置です。
7. プロンプトが出たら、インストールする装置の CONNECTION アドレスを入力する。接続アドレスは 2 桁の数字です。最初の数字は SCSI ID (ワークシートに記録しておいた値) です。2 番目の数字は装置の SCSI 論理装置番号 (LUN) で、特に記されていない限り、通常はゼロです。SCSI ID と LUN は、コンマ (,) で分離する必要があります。  
例えば、接続アドレス 4,0 は SCSI ID=4 および LUN=0 を持ちます。
8. 「実行 (DO)」をクリックします。

「1bX 使用可能」という形式のメッセージ (論理ファイル名) が出されます。X は、システムが自動的に割り当てる数字であることに注意してください。この情報を使用して、ワークシートの「装置名」フィールドを完成します。

例えば、メッセージが「1b0 使用可能」の場合、ワークシートの「装置名」フィールドは /dev/1b0 となります。SMIT が提供する名前には、常に接頭部 /dev/ を使用してください。

## **AIX** 磁気テープ・ドライブの IBM Spectrum Protect デバイス・ドライバー

ベンダーから取得したライブラリーのオートチェンジャー用の IBM Spectrum Protect デバイス・ドライバーを構成するには、次の手順を実行します。

### 手順

**重要:** IBM Spectrum Protect は、*tar* テープおよび *dd* テープを上書きすることはできませんが、*tar* あるいは *dd* は、IBM Spectrum Protect テープを上書きすることができます。

**制約事項:** 磁気テープ・ドライブは、ドライブが定義されていないとき、または サーバーが開始されていないときにのみ共用することができます。IBM Spectrum Protect と AIX の両方が同一のドライブを共用していると、**MKSYSB** コマンドは働きません。オペレーティング・システムの固有のテープ・デバイス・ドライバーを SCSI ドライブと一緒に使用するには、その装置を最初に AIX に対して構成し、次に IBM Spectrum Protect に対して構成する必要があります。これらの固有のデバイス・ドライバーに関しては、AIX の資料を参照してください。

SMIT プログラムを実行して、各ドライブ (ライブラリー内のドライブも含む) のためのデバイス・ドライバーを構成してください。

1. 「装置」を選択する。
2. **IBM Spectrum Protect** 「装置」を選択する。
3. 「テープ装置」を選択します。
4. 「テープ装置の追加 (Add a Tape Drive)」を選択します。
5. サポートされている任意の磁気テープ・ドライブに対して IBM Spectrum Protect-SCSI-MT を選択します。
6. 装置を接続するアダプターを選択する。この番号は、形式 00-0X で示され、X は SCSI アダプター・カードのスロット番号ロケーションです。
7. プロンプトが出たら、インストールする装置の CONNECTION アドレスを入力する。接続アドレスは 2 桁の数字です。最初の数字は SCSI ID (ワークシートに記録しておいた値) です。2 番目の数字は装置の SCSI 論理装置番号 (LUN) で、特に記されていない限り、通常はゼロです。SCSI ID と LUN は、コンマ (,) で分離する必要があります。  
例えば、接続アドレス 4,0 は SCSI ID=4 および LUN=0 を持ちます。
8. 「実行 (DO)」をクリックします。以下のようなメッセージが表示されます。

磁気テープ・ドライブのためにデバイス・ドライバーを構成している (ただし、IBM 磁気テープ・ドライブを除く) 場合は、「mtX 使用可能」の形式のメッセージ (論理ファイル名) が出されます。X は、システムが自動的に割り当てる数字であることに注意してください。この情報を使用して、ワークシートの「装置名」フィールドを完成します。

例えば、メッセージが「mt0 使用可能」の場合、ワークシートの「装置名」フィールドは /dev/mt0 となります。SMIT が提供する名前には、常に接頭部 /dev/ を使用してください。

## **AIX** ファイバー・チャネル SAN 接続装置の構成

ファイバー・チャネル SAN 接続装置を構成するには、以下の手順を実行します。

### 手順

1. SMIT プログラムを実行する。
2. 「装置」を選択する。
3. **IBM Spectrum Protect** 「装置」を選択する。

4. 「ファイバー・チャンネル SAN 接続装置」を選択する。
5. 「IBM Spectrum Protect でサポートされる装置の検出」を選択する。 ディスカバリー・プロセスには多少の時間がかかることがあります。
6. 「ファイバー・チャンネル」メニューに戻り、「検出した装置の属性のリスト」を選択する。
7. 3 文字の装置 ID を確認する。これは、装置へのパスを IBM Spectrum Protect に定義する時に使用します。  
例えば、磁気テープ・ドライブが mt2 という ID を持つ場合は、装置名として /dev/mt2 を指定します。

## Linux Linux システムでのテープ・デバイス・ドライバーの構成

Linux システムでテープ・デバイス・ドライバーをインストールおよび構成する場合は、以下のトピックを確認してください。

### Linux テープおよびライブラリー用の IBM Spectrum Protect パススルー・ドライバーの構成

IBM Spectrum Protect Linux パススルー・ドライバーを使用するためには、以下のステップを実行する必要があります。

#### 手順

1. デバイスがシステムに接続され、電源がオンで、活動状態であることを確認します。
2. 次のコマンドを出して、ご使用のシステムにデバイスが正しく検出されているか検査する。

```
cat /proc/scsi/scsi
```

3. IBM Spectrum Protect デバイス・ドライバー・パッケージ (tsmcscli) およびストレージ・サーバー・パッケージの両方がインストールされていることを確認する。
4. IBM Spectrum Protect デバイス・ドライバー・パッケージには、autoconf および tsmcscli の 2 つのドライバー構成方法があります。これらの方法はどちらも、以下のタスクを実行します。
  - Linux SCSI 汎用ドライバー (sg) をカーネルへロードする。
  - パススルー・ドライバ用に必要な特殊ファイルを作成する。
  - 装置情報ファイルをテープ装置 (/dev/tsmcscli/mtinfo) およびライブラリー (/dev/tsmcscli/lbinfo) 用に作成する。
5. IBM Spectrum Protect パススルー・ドライバーとして選択した構成方法 (autoconf または tsmcscli) を実行します。
  - autoconf による構成方法を実行するには、以下のコマンドを発行します。

```
autoconf
```

- tsmcscli による構成方法を実行するには、以下のステップを実行します。
  - a. インストール・ディレクトリーにある 2 つのサンプル構成ファイルを *mt.conf.smp* および *lb.conf.smp* から *mt.conf* および *lb.conf* にそれぞれコピーする。
  - b. *mt.conf* および *lb.conf* の各ファイルを編集します。各 SCSI ターゲットごとに SCSI ID と LUN の組み合わせのスタンザ (ファイルの先頭に例が示されています) を 1 つ追加します。各 SCSI ターゲット ID および LUN 項目の組み合わせは、構成する磁気テープ・ドライブまたはライブラリーに対応します。ファイルがこれらの要件を満たしていることを確認してください。
    - ファイルの先頭にある例を削除します。
    - 各スタンザの間には改行が必要です。
    - 最後のスタンザの後には改行が 1 つ必要です。
    - 必ず、どちらのファイルにも番号記号 (#) がないようにします。



- c. デバイス・ドライバーのインストール・ディレクトリーから `tsmcscli` スクリプトを実行する。
6. テープ装置 (`/dev/tsmcscli/mtinfo`) およびライブラリー (`/dev/tsmcscli/lbinfo`) 用のテキスト・ファイルを表示して、装置が正しく構成されたか検査する。
7. 磁気テープ・ドライブおよびライブラリーの特殊ファイル名を判別する。
- テープ装置の名前を判別するには、次のコマンドを出します。

```
> ls /dev/tsmcscli/mt*
```

- ライブラリーの名前を判別するには、次のコマンドを出します。

```
> ls /dev/tsmcscli/lb*
```

この情報は、**DEFINE PATH** コマンドを発行するときにサーバーに指定する特殊ファイル名が、`/dev/tsmcscli/mtx` と `/dev/tsmcscli/lbx` のどちらであることを識別するのに役立ちます。

## 次のタスク

ホスト・システムを再始動する場合、`autoconf` スクリプトまたは `tsmcscli` スクリプトを再実行して、IBM Spectrum Protect 装置を再構成する必要があります。IBM Spectrum Protect サーバー・インスタンスを再始動する場合、装置を再構成する必要はありません。一般的に、Linux SCSI 汎用ドライバーは、カーネルにプリインストールされます。カーネル内にドライバーがあることを確認するには、次のコマンドを発行します。

```
> lsmod | grep sg
```

ドライバーがカーネル内にない場合は、`modprobe sg` コマンドを発行して、`sg` ドライバーをカーネルにロードします。

## Linux zSeries Linux ファイバー・チャネル・アダプター (zfcp) デバイス・ドライバーのインストール

zSeries Linux ファイバー・チャネル・アダプター (zfcp) デバイス・ドライバーは、IBM zSeries システム上での特殊なアダプター・ドライバーです。

## このタスクについて

IBM Spectrum Protect および IBM テープ装置デバイス・ドライバーは、64 ビット環境の Linux オペレーティング・システムを搭載した zSeries プラットフォームで実行することができ、ファイバー・チャネル・インターフェースを備えたほとんどの相手先商標製造会社 (OEM) および IBM テープ装置をサポートします。

zfcp ドライバーについて詳しくは、IBM Redpaper の「*Getting Started with zSeries Fibre Channel Protocol*」(IBM Redbooks® から入手可能) を参照してください。

## 手順

1. `qdio` モジュールをロードします。
2. `zfcp` ドライバーをインストールします。
3. ファイバー・チャネル・プロトコル (FCP) をマップし、`zfcp` ドライバーを構成します。
4. IBM テープ・デバイス・ドライバーをインストールして構成します。

## Linux システムの SCSI 装置に関する情報

システムにより認識されるデバイスの情報は、`/proc/scsi/scsi` ファイルに記述されています。このファイルには、検出されたすべての SCSI 装置のリストが格納されています。

ホスト番号、チャネル番号、SCSI ID、論理装置番号 (LU)、ベンダー、ファームウェア、レベル、装置タイプ、SCSI モードという装置情報を知ることができます。例えば、複数の StorageTek および IBM ライブラ

リー、1つの SAN Gateway、複数の Quantum DLT ドライブを含むシステムの場合、`/proc/scsi/scsi` ファイルには以下のような情報が記述されます。

```
Attached devices:
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: STK      Model: 9738      Rev: 2003
  Type: Medium Changer      ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor: PATHLIGHT Model: SAN Gateway      Rev: 32aC
  Type: Unknown      ANSI SCSI revision: 03
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor: QUANTUM Model: DLT7000      Rev: 2560
  Type: Sequential-Access      ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 04
  Vendor: IBM      Model: 7337      Rev: 1.63
  Type: Medium Changer      ANSI SCSI revision: 02
```

## Linux 磁気テープ・ラベルの上書きの防止

IBM Spectrum Protect パススルー・デバイス・ドライバーは、Linux SCSI 汎用デバイス・ドライバー (sg) を使用して、システムに接続されているテープ装置を制御および操作します。Linux 汎用 SCSI テープ装置 (st) がカーネルにロードされて、接続されているテープ装置を構成すると、汎用 sg ドライバーと st ドライバーが両方とも同じ装置を制御できるために、装置の管理方法に関して競合が発生する可能性があります。

### このタスクについて

st ドライバーが、IBM Spectrum Protect によって使用される装置を制御すると、IBM Spectrum Protect 内部磁気テープ・ラベルが上書きされて、データが消失する可能性があります。アプリケーションが st ドライバーを使用して装置を制御し、non-rewind オプションが指定されていない場合は、操作が完了すると、テープが自動的に巻き戻されます。自動巻き戻し操作を実行すると、テープ・ヘッダーの位置が、テープの先頭に再配置されます。テープをドライブにロードしたままにすると、磁気テープ・ラベルがテープの先頭にあるため、次の非 IBM Spectrum Protect 書き込み操作によって、IBM Spectrum Protect の磁気テープ・ラベルが上書きされます。

IBM Spectrum Protect のラベルが上書きされてデータが消失しないようにするためには、IBM Spectrum Protect パススルー・ドライバーのみが、IBM Spectrum Protect の使用する装置を制御するようにしてください。カーネルから st ドライバーを除去してください。あるいは、そのドライバーがシステム上の一部のアプリケーションによって使用されている場合は、st ドライバーがそれらのファイルを制御できなくなるように、IBM Spectrum Protect 装置に対応する特殊ファイルを削除してください。

IBM テープ・デバイス・ドライバーを使用してシステム上の装置を制御している場合は、デバイス・ドライバーの制御の競合に関して同じ問題が発生する可能性があります。この問題を解決し、データ損失を防ぐ方法を確認するには、IBM テープの資料を参照してください。

#### st ドライバーの除去

システムに st 装置を使用しているアプリケーションが他にない場合は、カーネルから st ドライバーを除去してください。st ドライバーをアンロードするには、以下のコマンドを実行します。

```
rmmod st
```

#### IBM Spectrum Protect 装置に対応する、装置の特殊ファイルの削除

st ドライバーの使用が必要なアプリケーションがある場合は、IBM Spectrum Protect デバイスに対応する特殊ファイルを削除します。これらの特殊ファイルは、st ドライバーによって生成されます。これらのファイルが削除されると、st ドライバーは、対応する IBM Spectrum Protect 装置を制御できなくなります。磁気テープ・ドライブの装置の特殊ファイル名は、`/dev/` ディレクトリーに表示されます。これらのファイル名の形式は、`/dev/[n]st[0-1024][l][m][a]` です。

ls コマンドを使用して、st ドライブの特殊ファイル名と IBM Spectrum Protect 装置の特殊ファイル名をリストします。装置シーケンスの出力に基づいて、IBM Spectrum Protect 装置リスト内の装置に一致する装置を st 装置リストで見つけることができます。それから、rm コマンドを使用して、st 装置を削除できます。



st 装置および IBM Spectrum Protect 装置をリストするには、以下のコマンドを発行します。

```
ls -l /dev/*st*  
ls -l /dev/tsm SCSI/mt*
```

rm コマンドを使用して st 装置を削除します。

```
rm /dev/*st*
```

## Windows Windows システムでのテープ・デバイス・ドライバの構成

Windows システムでテープ装置およびライブラリーのドライバーをインストールして構成する手順を確認してください。

### Windows テープ装置およびライブラリーに IBM Spectrum Protect パススルー・ドライバーを使用するための準備

テープ装置およびライブラリーに IBM Spectrum Protect Windows パススルー・ドライバーを使用するには、ドライバーをインストールして、サーバーで使用する装置名を取得する必要があります。

#### 始める前に

1. テープ装置またはテープ・ライブラリーの製造元がデバイス・ドライバーを提供しているかどうかを判別します。
2. 製造元がデバイス・ドライバー・パッケージを提供している場合は、パッケージをダウンロードしてインストールします。
3. 製造元の指示に従って SCSI デバイス・ドライバーを構成します。

#### 手順

1. IBM Spectrum Protect パススルー・デバイス・ドライバーをインストールします。
2. 以下のいずれかのアクションを実行して、サーバーが使用する必要がある装置名を取得します。
  - サーバー上で、**QUERY SAN** コマンドを実行します。出力には、すべての装置名とそれらに関連付けられた装置シリアル番号が表示されます。
  - サーバー・ディレクトリー内で、**tsmdlst.exe** ユーティリティーを実行します。出力には、すべての装置名、それらに関連付けられたシリアル番号、および関連付けられた装置ロケーションが表示されます。
  - Windows システムのコマンド・プロンプトで、**regedit** コマンドを実行します。出力を参照して、装置ロケーションに基づいて装置ファイル名を確認します。ロケーションは、ポート ID、SCSI バス ID、LUN ID、および SCSI ターゲット ID から構成されます。IBM Spectrum Protect 装置ファイル名の形式は、mtA.B.C.D (テープ・ドライブの場合) および lbA.B.C.D (テープ・ライブラリーの場合) です。ここで、各値は以下のとおりです。
    - A は SCSI ターゲット ID です。
    - B は LUN ID です。
    - C は SCSI バス ID です。
    - D はポート ID です。

## Windows テープ装置およびライブラリー用の IBM Spectrum Protect SCSI ドライバーの構成

磁気テープ・ドライブまたはテープ・ライブラリーの製造元が SCSI デバイス・ドライバーを提供していない場合、IBM Spectrum Protect SCSI デバイス・ドライバー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

IBM Spectrum Protect SCSI デバイス・ドライバーのファイル名は `tsmscsi64.sys` です。

### 手順

1. 装置マネージャー・コンソール (`devmgmt.msc`) で装置を検索し、装置を選択します。磁気テープ・ドライブは「**磁気テープ・ドライブ**」の下にリストされ、メディア・チェンジャーは「**メディア・チェンジャー**」の下にリストされます。
2. 以下のように、`tsmscsi64.sys` デバイス・ドライバーで使用する装置を構成します。
  - a. 装置を右クリックし、「**ドライバー・ソフトウェアの更新 (Update Driver Software)**」をクリックします。
  - b. 「**コンピュータを参照してドライバソフトウェアを検索します**」をクリックします。
3. 「**コンピュータ上の装置 ドライバの一覧から選択します**」をクリックします。
4. 「**次へ**」をクリックします。
5. 以下の適切なオプションを選択します。
  - a. テープ・ドライブについては、「**テープ・ドライブ用の IBM Spectrum Protect**」を選択します。
  - b. メディア・チェンジャーについては、「**メディア・チェンジャー用の IBM Spectrum Protect**」を選択します。
6. 「**次へ**」をクリックします。
7. 「**クローズ**」をクリックします。
8. 以下のように、`tsmscsi64` デバイス・ドライバーに対して装置が正しく構成されていることを確認します。
  - a. 装置を右クリックし、「**プロパティ**」をクリックします。
  - b. 「**ドライバー**」タブをクリックし、「**ドライバーの詳細**」をクリックします。「**ドライバーの詳細**」ウィンドウに装置を制御するデバイス・ドライバーが表示されます。

## サーバーで使用するライブラリーの構成

1 つ以上のライブラリーを IBM Spectrum Protect サーバーのストレージ用に使用するには、最初にサーバー・システム上で装置をセットアップする必要があります。

### 始める前に

1. 装置をサーバー・ハードウェアに接続します。75 ページの『[ユーザーのシステムへの自動ライブラリー装置の接続](#)』の指示に従ってください。
2. テープ・デバイス・ドライバーを選択します。76 ページの『[テープ・デバイス・ドライバーの選択](#)』の指示に従ってください。
3. テープ・デバイス・ドライバーをインストールして構成します。79 ページの『[テープ・デバイス・ドライバーのインストールと構成](#)』の指示に従ってください。
4. ライブラリーをサーバーに定義するために必要な装置名を決めます。78 ページの『[テープ装置の特殊ファイル名](#)』の指示に従ってください。

## 手順

1. ライブラリーおよびサーバーからライブラリーへのパスを定義します。[92 ページの『ライブラリーの定義』](#)の指示に従ってください。
2. そのライブラリーにドライブを定義します。[93 ページの『ドライブの定義』](#)の指示に従ってください。

SCSI ライブラリーの場合、[91 ページの『2』](#)と [91 ページの『3』](#)の両方のステップを実行しなくても、**PERFORM LIBACTION** コマンドを使用してライブラリーのドライブおよびパスを 1 つのステップで定義することができます。**PERFORM LIBACTION** コマンドを使用してライブラリーのドライブおよびパスを定義するには、**SANDISCOVERY** オプションがサポートされて有効にされている必要があります。

3. **DEFINE PATH** コマンドを使用して、サーバーから各ドライブへのパスを定義します。
4. 装置クラスを定義します。[94 ページの『テープ装置クラスの定義』](#)の指示に従ってください。

装置クラスは、ドライブの記録形式を指定し、タイプに応じて分類します。装置クラスに関連付けられたすべてのドライブが、すべてのメディアに対して読み取りおよび書き込みができる場合にのみ、デフォルト値の **FORMAT=DRIVE** を記録形式として使用します。

例えば、Ultrium 第 3 世代と Ultrium 第 4 世代のドライブを混用しているが、Ultrium 第 3 世代のメディアしか持っていないとします。第 4 世代と第 3 世代のドライブは、どちらも第 3 世代のメディアに対して読み取りおよび書き込みを行うことができるため、**FORMAT=DRIVE** を指定することができます。

5. **DEFINE STGPOOL** コマンドを使用して、ストレージ・プールを定義します。

ストレージ・プールを定義するための以下の主な選択項目を考慮してください。

- スクラッチ・ボリュームは、使用可能な空のボリュームです。ストレージ・プール内のスクラッチ・ボリュームの最大数の値を指定した場合、サーバーは、ライブラリー内の使用可能なスクラッチ・ボリュームから選択することができます。

スクラッチ・ボリュームを使用しないことにしている場合は、ストレージ・プールの中で使用されるそれぞれのボリュームを明示的に定義する必要があります。また、スクラッチ・ボリュームが使用されないように、ストレージ・プールを定義するときに **MAXSCRATCH=0** パラメーターを指定します。

- 1 次ストレージ・プールのデフォルトの設定は、グループごとのコロケーションです。コピー・ストレージ・プールおよび活動データ・プールのデフォルト設定では、コロケーションは無効です。サーバーは、コロケーションを使用してクライアント・ノードのグループに属しているすべてのファイル、単一クライアント・ノード、クライアント・ファイル・スペース、あるいはクライアント・ファイル・スペースのグループを最小限の数のボリューム上に保持します。ストレージ・プールでコロケーションが使用不可の状態、クライアントがデータの保管を開始すると、プールのデータを容易に変更して併置されるようにすることはできません。
6. ライブラリー・ボリュームをチェックインし、ラベル付けします。[181 ページの『自動ライブラリーへのボリュームのチェックイン』](#)および [179 ページの『テープ・ボリュームのラベル付け』](#)の手順に従ってください。

ライブラリー内にサーバーが使用可能なボリュームが十分にあることを確認してください。クライアント・バックアップなどの操作中にボリュームが不足しないように、ラベルの付いたボリュームを十分に用意してください。後で行う可能性があるリカバリ操作に備えて、追加のスクラッチ・ボリュームにラベルを付けます。

ボリュームのチェックインとラベル付けの手順は、ライブラリーに含まれているドライブが単一の装置タイプであっても複数の装置タイプであっても同じです。**CHECKIN LIBVOLUME** コマンドを使用して、すでにラベル付けされているボリュームをチェックインすることができます。または、ボリュームのラベル付けとチェックインを 1 つのステップを実行したい場合は、**LABEL LIBVOLUME** コマンドを実行します。

**複数の装置タイプを持つライブラリー**：ライブラリーに複数の装置タイプのドライブがあり、IBM Spectrum Protect サーバーに対して 2 つのライブラリーを定義した場合、定義された 2 つのライブラリーは、1 つの物理ライブラリーを表します。テープ・ボリュームは、定義された各ライブラリーに個別にチェックインする必要があります。ボリュームを正しい IBM Spectrum Protect ライブラリーにチェックインしてください。

## 次のタスク

装置定義を検証して、すべてのものが正しく構成されていることを確認します。各ストレージ・オブジェクトに関する情報を参照するには、**QUERY** コマンドを使用します。

**QUERY DRIVE** コマンドの結果を確認する際に、ドライブの装置タイプが予想していたものであることを確認してください。パスが定義されていない場合、ドライブの装置タイプは **UNKNOWN** と示されます。誤ったパスが使用される場合は、**GENERIC\_TAPE** または別の装置タイプが表示されます。混合メディアを使用する場合は、このステップが特に重要です。

オプションで、ライブラリー共有を構成します。[101 ページの『ライブラリー共有の構成』](#) の指示に従ってください。

### 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[DEFINE STGPOOL \(ストレージ・プール内のボリュームの定義\)](#)

[LABEL LIBVOLUME \(ライブラリー・ボリュームのラベル付け\)](#)

[PERFORM LIBACTION \(ライブラリーのすべてのドライブとパスの定義または削除\)](#)

## テープ装置の定義

データをテープにバックアップまたはマイグレーションするには、事前にサーバーに対してテープ装置を定義する必要があります。

## ライブラリーおよびドライブの定義

テープ・ライブラリーには、1 つ以上の磁気テープ・ドライブを含めることができます。ライブラリー、ドライブ、および IBM Spectrum Protect サーバーへのパスを定義する方法を説明します。

### ライブラリーの定義

ドライブを使用できるようにするには、事前にドライブが属するライブラリーを定義する必要があります。

### 手順

1. **DEFINE LIBRARY** コマンドを使用してライブラリーを定義します。

例えば、IBM TS3500 テープ・ライブラリーがある場合、次のコマンドを使用して、**ROBOTMOUNT** という名前のライブラリーを定義することができます。

```
define library robotmount libtype=scsi
```

ライブラリー共有あるいは LAN フリー・データ移動が必要な場合は、以下の情報を参照してください。

- [101 ページの『ライブラリー共有の構成』](#)
- [120 ページの『LAN フリー・データ移動の構成』](#)

2. **DEFINE PATH** コマンドを使用して、サーバーからライブラリーへのパスを定義します。**DEVICE** パラメーターを指定する場合は、装置の特殊ファイル名を入力します。この名前は、サーバーが磁気テープ・ドライブ、メディア・チェンジャー、および取り外し可能メディア装置と通信するために必要です。装置の特殊ファイル名について詳しくは、[78 ページの『テープ装置の特殊ファイル名』](#) を参照してください。

```
AIX define path server1 robotmount srctype=server desttype=library
device=/dev/lb0
```

```
Linux define path server1 robotmount srctype=server desttype=library
device=/dev/tmscsi/lb0
```

```
Windows define path server1 robotmount srctype=server desttype=library
device=lb0.0.1.0
```

## 関連情報

[DEFINE LIBRARY \(ライブラリーの定義\)](#)

[DEFINE PATH \(パスの定義\)](#)

## SAN 上の SCSI ライブラリーの定義

SAN 上の SCSI タイプのライブラリーの場合、サーバーはライブラリーのシリアル番号を追跡できます。パスの定義時またはサーバーによる装置の使用時に、サーバーはこのシリアル番号を使用して装置を識別できます。

## このタスクについて

サーバーに対してライブラリーを定義するときに、必要に応じてシリアル番号を指定できます。便宜上、デフォルトではパスの定義時にサーバーがライブラリーからシリアル番号を取得することが許可されています。

シリアル番号を指定すると、ライブラリーへのパスを定義するときに、サーバーによりシリアル番号が正しいことが確認されます。パスの定義時に **AUTODETECT=YES** パラメーターを設定すると、シリアル番号がライブラリーの定義時に入力したシリアル番号と一致しない場合、サーバーによってシリアル番号が修正されます。ベスト・プラクティスとして、**AUTODETECT=YES** パラメーターを指定して、パスの定義時にデータベース内のドライブのシリアル番号が自動的に更新されるようにします。

ライブラリーの機能によっては、シリアル番号を自動的に検出できない場合があります。サーバーなどのアプリケーションによってプロンプトで要求されたときに、装置によってはシリアル番号を戻すことができないことがあります。この場合、サーバーはデバイスのシリアル番号を記録しません。このため、パスの定義時またはサーバーによるデバイスの使用時にデバイスを識別できません。詳細については、[131 ページの『SAN 上の装置変更の影響』](#)を参照してください。

## ドライブの定義

ストレージ・ボリュームにアクセスするために使用できるドライブについてサーバーに通知するには、**DEFINE DRIVE** コマンドに続けて **DEFINE PATH** コマンドを出します。

## 始める前に

ドライブ・オブジェクトは、取り外し可能メディアを使用するライブラリー内のドライブ・メカニズムを表します。複数のドライブを備えた装置の場合 (自動ライブラリーを含む)、各ドライブを別々に定義し、それをライブラリーと関連付ける必要があります。ドライブ定義には、SCSI のエレメント・アドレス、テープ・ドライブのクリーニング頻度、およびドライブをオンラインにするかどうかなどの情報を含めることができます。

IBM Spectrum Protect は、スタンドアロンで、あるいは自動ライブラリーの一部として使用できる磁気テープ・ドライブをサポートします。自動ライブラリーを使用してテープ・ソリューションを構成する方法が推奨されます。

## このタスクについて

**DEFINE DRIVE** コマンドを出す場合、次の情報の一部または全部を指定する必要があります。

### ライブラリー名

ドライブがあるライブラリーの名前。

### ドライブ名

ドライブに割り当てられた名前。

### シリアル番号

ドライブのシリアル番号。シリアル番号パラメーターは、SCSI のドライブにのみ適用されます。パスの定義時またはサーバーによる装置の使用時に、サーバーはこのシリアル番号を使用して装置を識別できます。

必要に応じて、シリアル番号を指定できます。デフォルトの場合、サーバーは、パスの定義時にドライブ自体からシリアル番号を取得できます。シリアル番号を指定すると、ドライブへのパスの定義時に、サーバーによってシリアル番号が正しいことが確認されます。パスの定義時に **AUTODETECT=YES**



パラメーターを設定すると、シリアル番号がドライブの定義時に入力したシリアル番号と一致しない場合、サーバーによってシリアル番号が修正されます。ベスト・プラクティスとして、**AUTODETECT=YES** パラメーターを指定して、パスの定義時にデータベース内のドライブのシリアル番号が自動的に更新されるようにします。

ドライブの機能によっては、サーバーがシリアル番号を自動的に検出できない場合があります。この場合、サーバーはデバイスのシリアル番号を記録しません。このため、パスの定義時またはサーバーによるデバイスの使用時にデバイスを識別できません。131 ページの『SAN 上の装置変更の影響』を参照してください。

### エレメント・アドレス

ドライブのエレメント・アドレス。**ELEMENT** パラメーターは、SCSI ライブラリーのドライブにのみ適用されます。エレメント・アドレスは、自動ライブラリー内のドライブの物理ロケーションを示す番号です。サーバーは、ドライブの物理的なロケーションをドライブの SCSI アドレスに結び付けるためにエレメント・アドレスを必要とします。サーバーは、パスの定義時にドライブからエレメント・アドレスを取得することができます。あるいは、ドライブの定義時にエレメント番号を指定することができます。ベスト・プラクティスとして、**ELEMENT=AUTODETECT** パラメーターを指定して、ドライブへのパスの定義時にサーバーが自動的にエレメント番号を検出するようにします。

ライブラリーの機能によっては、サーバーがエレメント・アドレスを自動的に検出できないことがあります。このような状況で、かつライブラリーに複数のドライブがある場合には、ドライブを定義するときにエレメント・アドレスを指定してください。エレメント・アドレスを取得するには、[IBM Support Portal for IBM Spectrum Protect](#) に進みます。

**ヒント :** IBM テープ・デバイス・ドライバーと IBM 以外のテープ・デバイス・ドライバーは、異なる装置ファイルおよびフォーマットを生成します。

- IBM の場合、装置名の先頭は **rmt** で、その後に整数が続きます (例えば、/dev/rmt0)。
- IBM Spectrum Protect テープ・デバイス・ドライバーの場合、テープ装置名の先頭は **mt** で、その後に整数が続きます (例えば、/dev/mt0)。

パスを定義する際には、正しい装置ファイルを使用する必要があります。

### 手順

1. **DEFINE DRIVE** コマンドを発行して、ドライブをライブラリーに割り当てます。
2. サーバーがドライブを使用できるようにするには、**DEFINE PATH** コマンドを発行します。

ライブラリー、パス、およびドライブの構成例については、例: [単一のドライブ装置タイプの SCSI ライブラリーまたは仮想テープ・ライブラリーの構成](#) および 例: [複数のドライブ装置タイプを含む SCSI ライブラリーまたは仮想テープ・ライブラリーの構成](#) を参照してください。

## テープ装置クラスの定義

装置クラスは、ストレージ・プールで作成できる一連のボリュームが使用する特性のセットを定義します。サーバーが確実に装置を使用できるようにするには、テープ装置の装置クラスを定義する必要があります。

### 始める前に

装置クラスを定義する前に、サーバーに対してライブラリーおよびドライブを定義する必要があります。

### このタスクについて

サポートされる装置および有効な装置クラス形式のリストについては、ご使用のオペレーティング・システム用の IBM Spectrum Protect Supported Devices Web サイトを参照してください。

- **Windows** | **AIX** [AIX および Windows でサポートされるデバイス](#)
- **Linux** [Linux でサポートされるデバイス](#)

それぞれの装置タイプに複数の装置クラスを定義することができます。例えば、同じタイプの磁気テープ・ドライブを使用する異なるストレージ・プールに異なる属性を指定する必要があるとします。装置に

固有ではなく、装置の使い方に固有の変量 (例えば、マウント保存や マウント数の限界など) が必要になる場合があります。

#### 指針:

- 1つの装置クラスを複数のストレージ・プールに関連付けることはできますが、各ストレージ・プールが関連付けられる装置クラスは1つのみです。
- SCSI ライブラリーには、複数の装置タイプの磁気テープ・ドライブを含めることができます。この環境で装置クラスを定義するときには、**FORMAT** パラメーターの値を宣言する必要があります。

詳細については、[17 ページの『単一ライブラリーでの混合装置タイプ』](#)を参照してください。

## 手順

装置クラスを定義するには、**DEVTYPE** パラメーターを指定して **DEFINE DEVCLASS** コマンドを使用します。これにより、装置タイプが装置クラスに割り当てられます。

## タスクの結果

DEVCONFIG オプションが `dsmserv.opt` ファイルに含まれていると、このオプションを付けて 指定したファイルは、**DEFINE DEVCLASS**、**UPDATE DEVCLASS**、および **DELETE DEVCLASS** コマンドの結果によって常に自動的に更新されます。

### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[QUERY DEVCLASS \(1 つ以上の装置クラスに関する情報の表示\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## LTO 装置クラスの定義

単一ライブラリー内で異なる世代の LTO ドライブおよびメディアを混用する場合の問題を回避するために、制約事項を確認してください。また、LTO ドライブの暗号化に関する制約事項も確認してください。

## 単一のライブラリー内における LTO ドライブとメディアの混合

異なる世代の LTO ドライブおよびメディアを混用する場合、各世代の読み取り/書き込み機能を考慮する必要があります。各世代のメディアに対して異なる装置クラスを構成する方法が推奨されます。

## このタスクについて

異なる世代の LTO メディアおよびドライブを混用することを検討している場合、以下の制約事項を確認してください。

表 22. 各世代の LTO ドライブの読み取り/書き込み機能									
ドライブ	第 1 世代メディア	第 2 世代メディア	第 3 世代メディア	第 4 世代メディア	第 5 世代メディア	第 6 世代メディア	第 7 世代メディア	第 8 世代メディア	第 9 世代メディア
第 1 世代	読み取り/書き込みアクセス	適用外	適用外	適用外	適用外	適用外	適用外	適用外	適用外
Generation 2	読み取り/書き込みアクセス	読み取り/書き込みアクセス	適用外	適用外	適用外	適用外	適用外	適用外	適用外
第 3 世代	読み取り専用アクセス	読み取り/書き込みアクセス	読み取り/書き込みアクセス	適用外	適用外	適用外	適用外	適用外	適用外
第 4 世代	適用外	読み取り専用アクセス	読み取り/書き込みアクセス	読み取り/書き込みアクセス	適用外	適用外	適用外	適用外	適用外
第 5 世代	適用外	適用外	読み取り専用アクセス	読み取り/書き込みアクセス	読み取り/書き込みアクセス	適用外	適用外	適用外	適用外



表 22. 各世代の LTO ドライブの読み取り/書き込み機能 (続き)									
ドライブ	第 1 世代メディア	第 2 世代メディア	第 3 世代メディア	第 4 世代メディア	第 5 世代メディア	第 6 世代メディア	第 7 世代メディア	第 8 世代メディア	第 9 世代メディア
第 6 世代	適用外	適用外	適用外	読み取り専用アクセス	読み取り/書き込みアクセス	読み取り/書き込みアクセス	適用外	適用外	適用外
第 7 世代	適用外	適用外	適用外	適用外	読み取りアクセス	読み取り/書き込みアクセス	読み取り/書き込みアクセス	適用外	適用外
第 8 世代	適用外	適用外	適用外	適用外	適用外	適用外	読み取り/書き込みアクセス	読み取り/書き込みアクセス	読み取り/書き込みアクセス

## 例

異なるタイプのドライブおよびメディアを混用している場合は、メディアのタイプごとに 1 つずつ、異なる装置クラスを構成します。メディア・タイプを指定するには、各装置クラス定義で **FORMAT** パラメーターを使用します。(FORMAT=DRIVE を指定しないでください。) 例えば、Ultrium 第 5 世代と Ultrium 第 6 世代のドライブを混用する場合、Ultrium 第 5 世代の装置クラスに FORMAT=ULTRIUM5C (または ULTRIUM5) を指定し、Ultrium 第 6 世代の装置クラスに FORMAT=ULTRIUM6C (または ULTRIUM6) を指定します。

この例では、どちらの装置クラスも、Ultrium 第 5 世代と Ultrium 第 6 世代のドライブを使用する同じライブラリーを指すことができます。ドライブは、2 つのストレージ・プール間で共用されます。片方のストレージ・プールが、最初の装置クラスおよび Ultrium 第 5 世代メディアを排他的に使用します。もう片方のストレージ・プールは、2 番目の装置クラスおよび Ultrium 第 6 世代メディアを排他的に使用します。2 つのストレージ・プールが単一のライブラリーを共有するため、マウント・ポイントの処理中に Ultrium 第 6 世代ドライブが使用可能になると、そのドライブに Ultrium 第 5 世代メディアをマウントすることができます。

古い世代の読み取り専用メディアと新しい読み取り/書き込みメディアを単一のライブラリー内で混用する場合、読み取り専用メディアを読み取り専用としてマークし、すべての読み取り専用スクラッチ・メディアをチェックアウトする必要があります。例えば、Ultrium 第 4 世代と Ultrium 第 6 世代のドライブおよびメディアを単一のライブラリー内で混用する場合、第 4 世代のメディアを読み取り専用としてマークする必要があります。さらに、すべての第 4 世代スクラッチ・ボリュームをチェックアウトする必要があります。

## LTO 混合メディア環境でのマウント・リミット

複数の装置クラスが同じライブラリーを指す混合メディア・ライブラリーでは、ストレージ・プール間で共用されるのは互換性のあるドライブです。MOUNTLIMIT パラメーターの値は、装置クラスごとに適切に設定する必要があります。

例えば、Ultrium 第 1 世代ドライブと Ultrium 第 2 世代ドライブおよびメディアを収容する混合メディア・ライブラリーでは、Ultrium 第 1 世代メディアは、Ultrium 第 2 世代ドライブにマウントすることができます。

以下のドライブおよびメディアで構成される混合ライブラリーの例を考えてみます。

- 4 つの LTO Ultrium 第 1 世代ドライブと LTO Ultrium 第 1 世代メディア
- 4 つの LTO Ultrium 第 2 世代ドライブと LTO Ultrium 第 2 世代メディア

以下の装置クラスを作成しました。

- FORMAT=ULTRIUM1C を指定している LTO Ultrium 第 1 世代装置クラス LTO1CLASS
- FORMAT=ULTRIUM2C を指定している LTO Ultrium 第 2 世代装置クラス LTO2CLASS

以下のストレージ・プールも作成しました。

- デバイス・クラス LTO1CLASS を基にした LTO Ultrium 第 1 世代ストレージ・プール LTO1POOL
- デバイス・クラス LTO2CLASS を基にした LTO Ultrium 第 2 世代ストレージ・プール LTO2POOL

各ストレージ・プールで使用可能なマウント・ポイント数は、**MOUNTLIMIT** パラメーターを使用して装置クラスで指定されます。LTO2CLASS 装置クラスの **MOUNTLIMIT** パラメーターは、LTO7 メディアのみをマウントできる使用可能ドライブ数に一致するように、4 に設定する必要があります。LTO1CLASS 装置クラスの **MOUNTLIMIT** パラメーターは、Ultrium 第 1 世代メディアが Ultrium 第 7 世代ドライブにマウントできるという事実に合わせて調整するため、使用可能なドライブの数より大きい値 (5 または可能であれば 6) に設定する必要があります。**MOUNTLIMIT** の最適な値は、ワークロードおよびストレージ・プールのアクセス・パターンによって決まります。

変化するワークロードに適合するように、**MOUNTLIMIT** の設定をモニターして調整します。LTO1POOL の **MOUNTLIMIT** が高く設定されていると、Ultrium 第 2 世代ドライブが Ultrium 第 1 世代マウント要求を満たすために使用されているため、LTO2POOL のマウント要求が遅延を起したり、失敗することがあります。最悪のシナリオでは、Ultrium 第 2 世代ドライブの競合が多すぎるために、第 2 世代メディアのマウントが以下のメッセージを出して失敗することがあります。

ANR8447E 現在、ライブラリーに使用可能なドライブはありません。

LTO1POOL の **MOUNTLIMIT** 値が十分に大きい値に設定されていない場合、LTO Ultrium 第 2 世代ドライブによって満たされる可能性のあるマウント要求が遅延します。

**制約事項:** Ultrium 第 1 世代ドライブを Ultrium 第 2 世代または Ultrium 第 3 世代のドライブと混用する場合、マウント・ポイントが割り振られる方法が原因で、制約事項が適用されます。例えば、Ultrium 第 1 世代および Ultrium 第 2 世代の両方のボリュームを含む複数のマウント・ポイントが必要なプロセスでは、使用可能な Ultrium 第 6 世代ドライブで 1 つのマウントが満たされる場合でも、Ultrium 第 2 世代ドライブのみを予約しようとしします。このような動作を行うプロセスには、**MOVE DATA** コマンドや **BACKUP STGPOOL** コマンドなどがあります。このような場合、必要な数のマウント・ポイントが Ultrium 第 2 世代ドライブで満たされるまで、プロセスは待機します。

#### 関連情報

[BACKUP STGPOOL \(1 次ストレージ・プール・データをコピー・ストレージ・プールにバックアップ\)](#)

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[MOVE DATA \(ストレージ・プール・ボリューム上のファイルの移動\)](#)

### LTO 第 4 世代以降の磁気テープ・ドライブのドライブ暗号化の有効化および無効化

IBM Spectrum Protect は、LTO 第 4 世代以降のドライブで使用可能な 3 つのタイプのドライブ暗号化 (アプリケーション、システム、およびライブラリー) をサポートします。これらの方式は、ハードウェアを通して定義されます。

## このタスクについて

**DEFINE DEVCLASS** コマンドの **DRIVEENCRYPTION** パラメーターは、IBM および HP LTO 第 4 世代以降、Ultrium 4、および Ultrium 4C のフォーマットでドライブ暗号化を許可するかどうかを指定します。このパラメーターを使用することで、IBM Spectrum Protect は、空のボリュームに対するハードウェア暗号化設定との互換性を確保できます。満杯あるいは埋め込み中のストレージ・プール・ボリュームに対してこのパラメーターを使用することはできません。

IBM Spectrum Protect は、IBM および HP LTO-4 以降のドライブでアプリケーション方式の暗号化をサポートします。IBM LTO-4 以降のみが、システム方式とライブラリー方式をサポートします。ライブラリー方式の暗号化は、ご使用のシステム・ハードウェア (例えば、IBM TS3500) がその方式をサポートする場合にのみ使用できます。

**制約事項:** ドライブの暗号化は、write-once read-many (WORM) メディアでは使用できません。

アプリケーション方式は、ハードウェアによって定義されます。IBM Spectrum Protect が暗号鍵を生成および管理するアプリケーションの方式を使用するには、**DRIVEENCRYPTION** パラメーターを ON に設定します。このアクションにより、空のボリュームのデータ暗号化が可能になります。このパラメーターが ON に設定され、ハードウェアが別の方式で暗号化されるように構成されていると、バックアップ操作は失敗します。

## 手順

次の簡単な例では、ストレージ・プール内の空のボリュームに対してデータ暗号化を有効化/無効化するためのステップを示しています。

1. 次のように **DEFINE LIBRARY** コマンドを発行して、ライブラリーを定義します。

```
define library 3584 libtype=SCSI
```

2. 次のように、鍵マネージャーとして IBM Spectrum Protect を指定して **DEFINE DEVCLASS** コマンドを発行し、装置クラス LTO\_ENCRYPT を定義します。

```
define devclass lto_encrypt library=3584 devtype=lto driveencryption=on
```

3. 次のように **DEFINE STGPPOOL** コマンドを発行して、ストレージ・プールを定義します。

```
define stgpool lto_encrypt_pool lto_encrypt
```

4. 新規ボリュームに対して暗号化を無効にするには、**DRIVEENCRYPTION** パラメーターを OFF に設定します。デフォルト値は ALLOW です。別の暗号化方式が有効にされている場合、空のボリュームのドライブ暗号化が許可されます。

## 関連概念

### テープ暗号化方式

使用する暗号化方式の決定は、データの管理方法によって異なります。

## 3592 装置クラスの定義

3592、TS1130、TS1140、TS1150、およびそれ以降の装置の装置クラス定義には、より高速なボリューム・アクセス速度とドライブの暗号化を実現するためのパラメーターが含まれます。異なる世代の 3592 および TS1130 以降のドライブがライブラリー内で混在する場合の問題を回避するには、ガイドラインを確認してください。

### 単一ライブラリー内での複数世代の 3592 ドライブおよびメディアの混用

最良のパフォーマンスを達成するために、1つのライブラリーの中に複数の世代の 3592 メディアを混在しないでください。世代の異なるドライブが混在すると、メディアの問題が発生する場合があります。例えば、IBM Spectrum Protect がボリュームのラベルを読み取れなくなる可能性があります。

## このタスクについて

以下の表は、各ドライブ世代の読み取り/書き込みの相互運用性を示しています。

ドライブ	第 1 世代 フォーマット	第 2 世代 フォーマット	第 3 世代 フォーマット	第 4 世代フォー マット	第 5 世代フォー マット
第 1 世代	読み取り/書き 込みアクセス	適用外	適用外	適用外	適用外
Generation 2	読み取り/書き 込みアクセス	読み取り/書き 込みアクセス	適用外	適用外	適用外
第 3 世代	読み取り専用ア クセス	読み取り/書き 込みアクセス	読み取り/書き 込みアクセス	適用外	適用外
第 4 世代	適用外	読み取り専用	読み取り/書き 込みアクセス	読み取り/書き 込みアクセス	適用外
第 5 世代	適用外	適用外	読み取りアクセ ス	読み取り/書き 込みアクセス	読み取り/書き 込みアクセス

ライブラリー内で複数の世代のドライブを混用する必要がある場合は、問題を回避するために、例および制約事項を確認してください。

表 23. 複数世代のドライブの混合	
ライブラリー・タイプ	例および制約事項
SCSI	<p>最新のドライブ世代用に新規のストレージ・プールおよび装置クラスを定義します。例えば、3592-2 用のストレージ・プールと装置クラスがあると想定します。ストレージ・プールには、第 2 世代のフォーマットで書き込まれたすべてのメディアが含まれます。装置クラス定義の <b>FORMAT</b> パラメーターの値が 3952-2 (<b>DRIVE</b> ではない) に設定されていると想定します。ライブラリーに第 3 世代ドライブを追加します。次の手順を実行してください。</p> <ol style="list-style-type: none"> <li>1. 第 3 世代ドライブ用の新しい装置クラス定義で、<b>FORMAT</b> パラメーターの値を 3592-3 または 3592-3C に設定します。<b>DRIVE</b> を指定しないでください。</li> <li>2. 第 2 世代ドライブと関連付けられたストレージ・プールの定義で、<b>MAXSCRATCH</b> パラメーターを 0 に更新します。例えば、次のようになります。</li> </ol> <pre>update stgpool genpool2 maxscratch=0</pre> <p>この方式では、両方の世代がそれぞれの最適なフォーマットを使用することができ、世代の混用によってメディアの問題が生じる可能性を最小限に抑えます。ただし、すべてのメディアの問題が解決されるわけではありません。例えば、マウント・ポイントの競合およびマウントの失敗が起こる可能性があります。(3592 ドライブおよびメディアのコンテキストにおけるマウント・ポイントの競合について詳しくは、98 ページの『3592 装置クラスの定義』を参照してください。)</p> <p><b>制約事項:</b> 次のリストでは、メディアの制限について説明します。</p> <ul style="list-style-type: none"> <li>• <b>CHECKIN LIBVOL:</b> ここでの問題は、CHECKLABEL=YES オプションの使用に関するものです。ラベルが第 3 世代以降のフォーマットで書き込まれていて、CHECKLABEL=YES オプションを指定した場合、前の世代のドライブではこのコマンドを使用すると障害が発生します。問題を回避するには、CHECKLABEL=BARCODE を指定します。</li> <li>• <b>LABEL LIBVOL:</b> サーバーが前の世代のドライブを使用して第 3 世代以降のフォーマットで書き込まれたラベルを読み取ろうとすると、OVERWRITE=YES を指定しない限り <b>LABEL LIBVOL</b> コマンドは失敗します。OVERWRITE=YES のラベルが付いたメディアに活動データがないことを確認してください。</li> <li>• <b>CHECKOUT LIBVOL:</b> IBM Spectrum Protect が、第 3 世代以降のフォーマットとしてラベルを検査し (CHECKLABEL=YES)、以前の世代のドライブを読み取った場合、コマンドは失敗します。この問題を回避するには、CHECKLABEL=NO を指定します。</li> </ul>

## 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[CHECKOUT LIBVOLUME \(ストレージ・ボリュームのライブラリーからのチェックアウト\)](#)

[LABEL LIBVOLUME \(ライブラリー・ボリュームのラベル付け\)](#)

[UPDATE STGPOOL \(ストレージ・プールの更新\)](#)

## 3592 ボリュームのデータ・アクセス速度の制御

ストレージ容量を最適化し、ボリューム作成時のデータ・アクセス速度を向上させることができます。ボリュームを持つストレージ・プールにデータを分割することで、最大のストレージ容量を提供するように、あるいはボリュームに対する高速アクセスを提供するようにスケール容量パーセンテージを指定することができます。

## このタスクについて

メディア容量を削減するには、**DEFINE DEVCLASS** コマンドを使用して装置クラスを定義する際、あるいは **UPDATE DEVCLASS** コマンドを使用して装置クラスを更新する際に、**SCALECAPACITY** パラメーターを指定します。

20、90、または 100 のいずれかのパーセント値を指定してください。20% の値を指定するとアクセス時間が最も速くなり、100% を指定するとストレージ容量が最大になります。例えば、圧縮せずに 3592 装置クラスに対してスケール容量 20 を指定すると、その装置クラスの 3592 ボリュームは全容量 300 GB の 20% (約 60GB) を保管します。

スケール容量が有効になるのは、データが最初にボリュームに書き込まれる時点のみです。装置クラスを更新してスケール容量を変更しても、既にデータが書き込まれているボリュームは、スクラッチ状況に戻されない限り影響を受けません。

### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## 3592 第 2 世代以降のドライブ暗号化の有効化/無効化

IBM Spectrum Protect では、3592 第 2 世代以降のドライブで、アプリケーション、システム、およびライブラリーの 3 つのドライブ暗号化タイプを使用できます。これらの方式は、ハードウェアを通して定義されます。

## このタスクについて

**DEFINE DEVCLASS** コマンドの **DRIVEENCRYPTION** パラメーターは、3592 第 2 世代以降のドライブでドライブ暗号化を許可するかどうかを指定します。このパラメーターは、IBM Spectrum Protect が空のボリュームに関するハードウェアの暗号化設定と互換性を確保できるように使用します。満杯あるいは埋め込み中のストレージ・プール・ボリュームに対してこのパラメーターを使用することはできません。

- IBM Spectrum Protect が暗号鍵を生成および管理するアプリケーションの方式を使用するには、**DRIVEENCRYPTION** パラメーターを ON に設定します。これにより、空のボリュームに対するデータの暗号化が許可されます。このパラメーターが ON に設定され、ハードウェアが別の方式で暗号化されるように構成されていると、バックアップ操作は失敗します。
- 暗号化のライブラリーまたはシステムの方式を使用するには、このパラメーターを **ALLOW** に設定します。これは、IBM Spectrum Protect はドライブの暗号化の鍵マネージャーではないが、いずれかの他の方式を使用してハードウェアがボリュームのデータを暗号化するのを許可することを指定します。このパラメーターを指定しても、ボリュームは自動的に暗号化されません。**ALLOW** パラメーターを指定して、ハードウェアがこれらの方式のいずれかを使用するように構成することによってのみ、データを暗号化することができます。

**DRIVEENCRYPTION** パラメーターはオプションです。デフォルトでは、ライブラリー方式またはシステム方式の暗号化が許可されます。

## 手順

次の簡単な例では、IBM Spectrum Protect を鍵マネージャーとして使用して、ストレージ・プール内の空のボリュームでデータを暗号化する方法を示しています。

- DEFINE LIBRARY** コマンドを発行して、ライブラリーを定義します。  
例えば、次のコマンドを発行します。

```
define library 3584 libtype=SCSI
```

- DRIVEENCRYPTION** パラメーターに値 ON を指定して **DEFINE DEVCLASS** コマンドを発行することで、装置クラス 3592\_ENCRYPT を定義します。  
例えば、次のコマンドを発行します。

```
define devclass 3592_encrypt library=3584 devtype=3592 driveencryption=on
```



3. 次のようにして、ストレージ・プールを定義します。  
例えば、次のコマンドを発行します。

```
define stgpool 3592_encrypt_pool 3592_encrypt
```

## 次のタスク

新規ボリュームでどの方式の暗号化も無効にするには、**DRIVEENCRYPTION** パラメーターを **OFF** に設定します。ハードウェアがライブラリー方式またはシステム方式によってデータを暗号化するように構成され、**DRIVEENCRYPTION** が **OFF** に設定されていると、バックアップ操作は失敗します。

## ライブラリー共用の構成

ストレージ・エリア・ネットワーク (SAN) を使用すると、複数の IBM Spectrum Protect サーバーがストレージ装置を共有することができます。1つのサーバーをライブラリー・マネージャーとしてセットアップし、別のサーバーをライブラリー・クライアントとしてセットアップします。

### 始める前に

ご使用のシステムが、ライブラリー共用のためのライセンス交付要件を満たしていることを確認してください。SAN 環境内でライブラリー・クライアントまたはライブラリー・マネージャーとして構成されている IBM Spectrum Protect サーバーごとに、IBM Spectrum Protect for SAN のライセンスが必要です。

### このタスクについて

LAN フリー・データ移動を使用すると、IBM Spectrum Protect クライアント・システムは、IBM Spectrum Protect サーバーに対して定義されているストレージ装置に直接アクセスできます。データ移動を実行するために、ストレージ・エージェントがクライアント・システムにインストールされ、構成されます。

ライブラリー共有をセットアップするには、1つの IBM Spectrum Protect サーバーを、ご使用の共有ライブラリー構成のライブラリー・マネージャーとして定義する必要があります。次に、ライブラリー・マネージャーと通信し、ライブラリー・マネージャーにストレージ・リソースを要求するライブラリー・クライアントとして、他の IBM Spectrum Protect サーバーをライブラリー・クライアントとして定義します。ライブラリー・マネージャー・サーバーのバージョンは、ライブラリー・クライアントとして定義されたサーバーと同じまたはそれ以降のバージョンでなければなりません。

### 手順

IBM Spectrum Protect サーバー間で SAN 上のライブラリー・リソースを共有するには、以下のステップを実行します。

1. サーバー間通信をセットアップする。

SAN 上でストレージ装置を共有するには、相互定義機能を使用してサーバーを相互に定義します。各サーバーに、固有の名前がなければなりません。

2. 共有ライブラリーを定義し、サーバー・システムでテープ装置をセットアップします。

90 ページの『サーバーで使用するライブラリーの構成』で説明されている手順を使用して、共有環境で使用するためのライブラリーを定義します。**DEFINE LIBRARY** コマンドに **SHARED=YES** パラメーターを指定して、ライブラリーを共有として定義するように、この手順を変更します。

3. ライブラリー・マネージャー・サーバーを定義します。
4. ライブラリー・クライアントであるサーバー上に共有ライブラリーを定義します。
5. ライブラリー・マネージャー・サーバーで、ライブラリー・クライアントから、ライブラリー・クライアントがアクセスできる各ドライブへのパスを定義します。

装置名は、ライブラリー・クライアント・システムがそのテープ装置を認識する経路を反映している必要があります。ライブラリー・クライアントがテープ装置を使用するには、ライブラリー・マネージャーから各ドライブへのパスが定義されている必要があります。

問題を回避するために、ライブラリー・マネージャーに対して定義されたすべてのドライブ・パス定義が各ライブラリー・クライアントに対しても定義されている必要があります。

例えば、ライブラリー・マネージャーが 3 つの磁気テープ・ドライブを定義する場合、ライブラリー・クライアントも 3 つの磁気テープ・ドライブを定義する必要があります。ライブラリー・クライアントが同時に使用できる磁気テープ・ドライブの数を制限するには、ライブラリー・クライアントで装置クラスの **MOUNTLIMIT** パラメーターを使用します。

#### 6. 共有ライブラリー用の装置クラスを定義します。

同じ装置タイプとライブラリー・パラメーターを使用して複数の装置クラスを定義する際の混乱を避けるために、両方のサーバーで装置クラス名を同一にする方法が推奨されます。データベース・バックアップなどの一部の操作では、装置クラス名を使用してバックアップ用のデータを識別します。

ライブラリー・マネージャーで指定された装置クラス・パラメーターは、ライブラリー・クライアントに対して指定されたパラメーターをオーバーライドします。装置クラス名が異なる場合、ライブラリー・マネージャーは、ライブラリー・クライアントに指定された装置タイプに合致する装置クラスに指定されたパラメーターを使用します。

#### 7. 共有ライブラリー用のストレージ・プールを定義します。

#### 8. 他のサーバーをライブラリー・クライアントとして構成するには、これらのステップを繰り返します。

### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[DEFINE LIBRARY \(ライブラリーの定義\)](#)

[DEFINE STGPOOL \(ストレージ・プール内のボリュームの定義\)](#)

Linux | AIX

## 例: AIX および Linux サーバーのライブラリー共有

AIX システムまたは Linux システム上で稼働するサーバー用に SCSI ライブラリー共有環境をセットアップする方法については、サンプル手順を参照してください。

### このタスクについて

この例では、ASTRO という名前のライブラリー・マネージャー・サーバーと JUDY という名前のライブラリー・クライアントが構成されます。各ステップがどこで実行されるかを明確にするために、コマンドの前に、コマンドが発行される元のサーバー名が付いています。大部分のコマンドはライブラリー・クライアントから発行されます。

SCSI ライブラリーの場合、**libtype=scsi** パラメーターを指定してライブラリーを定義します。

### 手順

1. ASTRO をライブラリー・マネージャー・サーバーとしてセットアップするために、SANGROUP という名前の共有 SCSI ライブラリーを定義します。

例えば次のとおりです。

```
astro> define library sangroup libtype=scsi shared=yes
```

次に、例: [単一のドライブ装置タイプの SCSI ライブラリーまたは仮想テープ・ライブラリーの構成](#)で説明されているとおりに残りのステップを実行して、ライブラリーを構成します。

**ヒント: PERFORM LIBACTION** コマンドを使用すると、ライブラリーのドライブとパスを 1 つのステップで定義することができます。

2. **DEFINE SERVER** コマンドを実行して、ASTRO をライブラリー・マネージャー・サーバーとして定義します。

```
judy> define server astro serverpassword=secret hladdress=192.0.2.24  
lladdress=1777 crossdefine=yes
```

3. **DEFINE LIBRARY** コマンドを実行して、共有ライブラリー SANGROUP を定義します。  
**PRIMARYLIBMANAGER** パラメーターでライブラリー・マネージャー・サーバー名を使用し、**LIBTYPE=SHARED** を使用する必要があります。

```
judy> define library sangroup libtype=shared primarylibmanager=astro
```



このライブラリー名はライブラリー・マネージャーのライブラリー名と一致していなければなりません。

4. **DEFINE PATH** コマンドを実行して、ライブラリー・マネージャー ASTRO から、共有ライブラリー内の2つのドライブへのパスを定義します。

```
AIX astro> define path judy drivea srctype=server desttype=drive
library=sangroup device=/dev/rmt6
astro> define path judy driveb srctype=server desttype=drive
library=sangroup device=/dev/rmt7
```

```
Linux astro> define path judy drivea srctype=server desttype=drive
library=sangroup device=/dev/IBMtape6
astro> define path judy driveb srctype=server desttype=drive
library=sangroup device=/dev/IBMtape7
```

5. 共有ライブラリーに関連付けられたすべての装置クラスを定義します。

```
AIX judy> define devclass tape library=sangroup devtype=lto
```

```
Linux judy> define devclass tape library=sangroup devtype=lto
```

装置クラス定義に関する以下のパラメーターは、ライブラリー・クライアントとライブラリー・マネージャーで同じでなければなりません。

- **LIBRARY**
- **DRIVEENCRYPTION**
- **WORM**
- **FORMAT**

6. 共有ライブラリーが使用するための BACKTAPE という名前のストレージ・プールを定義します。**DEFINE STGPOOL** コマンドを発行します。

```
judy> define stgpool backtape tape maxscratch=50
```

## 次のタスク

この手順を繰り返して、ライブラリー・マネージャーに対して追加のライブラリー・クライアントを定義します。

### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[DEFINE DRIVE \(ドライブのライブラリーへの定義\)](#)

[DEFINE LIBRARY \(ライブラリーの定義\)](#)

[DEFINE PATH \(パスの定義\)](#)

[DEFINE STGPOOL \(ストレージ・プール内のボリュームの定義\)](#)

## **Windows** 例: Windows サーバーのライブラリー共有

Windows システム上で稼働するサーバー用にライブラリー共有環境をセットアップする方法については、サンプル手順を参照してください。

## このタスクについて

この例では、ASTRO という名前のライブラリー・マネージャー・サーバーと JUDY という名前のライブラリー・クライアントが構成されます。

SCSI ライブラリーの場合、**libtype=scsi** パラメーターを指定してライブラリーを定義します。

## Windows ライブラリー・マネージャー・サーバーのセットアップ

IBM Spectrum Protect サーバーが SAN 接続装置を共用するように構成するために、ライブラリー・マネージャー・サーバーをセットアップする必要があります。

### 手順

以下の手順は、ASTRO という名前の IBM Spectrum Protect サーバーをライブラリー・マネージャーとしてセットアップする方法を示した例です。

1. 次のように、ライブラリー・マネージャー・サーバーが稼働していることを確認します。
  - a) Windows サービスの管理コンソール (services.msc) を開始します。
  - b) サービスを選択します。例えば、TSM Server1 です。
  - c) サービスが稼働していない場合は、サービス名を右クリックして「開始」をクリックします。
2. 共有ライブラリー装置のライブラリー情報およびドライブ情報を入手します。
  - a) tsmdlst.exe ユーティリティを実行します。このユーティリティは ¥Program Files ¥Tivoli¥TSM¥server ディレクトリーにあります。
3. ライブラリー・タイプが SCSI のライブラリーを定義します。  
例えば次のとおりです。

```
define library sangroup libtype=scsi shared=yes
```

この例では、ライブラリーのシリアル番号のデフォルトが使用されます。これにより、パスの定義時にサーバーがライブラリー自体からエレメント番号を取得します。ライブラリーの機能によっては、シリアル番号を自動的に検出できない場合があります。この場合、サーバーはデバイスのシリアル番号を記録しません。このため、パスの定義時またはサーバーによるデバイスの使用時にデバイスを識別できません。

4. サーバーからライブラリーへのパスを定義します。

```
define path astro sangroup srctype=server desttype=library  
device=lb0.0.0.2
```

ライブラリーの定義時にシリアル番号を指定しないと、サーバーは、ライブラリーを照会して、その情報を取得します。ライブラリーの定義時にシリアル番号を指定した場合は、サーバーが定義内容を検証し、不一致があるかどうかを示すメッセージを発行します。

5. そのライブラリーにドライブを定義します。

```
define drive sangroup drivea  
define drive sangroup driveb
```

この例では、ドライブのシリアル番号のデフォルトが使用されます。これにより、パスの定義時にサーバーがドライブ自体からエレメント番号を取得します。ドライブの機能によっては、サーバーはシリアル番号を自動的に検出できない場合があります。この場合、サーバーはデバイスのシリアル番号を記録しません。このため、パスの定義時またはサーバーによるデバイスの使用時にデバイスを識別できません。

この例では、ドライブのエレメント番号にもデフォルトを使用しています。すなわちパスの定義時にサーバーがドライブ自体からエレメント・アドレスを取得しています。

エレメント・アドレスは、自動ライブラリー内のドライブの物理ロケーションを示す番号です。サーバーは、ドライブの物理的なロケーションをドライブの SCSI アドレスに結び付けるためにエレメント・アドレスを必要とします。パスの定義時にサーバーがドライブ自体からエレメント番号を取得するようになるか、またはドライブの定義時にエレメント番号を指定することができます。

ライブラリーの機能によっては、サーバーがエレメント・アドレスを自動的に検出できないことがあります。この場合には、ドライブを定義するときにエレメント・アドレスを指定してください。多くのライブラリーのエレメント番号は、[IBM Support Portal for IBM Spectrum Protect](#) から入手できます。

6. サーバーから各ドライブへのパスを定義します。

```
define path astro drivea srctype=server desttype=drive library=sangroup
device=mt0.1.0.2
define path astro driveb srctype=server desttype=drive library=sangroup
device=mt0.2.0.2
```

ドライブの定義時にシリアル番号を指定していないと、サーバーはドライブまたはライブラリーを照会してこの情報を取得します。

7. 最低 1 つの装置クラスを定義します。

```
define devclass tape devtype=dlt library=sangroup
```

8. ライブラリー・インベントリーにチェックインします。次の例では、すべてのボリュームを、スクラッチ・ボリュームとしてライブラリー・インベントリーにチェックインします。サーバーは、バーコード・ラベル上の名前をボリューム名として使用します。

```
checkin libvolume sangroup search=yes status=scratch
checklabel=barcode
```

9. 最大 50 のスクラッチ・ボリュームを持つ共有ライブラリーのストレージ・プールをセットアップします。

```
define stgpool backtape tape
description='storage pool for shared sangroup' maxscratch=50
```

## 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[DEFINE DRIVE \(ドライブのライブラリーへの定義\)](#)

[DEFINE LIBRARY \(ライブラリーの定義\)](#)

[DEFINE PATH \(パスの定義\)](#)

[DEFINE STGPOOL \(ストレージ・プール内のボリュームの定義\)](#)

## Windows ライブラリー・クライアント・サーバーのセットアップ

SAN 接続された装置を共有するように IBM Spectrum Protect サーバーを構成するには、1 つ以上のライブラリー・クライアント・サーバーをセットアップする必要があります。

## 始める前に

ライブラリー・マネージャー・サーバーが定義されていることを確認します。

## このタスクについて

ライブラリー・マネージャー・サーバーを定義する必要があります。JUDY という名前の IBM Spectrum Protect サーバーをライブラリー・クライアントとしてセットアップする方法の例として、以下のプロシージャーを使用してください。

## 手順

- 次のように、ライブラリー・マネージャー・サーバーが稼働していることを確認します。
  - Windows サービスの管理コンソール (services.msc) を開始します。
  - サービスを選択します。例えば、TSM Server1 です。
  - サービスが稼働していない場合は、右クリックして「開始」を選択します。
- 共有ライブラリー装置のライブラリー情報およびドライブ情報を入手します。
  - tsmdlst.exe ユーティリティを実行します。このユーティリティは ¥Program Files ¥Tivoli¥TSM¥server ディレクトリーにあります。
- 共有ライブラリー SANGROUP を定義し、ライブラリー・マネージャーを指定します。このライブラリー名はライブラリー・マネージャーのライブラリー名と一致していなければなりません。

```
define library sangroup libtype=shared primarylibmanager=astro
```

4. 管理クライアントで次のようにコマンドを発行して、ライブラリー・クライアント・サーバーから各ドライブへのパスを定義します。

```
define path judy drivea srctype=server desttype=drive library=sangroup  
device=mt0.1.0.3  
define path judy driveb srctype=server desttype=drive library=sangroup  
device=mt0.2.0.3
```

5. ライブラリー・クライアントから次のようにコマンドを発行して、少なくとも 1 つの装置クラスを定義します。

```
define devclass tape devtype=dlt mountretention=1 mountwait=10  
library=sangroup
```

ライブラリー・クライアントでの装置クラスのパラメーターを、ライブラリー・マネージャーの対応するパラメーターと同一に設定します。両方のサーバーで装置クラス名を同一にすることが推奨されますが、これは必須ではありません。

ライブラリー・マネージャー・サーバーで指定された装置クラス・パラメーターは、ライブラリー・クライアント用に指定された装置クラス・パラメーターを指定変更します。これは、両方のサーバーの装置クラス名が同じである場合もそうでない場合も該当します。装置クラス名が異なる場合、ライブラリー・マネージャーは、ライブラリー・クライアントに指定された装置タイプに合致する装置クラスに指定されたパラメーターを使用します。

ライブラリー・クライアントの設定をライブラリー・マネージャーの装置クラスに指定されている設定と異なるようにする必要がある場合は (例えば、マウント・リミットを別の値にするなど)、以下のステップを実行します。

- a. ライブラリー・マネージャー・サーバーに追加の装置クラスを作成します。ライブラリー・クライアントが使用するためのパラメーター設定値を指定します。
  - b. ライブラリー・サーバーに作成した新規装置クラスと同じ名前と装置タイプの装置クラスをライブラリー・クライアント上に作成します。
6. 共有ライブラリーを使用するストレージ・プール BACKTAPE を定義します。

```
define stgpool backtape tape  
description='storage pool for shared sangroup' maxscratch=50
```

7. ライブラリー・クライアントとしてさらにサーバーを定義する場合には、この手順を繰り返します。

## 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[DEFINE LIBRARY \(ライブラリーの定義\)](#)

[DEFINE PATH \(パスの定義\)](#)

[DEFINE STGPOOL \(ストレージ・プール内のボリュームの定義\)](#)

# ストレージ・プール階層のセットアップ

実装プロセスの一環として、ストレージ・プール階層をセットアップする必要があります。ディスク上に少なくとも 1 つの 1 次ストレージ・プール、およびテープ上に 1 つの 1 次ストレージ・プールをセットアップします。データが毎日ディスクからテープにマイグレーションされるようにします。

## 始める前に

1. [20 ページの『ストレージ・プール階層の計画』](#)の情報を確認済みである必要があります。
2. クライアント・データをバックアップするための適切なルール (ポリシー と呼ばれる) が指定されている必要があります。[110 ページの『クライアント・データのバックアップおよびアーカイブに関するルールの指定』](#)の指示に従ってください。

3. ポリシーが各ノードに割り当てられている必要があります。ノードの登録時にポリシーを割り当てる手順については、[115 ページの『クライアントの登録』](#)を参照してください。

## 手順

ストレージ・プール階層をセットアップするには、以下のステップを実行します。

1. **DEFINE STGPOOL** コマンドを発行して、テープ装置の 1 次ストレージ・プールを定義します。

例えば、装置クラス LTO で 1 次ストレージ・プール TAPE1 を定義し、グループ・コロケーションを有効にします。このストレージ・プールに対してサーバーが要求できるスクラッチ・ボリュームの最大数を 999 に設定します。以下のコマンドを発行します。

```
define stgpool tape1 lto pooltype=primary collocate=group  
maxscratch=999
```

2. テープ上の 1 次ストレージ・プールのドライブ、パス、およびライブラリーを定義します。[92 ページの『テープ装置の定義』](#)の指示に従ってください。
3. **DEFINE STGPOOL** コマンドを発行して、ディスク装置の 1 次ストレージ・プールを定義します。

例えば、装置クラス FILE でストレージ・プール DISK1 を定義します。データを磁気テープ・ストレージ・プール TAPE1 にマイグレーションできるようにしますが、**HIGHMIG** パラメーターに 100 を指定し、**LOWMIG** パラメーターに 0 を指定することで自動マイグレーションは行われないようにします。**RECLAIM** パラメーターに 100 を指定して、レクラメーションが行われないようにします。ノード・コロケーションを有効にします。このストレージ・プールに対してサーバーが要求できるスクラッチ・ボリュームの最大数を 9999 に設定します。**MIGPROCESS** パラメーターを使用して、マイグレーション・プロセスの数を指定します。**MIGPROCESS** パラメーターの値は、ライブラリー内のドライブ数からリストア操作用に予約されているドライブの数を減算した値と等しい必要があります。以下のコマンドを発行します。

```
define stgpool disk1 file pooltype=primary nextstgpool=tape1  
highmig=100 lowmig=0 reclaim=100 collocate=node maxscratch=9999 migprocess=5
```

ディスクからテープへのマイグレーションをセットアップする 方法について詳しくは、[ディスク・ストレージ・プールのマイグレーション](#)を参照してください。

## 次のタスク

ストレージ・プール階層には、1 次ストレージ・プールのみが含まれます。ストレージ・プール階層をセットアップした後、以下のステップを実行します。

1. テープ装置上にコピー・ストレージ・プールを作成します。手順については、[DEFINE STGPOOL \(順次アクセス装置に割り当てられるコピー・ストレージ・プールの定義\)](#)を参照してください。
2. **BACKUP STGPOOL** コマンドを使用して、テープ・ベースの 1 次ストレージ・プールをコピー・ストレージ・プールにバックアップします。手順については、[BACKUP STGPOOL \(1 次ストレージ・プール・データをコピー・ストレージ・プールにバックアップ\)](#)を参照してください。
3. 災害時に確実にデータをリカバリーできるように、コピー・ストレージ・プールからオフサイト・ロケーションにテープ・ボリュームを移動するための手順をセットアップします。手順については、[215 ページの『DRM を使用した災害に対する準備と災害からのリカバリー』](#)を参照してください。

## 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[DEFINE STGPOOL \(ストレージ・プール内のボリュームの定義\)](#)

# アプリケーションおよびシステムの保護

---

サーバーは、アプリケーション、仮想マシン、およびシステムなどを含むクライアントのデータを保護します。

## クライアントの追加

---

IBM Spectrum Protect サーバーのセットアップが正常に行われた後、データのバックアップを開始するために、クライアント・ソフトウェアをインストールして構成します。

### このタスクについて

この手順では、クライアントを追加するための基本的な手順について説明します。クライアントの構成に関する具体的な手順については、クライアント・ノードにインストールする製品の資料を参照してください。以下のタイプのクライアント・ノードを使用することができます。

#### アプリケーション・クライアント・ノード

アプリケーション・クライアント・ノードには、E メール・サーバー、データベース、およびその他のアプリケーションなどがあります。例えば、以下のすべてのアプリケーションがアプリケーション・クライアント・ノードです。

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### システム・クライアント・ノード

システム・クライアント・ノードには、ワークステーション、Network Attached Storage (NAS) ファイル・サーバー、および API クライアントなどがあります。

#### 仮想マシン・クライアント・ノード

仮想マシン・クライアント・ノードは、ハイパーバイザー内の個々のゲスト・ホストで構成されます。各仮想マシンは、ファイル・スペースとして表示されます。

## 手順

クライアントを追加するには、以下の手順を実行します。

1. クライアント・ノードにインストールするソフトウェアを選択して、インストールを計画します。[109 ページの『クライアント・ソフトウェアの選択およびインストールの計画』](#)の指示に従ってください。
2. クライアント・データをバックアップおよびアーカイブする方法を指定します。[110 ページの『クライアント・データのバックアップおよびアーカイブに関するルールの指定』](#)の指示に従ってください。
3. クライアント・データをバックアップおよびアーカイブする時期を指定します。[114 ページの『バックアップおよびアーカイブの操作のスケジュール』](#)の指示に従ってください。
4. クライアントがサーバーに接続できるようにするには、クライアントを登録します。[115 ページの『クライアントの登録』](#)の指示に従ってください。
5. クライアント・ノードの保護を開始するには、選択したソフトウェアをクライアント・ノードにインストールして構成します。[116 ページの『クライアントのインストールおよび構成』](#)の指示に従ってください。



## クライアント・ソフトウェアの選択およびインストールの計画

異なるタイプのデータには異なるタイプの保護が必要です。保護する必要があるデータのタイプを確認して、適切なソフトウェアを選択してください。

### このタスクについて

すべてのクライアント・ノードにバックアップ/アーカイブ・クライアントをインストールし、クライアント・ノード上でクライアント・アクセプターを構成して開始できるようにする方法をお勧めします。クライアント・アクセプターは、スケジュールされた操作を効率的に実行するように設計されています。

クライアント・アクセプターは、バックアップ/アーカイブ・クライアント、IBM Spectrum Protect for Databases、IBM Spectrum Protect for Enterprise Resource Planning、IBM Spectrum Protect for Mail、および IBM Spectrum Protect for Virtual Environments の各製品のスケジュールを実行します。クライアント・アクセプターによってスケジュールが実行されない製品をインストールする場合、製品資料の構成手順に従い、スケジュールされた操作が行われることを確認する必要があります。

### 手順

目標に基づいて、インストールする製品を選択し、インストール手順を確認します。

**ヒント:** ここでクライアント・ソフトウェアをインストールする場合、クライアントを使用する前に、[116 ページの『クライアントのインストールおよび構成』](#)示されているクライアント構成タスクも完了する必要があります。

目標	製品および説明	インストール手順
ファイル・サーバーまたはワークステーションの保護	バックアップ/アーカイブ・クライアントは、ファイル・サーバーおよびワークステーションからストレージにファイルおよびディレクトリーをバックアップおよびアーカイブします。ファイルのバックアップ・バージョンおよびアーカイブ・コピーのリストアおよびリトリートも可能です。	<ul style="list-style-type: none"><li>• <a href="#">クライアント環境の要件</a></li><li>• <a href="#">UNIX および Linux バックアップ/アーカイブ・クライアントのインストール</a></li><li>• <a href="#">Windows クライアントの初回インストール</a></li></ul>
スナップショット・バックアップおよびリストアの機能を使用したアプリケーションの保護	IBM Spectrum Protect Snapshot は、統合されたアプリケーション認識スナップショットのバックアップおよびリストア機能を使用してデータを保護します。IBM Db2 データベース・ソフトウェア および SAP、Oracle、Microsoft Exchange、および Microsoft SQL Server のアプリケーションによって保管されたデータを保護できます。	<ul style="list-style-type: none"><li>• <a href="#">for UNIX and Linux のインストールおよびアップグレード</a></li><li>• <a href="#">for VMware のインストールおよびアップグレード</a></li><li>• <a href="#">for Windows のインストールおよび更新</a></li></ul>
IBM Domino サーバー上の E メール・アプリケーションの保護	IBM Spectrum Protect for Mail: Data Protection for IBM Domino は、データ保護を自動化して、IBM Domino サーバーをシャットダウンすることなくバックアップが実行されるようにします。	<ul style="list-style-type: none"><li>• <a href="#">UNIX、AIX、または Linux システムへの Data Protection for IBM Domino のインストール (V7.1.0)</a></li><li>• <a href="#">Windows システムへの Data Protection for IBM Domino のインストール (V7.1.0)</a></li></ul>
Microsoft Exchange サーバー上の E メール・アプリケーションの保護	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server は、データ保護を自動化して、Microsoft Exchange サーバーをシャットダウンすることなくバックアップが実行されるようにします。	<a href="#">のインストール、アップグレード、およびマイグレーション</a>



目標	製品および説明	インストール手順
Db2 データベースの保護	バックアップ/アーカイブ・クライアントのアプリケーション・プログラミング・インターフェース (API) を使用して、Db2 データを IBM Spectrum Protect サーバーにバックアップすることができます。	<a href="#">バックアップ/アーカイブ・クライアントのインストール (UNIX、Linux、および Windows)</a>
IBM Informix® データベースの保護	バックアップ/アーカイブ・クライアントの API を使用して、Informix データを IBM Spectrum Protect サーバーにバックアップすることができます。	<a href="#">バックアップ/アーカイブ・クライアントのインストール (UNIX、Linux、および Windows)</a>
Microsoft SQL データベースの保護	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server は、Microsoft SQL データを保護します。	<a href="#">Data Protection for SQL Server on Windows Server Core のインストール</a>
Oracle データベースの保護	IBM Spectrum Protect for Databases: Data Protection for Oracle は、Oracle データを保護します。	<a href="#">Data Protection for Oracle のインストール</a>
SAP 環境の保護	IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP は、SAP 環境向けにカスタマイズされた保護を提供します。この製品は、SAP データベース・サーバーの可用性の向上と管理ワークロードの軽減のために設計されています。	<ul style="list-style-type: none"> <li>• <a href="#">Data Protection for SAP for Db2 のインストール</a></li> <li>• <a href="#">Data Protection for SAP for Oracle のインストール</a></li> </ul>
仮想マシンの保護	<p>IBM Spectrum Protect for Virtual Environments は、Microsoft Hyper-V および VMware の仮想環境向けに調整された保護を提供します。IBM Spectrum Protect for Virtual Environments を使用して、中央のサーバーに保管される永久差分バックアップを作成し、バックアップ・ポリシーを作成して、仮想マシンまたは個々のファイルをリストアすることができます。</p> <p>あるいは、バックアップ/アーカイブ・クライアントを使用して、完全な VMware または Microsoft Hyper-V の仮想マシンをバックアップおよびリストアします。VMware 仮想マシンからファイルまたはディレクトリーをバックアップおよびリストアすることもできます。</p>	<ul style="list-style-type: none"> <li>• <a href="#">Data Protection for Microsoft Hyper-V のインストールとアップグレード</a></li> <li>• <a href="#">のインストールおよびアップグレード</a></li> <li>• <a href="#">バックアップ/アーカイブ・クライアントのインストール (UNIX、Linux、および Windows)</a></li> </ul>

**ヒント:** スペース管理用のクライアントを使用するために、IBM Spectrum Protect for Space Management または IBM Spectrum Protect HSM for Windows をインストールすることができます。

## クライアント・データのバックアップおよびアーカイブに関するルールの指定

クライアントを追加する前に、クライアント・データのバックアップおよびアーカイブの操作に関する適切なルールが指定されていることを確認します。クライアント登録プロセス中に、クライアント・ノードをポリシー・ドメインに割り当てます。ポリシー・ドメインには、クライアント・データを保管する方法と時期を制御するルールがあります。

### 始める前に

続行方法を以下から決定してください。

- ソリューション用に構成されたポリシーについて十分な知識を持っており、変更の必要がないことが分かっている場合は、[114 ページの『バックアップおよびアーカイブの操作のスケジュール』](#)に進みます。
- ポリシーについて十分な知識を持っていない場合は、この手順のステップに従ってください。

## このタスクについて

ポリシーは、ある期間にわたって保管するデータの量、データを保存する期間、およびクライアントのリストにデータを使用できる期間に影響を与えます。データ保護の目標に合わせてデフォルトのポリシーを更新して、お客様独自のポリシーを作成することができます。ポリシーには、以下のルールが含まれます。

- ファイルをサーバー・ストレージにバックアップしてアーカイブする 方法と時期。
- サーバー・ストレージに保持するファイルのコピー数と期間。

クライアント登録プロセス中に、クライアントをポリシー・ドメインに割り当てます。特定のクライアントのポリシーは、クライアントが割り当てられているポリシー・ドメインのルールによって決定されます。ポリシー・ドメインでは、有効なルールはアクティブ・ポリシー・セット内にあります。

クライアントがファイルをバックアップまたはアーカイブすると、ファイルはポリシー・ドメインのアクティブ・ポリシー・セット内の管理クラスにバインドされます。管理クラスは、クライアント・データを管理するためのルールのキー・セットです。ポリシーをさらに詳細にカスタマイズしない限り、クライアントでのバックアップおよびアーカイブ操作では、ポリシー・ドメインのデフォルト管理クラスの設定が使用されます。ポリシーをカスタマイズするには、追加の管理クラスを定義し、その使用法をクライアント・オプションにより割り当てます。

クライアント・オプションは、クライアント・システム上の編集可能ファイルでローカルに指定することも、サーバー上のクライアント・オプション・セットで指定することもできます。サーバー上のクライアント・オプション・セット内のオプションは、ローカルのクライアント・オプション・ファイル内のオプションをオーバーライドあるいは追加することができます。

## 手順

1. [111 ページの『ポリシーの表示』](#)の手順に従って、ご使用のソリューションに対して構成されたポリシーを確認してください。
2. データ保存要件に合わせて軽微な変更が必要な場合は、[112 ページの『ポリシーの編集』](#)の手順に従ってください。
3. オプション: データ保存要件を満たすためにポリシー・ドメインを作成したり、ポリシーに大幅な変更を加える必要がある場合は、[ポリシーのカスタマイズ](#)を参照してください。

## ポリシーの表示

ポリシーを表示して、要件に合うように編集する必要があるかどうかを判別します。

## 手順

1. ポリシー・ドメインのアクティブ・ポリシー・セットを表示するには、以下の手順を実行します。
  - a) Operations Center の「サービス」ページで、ポリシー・ドメインを選択して、「詳細」をクリックします。
  - b) ポリシー・ドメインの「要約」ページで、「ポリシー・セット」タブをクリックします。

**ヒント:** ランサムウェア攻撃後にデータを確実にリカバリーできるように、以下のガイドラインを適用してください。

  - 「バックアップ」列の値が 2 以上であることを確認します。推奨値は 3、4 またはそれ以上です。
  - 「追加バックアップの保持」列の値が 14 日以上であることを確認します。推奨値は 30 日以上です。
  - 「アーカイブの保持」列の値が 30 日以上であることを確認します。

IBM Spectrum Protect for Space Management ソフトウェアがクライアントにインストールされる場合、データがマイグレーション前にバックアップされていることを確認します。 **DEFINE MGMTCLASS** コマンドまたは **UPDATE MGMTCLASS** コマンドで、**MIGREQUIRESBKUP=YES** を指定します。次に、ヒントのガイドラインに従います。

2. ポリシー・ドメインの非アクティブなポリシー・セットを表示するには、以下の手順を実行します。
  - a) 「**ポリシー・セット**」 ページで、「**構成**」 トグルをクリックします。これで、非アクティブなポリシー・セットを表示および編集することができます。
  - b) 前後の矢印を使用して、非アクティブなポリシー・セットをスクロールします。非アクティブなポリシー・セットを表示すると、アクティブ・ポリシー・セットから非アクティブなポリシー・セットを区別する設定が強調表示されます。
  - c) 「**構成**」 トグルをクリックします。ポリシー・セットは編集不可になります。

## ポリシーの編集

ポリシー・ドメインに適用されるルールを変更するには、ポリシー・ドメインのアクティブ・ポリシー・セットを編集します。ドメインに対して別のポリシー・セットを活動化することもできます。

### 始める前に

ポリシーを変更すると、データ保存に影響する可能性があります。災害が発生した場合にデータを確実にリストアできるように、組織にとって重要なデータのバックアップを必ず続行してください。また、システムに、計画されたバックアップ操作に十分なストレージ・スペースがあることを確認してください。

### このタスクについて

ポリシー・セット内の 1 つ以上の管理クラスを変更することにより、ポリシー・セットを編集します。アクティブ・ポリシー・セットを編集する場合、ポリシー・セットを再び活動化するまで、クライアントで変更内容を使用できません。編集したポリシー・セットをクライアントで使用できるようにするには、ポリシー・セットを活動化します。

1 つのポリシー・ドメインに対して複数のポリシー・セットを定義することはできますが、活動状態にできるのは 1 つのポリシー・セットだけです。別のポリシー・セットを活動化すると、そのポリシー・セットが現在のアクティブ・ポリシー・セットに取って代わります。

ポリシーを定義する場合の推奨方法については、[ポリシーのカスタマイズ](#) を参照してください。

### 手順

1. Operations Center の「**サービス**」 ページで、ポリシー・ドメインを選択して、「**詳細**」 をクリックします。
2. ポリシー・ドメインの「**要約**」 ページで、「**ポリシー・セット**」 タブをクリックします。  
「**ポリシー・セット**」 ページには、アクティブ・ポリシー・セットの名前が示され、そのポリシー・セットのすべての管理クラスがリストされます。
3. 「**構成**」 トグルをクリックします。ポリシー・セットは編集可能です。
4. 活動状態にないポリシー・セットを編集するには、前後の矢印を使用してポリシー・セットを見つけます。
5. 以下のいずれかのアクションを実行して、ポリシー・セットを編集します。

オプション	説明
管理クラスの追加	<ol style="list-style-type: none"> <li>a. 「<b>ポリシー・セット</b>」 テーブルで、「<b>+ 管理クラス (Management Class)</b>」 をクリックします。</li> <li>b. データのバックアップおよびアーカイブに関するルールを指定するには、「<b>管理クラスの追加</b>」 ウィンドウのフィールドに入力します。</li> <li>c. この管理クラスをデフォルト管理クラスにするには、「<b>デフォルトに設定 (Make default)</b>」 チェック・ボックスを選択します。</li> </ol>

オプション	説明
	d.「追加」をクリックします。
管理クラスの削除	「管理クラス」列で、-をクリックします。 ヒント：デフォルト管理クラスを削除するには、最初に別の管理クラスをデフォルトとして割り当てる必要があります。
デフォルト管理クラスとしての管理クラスの設定	管理クラスの「デフォルト」列で、ラジオ・ボタンをクリックします。 ヒント：別の管理クラスがファイルに割り当てられていないか、ファイルの管理に適切でない場合に、デフォルト管理クラスがクライアント・ファイルを管理します。クライアントが常にファイルをバックアップおよびアーカイブできるように、ファイルのバックアップとアーカイブの両方のルールを含むデフォルト管理クラスを選択します。
管理クラスの変更	管理クラスのプロパティーを変更するには、テーブルのフィールドを更新します。

6.「保存」をクリックします。



**重要：**新規ポリシー・セットを活動化すると、データが失われる可能性があります。あるポリシー・セットで保護されているデータが、別のポリシー・セットでは保護されない可能性があります。したがって、ポリシー・セットを活動化する前に、以前のポリシー・セットと新規ポリシー・セットの相違点によってデータが失われないことを確認してください。

7.「活動化」をクリックします。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。以下のステップを実行して、新規ポリシー・セットの変更内容がデータ保存要件と一貫していることを確認します。

- 2つのポリシー・セットの中の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。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、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。
- 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、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。
- 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。

## クライアント・バックアップの範囲の変更

クライアント・バックアップ操作をセットアップする場合、不要なオブジェクトを除外する方法をお勧めします。例えば、バックアップ操作から一時ファイルを除外したい場合があります。

### このタスクについて

バックアップ操作から不要なオブジェクトを除外すると、バックアップ操作に必要なストレージ・スペースの量とストレージのコストを管理しやすくなります。ライセンス交付パッケージによっては、ライセンス交付のコストを制限できる場合があります。

### 手順

バックアップの適用範囲を変更する方法は、クライアント・ノードにインストールされている製品によって異なります。

- バックアップ/アーカイブ・クライアントの場合、include-exclude リストを作成して、ファイル、ファイル・グループ、あるいはディレクトリーをバックアップ操作に組み込みこんだり、バックアップ操作

から除外したりすることができます。include-exclude リストを作成するには、包含/除外リストの作成の手順に従います。

1つのタイプのすべてのクライアントに対して、確実に include-exclude リストを一貫して使用するために、必要なオプションが含まれるサーバー上にクライアント・オプション・セットを作成することができます。その後、クライアント・オプション・セットを同じタイプの各クライアントに割り当てます。詳細については、クライアント・オプション・セットによるクライアント操作の制御を参照してください。

- バックアップ/アーカイブ・クライアントの場合、**domain** オプションを使用して、差分バックアップ操作に含めるオブジェクトを指定することができます。ドメイン・オプション の指示に従ってください。
- その他の製品の場合、バックアップ操作に含めるオブジェクトおよびバックアップ操作から除外するオブジェクトを定義するには、製品資料の手順に従ってください。

## バックアップおよびアーカイブの操作のスケジュール

サーバーに新規クライアントを登録する前に、バックアップおよびアーカイブの操作を行う際に、指定するスケジュールが使用可能であることを確認します。登録プロセス中に、スケジュールをクライアントに割り当てます。

### 始める前に

続行方法を以下から決定してください。

- ソリューション用に構成されたスケジュールについて十分な知識を持っており、変更の必要がないことが分かっている場合は、115 ページの『クライアントの登録』に進みます。
- スケジュールについて十分な知識を持っていない場合、またはスケジュールを変更する必要がある場合は、この手順のステップに従ってください。


### このタスクについて

通常、すべてのクライアントのバックアップ操作を毎日実行する必要があります。ストレージ環境に最適なパフォーマンスを実現できるように、クライアントおよびサーバーのワークロードをスケジュールしてください。クライアントとサーバーの操作のオーバーラップを回避するために、クライアント・バックアップ/アーカイブの操作を夜間に実施するようにスケジュールすることを検討してください。クライアントおよびサーバーの操作が重なり合ったり、処理に十分な時間とリソースが与えられなかったりした場合、システム・パフォーマンスの低下、操作の失敗、その他の問題が生じる可能性があります。

### 手順

- Operations Center メニュー・バーの「クライアント」にマウス・カーソルを移動して、使用可能なスケジュールを確認します。「スケジュール」をクリックします。
- オプション: 以下のステップを実行して、スケジュールを変更または作成します。

オプション	説明
スケジュールの変更	a. 「スケジュール」ビューで、スケジュールを選択して「詳細」をクリックします。 b. 「スケジュールの詳細」ページで、行の先頭にある青色の矢印をクリックして詳細を表示します。 c. スケジュールの設定を変更し、「保存」をクリックします。
スケジュールの作成	「スケジュール」ビューで「+スケジュール」をクリックし、ステップを実行してスケジュールを作成します。

- オプション: Operations Center に表示されないスケジュール設定を構成するには、サーバー・コマンドを使用します。例えば、特定のディレクトリーをバックアップし、それをデフォルト以外の管理クラスに割り当てるクライアント操作をスケジュールしたいとします。
  - Operations Center の「概要」ページで、設定アイコン  上にカーソルを移動し、「コマンド・ビルダー」をクリックします。



- b) **DEFINE SCHEDULE** コマンドを発行してスケジュールを作成するか、**UPDATE SCHEDULE** コマンドを発行してスケジュールを変更します。コマンドについて詳しくは、[DEFINE SCHEDULE \(クライアント・スケジュールの定義\)](#) または [UPDATE SCHEDULE \(クライアント・スケジュールの更新\)](#) を参照してください。

## 関連情報

[日次操作のスケジュールのチューニング](#)

## クライアントの登録

クライアントを登録して、クライアントがサーバーに接続できること、およびサーバーがクライアント・データを保護できることを確認します。

### 始める前に

クライアント・ノードでクライアント所有者権限を持つ管理ユーザー ID がクライアントに必要なかどうかを判別します。クライアントに管理ユーザー ID が必要かどうかを判別するには、[技術情報 7048963](#) を参照してください。

**制約事項:**一部のタイプのクライアントでは、クライアント・ノード名と管理ユーザー ID が一致していません。これらのクライアントは、V7.1.7 で導入された Lightweight Directory Access Protocol 認証方式を使用して認証することができません。この認証方式 (統合モードと呼ばれる場合もある) の詳細は、[Active Directory データベースを使用したユーザーの認証](#) を参照してください。

### 手順

クライアントを登録するには、以下のいずれかのアクションを実行してください。

- クライアントに管理ユーザー ID が必要な場合、以下のように **REGISTER NODE** コマンドを使用し、**USERID** パラメーターを指定してクライアントを登録します。

```
register node node_name password userid=node_name
```

ここで *node\_name* はノード名を指定し、*password* はノードのパスワードを指定します。詳細については、[ノードの登録](#) を参照してください。

- クライアント・ノードに管理ユーザー ID が必要ない場合、Operations Center の「クライアントの追加」ウィザードを使用してクライアントを登録します。次の手順を実行してください。
  - Operations Center メニュー・バーで、「クライアント」をクリックします。
  - 「クライアント」テーブルで、「+ クライアント」をクリックします。
  - 「クライアントの追加」ウィザードのステップを実行します。
    - クライアントおよびサーバー上で冗長データを除去できるように指定します。「クライアント・サイド・データの重複排除」エリアで、「使用可能」チェック・ボックスを選択します。
    - 「構成」ウィンドウで、**TCPSERVERADDRESS**、**TCPPORT**、**NODENAME**、および **DEDUPLICATION** の値をコピーします。

**ヒント:** オプション値を記録し、安全な場所に保管します。クライアント登録が完了し、クライアント・ノードにソフトウェアをインストールした後、これらの値を使用してクライアントを構成します。
    - ウィザードの指示に従って、ポリシー・ドメイン、スケジュール、およびオプション・セットを指定します。
    - 危険な状態の設定を指定して、クライアントに関するリスクが表示される方法を設定します。
    - 「クライアントの追加」をクリックします。

## 関連情報

[tcpserveraddress オプション](#)

[tcpport オプション](#)

[nodename オプション](#)



## クライアントのインストールおよび構成

クライアント・ノードの保護を開始するには、選択したソフトウェアをインストールして構成する必要があります。

### 手順

ソフトウェアを既にインストール済みの場合、ステップ [117](#) ページの『2』を開始します。

1. 以下のいずれかのアクションを実行します。

- アプリケーション・ノードまたはクライアント・ノードにソフトウェアをインストールするには、以下の手順に従います。

ソフトウェア	説明へのリンク
IBM Spectrum Protect バックアップ/アーカイブ・クライアント	<ul style="list-style-type: none"> <li>- <a href="#">UNIX および Linux バックアップ/アーカイブ・クライアントのインストール</a></li> <li>- <a href="#">Windows クライアントの初回インストール</a></li> </ul> <p>ヒント : Operations Center を使用して既存のクライアントを更新することもできます。手順については、<a href="#">クライアント更新のスケジュール</a>を参照してください。</p>
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"> <li>- <a href="#">Data Protection for Oracle のインストール</a></li> <li>- <a href="#">Data Protection for SQL Server on Windows Server Core のインストール</a></li> </ul>
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> <li>- <a href="#">UNIX、AIX、または Linux システムへの Data Protection for IBM Domino のインストール (V7.1.0)</a></li> <li>- <a href="#">Windows システムへの Data Protection for IBM Domino のインストール (V7.1.0)</a></li> <li>- <a href="#">のインストール、アップグレード、およびマイグレーション</a></li> </ul>
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> <li>- <a href="#">for UNIX and Linux のインストールおよびアップグレード</a></li> <li>- <a href="#">for VMware のインストールおよびアップグレード</a></li> <li>- <a href="#">for Windows のインストールおよび更新</a></li> </ul>
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> <li>- <a href="#">Data Protection for SAP for Db2 のインストール</a></li> <li>- <a href="#">Data Protection for SAP for Oracle のインストール</a></li> </ul>

- 仮想マシン・クライアント・ノードにソフトウェアをインストールするには、選択したバックアップ・タイプの説明に従います。

バックアップ・タイプ	説明へのリンク
仮想マシンの完全 VMware バックアップを作成する予定の場合は、IBM Spectrum Protect バックアップ/アーカイブ・クライアントをインストールして構成します。	<ul style="list-style-type: none"> <li>- <a href="#">UNIX および Linux バックアップ/アーカイブ・クライアントのインストール</a></li> <li>- <a href="#">Windows クライアントの初回インストール</a></li> </ul>

バックアップ・タイプ	説明へのリンク
仮想マシンの永久増分フルバックアップを作成する予定の場合は、同じクライアント・ノードまたは別のクライアント・ノードに IBM Spectrum Protect for Virtual Environments およびバックアップ/アーカイブ・クライアントをインストールして構成します。	<p>– <a href="#">Data protection for VMware</a></p> <p><b>ヒント :</b> IBM Spectrum Protect for Virtual Environments およびバックアップ/アーカイブ・クライアントのソフトウェアは、IBM Spectrum Protect for Virtual Environments インストール・パッケージで入手できます。</p>

2. クライアントがサーバーに接続できるようにするには、クライアント・オプション・ファイルで **TCPSERVERADDRESS**、**TCPPORT**、および **NODENAME** オプションの値を追加または更新します。クライアントの登録時 (115 ページの『[クライアントの登録](#)』) に記録した値を使用します。
  - AIX、Linux、または Mac OS X のオペレーティング・システムにインストールされたクライアントの場合、クライアント・システムのオプション・ファイル **dsm.sys** に値を追加します。
  - Windows オペレーティング・システムにインストールされたクライアントの場合は、**dsm.opt** ファイルに値を追加します。

デフォルトでは、オプション・ファイルはインストール・ディレクトリーにあります。
3. オプション: Linux オペレーティング・システムまたは Windows オペレーティング・システムにバックアップ/アーカイブ・クライアントをインストールした場合は、クライアントにクライアント管理サービスをインストールしてください。[クライアント管理サービスのインストール](#) の指示に従ってください。
4. スケジュールされた操作を実行するようにクライアントを構成します。117 ページの『[スケジュール済み操作を実行するためのクライアントの構成](#)』の指示に従ってください。
5. オプション: ファイアウォール経由での通信を構成します。120 ページの『[ファイアウォールを介したクライアント/サーバー通信の構成](#)』の指示に従ってください。
6. テスト・バックアップを実行し、データが計画通りに保護されていることを確認します。  
例えば、バックアップ/アーカイブ・クライアントの場合、以下のステップを実行します。
  - a) Operations Center の「**クライアント**」ページで、バックアップするクライアントを選択し、「**バックアップ**」をクリックします。
  - b) バックアップが正常に完了したこと、および警告メッセージやエラー・メッセージがないことを確認します。
7. Operations Center で、クライアントに対してスケジュールされた操作の結果をモニターします。

## 次のタスク

クライアントからバックアップする対象を変更する必要がある場合は、113 ページの『[クライアント・バックアップの範囲の変更](#)』の手順を実行してください。

## スケジュール済み操作を実行するためのクライアントの構成

クライアント・ノードで、クライアント・スケジューラーを構成して開始する必要があります。クライアント・スケジューラーにより、スケジュール済み操作を実行するためのクライアントとサーバーの間の通信が可能になります。例えば、スケジュール済み操作には通常、クライアントからのファイルのバックアップが含まれます。

## このタスクについて

すべてのクライアント・ノードにバックアップ/アーカイブ・クライアントをインストールし、クライアント・ノード上でクライアント・アクセプターを構成して開始できるようにする方法が推奨されます。クライアント・アクセプターは、スケジュールされた操作を効率的に実行するように設計されています。クライアント・アクセプターは、以下の必要時にのみスケジューラーが実行されるようにクライアント・スケジューラーを管理します。

- 次回のスケジュール済み操作についてサーバーを照会する時間になった場合

- 次回のスケジュール済み操作を開始する時間になった場合

クライアント・アクセプターを使用すると、クライアント上のバックグラウンド・プロセスの数を減らし、メモリー保存の問題を回避することができます。

クライアント・アクセプターは、バックアップ/アーカイブ・クライアント、IBM Spectrum Protect for Databases、IBM Spectrum Protect for Enterprise Resource Planning、IBM Spectrum Protect for Mail、および IBM Spectrum Protect for Virtual Environments の各製品のスケジュールを実行します。クライアント・アクセプターによってスケジュールが実行されない製品をインストールした場合、製品資料の構成手順に従い、スケジュールされた操作が行われることを確認します。

お客様のビジネスで、サード・パーティー製スケジューリング・ツールを標準手法として使用している場合は、クライアント・アクセプターの代わりにそのスケジューリング・ツールを使用することができます。一般に、サード・パーティー製スケジューリング・ツールでは、オペレーティング・システムのコマンドを使用して直接にクライアント・プログラムを開始します。サード・パーティー製スケジューリング・ツールを構成するには、製品資料を参照してください。

## 手順

クライアント・アクセプターを使用して、クライアント・スケジューラーを構成して開始するには、クライアント・ノードにインストールされているオペレーティング・システムの手順に従ってください。

### AIX および Oracle Solaris

- バックアップ/アーカイブ・クライアント GUI から、「編集」 > 「クライアント・プリファレンス」をクリックします。
- 「**Web クライアント**」タブをクリックします。
- 「**管理対象サービス・オプション (Managed Services Options)**」フィールドで、「スケジュール」をクリックします。クライアント・アクセプターによっても Web クライアントを管理する場合は、「**両方**」オプションをクリックします。
- スケジューラーが無人で開始できるようにするには、dsm.sys ファイルで、**passwordaccess** オプションを **generate** に設定します。
- クライアント・ノードのパスワードを保管するには、次のコマンドを発行して、プロンプトが出されたときにクライアント・ノードのパスワードを入力します。

```
dsmc query sess
```

- コマンド・ラインで次のコマンドを発行して、クライアント・アクセプターを開始します。

```
/usr/bin/dsmcad
```

- システムの再始動後にクライアント・アクセプターが自動的に開始されるようにするには、システムのスタートアップ・ファイル (通常は /etc/inittab) に次の項目を追加します。

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Client Acceptor Daemon
```

### Linux

- バックアップ/アーカイブ・クライアント GUI から、「編集」 > 「クライアント・プリファレンス」をクリックします。
- 「**Web クライアント**」タブをクリックします。
- 「**管理対象サービス・オプション (Managed Services Options)**」フィールドで、「スケジュール」をクリックします。クライアント・アクセプターによっても Web クライアントを管理する場合は、「**両方**」オプションをクリックします。
- スケジューラーが無人で開始できるようにするには、dsm.sys ファイルで、**passwordaccess** オプションを **generate** に設定します。
- クライアント・ノードのパスワードを保管するには、次のコマンドを発行して、プロンプトが出されたときにクライアント・ノードのパスワードを入力します。

```
dsmc query sess
```

- f. root ユーザー ID でログインして次のコマンドを発行し、クライアント・アクセプターを開始します。

```
service dsmcad start
```

- g. システムの再始動後にクライアント・アクセプターが自動的に開始されるようにするには、シェル・プロンプトで次のコマンドを発行してサービスを追加します。

```
# chkconfig --add dsmcad
```

## MAC OS X

- バックアップ/アーカイブ・クライアント GUI で、「編集」 > 「クライアント・プリファレンス」をクリックします。
- スケジューラーが無人で開始できるようにするには、「権限」をクリックし、「パスワード生成」を選択し、「適用」をクリックします。
- サービスの管理方法を指定するには、「Web クライアント」をクリックし、「スケジュール」を選択し、「適用」をクリックし、「OK」をクリックします。
- 生成されたパスワードが保存されたことを確認するには、バックアップ/アーカイブ・クライアントを再始動します。
- IBM Spectrum Protect Tools for Administrators アプリケーションを使用して、クライアント・アクセプターを開始します。

## Windows

- バックアップ/アーカイブ・クライアント GUI で、「ユーティリティ」 > 「セットアップ・ウィザード」 > 「クライアント・スケジューラーの構成」をクリックします。「次へ」をクリックします。
- 「スケジューラー・ウィザード (Scheduler Wizard)」ページの情報を読み、「次へ」をクリックします。
- 「スケジューラー・タスク (Scheduler Task)」ページで、「新規または追加のスケジューラーのインストール (Install a new or additional scheduler)」を選択して、「次へ」をクリックします。
- 「スケジューラーの名前およびロケーション (Scheduler Name and Location)」ページで、追加するクライアント・スケジューラーの名前を指定します。次に、スケジューラーを管理するために「クライアント・アクセプター・デーモン (CAD) の使用 (Use the Client Acceptor daemon (CAD))」を選択して、「次へ」をクリックします。
- このクライアント・アクセプターに割り当てる名前を入力します。デフォルトの名前は、Client Acceptor です。「次へ」をクリックします。
- ウィザードの各ステップを実行して、構成を完了します。
- クライアント・オプション・ファイル dsm.opt を更新し、**passwordaccess** オプションを **generate** に設定します。
- クライアント・ノード・パスワードを保管するには、コマンド・プロンプトで次のコマンドを発行します。

```
dsmc query sess
```

プロンプトが表示されたら、クライアント・ノード・パスワードを入力します。

- 「サービス・コントロール」ページからクライアント・アクセプター・サービスを開始します。例えば、デフォルト名を使用した場合は、クライアント・アクセプター・サービスを開始します。「スケジューラーの名前およびロケーション」ページで指定したスケジューラー・サービスを開始しないでください。スケジューラー・サービスは、必要に応じてクライアント・アクセプター・サービスによって自動的に開始および停止されます。

## ファイアウォールを介したクライアント/サーバー通信の構成

クライアントがファイアウォールを介してサーバーと通信する必要がある場合は、ファイアウォール経由のクライアント/サーバー通信を有効にする必要があります。

### 始める前に

「クライアントの追加」ウィザードを使用してクライアントを登録した場合は、そのプロセス中に取得した、クライアント・オプション・ファイルのオプション値を検索してください。その値を使用して、ポートを指定することができます。

### このタスクについて



**重要:** サーバーまたはストレージ・エージェントによって使用されているセッションが終了される可能性がある方法でファイアウォールを構成しないでください。有効なセッションが終了すると、予測不能な結果が生じる可能性があります。入出力エラーが原因で、プロセスおよびセッションが終了したように見えることがあります。除外セッションがタイムアウト制限にかからないようにするには、IBM Spectrum Protect コンポーネントの既知のポートを構成します。**KEEPALIVE** サーバー・オプションがデフォルト値の YES に設定されたままであることを確認します。こうすると、クライアント/サーバー通信が確実に中断されなくなります。**KEEPALIVE** サーバー・オプションの設定手順については、[KEEPALIVE](#) を参照してください。

### 手順

以下のポートを開いて、ファイアウォール経由のアクセスを許可します。

#### バックアップ/アーカイブ・クライアント、コマンド・ライン管理クライアント、およびクライアント・スケジューラー用の TCP/IP ポート

クライアント・オプション・ファイルで **tcpport** オプションを使用して、ポートを指定します。クライアント・オプション・ファイル内の **tcpport** オプションは、サーバー・オプション・ファイル内の **TCPPORT** オプションと一致する必要があります。デフォルト値は 1500 です。デフォルト以外の値を使用する場合は、1024 から 32767 の範囲内の数値を指定します。

#### Web クライアントとリモート・ワークステーションの間の通信を可能にするための HTTP ポート

リモート・ワークステーションのクライアント・オプション・ファイルで **httpport** オプションを設定することにより、リモート・ワークステーション用のポートを指定します。デフォルト値は 1581 です。

#### リモート・ワークステーション用の TCP/IP ポート

デフォルト値 0 (ゼロ) を指定すると、2 つの空きポート番号がリモート・ワークステーションにランダムに割り当てられます。ポート番号がランダムに割り当てられないようにするには、リモート・ワークステーションのクライアント・オプション・ファイルで **webports** オプションを設定して値を指定します。

#### 管理セッション用の TCP/IP ポート

サーバーが管理クライアント・セッションの要求を待機するポートを指定します。クライアントの **tcpadminport** オプションの値は、**TCPADMINPORT** サーバー・オプションの値と一致する必要があります。こうすると、プライベート・ネットワーク内の管理セッションを保護できます。

## LAN フリー・データ移動の構成

クライアントおよびサーバーを構成することで、クライアントがストレージ・エージェントを介して SAN 上のストレージにデータを直接移動できるようになります。

### このタスクについて

LAN フリー・データ移動は、IBM Spectrum Protect for SAN 製品で提供されます。詳しくは、[IBM Spectrum Protect for SAN](#) の資料を参照してください。

## 手順

LAN フリー・データ移動を構成するには、以下のステップを実行します。

1. ネットワーク接続を検査します。
2. クライアント、ストレージ・エージェント、およびサーバーの間の通信を確立します。
3. クライアント・システムにソフトウェアをインストールして構成します。
4. ストレージ・エージェントがアクセスできるようにサーバー上の装置を構成します。
5. クライアントの LAN フリー・データ移動に関する IBM Spectrum Protect ポリシーを構成します。
6. 共有 FILE ストレージを使用している場合、IBM Spectrum Scale をインストールして構成します。

**制約事項:** **Windows** IBM Spectrum Scale ボリュームが AIX サーバーによってフォーマットされている場合、Windows システムは、ストレージ・エリア・ネットワークではなく TCP/IP を使用してデータを転送します。

7. ストレージ・エージェントからドライブまでのパスを定義します。
8. ストレージ・エージェントを開始し LAN フリー構成を検査します。

## 次のタスク

LAN リソースおよび SAN リソースの使用の調整を容易にするため、LAN フリー・データ移動機能を備えたクライアントへのデータ転送パスを制御できます。パスを制御するには、**UPDATE NODE** コマンドを実行します。

クライアントごとに、データの読み取り操作および書き込み操作に対して以下のいずれかの設定を選択することができます。**DATAREADPATH** パラメーターを使用してデータ読み取り操作を指定し、**DATAWRITEPATH** パラメーターを使用してデータ書き込み操作を指定します。このパラメーターはオプションです。デフォルト値は ANY です。

### LAN (LAN パスのみ)

以下のいずれかの条件に該当する場合、LAN 値を指定します。

- 少量のデータをバックアップまたはリストアしたい。
- クライアントに SAN 接続がない。

### LANFREE (LAN フリー・パスのみ)

クライアントとサーバーが同じ SAN 上にあり、以下のいずれかの条件が該当する場合は、LANFREE 値を指定します。

- 大量のデータをバックアップまたはリストアしたい。
- サーバー処理の負荷をクライアントにオフロードしたい。
- LAN 輻輳を軽減したい。

### ANY (任意の使用可能パス)

LAN フリー・パスを使用できる場合は、そのパスが使用されます。LAN フリー・パスが使用できない場合は、データは LAN を使用して移動されます。

## LAN フリー構成の妥当性検査

LAN フリー・データ移動用に IBM Spectrum Protect クライアントを構成した後、**VALIDATE LANFREE** コマンドを使用して、構成およびサーバー定義を検証することができます。

## このタスクについて

**VALIDATE LANFREE** コマンドにより、特定のストレージ・エージェントを使用するノードのどの宛先が LAN フリー・データ移動に対応しているかを判別できます。既存の LAN フリー構成に問題があるかどうかを識別するのに、このコマンド出力が役立つ場合があります。ノードおよびそのノードが使用するストレージ・エージェントのポリシー、ストレージ・プール、およびパスの定義を評価して、操作が正しく処理されることを確認できます。



## 手順

- **VALIDATE LANFREE** コマンドを発行して、クライアント・ノードに LAN フリー構成の問題がないかを判別します。例えば、クライアント・ノード FRED がストレージ・エージェント FRED\_STA を使用している場合、次のコマンドを発行します。

```
validate lanfree fred fred_sta
```

この結果は、ストレージ構成あるいはポリシーで必要となる可能性がある調整を識別するのに役立ちます。出力には、特定の操作タイプの管理クラスの宛先のうち、LAN フリー・データ転送に対応していないものが表示されます。また、LAN フリー宛先の総数も報告されます。

## 関連情報

[VALIDATE LANFREE \(LAN フリー・パスの妥当性検査\)](#)

# テープ暗号化方式

使用する暗号化方式の決定は、データの管理方法によって異なります。

クライアント・データを保護することは、特に機密性の高いデータの場合に重要です。オンサイトおよびオフサイトのボリューム内のデータが確実に保護されるようにするために、IBM テープ暗号化テクノロジーを使用できます。

このテクノロジーでは、256 ビット Advanced Encryption Standard (AES) 暗号鍵を要求することによって、より強力なレベルの暗号化を使用します。データの暗号化および暗号化解除を行うために、鍵が鍵マネージャーによってドライブに受け渡されます。

IBM テープ・テクノロジーは、以下の装置に対するさまざまなドライブ暗号化方式をサポートします。

- IBM 3592 第 2 世代および第 3 世代
- IBM Linear Tape-Open 第 4 世代および第 5 世代

IBM Spectrum Protect で使用できるドライブの暗号化方式は、ハードウェア・レベルでセットアップされます。IBM Spectrum Protect は、ハードウェア構成で使用されている暗号化方式を制御または変更することはできません。ハードウェアがアプリケーション方式用にセットアップされている場合、IBM Spectrum Protect は、装置クラスの **DRIVEENCRYPTION** 値に応じて暗号化をオン/オフすることができます。

特定の論理ライブラリー内のすべてのデータを暗号化する場合、あるいはストレージ・プール・ボリューム以外のデータも暗号化する場合は、ライブラリー方式またはシステム方式を使用します。暗号鍵マネージャーが鍵を共有するようにセットアップされている場合、ライブラリー方式およびシステム方式は、暗号鍵を共有することができます。これにより、2つの方式を交換することが可能になります。IBM Spectrum Protect は、アプリケーション方式とライブラリー方式またはシステム方式の暗号化の間で、暗号鍵を共有したり使用したりすることができません。

表 24. 暗号化方式

暗号化方式	説明
アプリケーション暗号化	<p>アプリケーションによって管理される暗号化では、暗号化されたボリュームのみが含まれる専用ストレージ・プールを作成することができます。この方法では、ストレージ・プール階層およびポリシーを使用してデータが暗号化される方法を管理することができます。</p> <p>暗号鍵は、アプリケーション (この場合は IBM Spectrum Protect) によって管理されます。IBM Spectrum Protect は、鍵を生成してサーバー・データベースに保管します。データは書き込み操作中に暗号化され、その間に暗号鍵がサーバーからドライブに受け渡されます。データは読み取り操作時に暗号化解除されます。</p> <p>ストレージ・プール・ボリュームを暗号化し、システム上で一部の暗号化処理を除去するには、アプリケーション方式を有効にします。アプリケーション管理の暗号化は、ストレージ・プール・ボリュームに対してのみ使用します。その他のボリューム (バックアップ・セット・テープ、エクスポート・ボリューム、データベース・バックアップなど) は、アプリケーション方式を使用して暗号化されません。</p> <p><b>要件:</b> アプリケーション暗号化が有効にされている場合、データの暗号化および暗号化解除に使用される暗号鍵がサーバーのデータベースに保管されるため、データベースのバックアップ保護には特に細心の注意が必要です。データをリストアするためには、正しいデータベースのバックアップと情報にアクセスするための対応する暗号鍵が必要です。頻繁にデータベースをバックアップし、データ損失またはデータの盗難を防ぐための保護を必ず行うようにします。データベースのバックアップおよび暗号鍵の両方にアクセスできる人は誰でもデータにアクセスできます。</p>
ライブラリー暗号化	<p>ライブラリーによって管理される暗号化では、シリアル番号を使用して、暗号化されるボリュームを制御することができます。暗号化するボリュームの範囲または集合を指定することができます。</p> <p>暗号鍵は、ライブラリーによって管理されます。鍵は暗号鍵マネージャーに保管され、ドライブに提供されます。ライブラリー管理の暗号化を使用するようにハードウェアをセットアップする場合、<b>DRIVEENCRYPTION=ALLOW</b> パラメーターを指定して <b>DEFINE DEVCLASS</b> コマンドを実行することで、この方式を使用することができます。</p> <p><b>制約事項:</b> 特定の IBM ライブラリーのみが、IBM LTO-4 以降の暗号化をサポートします。詳細については、124 ページの『磁気テープ・ドライブの暗号化の構成』を参照してください。</p>

表 24. 暗号化方式 (続き)

暗号化方式	説明
システム 暗号化	システムによって管理される暗号化は、AIX® オペレーティング・システムでのみ使用可能です。暗号鍵は、デバイス・ドライバーまたはオペレーティング・システムによって管理され、暗号鍵マネージャーに保管されます。システム暗号化を使用するようにハードウェアをセットアップする場合、 <b>DRIVEENCRYPTION=ALLOW</b> パラメーターを指定して <b>DEFINE DEVCLASS</b> コマンドを実行することで、この方式を使用することができます。

ボリュームが暗号化されているかどうか、およびどの方式が使用されたかを判別するには、**FORMAT=DETAILED** パラメーターを指定して **QUERY VOLUME** コマンドを実行します。

## 磁気テープ・ドライブの暗号化の構成

ドライブの暗号化を使用して、重要データや機密データが含まれるテープ (例えば、財務に関する機密情報が含まれるテープ) を保護することができます。ドライブの暗号化は、IBM Spectrum Protect サーバー環境からオンサイトまたはオフサイトの場所にテープを移動する場合に有効です。

### このタスクについて

さまざまなドライブ・タイプで利用できる暗号化方式を判別するには、以下の表を参照してください。

表 25. 使用可能な暗号化方式			
	アプリケーション方式	ライブラリー方式	システム方式
3592 第 2 世代以降	Yes	Yes	Yes
HP LTO-4 以降	Yes	No	No
IBM LTO-4 以降	Yes	Yes。ただし、ご使用システムのハードウェア (例えば TS3500 テープ・ライブラリー) がサポートする場合のみ。	Yes
Oracle StorageTek T10000B	Yes	No	No
Oracle StorageTek T10000C	Yes	No	No
Oracle StorageTek T10000D	Yes	No	No

1 つのライブラリー内で、暗号化をサポートするドライブと暗号化をサポートしないドライブを混用することができます。例えば、ライブラリーには、2 つの LTO-2 ドライブ、2 つの LTO-3 ドライブ、および 2 つの LTO-4 ドライブを含めることができます。また、例えば、異なるテープおよびドライブ・テクノロジーを持つ、暗号化および非暗号化の装置クラスを使用することで、ライブラリー内でメディアを混用することもできます。

#### 制約事項:

- LTO-4 ドライブに暗号化を適用するには、すべてのドライブが暗号化をサポートしている必要があります。

- ・ 論理ライブラリーに暗号化を適用するには、ライブラリー内のすべてのドライブに対して同じ暗号化方式を使用する必要があります。一部のドライブがアプリケーション方式の暗号化を使用し、他のドライブはライブラリー方式またはシステム方式の暗号化を使用するような環境は作成しないでください。

ドライブの暗号化を使用するためのハードウェア環境のセットアップについて詳しくは、ご使用のハードウェア資料を参照してください。

## 手順

1. ドライブの暗号化をサポートするデバイス・ドライバーをインストールします。
  - ・ IBM LTO-4 以降のドライブの暗号化を有効にするには、IBM RMSS Ultrium デバイス・ドライバーをインストールする必要があります。SCSI ドライブは、IBM LTO-4 以降の暗号化をサポートしません。
  - ・ HP LTO-4 以降のドライブの暗号化を有効にするには、IBM Spectrum Protect デバイス・ドライバーをインストールする必要があります。
2. 3592、LTO、または ECARTRIDGE 装置タイプの場合、**DEFINE DEVCLASS** コマンドあるいは **UPDATE DEVCLASS** コマンドで **DRIVEENCRYPTION** パラメーターを指定して、ドライブの暗号化を有効にします。

## 次のタスク

サポートされる暗号化方式を使って暗号化対応ドライブを使用している場合、暗号化データをテープに書き込むために、異なるフォーマットが使用されます。異なるフォーマットのボリュームにデータが書き込まれている場合、後でそのボリュームがスクラッチに戻されると、それらのボリュームには、暗号化対応のドライブでしか読み取ることができないラベルが含まれます。したがって、ハードウェアが暗号化対応でないか、暗号化方式が **NONE** に設定されているため、暗号化対応でないドライブで、このようなスクラッチ・ボリュームを使用するには、ボリュームのラベルを付け直す必要があります。

### 関連タスク

#### 3592 第 2 世代以降のドライブ暗号化の有効化/無効化

IBM Spectrum Protect では、3592 第 2 世代以降のドライブで、アプリケーション、システム、およびライブラリーの 3 つのドライブ暗号化タイプを使用できます。これらの方式は、ハードウェアを通して定義されます。

#### LTO 第 4 世代以降の磁気テープ・ドライブのドライブ暗号化の有効化および無効化

IBM Spectrum Protect は、LTO 第 4 世代以降のドライブで使用可能な 3 つのタイプのドライブ暗号化 (アプリケーション、システム、およびライブラリー) をサポートします。これらの方式は、ハードウェアを通して定義されます。

### 関連情報

DEFINE DEVCLASS (装置クラスの定義)

UPDATE DEVCLASS (装置クラスの更新)

## 磁気テープ・ストレージ操作の制御

テープの装置クラス定義には、ストレージ操作の制御を可能にするパラメーターが含まれます。

## IBM Spectrum Protect によるボリュームの満たし方

**DEFINE DEVCLASS** コマンドには、装置クラスと関連する順次ボリュームの見積容量を示すオプションの **ESTCAPACITY** パラメーターがあります。IBM Spectrum Protect は、ボリュームの見積容量を使用して、ストレージ・プールの見積容量と、使用率の見積もりを判別することができます。

**ESTCAPACITY** パラメーターが指定されていない場合、IBM Spectrum Protect は、**FORMAT** パラメーターを使用して装置クラスに対して指定された記録形式に基づくデフォルト値を使用します。

装置クラスのボリュームの実容量を超える見積容量を指定した場合、IBM Spectrum Protect は、ボリュームがいっぱいになったときに、ボリュームの見積容量を更新します。IBM Spectrum Protect は、ボリュームの終わりに達すると、ボリュームに書き込まれた量に一致するように容量を更新します。

ユーザーは、装置クラスについてデフォルトの見積容量を受け入れる か、または見積容量を明示的に指定することもできます。正確な見積容量の値は、必須ではありませんが役に立ちます。IBM Spectrum Protect は、ボリュームの見積容量を使用して、ストレージ・プールの見積容量と、使用率の見積もりを判別することができます。以下の条件のいずれかまたは両方が満たされる場合は、見積容量を変更することが推奨されます。

- データ圧縮のために、デフォルトの見積容量が不正確である。
- ボリュームのサイズが標準外である。

#### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## テープ・ボリュームの見積容量の指定

IBM Spectrum Protect は、見積容量も使用して、ストレージ・プール・ボリュームのレクラメーションを開始する時期を判別します。

### このタスクについて

テープ装置クラスの場合、サーバーによって選択されるデフォルトは、そのボリュームにデータを書き込むときに使用する記録形式によって決まります。装置タイプのデフォルトを受け入れても、値を指定しても構いません。

テープ・ボリュームの見積容量を指定するには、装置クラスを定義する際またはその定義を更新する際に **ESTCAPACITY** パラメーターを使用します。

#### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## テープ・メディアの記録形式の指定

IBM Spectrum Protect がデータをテープ・メディアに書き込むために使用する記録形式を指定することができます。ライブラリー内で異なる世代のドライブあるいは異なるドライブ・タイプを混用する予定の場合、各ドライブ世代および各ドライブ・タイプの記録形式を指定する必要があります。この方法で、サーバーは、ドライブ世代およびドライブ・タイプを区別することができます。

### このタスクについて

記録形式を指定するには、装置クラスを定義する際またはその定義を更新する際に **FORMAT** パラメーターを使用します。

その装置クラスに関連付けられたすべてのドライブが同一の場合は、**FORMAT=DRIVE** を指定します。サーバーは、ボリュームがマウントされているドライブのサポートする範囲で最高レベルのフォーマットを選択します。

その装置クラスに関連付けられた一部のドライブが他のドライブより高い密度のフォーマットをサポートする場合は、すべてのドライブに対応するフォーマットを指定してください。

1 つの SCSI ライブラリー内のドライブが複数の異なるテープ・テクノロジー (DLT や LTO Ultrium など) を使用している場合は、各装置クラス定義の **FORMAT** パラメーターに固有値を指定してください。

例については、[例: 複数のドライブ装置タイプを含む SCSI ライブラリーまたは仮想テープ・ライブラリーの構成を参照してください。](#)



ボリュームに対してサーバーが使用する記録形式は、データが最初にボリュームに書き込まれるときに選択されます。**FORMAT** パラメーターを更新しても、これらのメディアが先頭から再書き込みされるまでは、既にデータの入ったメディアには影響を与えません。このプロセスは、ボリュームがレクラメーション処理または削除された後、あるいはボリューム上のすべてのデータの有効期限が切れた後に行われることがあります。

#### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## ライブラリー・オブジェクトと装置クラスとの関連付け

ライブラリーには、ボリュームのマウントに使用できるドライブが入っています。装置クラスに関連付けることができるのは1つのライブラリーだけです。ただし、複数の装置クラスが同じライブラリーを参照することは可能です。

### このタスクについて

装置クラスをライブラリーに関連付けるには、装置クラスを定義する際またはその定義を更新する際に **LIBRARY** パラメーターを使用します。

#### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## テープ装置のメディア・マウント操作の制御

装置クラス定義を使用すると、マウントされたボリュームの数、ボリュームがマウントされた状態のまま置かれる時間、およびドライブが使用可能になるまで IBM Spectrum Protect サーバーが待機する時間を制御することができます。

### 同時にマウントされるボリュームの数の制御

装置クラスのマウント・リミットを設定する場合、システムに接続するストレージ装置の数を考慮する必要があります。また、同時書き込み機能を使用するかどうか、複数の装置クラスを単一ライブラリーに関連付けるかどうか、および同時に実行するプロセスの数も考慮する必要があります。

### このタスクについて

装置クラスのマウント・リミットを選択するときは、以下の問題について考慮してください。

- システムに何台のストレージ装置が接続されているか?

マウント数の限界の値として、ユーザー・システムの関連する使用可能ドライブ数より大きい値は指定しないでください。サーバーがマウント数の限界によって指定されている数のボリュームをマウントしようとしたが、要求されたボリュームに使用できるドライブがない場合には、エラーとなり、クライアントのセッションは終了することがあります。(この制限は、**DRIVES** パラメーターが指定されている場合には適用されません。)

SAN 上のライブラリー・リソースを IBM Spectrum Protect サーバー間で共有している場合、ライブラリー・クライアントが同時に使用できる磁気テープ・ドライブの数を制限する必要があります。複数のライブラリー・クライアント・サーバーが同時にライブラリーを使用できるようにするには、ライブラリー・クライアント上で装置クラスを定義あるいは更新する際に **MOUNTLIMIT** パラメーターを指定します。ライブラリー共有の構成について詳しくは、[101 ページの『ライブラリー共有の構成』](#)を参照してください。

- 同時書き込み機能を1次ストレージ・プール、コピー・ストレージ・プール、および活動データ・プールに対して使用するか?



1 次ストレージ・プールおよび関連するすべてのコピー・ストレージ・プールと活動データ・プールへのデータの同時書き込みをサポートするために、十分なマウント・ポイントを提供するマウント数の限界の値を指定します。

- 複数の装置クラスを、1 つのライブラリーと関連付けるか？

ライブラリーに関連付けられた装置クラスは、ライブラリー内の、その装置クラスの装置タイプと互換性のあるすべてのドライブを使用できます。複数の装置クラスを 1 つのライブラリーと関連付けることができるので、ライブラリー内の 1 つのドライブを、複数の装置クラスで使用することができます。IBM Spectrum Protect により、2 つの異なる装置クラスを使用することで、2 つの操作が同じドライブを同時に使用することがなくなります。

- この装置クラスの装置を使用して、同時にいくつかの IBM Spectrum Protect プロセスを実行したいか？

IBM Spectrum Protect は、優先順位の高い他のプロセスを実行するために、自動的にいくつかのプロセスを取り消します。装置クラスの使用可能なすべてのドライブが、優先順位の低いプロセスを完了するためにサーバーで使用されている場合は、優先順位の低いプロセスは、ドライブが使用可能になるまで待機する必要があります。例えば、IBM Spectrum Protect は、サーバー上でのマイグレーションまたはテープのレクラメーション・プロセスのためにドライブが必要になると、クライアントによるテープへの直接バックアップ・プロセスを取り消します。IBM Spectrum Protect は、ドライブがクライアントのリストア操作のために必要になると、テープのレクラメーション・プロセスを取り消します。詳細については、[129 ページの『操作の優先使用』](#)を参照してください。

プロセスが他のプロセスによって頻繁に取り消される場合は、IBM Spectrum Protect で使用できるドライブを増やすことを検討してください。それができない場合は、ドライブの競合を減らすように操作のスケジュールを見直してください。

この考慮事項は、同時書き込み機能にも適用されます。同時書き込み操作を成功させるには、十分なドライブを使用可能にする必要があります。

同時にマウントできるボリュームの最大数を指定するには、装置クラスを定義する際またはその定義を更新する際に **MOUNTLIMIT** パラメーターを使用します。

## 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## ボリュームのマウント保存期間の制御

マウントされたボリュームを、その最後の入出力活動以降にマウントされた状態のまま保持する時間を制御することができます。ボリュームが頻繁に使用される場合、不必要なマウントおよび取り外し操作を避けるために、マウント保存期間を長く設定すれば、パフォーマンスを改善することができます。

### このタスクについて

マウント操作を手作業、すなわちオペレーターによる作業で行っているときは、マウント保存期間を長めに指定することができます。例えば、週末にシステムの操作全体をたった 1 人のオペレーターがサポートしているような場合は、オペレーターが 2、3 分ごとにボリュームのマウントを依頼されたりすることのないように、マウント保存期間を長く定義してください。

マウントされたボリュームをそのままの状態で保持する時間を制御するには、装置クラスを定義する際またはその定義を更新する際に **MOUNTRETENTION** パラメーターを使用します。例えば、マウント保存値が 60 の場合、マウントされたボリュームが 60 分間アイドル状態のままであると、サーバーはそのボリュームをマウント解除します。

IBM Spectrum Protect がボリュームをマウントしている間は、そのドライブは IBM Spectrum Protect に割り当てられ、その他に使用することはできません。そのドライブを他で使用できるように解放する必要があるときは、そのドライブを使用している IBM Spectrum Protect 操作を取り消して、ボリュームを取り外すことができます。例えば、サーバー上でのマイグレーションまたはバックアップ操作を取り消すことができます。プロセスの取り消しおよびボリュームの取り外しについては、[196 ページの『サーバーによるボリューム要求の管理』](#)を参照してください。

## 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## サーバーがドライブを待つ時間の制御

ドライブが現在のマウント要求に使用できるようになるまで IBM Spectrum Protect サーバーが待機する最大時間 (分単位) を指定することができます。

### このタスクについて

ドライブがマウント要求に使用できるようになるまでの待機時間を制御するには、装置クラスを定義または更新するときに **MOUNTWAIT** パラメーターを使用します。

## 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## 操作の優先使用

マウント・ポイントが使用中で、他のポイントが使用できない場合、または特定のボリュームにアクセスする必要がある場合、サーバーは、サーバーまたはクライアントの操作に高い優先順位を与えることができます。操作の優先使用が行われると、その操作は取り消されます。

**QUERY MOUNT** コマンドを使用して、マウント・ポイントのボリュームの 状況を確認できます。

デフォルトでは、サーバーで優先使用は有効になっています。優先使用を無効にするには、サーバー・オプション・ファイルで **NOPREEMPT** オプションを指定します。このオプションを指定すると、他の操作より優先的に実行できる操作は、**BACKUP DB** コマンドと、エクスポート・コマンドおよびインポート・コマンドのみになります。

## 関連情報

[BACKUP DB \(データベースのバックアップ\)](#)

[QUERY MOUNT \(マウント済み順次アクセス・ボリュームに関する情報の表示\)](#)

## マウント・ポイントの優先権

優先順位の高い操作に、特定の装置クラスにあるマウント・ポイントが必要であり、その装置クラスのマウント・ポイントがすべて使用中である場合、その優先順位の高い操作は、優先順位の低い操作からマウント・ポイントを優先使用することができます。

マウント・ポイントを優先使用できるのは、優先権操作のために割り込む操作と割り込まれる操作の装置クラスが同じである場合のみです。

優先順位の高い以下の操作は、他の操作より優先してマウント・ポイントを使用できます。

- データベース・バックアップ操作
- クライアントによって開始されたリトリブ、リストア、または HSM 再呼び出し操作
- リモート・データ・ムーバーを使用したリストア操作
- エクスポート操作
- インポート操作
- バックアップ・セットを生成するための操作

以下のサーバー操作は、他の操作より優先的に実行したり、他の操作をこれらの操作より優先的に実行したりすることはできません。

- ボリュームの監査
- コピー・データ・プールまたは活動データ・プールからのデータのリストア
- リカバリー計画ファイルの準備

- ・ リモート・データ・ムーバーを使用したデータの保管

以下の操作は優先権を与えられ、優先順位の高いものから低いものの順にリストされています。サーバーは、最低の優先順位の操作 (例えば、重複の識別) を、優先権操作のために割り込む対象として選択します。

- ・ ノードの複製
- ・ コピー・ストレージ・プールへのデータのバックアップ
- ・ 活動データ・プールへの活動データのコピー
- ・ ストレージ・プール・ボリュームでのデータの移動
- ・ ディスクから順次メディアへのデータのマイグレーション
- ・ 順次メディアから順次メディアへのデータのマイグレーション
- ・ クライアントによって開始されたバックアップ、アーカイブ、または HSM マイグレーション操作
- ・ 順次アクセス・ストレージ・プール内のボリュームのレクラメーション処理
- ・ 重複の識別

## ボリューム・アクセスの優先権

優先順位の高い操作に、特定のボリュームへのアクセスが必要であり、そのボリュームが使用中である場合、その優先順位の高い操作は、そのボリュームについて優先順位の低い操作より優先使用することができます。

例えば、リストア要求で、レクラメーション操作によって使用中のボリューム にアクセスする必要があり、しかもドライブが利用可能な場合、そのレクラメーションのプロセスは取り消されます。

次は、特定のボリュームに対するアクセス操作を優先とする、高い優先順位の操作です。

- ・ データベース・バックアップ操作
- ・ クライアントによって開始されたリトリブ、リストア、または HSM 再呼び出し操作
- ・ リモート・データ・ムーバーを使用したリストア操作
- ・ エクスポート操作
- ・ インポート操作
- ・ バックアップ・セットを生成するための操作

以下の操作は、他の操作より優先的に実行したり、他の操作をこれらの操作より優先的に実行したりすることはできません。

- ・ ボリュームの監査
- ・ コピー・データ・プールまたは活動データ・プールからのデータのリストア
- ・ リカバリー計画の準備
- ・ リモート・データ・ムーバーを使用したデータの保管

以下の操作は優先権を与えられ、優先順位の高いものから低いものの順にリストされています。サーバーは、最低の優先順位の操作 (例えば、重複の識別) を、優先権操作のために割り込む対象として選択します。

- ・ ノードの複製
- ・ コピー・ストレージ・プールへのデータのバックアップ
- ・ 活動データ・プールへの活動データのコピー
- ・ ストレージ・プール・ボリュームでのデータの移動
- ・ ディスクから順次メディアへのデータのマイグレーション
- ・ 順次メディアから順次メディアへのデータのマイグレーション
- ・ クライアントによって開始されたデータのバックアップ、アーカイブ、または HSM マイグレーション
- ・ 順次アクセス・ストレージ・プール内のボリュームのレクラメーション処理
- ・ 重複の識別

## SAN 上の装置変更の影響

SAN 環境は、装置またはケーブル接続の変更によって大きく変化することがあります。動的な SAN の性質により、静的な定義が失敗したり、または意図しない結果になったりすることがあります。

SAN によって割り当てられ、サーバーまたはストレージ・エージェントが認識する装置 ID は、バスのリセットまたは他の環境の変更によって変更されることがあります。例えば、サーバーが、サーバーに対する元のパス指定および元の LAN 構成に基づいて、装置 X を *rmt0* (AIX 上) と認識しているとします。ただし、SAN における一部のイベント (例えば、新しい装置 Y の追加) によって、装置 X に *rmt1* が割り当てられる場合があります。サーバーが *rmt0* を使用して装置 X にアクセスしようとする、アクセスが失敗するか、誤ったターゲット装置にアクセスします。サーバーは、接続する装置の識別情報を確認するため、装置のシリアル番号を使用して SAN 上の装置に対する変更からのリカバリーを試行します。

ドライブまたはライブラリーを定義するときに、装置のシリアル番号を指定できます。装置の定義時にシリアル番号を指定しないと、装置パスの定義時にサーバーがシリアル番号を取得します。どちらの場合でも、サーバーのデータベースに装置のシリアル番号が保管されます。サーバーは、そのシリアル番号を使用して、操作する装置の ID を確認します。

サーバーが SAN 上のドライブおよびライブラリーを使用する場合、サーバーは、正しい装置が使用されているかを確認しようとします。サーバーは装置に接続するときに、この装置に対して定義されているパスの装置名を使用します。次に、サーバーは装置に対してシリアル番号を要求し、このシリアル番号と、サーバー・データベースに保管されているこの装置のシリアル番号を比較します。

シリアル番号が一致しない場合、サーバーは SAN 上でディスカバリー・プロセスを開始して、一致するシリアル番号を持つ装置を検出しようとします。一致するシリアル番号を持つ装置が検出されると、サーバーは、そのパス内の装置名を更新することで、サーバー・データベース内のパス定義を修正します。サーバーは、装置に加えられた変更に関する情報のメッセージを発行します。その後、サーバーは装置を使用します。

SAN 上での装置の変更が IBM Spectrum Protect サーバーに影響を与えたタイミングを判別するには、活動記録ログでメッセージをモニターすることができます。以下のメッセージはシリアル番号に関連します。

- ANR8952 から ANR8958
- ANR8961 から ANR8968
- ANR8974 から ANR8975

**制約事項：**一部の装置は、IBM Spectrum Protect サーバーなどのアプリケーションへシリアル番号を報告することができません。サーバーが装置からシリアル番号を取得できない場合、サーバーは、システムが SAN 上での装置ロケーションの変更からリカバリーするのを支援できません。

## Windows 装置情報の表示

装置情報ユーティリティ (tsmdlst) を使用して、サーバーに接続されている装置に関する情報を表示することができます。

### 始める前に

- HBA API がインストールされている必要があります。装置情報ユーティリティを実行するには、HBA API が必要です。
- テープ・デバイス・ドライバーがインストールおよび構成されている必要があります。

### 手順

1. コマンド・プロンプトから、サーバーのインストール・ディレクトリーの *server* サブディレクトリー (例えば、*C:\Program Files\Tivoli\TSM\server*) に移動します。
2. *tsmdlst.exe* 実行可能ファイルを実行します。

### 関連情報

[QUERY SAN \(SAN 上の装置の照会\)](#)

[tsmdlst \(装置に関する情報の表示\)](#)

## Write-once, read-many テープ・メディア

WORM (Write-once, read-many) テープ・メディアは、重要なデータを誤って削除したり、故意に削除したりするのを防止するのに役立ちます。ただし、IBM Spectrum Protect では、WORM メディアを使用する場合、特定の制約があり、ガイドラインに従う必要があります。

IBM Spectrum Protect では次のタイプの WORM メディアを使用できます。

- IBM 3592、サポートされるすべての世代
- IBM LTO-3 およびサポートされるすべての世代
- HP LTO-3 およびサポートされるすべての世代
- Quantum LTO-3 およびサポートされるすべての世代
- Quantum SDLT 600、Quantum DLT V4、および Quantum DLT S4
- StorageTek VolSafe
- Sony AIT50 および AIT100

ヒント：

- ストレージ・プールは、WORM メディアまたは RW メディアから構成されますが、この両方で構成することはできません。
- リストア操作またはインポート操作の後にテープが無駄にならないように、データベースのバックアップ操作やエクスポート操作に WORM テープを使用しないでください。

## WORM 対応ドライブ

WORM メディアをライブラリーで使用するには、ライブラリー内のすべてのドライブが WORM 対応でなければなりません。WORM カートリッジが読み取り/書き込み (RW) ドライブにマウントされると、マウントは失敗します。

ただし、装置クラスの WORM パラメーターを NO に設定すると、WORM 対応ドライブを RW ドライブとして使用することができます。すべてのドライブが WORM 対応であれば、どのタイプのライブラリーも WORM メディアと RW メディアの両方を持つことができます。この規則に対する唯一の例外は、WORM テープ・メディアを使用できない NAS 接続ライブラリーです。

### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## WORM メディアのチェックイン

WORM メディアのタイプによって、チェックイン時にメディア・ラベルを読み取る必要があるかどうかが決まります。

ライブラリー・チェンジャーは、標準の読み取り/書き込み (RW) 磁気テープ・メディアと以下のタイプの WORM 磁気テープ・メディアの違いを識別できません。

- VolSafe
- Sony AIT
- LTO
- SDLT
- DLT

使用されている WORM メディアのタイプを判別するには、ボリュームがドライブにロードされている必要があります。したがって、これらのタイプの WORM ボリュームのいずれかをチェックインする場合、

**CHECKIN LIBVOLUME** コマンドで **CHECKLABEL=YES** オプションを使用する必要があります。

IBM 3592 ライブラリー・チェンジャーは、WORM メディアのサポートを備えている場合、ボリュームをドライブにロードせずに、ボリュームが WORM メディアであるかどうかを検出できます。



CHECKLABEL=YES を指定する必要はありません。使用している 3592 ドライブおよびライブラリーが必要なサポートを提供することをハードウェアのベンダーに確認してください。

#### 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

## WORM メディアに対する制約事項

すでにラベルが付いている WORM メディアを LTO または ECARTRIDGE 装置クラスで使用することはできません。

以下のドライブのドライブ暗号鍵マネージャーとして IBM Spectrum Protect が指定された場合、WORM メディアを使用できません。

- IBM LTO-5、LTO-6、およびそれ以降
- HP LTO-5、LTO-6、およびそれ以降
- Oracle StorageTek T10000B
- Oracle StorageTek T10000C
- Oracle StorageTek T10000D

## WORM メディアのマウント障害

WORM テープ・メディアを読み取り/書き込み (RW) 装置クラス・マウント用のドライブにロードすると、マウント障害を招きます。同様に、RW テープ・メディアを WORM 装置クラス・マウント用のドライブにロードすると、マウントが失敗します。

## WORM メディアの再ラベル付け

WORM カートリッジにデータが入っている場合は再度ラベルを付けることができません。このことは、Sony AIT WORM、LTO WORM、SDLT WORM、DLT WORM、および IBM 3592 カートリッジについても同様です。VolSafe ボリュームのラベルを上書きできるのは一度だけであり、そのボリュームが使用可能、削除済み、有効期限切れのいずれのデータも含まない場合に限られます。

VolSafe ボリュームに対して **LABEL LIBVOLUME** コマンドを発行できるのは一度だけです。**LABEL LIBVOLUME** コマンドで **OVERWRITE=NO** オプションを使用することにより、ラベルが上書きされないように保護できます。

#### 関連情報

[LABEL LIBVOLUME \(ライブラリー・ボリュームのラベル付け\)](#)

## ライブラリーからの専用 WORM ボリュームの除去

WORM ボリュームに対してアクションを実行すると (例えばファイル・スペースを削除すると)、サーバーがボリュームにフルのマークを付けない場合には、ボリュームがスクラッチ状況に戻されます。WORM ボリュームにフルのマークが付けられず、ストレージ・プールから削除されると、そのボリュームは専用のままです。専用 WORM ボリュームをライブラリーから除去するには、**CHECKOUT LIBVOLUME** コマンドを発行する必要があります。

#### 関連情報

[CHECKOUT LIBVOLUME \(ストレージ・ボリュームのライブラリーからのチェックアウト\)](#)

## DLT WORM ボリュームの作成

DLT WORM ボリュームは、読み取り/書き込み (RW) ボリュームから変換することができます。

SDLT-600、DLT-V4、または DLT-S4 ドライブがあり、それらを WORM メディア用に使用可能に設定する場合、Quantum から入手できる V30 以降のファームウェアを使用してドライブをアップグレードします。また、DLTice ソフトウェアを使用して、フォーマットされていない RW ボリュームまたはブランク・ボリュームを WORM ボリュームに変換することもできます。



SCSI ライブラリーで、IBM Spectrum Protect サーバーは、ライブラリーのインベントリーにスクラッチ WORM ボリュームが見つからない場合に、自動的にスクラッチ DLT WORM ボリュームを作成します。サーバーは、使用可能な未フォーマットまたはブランク RW スクラッチ・ボリューム、または空の RW 専用ボリュームをスクラッチ WORM ボリュームに変換します。サーバーは、また既存の RW ボリューム上のラベル情報を使用して、新しく作成された WORM ボリュームのラベルを再書き込みします。

## 短いまたは通常の 3592 WORM テープのサポート

IBM Spectrum Protect は、短い 3592 WORM テープと通常の 3592 WORM テープの両方をサポートします。最高の結果を得るために、これらは別個のストレージ・プールで定義してください。

## WORM パラメーター設定の装置クラスの照会

装置クラスの WORM パラメーターの設定を確認するには、**QUERY DEVCLASS** コマンドを使用します。この出力には、WORM というラベルのフィールドと値 (YES または NO) が示されます。

### 関連情報

[QUERY DEVCLASS \(1 つ以上の装置クラスに関する情報の表示\)](#)

## 装置の問題のトラブルシューティング

IBM Spectrum Protect で装置を構成または使用するときには生じるエラー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

134 ページの表 26 を使用して、装置関連の問題の解決策を見つけてください。





表 26. 装置の問題の解決		
症状	問題	解決策
他のアプリケーションとの競合	IBM Spectrum Protect では、装置を共有するのにストレージ・エリア・ネットワークが必要です。	ストレージ・エリア・ネットワークをセットアップします。  <b>重要:</b> 複数の IBM Spectrum Protect サーバーが同じ装置を使用すると、データ損失が起きる場合があります。1 つの IBM Spectrum Protect サーバーのみで装置を定義または使用するようにしてください。   その他のアプリケーションは、SCSI テープ・ドライブを使用して IBM Spectrum Protect 装置にアクセスできません。
ラベル付けが失敗します。	ボリュームへのラベル付けを行う装置は、サーバーがその装置を他の処理に使用している時には使用できません。	ストレージ・プール内の既存のボリュームを上書きすることはできません。 ボリュームにラベルを付ける前に、ハードウェアの問題をすべて解決する必要があります。
	ライセンス登録が正しくないか不完全です。	購入した装置のサポートに必要なライセンスを登録してください。
デバイス・ドライバー間の矛盾	IBM Spectrum Protect は、順次アクセス装置を定義または使用するとき、入出力エラーに関するメッセージを発行します。	 IBM Spectrum Protect ドライバーが最初に開始されていないと、Windows デバイス・ドライバーおよび他のアプリケーションによって提供されているドライバーは、IBM Spectrum Protect デバイス・ドライバーを妨害することがあります。デバイス・ドライバーがシステムに開始された順序を調べるには、以下のステップを実行します。 <ol style="list-style-type: none"><li>1. 「コントロール・パネル」をクリックします。</li><li>2. 「装置」をクリックします。デバイス・ドライバーとそれらの開始タイプがリストされます。</li></ol>

表 26. 装置の問題の解決 (続き)		
症状	問題	解決策
入出力エラー	テープ装置を定義あるいは使用しようとする、デバイス・ドライバの競合が発生する可能性があります。IBM Spectrum Protect デバイス・ドライバは、Windows デバイス・ドライバおよび他のアプリケーションに提供されるドライバより先に開始しておかないと、これらのドライバにより動作が妨害されることがあります。	
<b>Linux</b> Linux プラットフォームで、永続予約との磁気テープ装置の予約競合を回避できない。	<b>Linux</b> Linux プラットフォームでは、IBM Spectrum Protect サーバーまたはストレージ・エージェントで、永続予約のために IBM lin_tape デバイス・ドライバが構成されていること、IBM 疑似装置ファイル /dev/TSMtape が作成されることが必要です。	<b>Linux</b> IBM lin_tape ドライバでデータ・パスのフェイルオーバーが有効になっている場合、/dev/TSMtape ファイルが自動的に作成され、永続予約を使用できます。そうでない場合、以下の手順に従って、Linux プラットフォームで磁気テープ装置の永続予約を構成します。  <b>ヒント:</b> デフォルトでは、IBM lin_tape デバイス・ドライバは SCSI-2 予約を使用して、磁気テープ装置を予約します。  <b>Linux</b> <ol style="list-style-type: none"> <li>IBM lin_tape デバイス・ドライバをアンロードします。</li> <li>lin_tape 構成ファイル /etc/modprobe.conf または /etc/modprobe.conf.local (あるいは RHEL 6 以上を実行している場合は /etc/modprobe.d/lin_tape.conf) に、以下の行を追加します。 <pre>options lin_tape tape_reserve_type=persistent</pre> </li> <li>ルール・ファイル /etc/udev/rules.d/98-lin_tape.rules には、以下の行を追加します。 <pre>KERNEL=="TSMtape", MODE=="0666"</pre> </li> <li>IBM lin_tape デバイス・ドライバを再ロードします。</li> </ol> <b>Linux</b> IBM 疑似ファイル /dev/TSMtape が作成され、IBM Spectrum Protect サーバーは Linux プラットフォームで永続予約を使用して、磁気テープ装置予約を回避できます。

## 実装の完了

IBM Spectrum Protect ソリューションを構成して稼働した後、バックアップ操作をテストし、モニターをセットアップして、すべてがスムーズに稼働することを確認します。

### 手順

- バックアップ操作をテストして、データが期待したとおりに保護されていることを確認します。
  - Operations Center の「クライアント」ページで、バックアップするクライアントを選択し、「バックアップ」をクリックします。
  - Operations Center の「サーバー」ページで、データベースをバックアップするサーバーを選択します。「バックアップ」をクリックして、「データベースのバックアップ」ウィンドウの指示に従います。
  - バックアップ操作が正常に完了し、警告メッセージおよびエラー・メッセージがないことを確認します。

**ヒント:**あるいは、バックアップ/アーカイブ・クライアントの GUI を使用してクライアント・データをバックアップすることができ、管理コマンド・ラインから **BACKUP DB** コマンドを発行してサーバー・データベースをバックアップすることができます。

2. [137 ページの『第 3 部 テープ・ソリューションのモニター』](#)の手順に従って、ご使用のソリューション用にモニタリングをセットアップします。

## 第3部 テープ・ソリューションのモニター

テープを使用したソリューションをモニターし、操作が適切かどうかを確認します。

### このタスクについて

IBM Spectrum Protect ソリューションを実装した後、既存の問題や潜在的な問題を特定するために、毎日および定期的にソリューションをモニターします。収集した情報は、問題のトラブルシューティングとシステム・パフォーマンスの最適化に使用できます。ソリューションをモニターするために推奨される方法は、システム状況の全体と詳細をグラフィカル・ユーザー・インターフェースで表示する Operations Center を使用することです。さらに、Operations Center を構成して、システム状況の要約を示す E メール・レポートを生成することができます。

### 手順

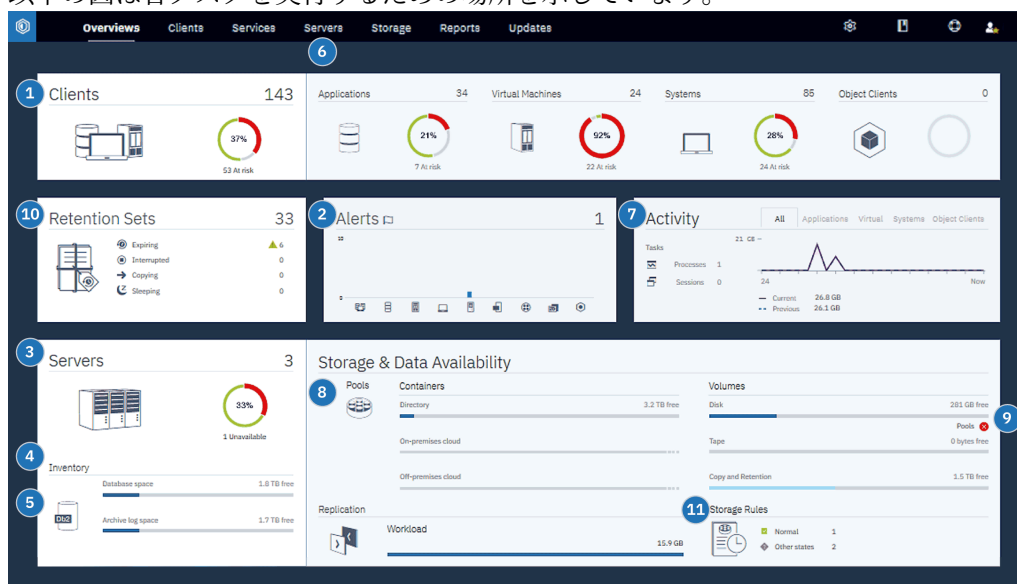
1. 日次モニター・タスクを実行します。手順については、[日次モニターのチェックリスト](#)を参照してください。
2. 定期的なモニター・タスクを実行します。手順については、[定期的なモニターのチェックリスト](#)を参照してください。
3. システムがライセンス 交付要件に準拠していることを確認します。手順については、[コンプライアンス 準拠性の確認](#)を参照してください。
4. オプション: システム状況の E メール・レポートをセットアップします。手順については、[157 ページの『E メール・レポートを使用したシステム状況のトラッキング』](#)を参照してください。

## 日次モニター・チェックリスト


IBM Spectrum Protect ソリューションの日次モニター・タスクを完了していることを確認するには、日次モニター・チェックリストを確認します。

Operations Center の「概要」ページから、日次モニター・タスクを実行します。「概要」ページにアクセスするには、Operations Center を開いて「概要」をクリックします。

以下の図は各タスクを実行するための場所を示しています。



**ヒント:** 拡張モニター・タスクの管理コマンドを実行するには、Operations Center コマンド・ビルダーを使用します。コマンド・ビルダーは、コマンドを入力するときにガイドとなる先行入力機能を提供します。

コマンド・ビルダーを開くには、Operations Center の「概要」ページに進みます。メニュー・バーで、設定アイコン  にマウス・カーソルを移動し、「コマンド・ビルダー」をクリックします。

次の表に、日次モニター・タスクをリストして、各タスクの実行手順を示します。

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
ランサムウェア攻撃を示す可能性があるセキュリティ通知を監視します。	ランサムウェア攻撃の可能性が IBM Spectrum Protect 環境で検出された場合、セキュリティ通知メッセージが Operations Center の前面に表示されます。詳しくは、メッセージをクリックして「 <b>セキュリティ通知</b> 」ページを開いてください。	<p>「<b>セキュリティ通知</b>」ページでは以下のアクションを実行できます。</p> <ul style="list-style-type: none"> <li>クライアントごとに通知詳細を表示する。</li> </ul> <p><b>制約事項:</b> バックアップ/アーカイブ・クライアントおよび IBM Spectrum Protect for Virtual Environments クライアントの通知のみ使用可能です。</p> <ul style="list-style-type: none"> <li>セキュリティ通知を選択して「<b>確認</b>」をクリックすることでセキュリティ通知を確認する。セキュリティ通知を確認すると、「<b>セキュリティ通知</b>」選択したクライアントの「確認済み」列にチェック・マークが追加されます。通知が確認済みになる基準は、所属する組織によって決まります。チェック・マークはその問題が調査済みであり、誤検出であると判明したことを意味する場合があります。あるいは、問題が存在しているものの、解決中であることを意味する場合もあります。</li> <li>管理者にセキュリティ通知を割り当てるために、セキュリティ通知を選択し、「<b>割り当て</b>」をクリックします。割り当てを表示するには、管理者が Operations Center にサインインして、「概要」&gt;「<b>セキュリティ</b>」をクリックする必要があります。管理者が定期的に「<b>セキュリティ通知</b>」ページをモニターしているかどうか定かではない場合は、管理者に割り当てに関して通知してください。</li> <li>通知が誤検出の場合、そのセキュリティ通知を選択して「<b>リセット</b>」をクリックできます。そうすると、セキュリティ通知が削除されます。最新のバックアップ操作とのベースライン比較に使用される履歴データも削除されます。その後は新規ベースラインが計算されます。</li> <li>オプションで、<b>SET SECURITYNOTIF</b> コマンドを使用して、セキュリティ通知を無効にすることができます。</li> </ul>

表 27. 日次モニター・タスク (続き)


タスク	基本的な手順	詳細手順およびトラブルシューティング情報
<p><b>①</b> バックアップ操作が失敗したか、未実行であるために、クライアントが保護されないリスクがあるかどうかを判別します。</p>	<p>クライアントが危険な状態にあるかどうかを確認するには、「クライアント」エリアで「<b>危険</b>」通知を探します。詳細を表示するには、「クライアント」エリアをクリックします。</p> <p> <b>重要:</b> 「危険」のパーセンテージが通常よりはるかに大きい場合、ランサムウェア攻撃を示している可能性があります。ランサムウェア攻撃により、バックアップ操作が失敗し、クライアントはリスクにさらされる可能性があります。例えば、「危険」のクライアントのパーセンテージが、通常は 5% から 10% であるにも関わらず、40% または 50% に増えた場合、その原因を調査してください。</p> <p>クライアント管理サービスをバックアップ/アーカイブ・クライアントにインストールしている場合、以下のステップを実行して、クライアント・エラーおよびスケジュール・ログを表示して分析することができます。</p> <ol style="list-style-type: none"> <li>1. 「クライアント」テーブルで、クライアントを選択して、「詳細」をクリックします。</li> <li>2. 問題を診断するには、「診断」をクリックします。</li> </ol>	<p>クライアント管理サービスがインストールされていないクライアントの場合、クライアント・システムにアクセスして、クライアント・エラー・ログを確認します。</p>
<p><b>②</b> クライアント関連エラーまたはサーバー関連エラーに注意が必要であるかどうかを判別します。</p>	<p>報告されたアラートの重大度を判別するには、「アラート」エリアで、列の上にカーソルを移動します。</p>	<p>アラートに関する追加情報を表示するには、以下のステップを実行します。</p> <ol style="list-style-type: none"> <li>1. 「アラート」エリアをクリックします。</li> <li>2. 「アラート」表でアラートを選択します。</li> <li>3. 「活動記録ログ」ペインでメッセージを確認します。このペインには、選択したアラートの発生前後に発行された関連メッセージが表示されます。</li> </ol>
<p><b>③</b> Operations Center によって管理されるサーバーがクライアントにデータ保護サービスを提供できるかどうかを判別します。</p>	<ol style="list-style-type: none"> <li>1. サーバーが危険な状態にあるかどうかを確認するには、「サーバー」エリアで「<b>使用不可</b>」通知を探します。</li> <li>2. 追加情報を表示するには、「サーバー」エリアをクリックします。</li> <li>3. 「サーバー」テーブルでサーバーを選択して、「詳細」をクリックします。</li> </ol>	<p><b>ヒント:</b> サーバー・プロパティに関連した問題を検出した場合は、次のようにして、サーバー・プロパティを更新します。</p> <ol style="list-style-type: none"> <li>1. 「サーバー」テーブルで、サーバーを選択して、「詳細」をクリックします。</li> <li>2. サーバー・プロパティを更新するには、「<b>プロパティ</b>」をクリックします。</li> </ol>



表 27. 日次モニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
<p><b>4</b> サーバー・データベース、活動ログ、およびアーカイブ・ログで構成されるサーバー・インベントリに十分なスペースを使用できるかどうかを判別します。</p>	<ol style="list-style-type: none"> <li>「サーバー」エリアをクリックします。</li> <li>テーブルの「状況」列でサーバーの状況を表示して、問題があれば解決します。 <ul style="list-style-type: none"> <li>「正常」  サーバー・データベース、活動ログ、およびアーカイブ・ログに十分なスペースを使用できます。</li> <li>「重大」  サーバー・データベース、活動ログ、またはアーカイブ・ログに使用できるスペースが不十分です。すぐにスペースを追加する必要があります。そうしないと、サーバーによって提供されるデータ保護サービスが中断されます。</li> <li>「警告」  サーバー・データベース、活動ログ、またはアーカイブ・ログがスペース不足になっています。この状態が続く場合は、スペースを追加する必要があります。</li> <li>「使用不可」  状況を取得できません。サーバーが実行中であること、およびネットワークに問題がないことを確認してください。この状況は、モニター管理者 ID がロックされている場合、またはそれ以外の理由でサーバー上で使用不可になっている場合にも表示されます。この ID の名前は、IBM-OC-hub_server_name です。</li> <li>「モニター対象外」  モニター対象外のサーバーがハブ・サーバーに定義されていますが、Operations Center で管理するようには構成されていません。モニター対象外サーバーを構成するには、サーバーを選択して、「スポークのモニター」をクリックします。</li> </ul> </li> </ol>	<p>「アラート」ページで、関連したアラートを検索することもできます。トラブルシューティングに関する詳細な説明については、<a href="#">サーバーの問題の解決</a>を参照してください。</p>

表 27. 日次モニター・タスク (続き)


タスク	基本的な手順	詳細手順およびトラブルシューティング情報
<p><b>5</b> サーバー・データベース・バックアップ操作を確認します。</p>	<p>サーバーが最後にバックアップされた時期を判別するには、以下の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. 「サーバー」エリアをクリックします。</li> <li>2. 「サーバー」テーブルで、「最終データベース・バックアップ」列を確認します。</li> </ol>	<p>バックアップ操作に関する詳細情報を取得するには、以下の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. 「サーバー」テーブルで、行を選択して、「詳細」をクリックします。</li> <li>2. 「DB バックアップ」エリアで、チェック・マークの上にカーソルを移動し、バックアップ操作に関する情報を表示します。</li> </ol> <p>データベースが最近 (例えば、過去 24 時間以内に) バックアップされていない場合、バックアップ操作を開始できます。</p> <ol style="list-style-type: none"> <li>1. Operations Center の「概要」ページで、「サーバー」エリアをクリックします。</li> <li>2. テーブルで、サーバーを選択して、「バックアップ」をクリックします。</li> </ol> <p>サーバー・データベースが自動バックアップ操作に構成されているかどうかを判別するには、以下の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. メニュー・バーで、設定アイコン  にマウス・カーソルを移動し、「コマンド・ビルダー」をクリックします。</li> <li>2. <b>QUERY DB</b> コマンドを発行します。</li> </ol> <pre>query db f=d</pre> <ol style="list-style-type: none"> <li>3. 出力で、「完全装置クラス名」フィールドを確認します。装置クラスが指定されている場合、サーバーは、自動データベース・バックアップ用に構成されています。</li> </ol>
<p><b>6</b> その他のサーバー保守タスクをモニターします。サーバー保守タスクには、管理コマンド・スケジュール、保守スクリプト、および関連コマンドの実行が含まれる場合があります。</p>	<p>サーバーの問題が原因で失敗したプロセスに関する情報を検索するには、以下の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. 「サーバー」 &gt; 「保守」をクリックします。</li> <li>2. プロセスの 2 週間の履歴を取得するには、「ヒストリー」列を確認します。</li> <li>3. スケジュール済みプロセスに関する詳細情報を取得するには、そのプロセスに関連したチェック・ボックスの上にカーソルを移動します。</li> </ol>	<p>プロセスのモニターおよび問題解決について詳しくは、Operations Center オンライン・ヘルプを参照してください。</p>

表 27. 日次モニター・タスク (続き)


タスク	基本的な手順	詳細手順およびトラブルシューティング情報
<p><b>7</b> サーバーとの間で最近送受信されたデータの量が、予期した範囲内に収まっていることを確認します。</p>	<ul style="list-style-type: none"> <li>過去 24 時間のアクティビティの 概要を取得するには、「アクティビティ」エリアを確認します。</li> <li>過去 24 時間のアクティビティを、その前の 24 時間のアクティビティと比較するには、「現行」エリアと「前へ」エリアの図を確認します。</li> </ul>	<ul style="list-style-type: none"> <li>予期したよりも多くのデータがサーバーに送信されていた場合、どのクライアントが多くのデータをバックアップしているかを判別して、原因を調べます。クライアント・サイドのデータ重複排除が正しく機能していない可能性があります。</li> </ul> <p> <b>重要:</b> バックアップ・データの量が通常より大幅に多い場合、ランサムウェア攻撃を示している可能性があります。ランサムウェアがデータを暗号化すると、システムはそのデータを変更されているものとみなし、変更されたデータがバックアップされます。そのため、バックアップ・ボリュームが大きくなります。影響を受けるクライアントを判別するには、「アプリケーション」、「仮想マシン」、または「システム」タブをクリックします。</p> <ul style="list-style-type: none"> <li>予期したよりも少ないデータがサーバーに送信されていた場合は、クライアント・バックアップ操作がスケジュールどおりに行われているかどうかを調べます。</li> </ul>

表 27. 日次モニター・タスク (続き)




タスク	基本的な手順	詳細手順およびトラブルシューティング情報
<p><b>8</b> ストレージ・プールをクライアント・データのバックアップに使用できることを確認します。</p>	<p>1. 「ストレージおよびデータの可用性 (Storage &amp; Data Availability)」エリアに問題が示されている場合、「プール」をクリックして、詳細を表示します。</p> <ul style="list-style-type: none"> <li>・「重大」 状況が表示されている場合、ストレージ・プールで利用できるスペースが不十分か、アクセス状況が「使用不可」です。</li> </ul> <p> <b>重要:</b> 状況が重大な場合、その原因を次のように調査します。</p> <ul style="list-style-type: none"> <li>－ ストレージ・プールのデータ重複排除率が大幅に下がった場合、ランサムウェア攻撃を示している可能性があります。ランサムウェア攻撃中はデータが暗号化され、重複排除を行うことはできません。データ重複排除率を確認するには、「ストレージ・プール」テーブルで、「節約 (%)」列の値を参照します。</li> <li>－ ストレージ・プールが予想せずに 100% 利用されるようになった場合、ランサムウェア攻撃を示している可能性があります。使用率を確認するには、「使用容量」列の値を参照してください。値の上にマウスを移動し、使用スペースとフリー・スペースのパーセンテージを確認してください。</li> <li>・「警告」 状況が表示されている場合、ストレージ・プールがスペース不足になっているか、そのアクセス状況が「読み取り専用」です。</li> </ul> <p>2. 選択したストレージ・プールの使用済みスペース、フリー・スペース、および合計スペースを表示するには、「使用済み容量」列の項目の上にカーソルを移動します。</p>	<p>過去 2 週間に使用されたストレージ・プールの容量を表示するには、「ストレージ・プール」テーブルの行を選択して、「詳細」をクリックします。</p>

表 27. 日次モニター・タスク (続き)



タスク	基本的な手順	詳細手順およびトラブルシューティング情報
<p><b>9</b> ストレージ装置がバックアップ操作に使用可能であることを確認します。</p>	<p>「ストレージおよびデータ可用性」エリアで、「ボリューム」セクションの容量バーの下で、「装置」の横に報告されている状況を確認します。「<b>重大</b>」または「<b>警告</b>」状況がいずれかの装置について表示されている場合は、問題を調べてください。詳細を表示するには、「装置」をクリックします。</p>	<p>ドライブを使用できない場合、テープ装置が警告状況または重大状況になる可能性があります。ドライブがオフラインの場合、サーバーに対する応答を停止した場合、またはそのドライブのパスがオフラインの場合に、ドライブは使用不可になります。ライブラリーがオフラインの場合も、テープ装置が重大状況になる可能性があります。「テープ装置」表のその他の列は、ライブラリー・ロボット装置、ドライブ、およびパスの状態を示します。</p> <p>重大状態の磁気テープ・ドライブに関する問題を解決するには、保守など他のアクティビティーに使用する必要がある場合は、ドライブをオフラインにすることができます。ドライブをオフラインにするには、以下のステップを実行します。</p> <ol style="list-style-type: none"> <li>1. Operations Center の「<b>ストレージ</b>」ページで、テープ装置を選択します。</li> <li>2. テープ・ライブラリーの詳細情報を表示するには、行を選択して「<b>詳細</b>」をクリックします。</li> <li>3. ドライブをオフラインにするには、磁気テープ・ドライブを選択し、「<b>オフライン</b>」をクリックします。</li> </ol> <p>テープ・バックアップ操作では、十分なスクラッチ・テープが使用可能であることを確認してください。使用可能なスクラッチ・テープの数が十分であるかが不明な場合は、詳細ノートブックを開いてテープ使用量と、使用可能なスクラッチ・テープの推定値を参照してください。詳細ノートブックを開くには、表でライブラリーを選択し、「<b>詳細</b>」をクリックします。</p>

表 27. 日次モニター・タスク (続き)






タスク	基本的な手順	詳細手順およびトラブルシューティング情報
<p><b>10</b> 保存セットをモニターします。</p>	<p>保存セットの全体的な状況を取得するには、Operations Center の「概要」ページで「保存セット」エリアを確認します。</p> <ul style="list-style-type: none"> <li>「完了」フィールドは、サーバー・データベースで作成され、サーバー・インベントリ内で追跡される保存セットの数を指定します。</li> <li>「有効期限切れ」フィールドは、データの有効期限が切れる保存セットの数を指定します。</li> <li>「削除済み」フィールドは、削除された保存セットの数を指定します。</li> </ul> <p>保存ルールを表示または変更するには、「サービス」 &gt; 「保存ルール」をクリックします。</p>	<p>保存セットについて詳しくは、「保存セット」エリアをクリックし、「保存セット」ページを開きます。保存セット・プロパティを表示または変更するには、保存セットをダブルクリックします。</p> <p>詳細情報については以下の関連コマンドを実行します。</p> <ol style="list-style-type: none"> <li>Operations Center の「概要」ページで、設定アイコン  の上にカーソルを移動し、「コマンド・ビルダー」をクリックします。</li> <li>実行中、中断、または完了済みの保存セット作成ジョブを判別するには、<b>QUERY JOB</b> コマンドを実行します。手順については、<a href="#">QUERY JOB (ジョブの照会)</a>を参照してください。</li> <li>保存ルールを照会するには、<b>QUERY RETRULE</b> コマンドを実行します。手順については、<a href="#">QUERY RETRULE (保存ルールの照会)</a>を参照してください。</li> <li>保存セットを照会するには、<b>QUERY RESET</b> コマンドを実行します。手順については、<a href="#">QUERY RESET (保存セットの照会)</a>を参照してください。</li> <li>保存セットの内容を照会するには、<b>QUERY RESETCONTENTS</b> コマンドを実行します。手順については、<a href="#">QUERY RESETCONTENTS (保存セットの内容の照会)</a>を参照してください。</li> </ol>



表 27. 日次モニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
<p><b>11</b> ストレージ・ルールをモニターします。</p>	<p>ストレージ・ルール操作の全体的な状況を取得するには、Operations Center の「概要」ページで「ストレージ・ルール」エリアを確認します。</p>	<p>状況要約には、ストレージ・ルールの最新の処理結果が表示されます。以下の各状態にあるストレージ・ルールの数が示されます。</p> <p> <b>正常</b> エラーなしで実行されたストレージ・ルールの数。</p> <p> <b>警告</b> 処理を完了したが、適格データを一部のみ移動またはコピーしたストレージ・ルールの数。一部のファイルがスキップされたか、ルールの制限時間に達したか、または処理が取り消されました。</p> <p> <b>失敗</b> 処理を完了しなかったストレージ・ルールの数。例えば、ターゲット・ストレージ・プールに十分なスペースがないため、あるいはサーバーがストレージ・プールにアクセスできないために、サーバーがデータの処理に失敗する場合があります。</p> <p> <b>その他の状態</b> その他の状態のストレージ・ルールの数。ストレージ・ルールが定義されているサーバーが、データの提供に使用できないか、または状況をサポートしていない以前のバージョンの IBM Spectrum Protect を実行している可能性があります。ストレージ・ルールがアクティブ化されていないか、実行されなかったために、状況が適用されない場合があります。</p> <p><b>ヒント:</b></p> <ul style="list-style-type: none"> <li>アイコンが表示されるのは、1 つ以上のストレージ・ルールが対応する状態にある場合のみです。各ストレージ・ルールの詳細情報を表示するには、「ストレージ・ルール」をクリックして、「ストレージ・ルール」ページを表示します。</li> <li>実行中または完了済みのストレージ・ルール・ジョブを判別するには、<b>QUERY JOB</b> コマンドを実行します。手順については、<a href="#">QUERY JOB (ジョブの照会)</a>を参照してください。</li> </ul>

## 定期的なモニター・チェックリスト

---

操作を適切に実行できるようにするために、定期的なモニター・チェックリストのタスクを実行します。大きな問題となる前に潜在的な問題点を検出できるように、十分な頻度で定期的なタスクをスケジュールしてください。


**ヒント：**拡張モニター・タスクの管理コマンドを実行するには、Operations Center コマンド・ビルダーを使用します。コマンド・ビルダーは、コマンドを入力するときにガイドとなる先行入力機能を提供します。コマンド・ビルダーを開くには、Operations Center の「概要」ページに進みます。メニュー・バーで、設定アイコン  にマウス・カーソルを移動し、「コマンド・ビルダー」をクリックします。

表 28. 定期的なモニター・タスク

タスク	基本的な手順	詳細手順およびトラブルシューティング
システム・パフォーマンスをモニターします。	<p>クライアント・バックアップ操作に必要な時間の長さを判別します。</p> <ol style="list-style-type: none"> <li>1. Operations Center の「<b>概要</b>」ページで、「<b>クライアント</b>」をクリックします。クライアントに関連付けられているサーバーを見つけます。</li> <li>2. 「<b>サーバー</b>」をクリックします。サーバーを選択し、「<b>詳細</b>」をクリックします。</li> <li>3. 過去 24 時間の完了タスクの所要時間を表示するには、「<b>完了タスク</b>」をクリックします。</li> <li>4. 24 時間より前に完了したタスクの期間を表示するには、<b>QUERY ACTLOG</b> コマンドを使用します。このコマンドについては、<a href="#">QUERY ACTLOG (活動記録ログの照会)</a>を参照してください。</li> <li>5. クライアント・バックアップ操作の所要時間が長くなっている、理由が不明である場合は、原因を調べてください。</li> </ol> <p>バックアップ/アーカイブ・クライアントにクライアント管理サービスをインストールしている場合、以下のステップを実行して、バックアップ/アーカイブ・クライアントのパフォーマンスの問題を診断することができます。</p> <ol style="list-style-type: none"> <li>1. Operations Center の「<b>概要</b>」ページで、「<b>クライアント</b>」をクリックします。</li> <li>2. バックアップ/アーカイブ・クライアントを選択して、「<b>詳細</b>」をクリックします。</li> <li>3. クライアント・ログを取得するには、「<b>診断</b>」をクリックします。</li> </ol>	<p>クライアント・バックアップ操作の時間を 8 時間から 12 時間に制限します。クライアント・スケジュールがサーバー保守タスクとオーバーラップしないようにしてください。</p> <p>クライアントがサーバーにデータをバックアップするのにかかる時間を短縮するための手順については、<a href="#">一般的なクライアントのパフォーマンス問題の解決</a>を参照してください。</p> <p>パフォーマンスのボトルネックを探してください。手順については、<a href="#">パフォーマンス・ボトルネックの識別</a>を参照してください。</p> <p>その他のパフォーマンスの問題の識別および解決については、<a href="#">パフォーマンス</a>を参照してください。</p>

表 28. 定期的なモニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング
<p>装置構成およびボリューム・ヒストリー情報の現行のバックアップ・ファイルが保存されていることを確認します。</p>	<p>保管場所にアクセスして、ファイルを使用できることを確認します。推奨される方法は、バックアップ・ファイルを2つの場所に保存することです。</p> <p>ボリューム・ヒストリーおよび装置構成ファイルを見つけるには、以下の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. Operations Center の「概要」ページで、設定アイコンにマウス・カーソルを移動し、「<b>コマンド・ビルダー</b>」をクリックします。</li> <li>2. ボリューム・ヒストリーおよび装置構成ファイルを見つけるには、次のコマンドを発行します。 <div data-bbox="532 804 906 856" data-label="Text"> <pre>query option volhistory</pre> </div> <div data-bbox="532 867 906 919" data-label="Text"> <pre>query option devconfig</pre> </div> </li> <li>3. 出力で「オプション設定」列を確認して、ファイルの場所を見つけます。</li> </ol> <p>災害が発生した場合、サーバー・データベースをリストアするためには、ボリューム・ヒストリー・ファイルと装置構成ファイルの両方が必要です。</p>	

表 28. 定期的なモニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング
<p>サーバー・インスタンスのディレクトリー内に使用可能なスペースが十分にあるかどうかを判別します。</p>	<p>サーバー・インスタンスのディレクトリー内で少なくとも 50 GB のフリー・スペースが使用可能であることを確認します。ご使用のオペレーティング・システムに適した処置を実行します。</p> <ul style="list-style-type: none"> <li> <b>AIX</b> ファイル・システム内で使用可能なスペースを表示するには、オペレーティング・システムのコマンド・ラインで以下のコマンドを発行します。 <pre>df -g instance_directory</pre> <p>ここで、<i>instance_directory</i> は、インスタンス・ディレクトリーを指定します。</p> </li> <li> <b>Linux</b> ファイル・システム内で使用可能なスペースを表示するには、オペレーティング・システムのコマンド・ラインで以下のコマンドを発行します。 <pre>df -h instance_directory</pre> <p>ここで、<i>instance_directory</i> は、インスタンス・ディレクトリーを指定します。</p> </li> <li> <b>Windows</b> Windows エクスプローラー・プログラムで、ファイル・システムを右クリックして、「<b>プロパティ</b>」をクリックします。容量情報を表示します。 </li> </ul> <p>インスタンス・ディレクトリーの推奨される場所は、サーバーがインストールされているオペレーティング・システムによって異なります。</p> <ul style="list-style-type: none"> <li> <b>Linux   AIX</b> /home/tsminst1/tsminst1 </li> <li> <b>Windows</b> C:¥tsminst1 </li> </ul> <p><b>ヒント:</b> 計画ワークシートを完了している場合、インスタンス・ディレクトリーの場所はワークシートに記録されています。</p>	

表 28. 定期的なモニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング
予期しないクライアント・アクティビティを識別します。	<p>クライアント・アクティビティをモニターして、データ・ボリュームが予期した容量を超えているかどうかを判別するには、以下の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. Operations Center の「概要」ページで、「クライアント」エリアをクリックします。</li> <li>2. 過去 2 週間のアクティビティを表示するには、任意のクライアントをダブルクリックします。</li> <li>3. クライアントに送信されたバイト数を表示するには、「プロパティ」タブをクリックします。</li> <li>4. 「最終セッション」エリアで、「クライアントに送信」行を確認します。</li> </ol>	<p>「クライアント」テーブルでクライアントをダブルクリックすると、「<b>2 週間のアクティビティ</b>」エリアに、クライアントが毎日サーバーに送信したデータの容量が表示されます。</p> <p>クライアント・セッションに関する統計が入っている SQL アクティビティの要約テーブルを定期的に確認してください。現在のアクティビティと過去のアクティビティを比較する場合、SQL SELECT ステートメントを使用してください。アクティビティのレベルが前のアクティビティとは大きく異なる場合、ランサムウェア攻撃を示している可能性があります。</p> <p>アクティビティ・ログを定期的に確認してください。バックアップされ、検査されたファイルの数を示す ANE メッセージを検索してください。現在のデータ重複排除率を前の率と比べてください。バックアップされたファイル数が異常に多かった場合、またはデータ重複排除率が予期せずに 0 まで落ちた場合に、それはランサムウェア攻撃を示している可能性があります。</p>



表 28. 定期的なモニター・タスク (続き)		
タスク	基本的な手順	詳細手順およびトラブルシューティング
<p>時間の経過に伴うストレージ・プールの増大をモニターします。</p>	<ol style="list-style-type: none"> <li>1. Operations Center の「概要」ページで、「プール」エリアをクリックします。</li> <li>2. 過去 2 週間に使用された容量を表示するには、プールを選択して、「詳細」をクリックします。</li> </ol>	<p><b>ヒント：</b></p> <ul style="list-style-type: none"> <li>重複排除されたエクステントが参照されなくなった後、それらのエクステントすべてをディレクトリー・コンテナ・ストレージ・プールまたはクラウド・コンテナ・ストレージ・プールから除去するまでの期間を指定するには、以下のステップを実行します。 <ol style="list-style-type: none"> <li>1. Operations Center の「ストレージ・プール」ページで、ストレージ・プールを選択します。</li> <li>2. 「詳細」 &gt; 「プロパティ」をクリックします。</li> <li>3. 「コンテナ再利用の遅延期間」フィールドに期間を指定します。</li> </ol> </li> <li>ディレクトリー・コンテナ・ストレージ・プールとクラウド・コンテナ・ストレージ・プールのデータ重複排除のパフォーマンスを判別するには、<b>GENERATE DEDUPSTATS</b> コマンドを使用します。</li> <li>ストレージ・プールのデータ重複排除の統計を表示するには、以下の手順を実行します。 <ol style="list-style-type: none"> <li>1. Operations Center の「ストレージ・プール」ページで、ストレージ・プールを選択します。</li> <li>2. 「詳細」 &gt; 「プロパティ」をクリックします。</li> </ol> <p>あるいは、<b>QUERY EXTENTUPDATES</b> コマンドを使用して、ディレクトリー・コンテナ・ストレージ・プールまたはクラウド・コンテナ・ストレージ・プール内のデータ・エクステントに対する更新の情報を表示します。このコマンド出力は、参照されなくなったデータ・エクステント、およびシステムから削除するのに適格なデータ・エクステントを判別するのに役立ちます。出力で、システムから削除するのに適格なデータ・エクステントの数をモニターします。この測定基準には、コンテナ・ストレージ・プール内で使用可能なフリー・スペースの量と直接的な相関関係があります。</p> </li> <li>データ重複排除による節約量を取り除いた後、ファイル・スペースにより占有される物理スペースの量を表示するには、<b>select * from occupancy</b> コマンドを使用します。コマンド出力には LOGICAL_MB 値が含まれます。LOGICAL_MB は、このファイル・スペースによって使用されているスペース量です。</li> </ul>

表 28. 定期的なモニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング
<p>テープ装置をモニターおよび保守します。</p>	<p>磁気テープ・ドライブやテープ・ライブラリーにハードウェア・エラーがないか、ご使用の環境をモニターします。手順については、<a href="#">154 ページの『ハードウェア・エラーに関するテープ・アラート・メッセージのモニター』</a>を参照してください。</p> <p>磁気テープ・ドライブでのエラーを防止するために、メディアの互換性をモニターします。手順については、<a href="#">154 ページの『メディアの非互換性によるエラーの防止』</a>を参照してください。</p> <p>磁気テープ・ドライブのクリーニング・メッセージをモニターします。手順については、<a href="#">155 ページの『クリーナー・カートリッジでの操作』</a>を参照してください。</p>	
<p>クライアント・スケジュールのタイミングを評価します。クライアント・スケジュールの開始時刻と終了時刻がサーバー保守タスクとオーバーラップしていないことを確認します。クライアント・バックアップ操作の時間を 8 時間から 12 時間に制限します。</p>	<p>Operations Center の「<b>概要</b>」ページで、「<b>クライアント</b>」&gt;「<b>スケジュール</b>」をクリックします。</p> <p>「スケジュール」テーブルで、「開始」列に、スケジュール済み操作用に構成された開始時刻が表示されます。最近の操作が開始された時刻を確認するには、クロック・アイコンの上にカーソルを移動します。</p>	<p><b>ヒント:</b> クライアント操作が予想以上に長く実行されている場合に警告メッセージを受け取ることができます。次の手順を実行してください。</p> <ol style="list-style-type: none"> <li>1. Operations Center の「概要」ページで、「<b>クライアント</b>」の上にカーソルを移動して、「<b>スケジュール</b>」をクリックします。</li> <li>2. スケジュールを選択して、「<b>詳細</b>」をクリックします。</li> <li>3. 行の横にある青色の矢印をクリックして、スケジュールの詳細を表示します。</li> <li>4. 「<b>ランタイム・アラート</b>」フィールドに、スケジュール済み操作が完了しなかった場合に警告メッセージが発行される時刻を指定します。</li> <li>5. 「<b>保存</b>」をクリックします。</li> </ol>

表 28. 定期的なモニター・タスク (続き)		
タスク	基本的な手順	詳細手順およびトラブルシューティング
保守タスクのタイミングを評価します。保守タスクの開始時刻と終了時刻がクライアント・スケジュールとオーバーラップしていないことを確認します。	<p>Operations Center の「概要」ページで、「サーバー」 &gt; 「保守」をクリックします。</p> <p>「保守」テーブルで、「最終実行時刻」列の情報を確認します。最後の保守タスクが開始された時刻を確認するには、クロック・アイコンの上にカーソルを移動します。</p>	<p>各保守タスクが次の保守タスクの開始前に実行を完了するようにする方法が推奨されます。保守タスクの例には、インベントリ・期限切れ、ストレージ・プールのコピー、スペース・レクラメーション、およびデータベース・バックアップが含まれます。</p> <p><b>ヒント:</b> 保守タスクの実行時間が長すぎる場合、開始時刻または最大実行時間を変更します。次の手順を実行してください。</p> <ol style="list-style-type: none"> <li>1. Operations Center の「概要」ページで、設定アイコンにマウス・カーソルを移動し、「コマンド・ビルダー」をクリックします。</li> <li>2. タスクの開始時刻または最大実行時間を変更するには、<b>UPDATE SCHEDULE</b> コマンドを発行します。このコマンドについては、<a href="#">UPDATE SCHEDULE (クライアント・スケジュールの更新)</a>を参照してください。</li> </ol>

#### 関連情報

[QUERY ACTLOG \(活動記録ログの照会\)](#)

## ハードウェア・エラーに関するテープ・アラート・メッセージのモニター

テープ・アラート・メッセージは、ハードウェア・エラーを報告するために、テープ装置およびライブラリー装置によって生成されます。このメッセージは、サーバーに関連のない問題を判別するのに便利です。

### このタスクについて

ログ・ページが作成され、いつでも、またはドライブを取り外すときなどの特定のときに検索することができます。

テープ・アラート・メッセージには、以下のいずれかの重大度レベルがあります。

- 通知 (サポートされていないカートリッジ・タイプをロードしようとした場合など)
- 警告 (ハードウェア障害が予想される場合など)
- 重大 (磁気テープに問題があり、データが危険な状態にある場合など)

テープ・アラート・メッセージは、デフォルトではオフになっています。

### 手順

- テープ・アラート・メッセージを有効にするには、次のように **SET TAPEALERTMSG** コマンドを発行して **ON** 値を指定します: `set tapealertmsg on`
- テープ・アラート・メッセージが有効にされているかどうかを確認するには、次のように **QUERY TAPEALERTMSG** コマンドを発行します: `query tapealertmsg`

## メディアの非互換性によるエラーの防止

メディアの互換性の問題をモニターして解決することで、テープ・ベースのソリューションでのエラーを防止することができます。新規ドライブは、以前のバージョンのドライブでサポートされていたメディア・

フォーマットを限定的にしか使用できない場合があります。多くの場合、新規ドライブは、以前のメディア・フォーマットの読み取りはできますが書き込みができません。

## このタスクについて

デフォルトでは、FILLING 状況の既存のボリュームは、ドライブのアップグレード後もその状態のままです。場合によっては、これらのボリュームを充てんするために以前のドライブを使用し続けることができます。これにより、既存のボリュームのレクラメーション処理が行われるまで、既存のボリュームの読み取り/書き込み機能が保持されます。ライブラリー内のすべてのドライブをアップグレードする場合は、新規ハードウェアでメディア・フォーマットがサポートされていることを確認してください。新規ドライブで最新のメディアのみを使用する予定でない限り、すべての互換性の問題を知っておく必要があります。マイグレーションの説明については、[208 ページの『アップグレードされたドライブへのデータのマイグレーション』](#)を参照してください。

読み取りはできるが書き込みはできないメディアを新規ドライブで使用するには、**UPDATE VOLUME** コマンドを発行して、そのボリュームへのアクセスを読み取り専用に設定してください。これにより、読み取り/書き込みの非互換性により生じるエラーを防ぐことができます。例えば、新規ドライブは、そのドライブがサポートしていないフォーマットで書き込まれたメディアがドライブにロードされると、即時にそのメディアを排出する場合があります。あるいは、新規ドライブでは、そのドライブがサポートしていないフォーマットで部分的に書き込まれたメディアに対する最初の書き込みコマンドが失敗する場合があります。

読み取り専用メディア上のデータの有効期限が切れ、ボリュームがレクラメーション処理される場合は、そのメディアを、新規ドライブと完全に互換性のあるメディアと置き換えてください。新規ドライブが以前のフォーマットを使用して書き込まれたボリュームを正しく調整することができない場合は、エラーが生じる可能性があります。このような問題を回避するためには、元のドライブが正常に作動し、現行のマикроコード・レベルであることを確認してください。

## クリーナー・カートリッジでの操作

磁気テープ・ドライブが必要ときに確実にクリーニングされるようにし、磁気テープ・ストレージの問題を防止するには、次のガイドラインに従います。

### クリーニング・プロセスのモニター

クリーナー・カートリッジがライブラリーにチェックインされており、ドライブをクリーニングする必要がある場合、サーバーは、データ・ボリュームをマウント解除してクリーニング操作を実行します。クリーニング操作が失敗あるいは取り消されるか、使用可能なクリーナー・カートリッジがない場合、ドライブをクリーニングする必要があることに気付かない可能性があります。このような問題に関するクリーニング・メッセージをモニターして、ドライブが必要時にクリーニングされていることを確認してください。必要に応じて、**CLEAN DRIVE** コマンドを発行してサーバーに再度クリーニングを試行させるか、またはクリーナー・カートリッジを手操作でドライブにロードしてください。

### 複数のクリーナー・カートリッジの使用

1つのクリーナー・カートリッジをチェックインすると、サーバーはそのクリーナー・カートリッジを指定されたクリーニング回数だけ使用します。複数のクリーナー・カートリッジをチェックインすると、そのカートリッジに指定されたクリーニング回数に達するまで、サーバーは1つのカートリッジのみを使用します。その後、サーバーは次のクリーナー・カートリッジを使用します。複数のクリーナー・カートリッジをチェックインして、複数の **CLEAN DRIVE** コマンドを同時に発行すると、サーバーは同時に複数のカートリッジを使用して、各カートリッジの残りのクリーニング回数を減らします。

### 関連情報

[AUDIT LIBRARY \(自動化ライブラリーにあるボリューム・インベントリーの監査\)](#)

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[CLEAN DRIVE \(ドライブのクリーニング\)](#)

[LABEL LIBVOLUME \(ライブラリー・ボリュームのラベル付け\)](#)

[QUERY LIBVOLUME \(ライブラリー・ボリュームの照会\)](#)

## ライセンス準拠の検証

IBM Spectrum Protect ソリューションがご使用条件の条項に準拠していることを確認します。準拠を定期的に確認することで、データの増加またはプロセッサ・バリュー・ユニット (PVU) 使用量の傾向を追跡できます。この情報を使用して、将来のライセンスの購入について計画します。

### このタスクについて

ご使用のソリューションがライセンス条件に準拠しているかを確認するために使用する方法は、IBM Spectrum Protect のご使用条件の条項によって異なります。

#### フロントエンド・キャパシティー・ライセンス

フロントエンド・モデルでは、クライアントによってバックアップされていることが報告された 1 次データの量に基づいてライセンス要件が決定されます。クライアントには、アプリケーション、仮想マシン、およびシステムが含まれます。

#### バックエンド・キャパシティー・ライセンス

バックエンド・モデルでは、1 次ストレージ・プールおよびリポジトリに保管されているデータのテラバイト単位に基づいてライセンス要件が決定されます。

#### ヒント:

- フロントエンドおよびバックエンドの容量見積りの正確性を確保するには、各クライアント・ノードに最新バージョンのクライアント・ソフトウェアをインストールします。
- Operations Center のフロントエンドおよびバックエンドの容量情報は、計画と見積りを目的として使用されます。

#### PVU ライセンス

PVU モデルは、サーバー装置による PVU の使用量に基づいています。


**重要:** IBM Spectrum Protect によって提供される PVU の計算は見積もりと見なされ、法的拘束力はありません。IBM Spectrum Protect によって報告される PVU ライセンス情報は、IBM License Metric Tool の受け入れ可能な代替とは見なされません。IBM License Metric Tool は実際の使用状況を反映するように設計されています。例えば、IBM Spectrum Protect バックアップ/アーカイブ・クライアントのインストール後、ツールでは初回の使用の後にのみ、クライアントをカウントします。IBM License Metric Tool について詳しくは、[IBM ライセンス・メトリック・ツール](#)を参照してください。


ライセンス要件について質問または懸念がある場合は、IBM Spectrum Protect ソフトウェア・プロバイダーにお問い合わせください。

### 手順

ライセンス準拠をモニターするには、ご使用条件の条項に対応しているステップを実行します。

**ヒント:** Operations Center は、フロントエンドおよびバックエンドの容量使用量の概要を示す E メール・レポートを提供します。レポートは、定期的に 1 人以上の受信者に自動的に送信することができます。E メール・レポートを構成して管理するには、Operations Center メニュー・バーの「**レポート**」をクリックします。

オプション	説明
フロントエンド・モデル	<p>a. Operations Center メニュー・バーで、設定アイコン  の上にカーソルを移動して、「<b>ライセンス交付</b>」をクリックします。</p> <p>フロントエンド・キャパシティーの見積もりが「フロントエンド使用量 (Front-end Usage)」ページに表示されます。</p> <p>b. 「報告なし (Not Reporting)」列に値が表示される場合は、番号をクリックして、容量使用量を報告しなかったクライアントを特定します。</p>

オプション	説明
	<p>c. 容量使用量を報告しなかったクライアントの容量を見積もるには、測定ツールと説明を提供する次のダウンロード・サイトにアクセスします。</p> <p><a href="https://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools">https://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</a></p> <p>スクリプトによってフロントエンド容量を測定するには、入手可能な最新のライセンス交付ガイドの手順を実行します。</p> <p>d. Operations Center の見積もりと、スクリプトを使用して得られた見積もりを加算します。</p> <p>e. 見積もられた容量がご使用条件に準拠していることを確認します。</p>
バックエンド・モデル	<p><b>制約事項:</b> ソース複製サーバーとターゲット複製サーバーが同じポリシー設定を使用していない場合、Operations Center を使用して、複製されたクライアントのバックエンド容量の使用量をモニターすることはできません。これらのクライアントの容量使用量を見積もる方法については、<a href="#">技術情報 1656476</a> を参照してください。</p> <p>a. Operations Center メニュー・バーで、設定アイコン  の上にカーソルを移動して、「ライセンス交付」をクリックします。</p> <p>b. 「バックエンド (Back-end)」タブをクリックします。</p> <p>c. データの見積もり容量がご使用条件に準拠していることを確認します。</p>
PVU モデル	<p>PVU ライセンス交付条件の準拠性を評価する方法については、<a href="#">PVU ライセンス・モデルの準拠性の評価</a>を参照してください。</p>

## E メール・レポートを使用したシステム状況のトラッキング

システム状況を要約する E メール・レポートを生成するように Operations Center をセットアップします。メール・サーバー接続の構成、レポート設定の変更、オプションのカスタム・レポートの作成を実行できます。

### 始める前に

E メール・レポートをセットアップする前に、以下の要件が満たされていることを確認します。

- レポートを E メールで送受信するために Simple Mail Transfer Protocol (SMTP) ホスト・サーバーを使用できます。SMTP サーバーは、オープン・メール・リレーとして構成されている必要があります。また、E メール・メッセージを送信する IBM Spectrum Protect サーバーに、SMTP サーバーへのアクセス権限があることを確認する必要があります。Operations Center が別のコンピューターにインストールされている場合、そのコンピューターには、SMTP サーバーへのアクセス権限は必要ありません。
- E メール・レポートをセットアップするには、サーバーのシステム特権が必要です。
- 受信者を指定するために、1 つ以上の E メール・アドレスまたは管理者 ID を入力できます。管理者 ID を入力する予定の場合は、ID がハブ・サーバーに登録されていて、その ID に E メール・アドレスが関連付けられている必要があります。管理者の E メール・アドレスを指定するには、**UPDATE ADMIN** コマンドの **EMAILADDRESS** パラメーターを使用します。

### このタスクについて

一般的な運用レポート、ライセンス準拠レポート、1 つ以上のカスタム・レポートを送信するように Operations Center を構成できます。カスタム・レポートを作成する際は、よく使われるレポート・テンプレ



レポートのセットからテンプレートを選択するか、管理対象サーバーを照会するために SQL SELECT ステートメントを入力します。

## 手順

E メール・レポートをセットアップして管理するには、以下の手順を実行します。

1. Operations Center メニュー・バーで、「**レポート**」をクリックします。
2. E メール・サーバー接続がまだ構成されていない場合は、「**メール・サーバーの構成**」をクリックして、フィールドに入力します。  
メール・サーバーを構成すると、一般的な運用レポートとライセンス準拠レポートが有効になります。
3. レポート設定を変更するには、レポートを選択し、「**詳細**」をクリックして、フォームを更新します。
4. オプション: カスタム・レポートを追加するには、「**+ レポート**」をクリックし、フィールドに入力します。

**ヒント:** レポートを即時に実行して送信するには、レポートを選択して「**送信**」をクリックします。

## タスクの結果

指定された設定に基づいて、有効になったレポートが送信されます。

## 次のタスク

一般的な運用レポートには、添付ファイルが含まれています。詳細情報を確認するには、添付ファイルのセクションを展開します。

レポートの画像を表示できない場合は、HTML を別の形式に変換する E メール・クライアントを使用している可能性があります。制約事項については、Operations Center オンライン・ヘルプを参照してください。

---

## 第 4 部 テープ・ソリューションの操作の管理

この情報を使用して、IBM Spectrum Protect サーバーでのテープ実装の操作を管理します。

### Operations Center の管理

---

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。

#### このタスクについて

Operations Center を使用して、複数のサーバーをモニターし、いくつかの管理タスクを実行することができます。また、Operations Center では、IBM Spectrum Protect コマンド・ラインへの Web アクセスも可能です。Operations Center の管理について詳しくは、[Operations Center の管理](#)を参照してください。

### クライアントの操作の管理

---

クライアント・エラーの解決、クライアント・アップグレードの管理、および不要になったクライアント・ノードの廃止を行うことができます。サーバー上のストレージ・スペースを解放するために、アプリケーション・クライアントによって保管された廃止データを非アクティブ化することができます。

#### このタスクについて

場合によっては、クライアント・アクセプターを停止してから開始することで、クライアント・エラーを解決できることがあります。クライアント・ノードまたは管理者 ID がロックされている場合は、クライアント・ノードまたは管理者 ID をアンロックすることで問題を解決してから、パスワードをリセットすることができます。

クライアント・エラーの特定および解決に関する詳細な手順については、[クライアントの問題の解決](#)を参照してください。

クライアントの追加手順については、[108 ページの『アプリケーションおよびシステムの保護』](#)を参照してください。

### クライアント・エラー・ログのエラーの評価

---

Operations Center からの提案を取得するか、クライアント上のエラー・ログを調べると、クライアント・エラーを解決することができます。

#### 始める前に

オプションで、Linux オペレーティング・システムまたは Windows オペレーティング・システムでバックアップ/アーカイブ・クライアントのエラーを解決するには、クライアント管理サービスがインストール済みで開始されている必要があります。インストールの手順については、[クライアント管理サービスのインストール](#)を参照してください。

#### 手順

クライアント・エラーを診断して解決するには、以下のいずれかの処置を行ってください。

- クライアント管理サービスがクライアント・ノードにインストールされている場合は、以下の手順を実行してください。
  - a) Operations Center の「概要」ページで、「クライアント」をクリックして、クライアントを選択します。

- b) 「詳細」をクリックします。
- c) クライアントの「要約」ページで、「診断」タブをクリックします。
- d) 取得したログ・メッセージを確認します。

**ヒント：**

- 「クライアント・ログ」ペインを表示するか非表示にするには、「クライアント・ログ」バーをダブルクリックします。
- 「クライアント・ログ」ペインのサイズを変更するには、「クライアント・ログ」バーをクリックしてドラッグします。

「診断」ページに提案が表示された場合は、提案を選択します。「クライアント・ログ」ペインで、提案に関連するクライアント・ログ・メッセージが強調表示されます。

- e) 提案を使用して、エラー・メッセージに示された問題を解決します。

**ヒント：**提案は、クライアント・メッセージのサブセットでのみ提供されます。

- クライアント管理サービスがクライアント・ノードにインストールされていない場合は、インストール済みのクライアントのエラー・ログを確認してください。

## クライアント・アクセプターの停止および再始動

ソリューションの構成を変更する場合、バックアップ/アーカイブ・クライアントがインストールされているすべてのクライアント・ノードでクライアント・アクセプターを再開する必要があります。

### このタスクについて

場合によっては、クライアント・アクセプターを停止してから再開することにより、クライアント・スケジューリングの問題を解決できることがあります。スケジュールされた操作を確実にクライアントで実行できるように、クライアント・アクセプターが実行されている必要があります。例えば、サーバーの IP アドレスまたはドメイン名を変更する場合、クライアント・アクセプターを再開する必要があります。

### 手順

クライアント・ノードにインストールされているオペレーティング・システムの手順に従ってください。

#### AIX および Oracle Solaris

- クライアント・アクセプターを停止するには、以下のステップを完了させます。
  - a. コマンド・ラインで次のコマンドを発行して、クライアント・アクセプターのプロセス ID を判別します。

```
ps -ef | grep dsmcad
```

出力を確認します。次の出力例では、6764 がクライアント・アクセプターのプロセス ID です。

```
root 6764      1   0 16:26:35 ?          0:00 /usr/bin/dsmcad
```

- b. コマンド・ラインで以下のコマンドを発行します。

```
kill -9 PID
```

ここで、*PID* は、クライアント・アクセプターのプロセス ID を指定します。

- クライアント・アクセプターを開始するには、コマンド・ラインで次のコマンドを発行します。

```
/usr/bin/dsmcad
```

#### Linux

- クライアント・アクセプターを (再開せずに) 停止するには、次のコマンドを発行します。

```
# service dsmscad stop
```

- ・クライアント・アクセプターを停止して再始動するには、次のコマンドを実行します。

```
# service dsmscad restart
```

## MAC OS X

「アプリケーション」 > 「ユーティリティ」 > 「端末 (Terminal)」をクリックします。

- ・クライアント・アクセプターを停止するには、以下のコマンドを発行します。

```
/bin/launchctl unload -w com.ibm.tivoli.dsmscad
```

- ・クライアント・アクセプターを開始するには、以下のコマンドを発行します。

```
/bin/launchctl load -w com.ibm.tivoli.dsmscad
```

## Windows

- ・クライアント・アクセプター・サービスを停止するには、以下のステップを完了させます。
  - a. 「スタート」 > 「管理ツール」 > 「サービス」をクリックします。
  - b. クライアント・アクセプター・サービスをダブルクリックします。
  - c. 「停止」をクリックしてから、「OK」をクリックします。
- ・クライアント・アクセプター・サービスを再始動するには、以下のステップを完了させます。
  - a. 「スタート」 > 「管理ツール」 > 「サービス」をクリックします。
  - b. クライアント・アクセプター・サービスをダブルクリックします。
  - c. 「開始」をクリックしてから、「OK」をクリックします。

## 関連情報

[クライアントのスケジューリング問題の解決](#)

# パスワードの再設定

クライアント・ノードまたは管理者 ID のパスワードを紛失したり忘れたりした場合は、パスワードをリセットできます。誤ったパスワードを使用してシステムへのアクセスを複数回試みると、クライアント・ノードまたは管理者 ID がロックされる場合があります。この問題を解決する手順を実行できます。

## 手順

パスワードの問題を解決するには、以下のいずれかの処置を行ってください。

- ・バックアップ/アーカイブ・クライアントがクライアント・ノードにインストールされていて、パスワードを紛失したり忘れたりした場合は、以下の手順を実行します。

1. **UPDATE NODE** コマンドを発行して、新規パスワードを生成します。

```
update node node_name new_password forcepwreset=yes
```

ここで、*node\_name* にはクライアント・ノードを指定し、*new\_password* には割り当てるパスワードを指定します。

2. 変更したパスワードについて、クライアント・ノードの所有者に通知します。クライアント・ノードの所有者が指定のパスワードでログインすると、新規パスワードが自動的に生成されます。セキュリティを強化するため、このパスワードはユーザーには表示されません。

**ヒント:** 以前にクライアント・オプション・ファイルで **passwordaccess** オプションを **generate** に設定した場合は、パスワードが自動的に生成されます。

- ・パスワードの問題が原因で管理者がロックアウトされた場合は、以下の手順を実行します。

1. サーバーへのアクセス権限を管理者に付与するには、**UNLOCK ADMIN** コマンドを発行します。手順については、[UNLOCK ADMIN \(管理者のアンロック\)](#)を参照してください。
2. **UPDATE ADMIN** コマンドを使用して新規パスワードを設定します。

```
update admin admin_name new_password forcepwreset=yes
```

ここで、*admin\_name* には管理者の名前を指定し、*new\_password* には割り当てるパスワードを指定します。

- クライアント・ノードがロックされている場合、以下の手順を実行します。
  1. クライアント・ノードがロックされている理由と、そのクライアント・ノードをアンロックする必要があるかどうかを判別します。例えば、クライアント・ノードが廃止されている場合、そのクライアント・ノードは実稼働環境から除去されています。廃止操作を元に戻すことはできないため、クライアント・ノードはロックされたままになります。また、クライアント・データが法的調査の対象である場合に、クライアント・ノードがロックされることもあります。
  2. クライアント・ノードをアンロックする必要がある場合は、**UNLOCK NODE** コマンドを使用します。手順については、[UNLOCK NODE \(クライアント・ノードのアンロック\)](#)を参照してください。
  3. **UPDATE NODE** コマンドを発行して、新規パスワードを生成します。

```
update node node_name new_password forcepwreset=yes
```

ここで、*node\_name* にはノードの名前を指定し、*new\_password* には割り当てるパスワードを指定します。

4. 変更したパスワードについて、クライアント・ノードの所有者に通知します。クライアント・ノードの所有者が指定のパスワードでログインすると、新規パスワードが自動的に生成されます。セキュリティを強化するため、このパスワードはユーザーには表示されません。

**ヒント:** 以前にクライアント・オプション・ファイルで **passwordaccess** オプションを **generate** に設定した場合は、パスワードが自動的に生成されます。

## クライアント・アップグレードの管理

クライアントのフィックスパックまたは暫定修正が入手可能になると、製品の改善点を利用するためにクライアントをアップグレードすることができます。サーバーおよびクライアントは、さまざまな時点で、さまざまなレベルにアップグレードできますが、いくつかの制約事項があります。

### 始める前に

1. [IBM Spectrum Protect のサーバーとクライアントの互換性とアップグレードの考慮事項](#)でクライアント/サーバーの互換性要件を確認します。ソリューションに V7.1 より前のレベルのサーバーまたはクライアントが含まれている場合、ガイドラインを調べて、クライアント・バックアップおよびアーカイブの操作が中断されないようにしてください。
2. [Supported Operating Systems](#) で、クライアントのシステム 要件を確認します。
3. ソリューションにストレージ・エージェントまたはライブラリー・クライアントが含まれている場合、ライブラリー・マネージャーとして構成されているサーバーとのストレージ・エージェントおよびライブラリー・クライアントの互換性に関する情報を確認してください。[IBM Spectrum Protect サーバーとストレージ・エージェントおよびライブラリー・クライアントの互換性](#)を参照してください。

ライブラリー・マネージャーおよびライブラリー・クライアントをアップグレードする 予定の場合は、最初にライブラリー・マネージャーをアップグレードする必要があります。

### 手順

ソフトウェアをアップグレードするには、以下の表にリストされた手順を実行します。

ソフトウェア	説明へのリンク
IBM Spectrum Protect バックアップ/アーカイブ・クライアント	<ul style="list-style-type: none"> <li>• <a href="#">クライアント更新のスケジュール</a></li> </ul>
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> <li>• <a href="#">for UNIX and Linux のインストールおよびアップグレード</a></li> <li>• <a href="#">for VMware のインストールおよびアップグレード</a></li> <li>• <a href="#">for Windows のインストールおよび更新</a></li> </ul>
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"> <li>• <a href="#">Data Protection for SQL Server のアップグレード</a></li> <li>• <a href="#">Data Protection for Oracle のインストール</a></li> <li>• <a href="#">のインストール、アップグレード、およびマイグレーション</a></li> </ul>
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> <li>• <a href="#">のアップグレード</a></li> <li>• <a href="#">のアップグレード</a></li> </ul>
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> <li>• <a href="#">UNIX、AIX、または Linux システムへの Data Protection for IBM Domino のインストール (V7.1.0)</a></li> <li>• <a href="#">Windows システムへの Data Protection for IBM Domino のインストール (V7.1.0)</a></li> <li>• <a href="#">のインストール、アップグレード、およびマイグレーション</a></li> </ul>
IBM Spectrum Protect for Virtual Environments	<ul style="list-style-type: none"> <li>• <a href="#">のインストールおよびアップグレード</a></li> <li>• <a href="#">Data Protection for Microsoft Hyper-V のインストールとアップグレード</a></li> </ul>

## クライアント・ノードの廃止

クライアント・ノードが不要になった場合、実稼働環境から削除するためのプロセスを開始できます。例えば、ワークステーションが IBM Spectrum Protect サーバーにデータをバックアップしていて、ワークステーションが使用されなくなった場合、ワークステーションを廃止できます。

### このタスクについて

廃止プロセスを開始すると、サーバーは、クライアント・ノードをロックして、サーバーにアクセスできないようにします。クライアント・ノードに属するファイルは段階的に削除され、その後クライアント・ノードが削除されます。以下のタイプのクライアント・ノードを廃止できます。

#### アプリケーション・クライアント・ノード

アプリケーション・クライアント・ノードには、E メール・サーバー、データベース、およびその他のアプリケーションなどがあります。例えば、以下のすべてのアプリケーションがアプリケーション・クライアント・ノードです。

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### システム・クライアント・ノード

システム・クライアント・ノードには、ワークステーション、Network Attached Storage (NAS) ファイル・サーバー、および API クライアントなどがあります。

#### 仮想マシン・クライアント・ノード

仮想マシン・クライアント・ノードは、ハイパーバイザー内の個々のゲスト・ホストで構成されます。各仮想マシンは、ファイル・スペースとして表示されます。



**制約事項:** オブジェクト・クライアント・ノードを廃止することはできません。

クライアント・ノードを廃止するための最も単純な方法は、Operations Center を使用することです。廃止プロセスはバックグラウンドで実行されます。クライアントがクライアント・データを複製するように構成されている場合、Operations Center は、クライアントを廃止する前に、ソース複製サーバーとターゲット複製サーバー上の複製からクライアントを自動的に削除します。

**ヒント:** あるいは、**DECOMMISSION NODE** コマンドまたは **DECOMMISSION VM** コマンドを発行して、クライアント・ノードを廃止できます。この方法は、以下の場合に使用できます。

- 将来の廃止プロセスをスケジュールするか、スクリプトを使用して一連のコマンドを実行するには、廃止プロセスをバックグラウンドで実行することを指定します。
- デバッグの目的で廃止プロセスをモニターするには、廃止プロセスをフォアグラウンドで実行することを指定します。フォアグラウンドでプロセスを実行する場合は、他のタスクを続行する前に処理が完了するまで待つ必要があります。

## 手順

次のアクションのいずれか 1 つを実行してください。

- Operations Center を使用してバックグラウンドでクライアントを廃止するには、以下の手順を実行します。
  - a) Operations Center の「概要」ページで、「クライアント」をクリックして、クライアントを選択します。
  - b) 「その他」 > 「廃止」をクリックします。
- 管理コマンドを使用してクライアント・ノードを廃止するには、以下のいずれかの処置を行ってください。
  - アプリケーションまたはシステムのクライアント・ノードをバックグラウンドで廃止するには、**DECOMMISSION NODE** コマンドを発行します。例えば、クライアント・ノードの名前が AUSTIN である場合、次のコマンドを発行します。

```
decommission node austin
```

- アプリケーションまたはシステムのクライアント・ノードをフォアグラウンドで廃止するには、**DECOMMISSION NODE** コマンドを発行して、wait=yes パラメーターを指定します。例えば、クライアント・ノードの名前が AUSTIN である場合、次のコマンドを発行します。

```
decommission node austin wait=yes
```

- 仮想マシンをバックグラウンドで廃止するには、**DECOMMISSION VM** コマンドを発行します。例えば、データ・センター・ノードが AUSTIN でファイル・スペース ID が 7 の場合、以下のコマンドを発行します。

```
decommission vm austin 7 nametype=fsid
```

仮想マシン名に 1 つ以上のスペースが含まれている場合、名前を二重引用符で囲みます。例えば、仮想マシン名が CODY 2 でファイル・スペース名が ¥VMFULL-CODY 2 の場合、以下のコマンドを発行します。

```
decommission vm austin "\vmfull-cody 2"
```

- 仮想マシンをフォアグラウンドで廃止するには、**DECOMMISSION VM** コマンドを発行して、wait=yes パラメーターを指定します。例えば、次のコマンドを発行します。

```
decommission vm austin 7 nametype=fsid wait=yes
```

仮想マシン名に1つ以上のスペースが含まれている場合、名前を二重引用符で囲みます。例えば、仮想マシン名が CODY 2 でファイル・スペース名が ¥VMFULL-CODY 2 の場合、以下のコマンドを発行します。

```
decommission vm austin "\vmfull-cody 2" wait=yes
```

## 次のタスク

プロセスを実行した直後にユーザー・インターフェースやコマンド出力にエラー・メッセージが表示される場合がありますので、それを注意して確認します。

クライアント・ノードが廃止されたことを確認できます。

1. Operations Center の「概要」ページで、「クライアント」をクリックします。
2. 「クライアント」テーブルの「危険」列で、以下のような状態を確認します。
  - ・「DECOMMISSIONED」状態は、ノードが廃止されていることを示します。
  - ・ヌル値は、ノードが廃止されていないことを示します。
  - ・「PENDING」状態は、ノードを廃止中であるか、廃止プロセスが失敗したことを示します。

**ヒント：**保留中の廃止プロセスの状況を確認したい場合は、次のコマンドを実行します。

```
query process
```

3. コマンドの出力を確認します。

- ・廃止プロセスが進行中の場合、そのプロセスについての状況が表示されます。例えば次のとおりです。

```
query process
```

Process Number	Process Description	Process Status
3	DECOMMISSION NODE	Number of backup objects deactivated for node NODE1: 8 objects deactivated.

- ・廃止プロセスについての状況が表示されなくて、エラー・メッセージも表示されない場合は、プロセスが完了していません。ノードに関連付けられたファイルがまだ非活動化されていない場合、プロセスが完了しない場合があります。ファイルが非活動状態になったあと、廃止プロセスを再度実行してください。
- ・廃止プロセスについての状況が表示されなくて、エラー・メッセージが表示される場合は、プロセスが失敗しています。廃止プロセスを再度実行してください。

## 関連情報

[DECOMMISSION NODE \(クライアント・ノードの廃止\)](#)

[DECOMMISSION VM \(仮想マシンの廃止\)](#)

## ストレージ・スペースを解放するためのデータの非活動化

場合によっては、IBM Spectrum Protect サーバーに保管されているデータを非活動化することができます。非活動化プロセスを実行すると、指定された日時より前に保管されたすべてのバックアップ・データが非活動化され、有効期限が切れると削除されます。こうすると、サーバー上のスペースを解放できます。

## このタスクについて

一部のアプリケーション・クライアントは常にデータを活動バックアップ・データとしてサーバーに保存します。活動バックアップ・データはインベントリ満了ポリシーによって管理されていないので、そのデータは自動的に削除されず、サーバーのストレージ・スペースを無期限に使用します。不要なデータによって使用されているストレージ・スペースを解放するために、データを非活動化することができます。

非活動化プロセスを実行すると、指定された日付より前に保管されたすべての活動バックアップ・データが非活動状態になります。データは、有効期限が切れると削除され、リストアできません。非活動化機能は、Oracle データベースを保護するアプリケーション・クライアントにのみ適用されます。

## 手順

1. Operations Center の「概要」ページで、「クライアント」をクリックします。
2. 「クライアント」テーブルで、1 つ以上のクライアントを選択して、「その他」>「クリーンアップ (Clean Up)」をクリックします。

コマンド・ライン方式: **DEACTIVATE DATA** コマンドを使用して、データを非活動化します。

## 関連情報

[DEACTIVATE DATA \(クライアント・ノードのデータの非活動化\)](#)

# データ・ストレージの管理

効率性を高めるためにデータを管理し、クライアント・データを保管するためのサポート対象装置およびメディアをサーバーに追加します。

## 関連情報

[ストレージ・プール・タイプ](#)

# インベントリー容量の管理

データベース、活動ログ、およびアーカイブ・ログの容量を管理して、ログの状況に基づいてタスク用にインベントリーがサイジングされていることを確認します。

## 始める前に

活動ログとアーカイブ・ログには以下の特性があります。

- 活動ログは最大サイズ 512 GB にすることができます。ご使用のシステム用の活動ログのサイジングについて詳しくは、[12 ページの『ストレージ・アレイの計画』](#)を参照してください。
- アーカイブ・ログ・サイズは、それがインストールされているファイル・システムのサイズに制限されます。アーカイブ・ログのサイズは、活動ログのように定義済みサイズで維持されません。アーカイブ・ログ・ファイルは、必要がなくなったときに自動的に削除されます。

ベスト・プラクティスとして、アーカイブ・ログ・ディレクトリーがフルになった場合にアーカイブ・ログ・ファイルを保管するために、オプションでアーカイブ・フェイルオーバー・ログを作成することができます。

フルになっているインベントリーのコンポーネントを判別するには、Operations Center を確認します。いずれかのインベントリー・コンポーネントのサイズを増やす前に、必ずサーバーを停止してください。

## 手順

- データベース用のディスク・スペースを増やすには、以下のステップを実行します。
  - 別々のドライブまたはファイル・システムで、データベースのディレクトリーを 1 つ以上作成します。
  - **EXTEND DBSPACE** コマンドを実行して、データベースに 1 つ以上のディレクトリーを追加します。このディレクトリーは、データベース・マネージャーのインスタンス・ユーザー ID からアクセス可能でなければなりません。デフォルトで、データはすべてのデータベース・ディレクトリー全体に再配布され、スペースはレクラメーション処理されます。

ヒント:

- データの再配布とスペースのレクラメーション処理を実行するのに必要な時間は、ご使用のデータベースのサイズに応じて変化します。適切な計画を立てていることを確認してください。
- データベース操作での並列処理の整合度を確保するために、必ず既存のディレクトリーと同じサイズのディレクトリーを指定してください。データベース用のディレクトリーの中に他のディレクトリーより小さいものが1つ以上ある場合、並列プリフェッチおよびデータベース分散が最適化される可能性が低下します。
- ・ サーバーを一時停止してから再始動して、新規ディレクトリーを完全に使用します。
- ・ 必要な場合は、データベースを再編成してください。サーバー・データベースの索引および表の再編成を行うと、予期しないデータベースの増加やパフォーマンスの問題を回避するために役立ちます。データベースの再編成について詳しくは、[Tivoli Storage Manager V7.1.1.200 以降のサーバーのデータベースの拡大とパフォーマンス低下問題の解決と防止](#)を参照してください。
- ・ V7.1 以降のサーバーでデータベースのサイズを減らすには、[Tivoli Storage Manager V7.1.1.200 以降のサーバーのデータベースの拡大とパフォーマンス低下問題の解決と防止](#)の情報を参照してください。

**制約事項：**これらのコマンドは入出力アクティビティーを増やすので、サーバーのパフォーマンスに影響を与える可能性があります。パフォーマンス上の問題を最小限に抑えるために、1つのコマンドが完了するまで待ってから、次のコマンドを発行してください。Db2 コマンドは、サーバーの実行中に発行することができます。

- ・ 活動ログのサイズを増やすか減らすには、以下の手順を実行します。
  - a) 活動ログの場所に、増加したログ・サイズに必要なスペースがあることを確認します。
  - b) サーバーを停止します。
  - c) dsmserv.opt ファイルで、**ACTIVELOGSIZE** オプションを活動ログの新規サイズ (メガバイト単位) に更新します。

活動ログ・ファイルのサイズは、ACTIVELOGSIZE オプションの値に基づきます。スペース所要量についてのガイドラインを以下の表に示します。

表 29. ボリュームおよびファイルのスペース要件の見積もり方法	
ACTIVELOGSize オプションの値	ACTIVELOGSize スペースに加えて、活動ログ・ディレクトリー内に予約するフリー・スペース容量
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

活動ログのサイズを最大サイズ 512 GB に変更するには、次のサーバー・オプションを入力します。

```
activelogsiz 524288
```

- d) 新しい活動ログ・ディレクトリーを使用する計画の場合は、**ACTIVELOGDIRECTORY** サーバー・オプションに指定したディレクトリー名を更新します。新しいディレクトリーは空であり、データベース・マネージャーのユーザー ID からアクセス可能でなければなりません。
  - e) サーバーを再始動します。
- ・ ストレージに必要なスペースの量を減らすには、アーカイブ・ログを圧縮します。次のコマンドを発行して、アーカイブ・ログの動的圧縮を有効にします。

```
setopt archlogcompress yes
```

**制約事項：**ボリュームの使用率が高く、過重な作業負荷が続くシステムで **ARCHLOGCOMPRESS** サーバー・オプションを有効にする場合には、注意が必要です。このようなシステム環境でこのオプションを有効にすると、活動ログ・ファイル・システムからアーカイブ・ログ・ファイル・システムへのログ・ファイルのアーカイブが遅延する可能性があります。この遅延によって、活動ログ・ファイル・システムがスペース不足になる場合があります。アーカイブ・ログ圧縮が有効になった後で、必ず、活動ログ・ファイル・システム内の使用可能なスペースをモニターしてください。活動ログ・ディレクトリ

ー・ファイル・システムの使用量がスペース不足状態に近づいてきたら **ARCHLOGCOMPRESS** サーバー・オプションを無効にする必要があります。 **SETOPT** コマンドを使用すると、サーバーを一時停止せずに、アーカイブ・ログの圧縮を即座に無効にできます。

#### 関連情報

[ACTIVELOGSIZE サーバー・オプション](#)

[EXTEND DBSPACE \(データベースのスペースの拡張\)](#)

[SETOPT \(動的更新用サーバー・オプションの設定\)](#)

## スケジュール済み活動のチューニング

保守タスクを毎日スケジュールし、ソリューションが正しく動作するようにしてください。ソリューションのチューニングにより、サーバー・リソースを最大限に活用して、ソリューションで利用可能な各種の機能を効果的に使用します。

### 手順

1. 定期的にシステム・パフォーマンスをモニターし、バックアップ・タスクおよび保守タスクが正常に完了していることを確認します。モニターについて詳しくは、[137 ページの『第3部 テープ・ソリューションのモニター』](#)を参照してください。
2. モニター情報でサーバー・ワークロードが増加していることが示された場合は、計画情報の再検討が必要になる場合があります。以下のケースでシステムの容量が適切であるかを確認します。
  - ・ クライアント数が増加した場合
  - ・ バックアップするデータ量が増加した場合
  - ・ バックアップに使用可能な時間が変更された場合
3. ソリューションにパフォーマンスの問題があるかどうかを判断します。クライアント・スケジュールを参照し、タスクがスケジュールされた時間フレーム内に完了しているかを確認します。
  - a. Operations Center の「**クライアント**」ページで、クライアントを選択します。
  - b. 「**詳細**」をクリックします。
  - c. クライアントの「**要約**」ページから、「**バックアップ済み**」および「**複製済み**」アクティビティを確認し、リスクがないかを識別します。必要に応じて、クライアント・バックアップ操作の時間および頻度を調整します。
4. 以下の保守タスクについて、24 時間以内に正常に完了するように、十分な時間をスケジュールします。
  - a. データベースをバックアップする。
  - b. 満了処理を実行し、サーバー・ストレージからクライアント・バックアップおよびアーカイブ・ファイルのコピーを削除します。

#### 関連情報

[データの重複排除 \(V7.1.1\)](#)

[パフォーマンス](#)

## クライアント・ファイルのコロケーションの使用可能化による操作の最適化

クライアント・ファイルのコロケーションは、ユーザーがストレージ・プールから多くのファイルをリストア、リトリブ、または再呼び出しする際に必要なボリューム・マウントの数を削減します。このように、コロケーションにより、これらの操作に必要な時間が短縮されます。

### このタスクについて

コロケーションが使用可能である場合、サーバーは、ファイルを最少数の順次アクセス・ストレージ・ボリュームに保持しようとします。これらのファイルは、単一のクライアント・ノード、クライアント・ノードのグループ、クライアント・ファイル・スペース、またはファイル・スペースのグループに属する場合があります。プールの定義または更新を行うとき、それぞれの順次アクセス・ストレージ・プール用のコロケーションを設定することができます。

169 ページの図 7 は、3 つのクライアントを持つクライアント・ノードによるコロケーションの例を示し、それぞれのクライアントは、そのクライアントのデータを含む個別のボリュームを持っています。

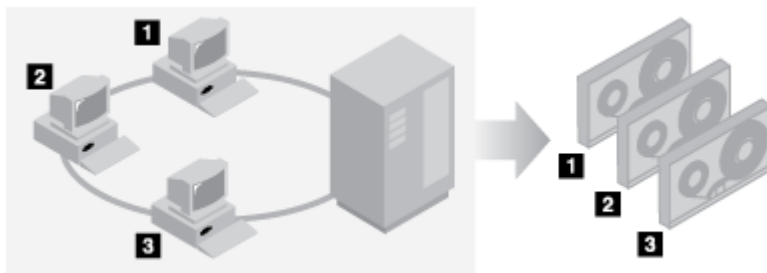


図 7. ノードごとに使用可能にされたコロケーションの例

169 ページの図 8 に、クライアント・ノードのグループによりコロケーションの例を示します。3 つのグループが定義されており、各グループのデータは別個のボリュームに保管されています。

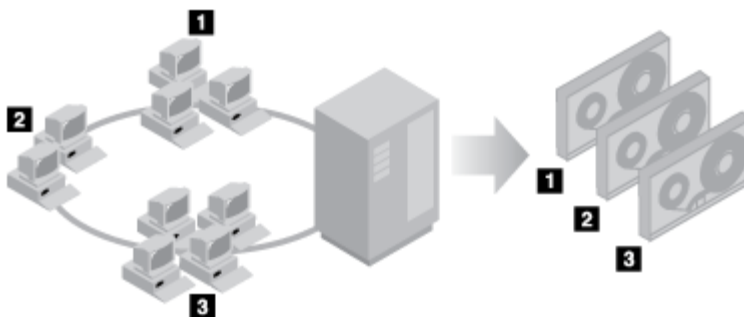


図 8. ノード・コロケーション・グループごとに使用可能にされたコロケーションの例

170 ページの図 9 に、ファイル・スペース・グループによりコロケーションの例を示します。6 つのグループが定義されています。各グループには、単一ノードに属するファイル・スペースからのデータが入っています。グループごとのデータは別々のボリュームに保管されます。



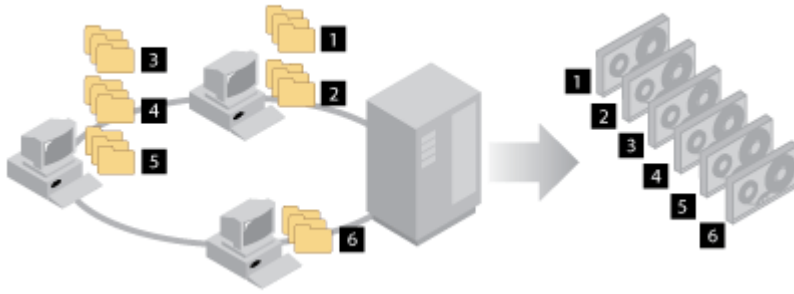


図 9. ファイル・スペース・コロケーション・グループごとに使用可能にされたコロケーションの例

コロケーションが使用不可にされると、サーバーは、新規ボリュームを選択する前に、各ボリューム上のすべての使用可能スペースの使用を試行します。このプロセスは、個々のボリュームの利用率を改善し、同時にユーザー・ファイルを、多くのボリュームにまたがって分散することができます。[170 ページの図 10](#) は、コロケーションが使用不可にされ、3 つのクライアントが単一ボリューム上のスペースを共有している例を示しています。

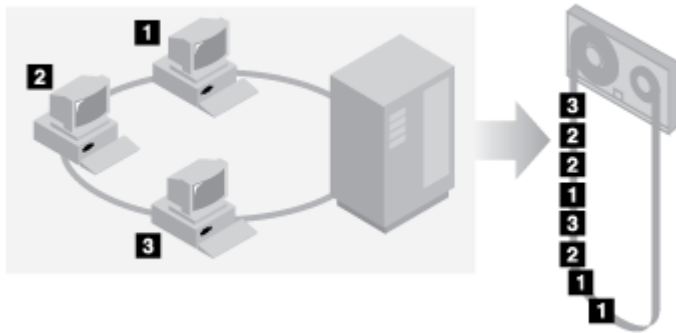


図 10. 使用不可にされたコロケーションの例

コロケーションを使用不可にすると、ユーザーが多くのファイルをリストア、リトリブ、または再呼び出しする際に、ボリュームをマウントするために必要なメディア・マウント操作が増える可能性があります。

グループごとのコロケーションは、1 次順次アクセス・ストレージ・プールの場合の IBM Spectrum Protect のシステム・デフォルトです。デフォルトのコピー・ストレージ・プールおよび保存ストレージ・プールはコロケーションなしです。

## 操作に対するコロケーションの影響

コロケーションがリソースおよびシステム・パフォーマンスに与える影響は、実行中の操作のタイプによって異なります。

[170 ページの表 30](#) は、操作に対するコロケーションの影響を要約したものです。

表 30. 操作に対するコロケーションの影響

操作	コロケーションが使用可能な場合	コロケーションが使用不可の場合
クライアント・ファイルのバックアップ、アーカイブ、またはマイグレーション	ファイルのコロケーションを行うためにメディアのマウント回数が増える。	メディアのマウント回数が少なくなる。

表 30. 操作に対するコロケーションの影響 (続き)

操作	コロケーションが使用可能な場合	コロケーションが使用不可の場合
クライアント・ファイルのリストア、リトリブ、または再呼び出し	ファイルが置かれるボリューム数が少なくなるので、多くのファイルをより速くリストア、リトリブ、または再呼び出しすることができる。	ファイルが多く、多くのボリュームに分散される可能性があるため、単一のユーザーについて、メディアのマウント回数が多くなる場合がある。  複数のユーザーのファイルが、同じ順次アクセス・ストレージ・ボリュームに保管されている可能性がある。例えば、二人のユーザーが、同じボリューム上にあるファイルを回復しようとした場合、2 番目のユーザーは、最初のユーザーのファイルが回復されるまで、強制的に待たされることになる。
テープへのデータの保管	サーバーは、個別のユーザー・ファイルに使用可能なすべてのテープ・ボリュームの使用を試みてから、各テープ・ボリューム上の使用可能なすべてのスペースを使用する。	サーバーは、各テープ・ボリューム上の使用可能なすべてのスペースの使用を試みてから、別のテープ・ボリュームを使用する。
メディアのマウント 操作回数	ユーザー・ファイルをクライアント・ノードから順次アクセス・ボリュームへ直接バックアップ、アーカイブ、またはマイグレーションする場合に、必要なマウント操作回数が増える。  レクラメーション時およびストレージ・プールのマイグレーション時に必要なマウント操作回数が増える。  ボリュームが完全に使用されないの で、管理するボリューム数が増える。	クライアント・ファイルのリストア、リトリブ、および再呼び出し時に必要なマウント操作回数が増える。
バックアップ・セットの生成	データベース項目の検索時間が短くなり、必要なマウント操作回数が減る。	データベース項目の検索時間が長くなり、必要なマウント操作回数が減る。
テープへの保存セットのコピー  <b>重要:</b> コロケーション設定が原因で、保存セットに必要なテープ・ボリュームの数が大幅に増加する可能性があります。	サーバーは、同じ連結エンティティからのファイルをできるだけ少数のテープ・ボリュームに保持しようと試みる。  保存セットをテープに書き込む際の処理時間が長くなる可能性がある。	サーバーは、各テープ・ボリューム上の使用可能なすべてのスペースの使用を試みてから、別のテープ・ボリュームを使用する。  保存セットからデータをリストアする必要がある場合、ファイルが複数のボリュームに分散されている可能性があるため、単一の保存セット・ユーザーについて、より多くのテープ・マウントが必要になる場合がある。

グループ、単一のクライアント・ノードまたはファイル・スペースのコロケーションが使用可能になると、そのグループ、ノード、またはファイル・スペースに属するすべてのデータが、1つのサーバー・プロセスで移動またはコピーされます。例えば、データがグループごとに併置されると、同じコロケーション・グループに属するすべてのノードのすべてのデータが同じプロセスによってマイグレーションされます。

データのコロケーション中、IBM Spectrum Protect サーバーは、ファイルを最少数の順次アクセス・ストレージ・ボリュームと一緒に保持しようとします。ただし、サーバーが順次アクセス・ストレージ・プールのボリュームにデータをバックアップする場合、バックアップ・プロセスの方がコロケーション設定より優先されます。その結果、サーバーは、バックアップ操作を完了しても、データを連結できない場合があります。

例えば、ノードを連結する場合に、ノードがサーバー上の2つのマウント・ポイントを使用できるように指定したとします。また、ノードからバックアップされるデータが1つのテープ・ボリュームに容易に収まるとします。バックアップ時に、サーバーは2つのテープ・ボリュームをマウントし、ノードのデータは1つではなく2つのテープに分散される可能性があります。コロケーションを有効にした場合、以下のサーバー操作で1つのサーバー・プロセスが使用されます。

- ランダム・アクセスおよび順次アクセス・ボリュームからのデータの移動
- 順次アクセス・ボリュームからのノード・データの移動
- ランダム・アクセスまたは順次アクセス・ストレージ・プールのバックアップ
- 順次アクセス・ストレージ・プールのリストア
- 順次アクセス・ストレージ・プールまたはオフサイト・ボリュームでのスペースのレクラメーション
- ランダム・アクセス・ストレージ・プールからのデータのマイグレーション

ランダム・アクセス・ディスク・ストレージ・プールから順次アクセス・ストレージ・プールにデータをマイグレーションし、マイグレーションがノードまたはファイル・スペースごとである場合、マイグレーションするデータの量に基づいて、マイグレーション対象とするノードまたはファイル・スペースが自動的に選択されます。最もデータが多いノードまたはファイル・スペースが最初にマイグレーションされます。グループごとのコロケーションの場合は、ストレージ・プールのすべてのノードが評価され、最もデータが多いノードが判別されます。最もデータが多いノードが、そのコロケーション・グループに属するすべてのノードのすべてのデータとともに最初にマイグレーションされます。このプロセスは、ノードのファイル・スペースに保管されているデータの量や、マイグレーション停止しきい値(低しきい値)に達したかどうかにかかわらず行われます。

ただし、コロケーションされたデータを順次アクセス・ストレージ・プールから別の順次アクセス・ストレージ・プールにマイグレーションする場合、サーバーは、ボリュームが最後にアクセスされた日付にしたがってボリュームを配列します。アクセス日が最も早いボリュームが最初にマイグレーションされ、アクセス日が最も遅いボリュームが最後にマイグレーションされます。

グループごとのコロケーションを行う理由の1つに、多くの場合、個々のクライアント・ノードには大容量テープ・ボリュームを満たすほどのデータがないことがあげられます。ノードのグループごとにデータを併置すると、より多くの併置されたデータが個々のテープに書き込まれ、未使用のテープ容量を削減できます。また、ファイル・スペースのグループごとにデータをコロケーションすると、未使用のテープをより細かく削減することもできます。

同じコロケーション・グループのすべてのノードに属するデータは、同じプロセスによってマイグレーションされます。したがって、グループごとのコロケーションにより、マイグレーション対象のボリュームのマウントが必要になる回数を減らすことができます。また、グループごとのコロケーションにより、データベースのスキャンが最小化され、順次アクセス・ストレージ・プール間でデータを転送するときのテープ受け渡しも削減できます。

## コロケーションが有効にされたボリュームの選択

ボリュームの選択は、コロケーションをグループ、ノード、またはファイル・スペースごとに行うかどうかによって異なります。

173 ページの表 31 は、クライアント・ノード・レベル、コロケーション・グループ・レベル、およびファイル・スペース・レベルでストレージ・プールのコロケーションが有効にされている場合に、IBM Spectrum Protect サーバーがどのように最初のボリュームを選択するかを示しています。

表 31. コロケーションが使用可能時のサーバーのボリューム選択方法

ボリューム選択順序	グループごとのコロケーションの場合	ノードごとのコロケーションの場合	ファイル・スペースごとのコロケーションの場合
1	クライアントが属するコロケーション・グループからのファイルが既に入っているボリューム	同じクライアント・ノードからのファイルが既に入っているボリューム	そのクライアント・ノードの同じファイル・スペースからのファイルが既に入っているボリューム
2	空の事前定義済みボリューム	空の事前定義済みボリューム	空の事前定義済みボリューム
3	空のスクラッチ・ボリューム	空のスクラッチ・ボリューム	空のスクラッチ・ボリューム
4	既にデータが入っているボリュームの中で、最も使用可能なフリー・スペースがあるボリューム	既にデータが入っているボリュームの中で、最も使用可能なフリー・スペースがあるボリューム	同じクライアント・ノードからのデータが入っているボリューム
5	適用外	適用外	既にデータが入っているボリュームの中で、最も使用可能なフリー・スペースがあるボリューム

サーバーが、引き続き 2 番目のボリュームにデータを保管する必要がある場合、次の選択順序で、追加スペースを獲得します。

1. 空の事前定義済みボリューム
2. 空のスクラッチ・ボリューム
3. 既にデータが入っているボリュームの中で、最も使用可能なフリー・スペースがあるボリューム
4. ストレージ・プール内の使用可能なボリューム

クライアント・ノードまたはファイル・スペースごとのコロケーションの場合、サーバーは、個々のボリュームの最適な使用を試み、異なるクライアントまたはボリューム上のファイル・スペースからのファイルの混合を最小化します。この構成を [173 ページの図 11](#) に示します。ここには、水平型のボリューム選択を示しています。この場合、すべての使用可能なボリュームが使用された後で、各ボリューム上のすべての使用可能なスペースが使用されます。A、B、C、および D は、4 つの異なるクライアント・ノードからのファイルを表します。

#### ヒント:

1. ノードごとのコロケーションを行い、かつそのノードに複数のファイル・スペースがある場合は、サーバーは、それらのファイル・スペースを併置しようとしません。
2. ファイル・スペースごとのコロケーションを行い、かつノードに複数のファイル・スペースがある場合は、サーバーは、ボリュームごとに異なるファイル・スペースにデータを書き込もうとします。

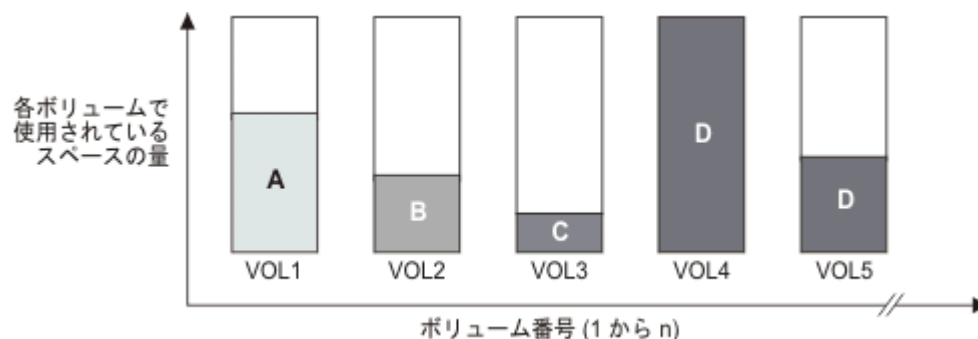


図 11. ノード・レベルまたはファイル・スペース・レベルでコロケーションが使用可能時のすべての使用可能な順次アクセス・ストレージ・ボリュームの使用

コロケーションはファイル・スペース・グループまたはノード・グループごとに行うことができます。ノード・グループ (ノード・コロケーション・グループ) ごとのコロケーションの場合、サーバーは、同じコロケーション・グループに属するノードからのデータを併置しようとします。ファイル・スペース・コロケーション・グループでは、ノード・コロケーション・グループと同じ方法を使用しますが、ファイル・スペース・サイズの細分性のために使用するスペースが増える場合があります。174 ページの図 12 に示すように、以下のノードのグループのデータは併置されています。

- グループ 1 はノード A、B、および C から構成されます
- グループ 2 はノード D および E から構成されます
- グループ 3 はノード F、G、H、および I から構成されます

可能な場合は、IBM Spectrum Protect サーバーは、図のグループ 2 に示すように、ノードのグループに属するデータを単一のテープに併置します。単一ノードのデータは、グループ (グループ 1 および 2) に関連した複数のテープに含まれても構いません。コロケーション・グループ内のノードに複数のファイル・スペースがある場合は、サーバーは、それらのファイル・スペースを併置しようとしません。

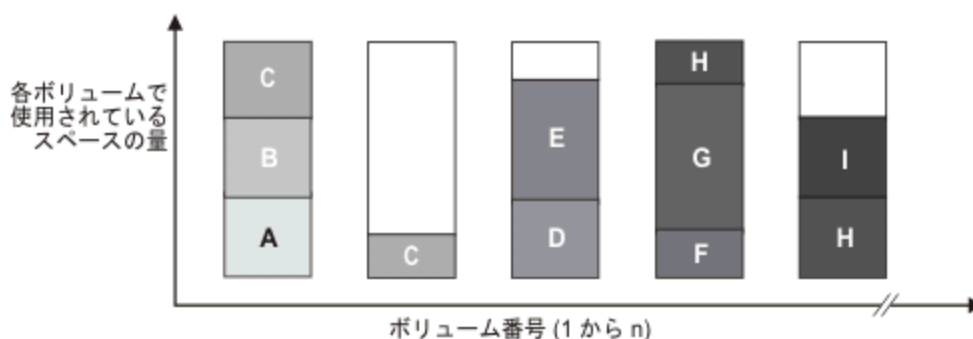


図 12. グループ・レベルでコロケーションが使用可能時のすべての使用可能な順次アクセス・ストレージ・ボリュームの使用

多くの場合、IBM Spectrum Protect サーバーは必ず、実行中の操作で埋め込まれている現行ボリュームにデータを書き込みます。ただし、コロケーション・ストレージ・プールに埋め込み中のボリュームが複数ある場合があります。コロケーション・ストレージ・プールに埋め込み中のボリュームが複数あるのは、異なるサーバー・プロセスまたはクライアント・セッションがコロケーション・プールにデータを同時に保管しようとした場合です。この場合、IBM Spectrum Protect は、ボリュームを必要とするプロセスまたはセッションごとにボリュームを割り振って、可能な限り迅速に両方の操作が完了するようにします。

## コロケーションが無効にされたボリュームの選択

コロケーションが使用不可な場合、サーバーは、ストレージ・ボリューム内のすべての使用可能なスペースを使用して、別のボリュームをアクセスします。

コロケーションが無効にされた順次アクセス・ストレージ・プールにクライアント・ファイルを保管する場合、サーバーは、以下の選択順序を使用してボリュームを選択します。

1. 使用可能スペースのある、以前に使用された順次ボリューム (データ量の最も多いボリュームが最初に選択されます)。
2. 空のボリューム

データを保管するために 2 番目のボリュームが必要になった場合、サーバーは 空のボリュームを選択しようとします。空のボリュームがない場合、サーバーは、ストレージ・プール内の残りの使用可能ボリュームのいずれかを選択します。

175 ページの図 13 は、コロケーションが無効にされており、ボリューム使用が垂直型であることを示しています。この例では、サーバーが、個々のボリューム上のクライアント・ファイルを混合することにより、すべての使用可能スペースを使用しようとしているため、より少ないボリュームが使用されています。

A、B、C、および D は、4 つの異なるクライアント・ノードからのファイルを表します。

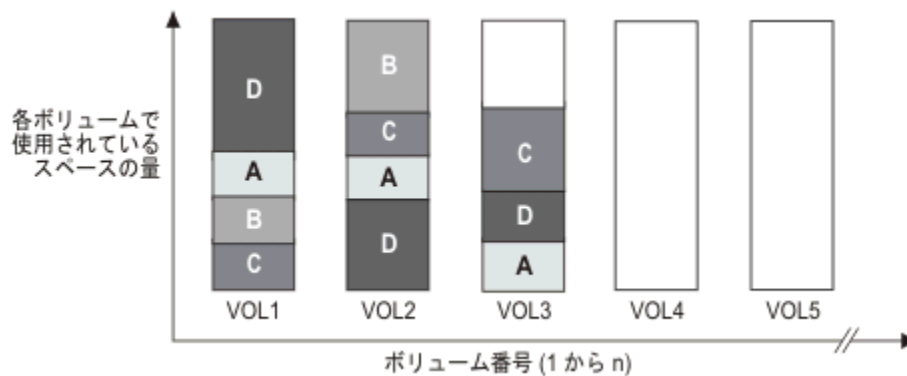


図 13. コロケーションが無効にされた順次アクセス・ボリューム上のすべての使用可能スペースの使用

## コロケーション設定

ストレージ・プールを定義した後、ストレージ・プールを更新することによってコロケーションの設定を変更することができます。プールに関するコロケーションの変更は、プール内に既に保管されているファイルには影響を与えません。

例えば、あるストレージ・プールに関してコロケーションがオフになっていて、オンに変更した場合、その時点からプールに保管されるクライアント・ファイルがコロケーションの対象になります。以前にストレージ・プールに保管されていたファイルは、コロケーションのために移動されません。ボリュームがレクラメーション処理またはリストアされるに従って、プール内のデータは徐々に併置（コロケーション）されます。コロケーションを増加するために、**MOVE DATA** コマンドまたは **MOVE NODEDATA** コマンドを使用してデータを新しいボリュームに移動することもできます。新規ボリュームにデータを移動すると、処理時間とボリューム・マウント作業が増えます。

**ヒント：**ファイル・スペースによるコロケーションが有効にされており、複数のファイル・スペースが含まれるボリュームがノードにある場合、マウント待機が発生したり、通常より長時間かかったりする可能性があります。ボリュームがデータを受信するのに適格である場合、IBM Spectrum Protect はそのボリュームを待ちます。

## コピー・ストレージ・プールのコロケーション

コピー・ストレージ・プールでコロケーションを使用する場合には、特別な考慮事項があります。コピー・ストレージ・プールでコロケーション（特に、ノードまたはファイル・スペースによる）を行うと、部分的に埋められたボリュームが増える結果となり、不要なオフサイト・レクラメーション活動が生じる可能性があります。

1次ストレージ・プールは、コピー・ストレージ・プールとは別のリカバリー役割を果たします。通常は、1次ストレージ・プールを使用して、データを直接クライアントにリカバリーします。災害によってクライアントとサーバーの両方が失われた場合、オフサイトのコピー・ストレージ・プール・ボリュームを使用して、1次ストレージ・プールをリカバリーできる場合があります。リカバリー・シナリオのタイプは、コピー・ストレージ・プールでコロケーションを使用するかどうかを判断するのに役立ちます。

ノードまたはファイル・スペースごとにコロケーションする場合、通常、コロケーションにより、部分的に埋め込まれたボリュームが発生します。ただし、グループごとのコロケーションを行う場合は、部分的に埋め込まれたボリュームはそれほど発生しません。部分的に埋め込まれたボリュームは使用可能なままになり、次のマイグレーション・プロセスで埋め込むことができるので、1次ストレージ・プールの場合には問題になりません。しかし、ストレージ・プール・ボリュームが即時にオフサイトに送られるコピー・ストレージ・プールでは、部分的に埋め込まれたボリュームを許容できない場合があります。コピー・ストレージ・プールに対してコロケーションを使用する場合には、以下のことを決定する必要があります。

- より多くの部分的にしか埋め込まれていないボリュームをオフサイトで受け取るにより、レクラメーションしきい値が下げられるかそれに達したときのレクラメーション活動が増える。
- これらの部分的に埋め込まれたボリュームが埋め込まれるまでオンサイトのままにし、これらのボリューム内のデータのオフサイト・コピーが作成されない危険性を残す。
- グループごとにコロケーションを行い、できるだけ多くのテープ容量を使用するかどうか。



コピー・ストレージ・プールでコロケーションが無効にされている場合、通常は、データがコピー・ストレージ・プールにバックアップされた後には、数個のボリュームのみが部分的に埋め込まれた状態で残ります。

コピー・ストレージ・プールに対してコロケーションを使用する場合は、選択肢についてあらかじめ慎重に検討する必要があります。また、同時書き込みを使用するかどうかを検討します。同時書き込みを使用せず、コロケーションを1次ストレージ・プールに使用する場合は、コピー・ストレージ・プールに対するコロケーションを無効にすることが推奨されます。コピー・ストレージ・プールのコロケーションが望ましいのは、クライアントの数が少なくても、それぞれのクライアントに毎日、大量の差分バックアップ・データがある場合です。同時書き込みとのコロケーションの場合は、1次ストレージ・プールおよびコピー・ストレージ・プールのコロケーション設定が同一であることを確認する必要があります。

## 保存ストレージ・プールのコロケーション

コロケーション・プロパティに対して選択する値は、保存セットのデータがテープ・ボリューム上でどのように分散されるかに影響を与えます。一般に、使用するテープ・ボリュームの数を最小限にするには、コロケーションを無効にする必要があります。デフォルトで、保存ストレージ・プールに対するコロケーション設定は無効になっています。

コロケーション設定を無効にすると、保存セット・コピー・プロセスのボリューム選択時に、サーバーは、新規ボリュームを選択する前に、各テープ・ボリュームのすべての使用可能スペースの使用を試みます。このプロセスでは個別のテープ・ボリュームを効率的に使用できる一方、各保存セットのデータは連結されておらず、多くのテープ・ボリュームに分散している可能性があります。

コロケーション設定は、保存セット・データをテープに書き込む際のシステム・パフォーマンス、および保存セット・データのリストア操作時のシステム・パフォーマンスに大きな影響を及ぼす場合があります。保存ストレージ・プールについてコロケーション設定を有効にするかどうかを検討する前に、要件とパフォーマンスのトレードオフを検討してください。

- コロケーションが有効である場合、サーバーは、各エンティティのファイルを最小限の数のテープ・ボリュームに保持しようとします。ただし、このオプションでは保管するファイルの連結に要するサーバー処理時間と必要なボリューム数が両方とも増加します。保存セットに定義されている **STACK** パラメータの設定も関連します。

**ヒント:** 保存セットのボリューム・スタッキングが有効な場合、保存セット・データが、他の保存セットからコピーされたデータとテープ・ボリュームを共有できます。ボリュームを選択する際に、データが既に含まれている **FILLING** 状態のボリュームを最初に見つけます。ただしそれらのボリュームが、個別のボリュームを必要とする保存セットによってまだ使用されていない場合に限りです。保存セットのボリューム・スタッキングが有効ではない場合、保存セット・データは1つ以上のテープ・ボリュームに連結され、他の保存セットのデータは、それらのボリュームに配置されません。ボリュームを選択する際に、まず空のボリュームを見つけていますが、データは **FILLING** ボリュームにもコピーできます (そのボリュームに、コピー中のその保存セットのデータが既に含まれている場合に限りです)。

- コロケーションを無効にすると、個々の保存セットのデータが多くのボリュームに分散される可能性があるため、保存セットからデータをリストアする必要がある場合は必要なテープ・マウント回数が増える可能性があります。必要なテープ・マウント回数が増えた場合、リストア操作に必要な処理時間が増加する場合があります。

**ヒント:** **DEFINE STGPOOL** コマンドまたは **UPDATE STGPOOL** コマンドに **COLLOCATE** パラメータを指定することで、コロケーションを有効にしたり、コロケーション設定を変更したりすることができます。

コロケーション設定の変更は、それ以降に保存ストレージ・プールに書き込まれるデータのみに影響します。プールに既に保管されているファイルは影響を受けません。

### 関連概念

[174 ページの『コロケーションが無効にされたボリュームの選択』](#)

コロケーションが使用不可な場合、サーバーは、ストレージ・ボリューム内のすべての使用可能なスペースを使用して、別のボリュームをアクセスします。

[170 ページの『操作に対するコロケーションの影響』](#)

コロケーションがリソースおよびシステム・パフォーマンスに与える影響は、実行中の操作のタイプによって異なります。

## コロケーションの計画と使用可能化

コロケーションの効果を理解すると、メディアのマウント回数の削減、順次ボリュームのスペースのより効率的な使用、およびサーバー操作の効率の改善に役立てることができます。

### このタスクについて

177 ページの表 32 に、**DEFINE STGPOOL** および **UPDATE STGPOOL** コマンドで指定できる 4 つのコロケーション・オプションをリストします。この表では、コロケーション・グループのメンバーであるノード、およびメンバーでないノードに属するデータでのコロケーションの効果も示します。

表 32. コロケーション・オプションおよびノード・データに対する効果

コロケーション・オプション	ノードがコロケーション・グループのメンバーとして定義されていない場合	ノードがコロケーション・グループのメンバーとして定義されている場合
<b>No</b>	ノードのデータは併置されません。	ノードのデータは併置されません。
<b>グループ</b>	サーバーは、ノードのデータをストレージ・プール上の可能な限り少ないボリュームに保管します。	サーバーは、ノードのデータと同じコロケーション・グループに属する他のノードのデータを可能な限り少ないボリュームに保管します。
<b>ノード</b>	サーバーは、ノードのデータを可能な限り少ないボリュームに保管します。	サーバーは、ノードのデータを可能な限り少ないボリュームに保管します。
<b>ファイル・スペース</b>	サーバーは、ノードのファイル・スペースのデータを可能な限り少ないボリュームに保管します。ノードに複数のファイル・スペースがある場合、サーバーは異なるファイル・スペースのデータをストレージ・プール内のそれぞれ異なるボリュームに保管します。	サーバーは、ノードのファイル・スペースのデータを可能な限り少ないボリュームに保管します。ノードに複数のファイル・スペースがある場合、サーバーは異なるファイル・スペースのデータをストレージ・プール内のそれぞれ異なるボリュームに保管します。

表 33. コロケーション・グループ・オプションおよびファイル・スペース・データに対する効果

コロケーション・オプション	ファイル・スペースがコロケーション・グループのメンバーとして定義されていない場合	ファイル・スペースがコロケーション・グループのメンバーとして定義されている場合
<b>No</b>	ファイル・スペースのデータは併置されません。	ファイル・スペースのデータは併置されません。
<b>グループ</b>	サーバーは、ファイル・スペースのデータをストレージ・プール上の可能な限り少ないボリュームに保管します。	サーバーは、ファイル・スペースのデータと、同じコロケーション・グループに属する他のファイル・スペースのデータを可能な限り少ないボリュームに保管します。
<b>ノード</b>	サーバーは、ノードのデータを可能な限り少ないボリュームに保管します。	サーバーは、ノードのデータを可能な限り少ないボリュームに保管します。
<b>ファイル・スペース</b>	サーバーは、ノードのファイル・スペースのデータを可能な限り少ないボリュームに保管します。ノードに複数のファイル・スペースがある場合、サーバーは異なるファイル・スペースのデータをストレージ・プール内のそれぞれ異なるボリュームに保管します。	サーバーは、ファイル・スペースのデータを可能な限り少ないボリュームに保管します。ノードに複数のファイル・スペースがある場合、サーバーは異なるファイル・スペースのデータをストレージ・プール内のそれぞれ異なるボリュームに保管します。

## 手順

データをコロケーションするかどうか、およびどのようにコロケーションするかを決定するには、以下のステップを実行します。

1. データをどのように編成するか (クライアント・ノードごと、クライアント・ノードのグループごと、あるいはファイル・スペースごと) を決定します。グループごとにコロケーションするには、どのようにノードをグループ化するかを決定する必要があります。
  - スペースの節約を目的とする場合は、テープを効率的に使用するように小さいノードをグループ化します。
  - クライアント・リストアの高速化を目的とする場合は、ノードをグループ化して、できるだけ多くのテープが満たされるようにします。ノードをグループ化することで、個々のノード・データが複数のテープに分散され、マルチセッション無照会リストア操作中に同時に多くのテープをマウントできるようになります。
  - データの分類を目的とする場合は、部門ごとにノードをグループ化できます。
2. グループをコロケーションするには、以下のステップを実行します。
  - a) **DEFINE COLLOGROUP** コマンドを使用して、コロケーション・グループを定義します。
  - b) **DEFINE COLLOCMEMBER** コマンドを使用して、クライアント・ノードをコロケーション・グループに追加します。

以下の **QUERY** コマンドを使用すると、グループの併置時に役立ちます。

### **QUERY COLLOGROUP**

サーバー上で定義されているコロケーション・グループを表示します。

### **QUERY NODE**

ノードが属するコロケーション・グループ (ある場合) を表示します。

### **QUERY NODEDATA**

順次アクセス・ストレージ・プールの 1 つ以上のノードのデータに関する情報を表示します。

### **QUERY STGPOOL**

順次アクセス・ストレージ・プールにあるクライアント・データのロケーションと、ノードがボリュームで占有するスペースの量に関する情報を表示します。

IBM Spectrum Protect サーバー・スクリプトまたは Perl スクリプトを使用してコロケーション・グループの定義に役立つ情報を表示させることもできます。

3. **COLLOCATE** パラメーターを指定して **DEFINE STGPOOL** コマンドまたは **UPDATE STGPOOL** コマンドを発行することで、ストレージ・プール内でどのようにデータをコロケーションする必要があるかを指定します。

## 次のタスク

**ヒント:** メディア・マウントの数を減らし、順次ボリューム上のスペースをより効率的に使用し、コロケーションを有効にするには、以下のステップを実行します。

- バックアップ、アーカイブ、またはスペース管理対象ファイルを最初、ディスク・ストレージ・プールに保管させるような、ストレージ・プール階層とポリシーを定義する。

ファイルがディスク・ストレージ・プールからマイグレーションされる時、サーバーは、ストレージ・プール内の大部分のディスク・スペースを使用するクライアント・ノードまたはコロケーション・グループに属するすべてのファイルのマイグレーションを試みます。このプロセスは、コロケーション・オプションを指定するとうまく実行されます。サーバーは、特定のクライアントからのすべてのファイルを、同じ順次アクセス・ストレージ・ボリュームに入れようとするからです。
- 順次アクセス・ストレージ・プールのスクラッチ・ボリュームを使用して、サーバーが、コロケーション用の新規ボリュームを選択することができるようにする。
- クライアント・オプション **COLLOCATEBYFILESPEC** を指定して、1 つのファイル指定に関連付けられているオブジェクトの書き込み先テープ数を制限する。このコロケーション・オプションにより、サーバーによるコロケーションの効率性が向上します。このオプションは、ファイル・スペース別コロケーションまたはノード別コロケーションを上書きしません。

## テープ装置の管理

テープの日常操作には、テープ・ボリュームを使用するための準備、ボリュームを再使用方法とタイミングの制御、十分な使用可能ボリュームの確保などがあります。また、オペレーター要求への応答と、ライブラリー、ドライブ、ディスク、パス、およびデータ・ムーバーの管理も必要です。

### 取り外し可能メディアの準備

データの保管に使用できるようにするには、その前に、取り外し可能メディアの準備を行う必要があります。代表的な準備作業には、ボリュームのラベル付けとチェックインが含まれます。

#### このタスクについて

IBM Spectrum Protect は、取り外し可能メディア・ボリュームにアクセスする際、ラベル・ヘッダーのボリューム名を検査して、アクセスするボリュームが正しいことを確認します。

テープ・ボリュームも、サーバーが使用する前に、ラベル付けしておく必要があります。

#### 手順

ボリュームを使用できるように準備するには、以下のステップを実行します。

1. ボリュームにラベルを付けるには、**LABEL LIBVOLUME** コマンドを発行します。
2. 自動ライブラリーの場合は、ボリュームをライブラリーにチェックインします。方法については、[181 ページの『自動ライブラリーへのボリュームのチェックイン』](#)を参照してください。

**ヒント:** 自動ライブラリー内のドライブに **LABEL LIBVOLUME** コマンドを使用する場合には、ボリュームのラベル付けおよびチェックインを 1 つのコマンドで行うことができます。

3. ストレージ・プールにスクラッチ・ボリュームを入れることができない場合 (**MAXSCRATCH=0**) は、IBM Spectrum Protect に対してボリュームを名前で示し、後でそのボリュームにアクセスできるようにします。

ストレージ・プールにスクラッチ・ボリュームを入れることができる場合 (**MAXSCRATCH** がゼロ以外の値に設定されている場合) は、このステップをスキップしてください。

### テープ・ボリュームのラベル付け

サーバーでテープ・ボリュームを使用するには、その前に、テープ・ボリュームにラベルを付ける必要があります。

#### このタスクについて

自動ライブラリーの場合は、ライブラリーの出入り口スロットにボリュームを挿入するように求めるプロンプトが表示されます。使用可能な都合のよい入出力 (I/O) 装置がない場合は、ボリュームを空のスロットに挿入します。ボリュームのチェックイン時、あるいはチェックイン前にボリュームにラベルを付けることができます。

#### 手順

テープ・ボリュームをチェックインする前にラベルを付けるには、以下のステップを実行します。

1. **LABEL LIBVOLUME** コマンドを発行して、テープ・ボリュームにラベルを付けます。  
例えば、**LIBRARY 1** という名前のライブラリー内のライブラリー・ボリューム **VOLUME1** にラベルを付けるには、次のコマンドを発行します。

```
label libvolume library1 volume1
```

**要件:** 少なくとも 1 つのドライブが使用可能でなければなりません。このドライブは、別の IBM Spectrum Protect プロセスで使用することはできません。ドライブがアイドル状態の場合、そのドライブは、使用不可と見なされます。

2. 既存のラベルを上書きするには、**OVERWRITE=YES** パラメーターを指定します。デフォルトでは、**LABEL LIBVOLUME** コマンドは既存のラベルを上書きしません。

## 関連タスク

AUTOLABEL による新規ボリュームへのラベル付け

**DEFINE LIBRARY** コマンドまたは **UPDATE LIBRARY** コマンドで **AUTOLABEL** パラメーターを使用すると、**LABEL LIBVOLUME** コマンドを使用するより効率的です。**LABEL LIBVOLUME** コマンドの場合は、ボリュームを個別にマウントする必要があります。

## 関連情報

[LABEL LIBVOLUME \(ライブラリー・ボリュームのラベル付け\)](#)

## SCSI ライブラリー内のボリュームへのラベル付け

ボリュームのラベルは個別に付けることも、IBM Spectrum Protect を使用してライブラリーでボリュームを検索し、見つかったボリュームにラベルを付けることもできます。

## 個々のボリュームのラベル付け

**LABEL LIBVOLUME** コマンドを使用して個々のボリュームにラベルを付ける場合、ボリューム名を指定する必要があります。

## 手順

1. サーバーによってプロンプトが表示されたら、ライブラリーの出入り口スロットにボリュームを挿入します。ライブラリーが、挿入された各ボリュームをドライブにマウントします。
2. SCSI ライブラリーの場合、プロンプトが表示されたらボリューム名を入力します。指定された名前のラベルがボリュームに書き込まれます。

**ヒント:** SCSI ライブラリーのボリューム名を要求するプロンプトを表示するには、**LABEL LIBVOLUME** コマンドを発行して **LABELSOURCE=PROMPT** パラメーターを指定します。

3. ライブラリーに出入り口ポートがない場合は、指定されたスロット番号からテープを除去するように要求するプロンプトが表示されます。指定されたスロットからテープを除去します。

ライブラリーに出入り口ポートがある場合には、デフォルトの設定により、コマンドはそのライブラリーの出入り口ポートにラベル付きの各ボリュームを戻します。

## SCSI ライブラリーのボリューム・ラベルの上書き

ストレージ・ボリューム内に有効なデータが存在しない場合、**LABEL LIBVOLUME** コマンドを使用して、既存のボリューム・ラベルを上書きすることができます。

## このタスクについて

SCSI ライブラリーに出入り口ポートがない場合でも、SCSI ライブラリー内のボリュームにラベルを付けることができます。各新規ボリュームをライブラリーに手動で挿入し、そのボリュームにラベルが書き込まれた後、ライブラリー内部のストレージ・スロットにボリュームを入れます。

## 手順

**LABEL LIBVOLUME** コマンドを発行して、既存のボリューム・ラベルを上書きします。例えば、ライブラリーの名前が LIB1 で、ボリューム名が VOLNAME である場合、次のコマンドを発行します。

```
label libvolume lib1 volname overwrite=yes
```



## AUTOLABEL による新規ボリュームへのラベル付け

**DEFINE LIBRARY** コマンドまたは **UPDATE LIBRARY** コマンドで **AUTOLABEL** パラメーターを使用すると、**LABEL LIBVOLUME** コマンドを使用するより効率的です。LABEL LIBVOLUME コマンドの場合は、ボリュームを個別にマウントする必要があります。

### 手順

**DEFINE LIBRARY** コマンドまたは **UPDATE LIBRARY** コマンドを発行して、**AUTOLABEL** パラメーターを指定します。

ヒント: SCSI ライブラリーで **AUTOLABEL** パラメーターを使用する場合は、**CHECKIN LIBVOLUME** コマンドで **CHECKLABEL=BARCODE** パラメーターを指定して、テープをチェックインする必要があります。

**AUTOLABEL** パラメーターのデフォルトは、すべての非 SCSI ライブラリーに対しては YES、SCSI ライブラリーに対しては NO になります。**CHECKLABEL=BARCODE** パラメーターは、ライブラリーにバーコード・リーダーがある場合にのみ使用できます。

### 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[DEFINE LIBRARY \(ライブラリーの定義\)](#)

[LABEL LIBVOLUME \(ライブラリー・ボリュームのラベル付け\)](#)

## ライブラリーの検索とボリュームのラベル付け

IBM Spectrum Protect では、ライブラリー内のすべてのストレージ・スロットを検索してボリュームを見つけ、見つけたボリュームに 1 つずつラベルを付けることができます。

### 手順

ライブラリーを検索してボリュームにラベルを付けるには、**LABEL LIBVOLUME** コマンドを発行して **SEARCH=YES** パラメーターを指定します。

ヒント: SCSI ライブラリーを使用していて、ライブラリーにバーコード・リーダーがある場合、**LABEL LIBVOLUME** コマンドはユーザーにボリューム名の入力をプロンプト指示せずに、そのリーダーを使用してボリューム名を入力することができます。**LABELSOURCE=BARCODE** パラメーターが有効なのは、SCSI ライブラリーの場合のみです。

例えば、SCSI ライブラリー内のすべてのボリュームにラベルを付けるには、以下のコマンドを発行します。

```
label libvolume library_name search=yes labelsource=barcode
```

IBM Spectrum Protect は、次に使用可能なドライブを選択して、ユーザーが検索を続行できるようにします。

### タスクの結果

ボリュームにラベルを付けた後、そのボリュームはライブラリー内の元のロケーションに戻されます。

### 関連情報

[LABEL LIBVOLUME \(ライブラリー・ボリュームのラベル付け\)](#)

## 自動ライブラリーへのボリュームのチェックイン

**CHECKIN LIBVOLUME** コマンドを使用して、ボリュームを自動ライブラリーにチェックインすることができます。

### 始める前に

テープをチェックインする前に、自動的にテープにラベルを付けるには、**DEFINE LIBRARY** コマンドを発行して **AUTOLABEL=YES** パラメーターを指定します。**AUTOLABEL** パラメーターを使用することで、一連のテープに事前にラベルを付けておく必要がなくなります。



## このタスクについて

目的にかかわらず、サーバーによって使用される各ボリュームには固有の名前が必要です。この要件は、ボリュームをストレージ・プールに使用するか、データベースのバックアップやエクスポートなどの操作に使用するにかかわらず、すべてのボリュームに適用されます。この要件は、同じサーバーによって使用される別のライブラリー内のボリュームにも適用されます。

### ヒント:

- バーコード・ラベルを持つボリュームとバーコード・ラベルを持たないボリュームがある場合、単一のライブラリーを使用しないでください。バーコードのスキャンは、ラベルのないボリュームには時間がかかることがあります。
- サーバーは、IBM 標準ラベルが付いたテープのみを受け入れます。
- CLN で始まるバーコードを持つボリュームはいずれもクリーニング・テープとして扱われます。
- ボリュームがボリューム・ヒストリー内に項目を持っている場合は、そのボリュームをスクラッチ・ボリュームとしてチェックインできません。

## 手順

1. ストレージ・ボリュームをライブラリーにチェックインするには、**CHECKIN LIBVOLUME** コマンドを発行します。

**ヒント:** このコマンドは常に、バックグラウンド・プロセスとして実行されます。**CHECKIN LIBVOLUME** プロセスの処理が完了するまで待ってから、ボリュームを定義してください。そうしないと、定義処理が失敗します。ボリュームのチェックインをラベル付け操作の一環として行うことで、時間を節約できます。

2. ライブラリーに名前を付けて、ボリュームが専用ボリュームかスクラッチ・ボリュームかを指定します。スクラッチ・ボリュームまたは専用ボリュームのいずれを使用するかによって、以下のいずれかのステップを実行します。
  - スクラッチ・ボリュームだけを使用する場合は、十分なスクラッチ・ボリュームが使用可能になっていることを確認します。例えば、もっと多くのボリュームにラベルを付ける必要がある場合もあります。ボリュームを使用していくに従って、このライブラリーに定義したストレージ・プールで利用できるスクラッチ・ボリューム数を増やす必要が出てくることもあります。
  - ライブラリーの中のスクラッチ・ボリュームの代わりに、またはそれに加えて専用ボリュームを使用したい場合は、**DEFINE VOLUME** コマンドを使用して、ストレージ・プールにボリュームを定義します。定義したボリュームにはラベルを付け、そのボリュームをチェックインする必要があります。

## 関連タスク

### テープ・ボリュームのラベル付け

サーバーでテープ・ボリュームを使用するには、その前に、テープ・ボリュームにラベルを付ける必要があります。

## 単一ボリュームの SCSI ライブラリーへのチェックイン

**CHECKIN LIBVOLUME** コマンドを発行して **SEARCH=NO** パラメーターを指定することで、単一ボリュームをチェックインすることができます。IBM Spectrum Protect は、マウント・オペレーターがライブラリーの出入り口ポートにボリュームをロードするように要求します。

## 手順

1. **CHECKIN LIBVOLUME** コマンドを発行します。

例えば、ボリューム VOL001 をチェックインするには、次のコマンドを入力します。

```
checkin libvolume tapelib vol001 search=no status=scratch
```

2. サーバーからのプロンプトに応答します。

- ライブラリーに出入り口ポートがある場合には、テープを出入り口ポートに挿入するようにプロンプトが出されます。
- ライブラリーに出入り口ポートがない場合は、テープをライブラリー内のいずれかのスロットに挿入するようプロンプトが出されます。エレメント・アドレスが、これらのスロットを識別します。例えば、最初の空のスロットがエレメント・アドレス 5 にあることをサーバーが検出すると、次のメッセージが返されます。

```
ANR8306I 001: 8MM ボリューム VOL001 R/W を 60 分以内にスロットの中に
ライブラリー TAPELIB のエレメント・アドレス 5 を付けて挿入してください。
準備ができたなら要求 ID と一緒に
'REPLY' を発行してください。
```

ライブラリー内のエレメント・アドレス 5 の位置が不明な場合は、装置のワークシートを確認してください。ワークシートを見つけるには、ご使用のライブラリーの資料を参照してください。要求に従ってボリュームを挿入した後、IBM Spectrum Protect 管理クライアントからのメッセージに回答します。**REPLY** コマンドの後に要求番号 (マウント要求の先頭の番号) を指定して発行します。例えば、次のようになります。

```
reply 1
```

**ヒント:** エレメント・アドレスは、1 以外の番号から始まる場合があります。ワークシートを調べて確認してください。ご使用の装置のワークシートが [IBM Support Portal for IBM Spectrum Protect](#) にリストされていない場合は、ご使用のライブラリーの資料を参照してください。

**CHECKIN LIBVOLUME** コマンドでオプションの **WAITTIME** パラメーターを使用して待機時間 0 を指定した場合、**REPLY** コマンドは不要です。デフォルトの待機時間は 60 分です。

## ライブラリー・ストレージ・スロットからのボリュームのチェックイン

チェックインするボリュームが大量にあり、ボリュームごとに **CHECKIN LIBVOLUME** コマンドを発行するのを回避したい場合、ストレージ・スロットを検索して新規ボリュームがないかを調べることができます。サーバーは、まだボリューム・インベントリーに追加されていないボリュームを検出します。

### 手順

- ライブラリーを開き、未使用スロットに新規ボリュームを置きます。  
例えば SCSI 装置の場合は、ライブラリーのアクセス・ドアを開いて、すべての新規ボリュームを未使用スロットに置き、ドアを閉じます。
- ボリュームにラベルが付けられていない場合、**LABEL LIBVOLUME** コマンドを使用してボリュームにラベルを付けます。
- SEARCH=YES** パラメーターを指定して **CHECKIN LIBVOLUME** コマンドを発行します。

### 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

## ライブラリー出入り口ポートからのボリュームのチェックイン

一括出入り口ポートのすべてのスロットを検索してラベル付きのボリュームがないかを調べ、サーバーはそれらのボリュームを自動的にチェックインすることができます。

### 始める前に

**LABEL LIBVOLUME** コマンドを発行して、ラベル付けされていないボリュームにラベルを付けます。

### このタスクについて

SCSI ライブラリーでは、サーバーはライブラリー内のすべての出入り口ポートをスキャンしてボリュームがあるか確認します。有効なボリューム・ラベルが含まれているボリュームが見つかったら、それが自動的にチェックインされます。

## 手順

**CHECKIN LIBVOLUME** コマンドを発行して **SEARCH=BULK** パラメーターを指定します。

- ドライブ内のテープをロードしてラベルを読み取るには、**CHECKLABEL=YES** パラメーターを指定します。サーバーはラベルを読み取った後に、テープをドライブからストレージ・スロットに移動します。
- サーバーがバーコード・リーダーを使用してテープの外部ラベルを確認するには、**CHECKLABEL=BARCODE** パラメーターを指定します。バーコードの読み取りが有効にされている場合、サーバーはラベルを読み取り、テープを出入り口ポートからストレージ・スロットに移動します。

## ライブラリーのバーコード・リーダーを使用したボリュームのチェックイン

バーコード・リーダーを備えたライブラリーにボリュームをチェックインする場合、バーコード・ラベルの文字をボリュームの名前として使用することで時間を節約できます。

### このタスクについて

サーバーは、バーコード・ラベルを読み取り、その情報を使用して内部メディア・ラベルを書き込みます。バーコード・ラベルがないボリュームの場合、サーバーは、ドライブにボリュームをマウントし、内部に記録されたラベルの読み取りを試行します。

## 手順

**CHECKLABEL=BARCODE** パラメーターを指定して **CHECKIN LIBVOLUME** コマンドを発行します。

例えば、バーコード・リーダーを使用して **TAPELIB** という名前のライブラリーを検索し、スクラッチ・テープをチェックインするには、次のコマンドを発行します。

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

## バーコード・リーダーを使用したボリュームのチェックイン

ライブラリーにバーコード・リーダーがある場合は、バーコード・リーダーを使用してボリュームをチェックインすると、時間を節約することができます。

### このタスクについて

ボリュームをチェックインする際に、チェックイン処理中にメディア・ラベルを読み取るかどうかを指定することができます。ラベル検査がオンにされている場合、IBM Spectrum Protect は、各ボリュームをマウントして内部ラベルを読み取り、正しくラベル付けされている場合にのみボリュームをチェックインします。ラベル検査により、ボリュームがストレージ・プールで使用されるとき将来のエラーを防止できますが、チェックイン時の処理時間が増えます。

ボリュームにバーコード・ラベルがなければ、IBM Spectrum Protect はドライブにボリュームをマウントし、記録されているラベルを読み取ろうとします。

## 手順

バーコード・リーダーを使用してボリュームをチェックインするには、**CHECKIN LIBVOLUME** コマンドを発行して **CHECKLABEL=BARCODE** を指定します。例えば、バーコード・リーダーを使用してすべてのボリュームをスクラッチ・ボリュームとして **TAPELIB** という名前のライブラリーにチェックインするには、次のコマンドを発行します。

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

### 関連タスク

[取り外し可能メディアの準備](#)

データの保管に使用できるようにするには、その前に、取り外し可能メディアの準備を行う必要があります。代表的な準備作業には、ボリュームのラベル付けとチェックインが含まれます。

## 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

## いっぱいライブラリーへのスワッピングによるボリュームのチェックイン

ボリュームをチェックインするときにライブラリーに使用可能な空スロットがない場合、スワッピングが使用できなければこのチェックイン操作は失敗します。スワッピングが有効で、ライブラリーがいっぱいの場合、サーバーは排出するボリュームを選択してから、ユーザーが要求したボリュームをチェックインします。

## このタスクについて

サーバーは、排出するボリュームを選択するために、まず、使用可能なスクラッチ・ボリュームがあるかどうかを検査し、次に、最もマウント頻度が少ないボリュームを探します。サーバーは、スワップ操作作用に選択したボリュームをライブラリーから排出し、排出したボリュームを、チェックインするボリュームと置き換えます。

## 手順

- ボリュームのチェックインに使用可能な空のライブラリー・スロットがない場合に、ボリュームをスワップするには、**CHECKIN LIBVOLUME** コマンドを発行して **SWAP=YES** パラメーターを指定します。例えば、**AUTO** という名前のライブラリーに **VOL1** という名前のボリュームをチェックインして、スワッピングを指定するには、以下のコマンドを発行します。

```
checkin libvolume auto vol1 swap=yes
```

## 関連タスク

[オーバーフロー・ロケーションを使用した満杯のライブラリーの管理](#)

ストレージの要求が増えるに従って、ストレージ・プールに必要なボリューム数が自動ライブラリーの物理容量を超えることがあります。新規ボリュームがスペースを使用できるようにする場合、および既存のボリュームをモニターする場合には、ストレージ・プールのオーバーフロー・ロケーションを定義することができます。

## 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

## 専用ボリュームおよびスクラッチ・ボリューム

磁気テープ・ストレージを最適化するには、専用ボリュームおよびスクラッチ・ボリュームに関する情報を確認してください。専用ボリュームおよびスクラッチ・ボリュームを適切に使用してください。

スクラッチ・マウントが要求された場合でも、専用ボリュームを上書きすることはできません。スクラッチ状況のボリュームがストレージ・プールによって使用されている場合、そのボリュームをチェックインして、データのエクスポート、データベースのバックアップ、あるいはバックアップ・セット・ボリュームのバックアップを行うことはできません。

部分的に書き込まれているボリュームは常に専用ボリュームになります。ボリュームの状況は専用またはスクラッチですが、いったん IBM Spectrum Protect がデータを保管すると、そのボリュームの状況は専用になります。

表 34. 専用ボリュームおよびスクラッチ・ボリュームの使用

ボリュームのタイプ	用途
専用ボリューム	個別のストレージ・プールで使用されるボリュームを調整し、手動でボリュームを制御するには、専用ボリュームを使用してください。専用ボリュームを定義するには、 <b>DEFINE VOLUME</b> コマンドを発行します。データベース・リストア、メモリー・ダンプ、またはロードの場合、あるいはサーバーのインポート操作の場合は、専用ボリュームを指定する必要があります。
スクラッチ・ボリューム	<p>場合によっては、スクラッチ・ボリュームを使用することでボリューム管理を簡素化することができます。以下の状況で、スクラッチ・ボリュームを使用することができます。</p> <ul style="list-style-type: none"> <li>各ストレージ・プール・ボリュームを定義する必要がない。</li> <li>ロボット装置の自動化の利点を活用したい。</li> <li>さまざまなストレージ・プールが自動ライブラリーを共有しており、ストレージ・プールがライブラリー内のスクラッチ・ボリュームから動的にボリュームを獲得できる。ボリュームをストレージ・プールに事前に割り振る必要はありません。</li> </ul>

## 関連タスク

自動ライブラリーのボリュームの状況の変更

ボリュームの状況を専用からスクラッチへ、またはスクラッチから専用へ変更することができます。

## 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[DELETE VOLUME \(ストレージ・プール・ボリュームの削除\)](#)

## ライブラリー・ストレージ・スロットの元素ト・アドレス

元素ト・アドレスは、自動ライブラリー内のストレージ・スロットの物理的な位置を示す番号です。

ライブラリーに出入り口ポートがある場合、そのポートを使用してメディアの追加および除去を行うことができます。出入り口ポートが存在しない場合は、テープをストレージ・スロットにロードする必要があります。

テープをストレージ・スロットにロードする場合は、元素ト・アドレスを使用してストレージ・スロットを識別するマウント要求に応答する必要があります。**CHECKIN LIBVOLUME** コマンドまたは **LABEL LIBVOLUME** コマンドに待機時間ゼロを指定した場合は、マウント要求に応答する必要はありません。

元素ト・アドレスについては、装置の製造元の資料を参照するか、[IBM Support Portal for IBM Spectrum Protect](#) にアクセスして元素ト・アドレスを検索してください。

## 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[LABEL LIBVOLUME \(ライブラリー・ボリュームのラベル付け\)](#)

## ボリューム・インベントリーの管理

ボリュームへのサーバーのアクセスの制御、テープの再使用、データベースのバックアップ操作やエクスポート操作に使用されたボリュームの再使用によって、ボリューム・インベントリーを管理することがで



きます。また、スクラッチ・ボリュームの提供を維持することによってもインベントリーの管理ができます。

## このタスクについて

サーバーが使用する各ボリュームには、そのボリュームがストレージ・プールに使用されるか、データベースのバックアップやエクスポートなどの操作に使用されるかに関係なく、固有の名前がなければなりません。異なるライブラリー内にあるが同じサーバーによって使用されているボリュームにも固有の名前が必要です。

## ボリュームへのアクセスの制御

さまざまな方法を使用して、ボリュームへのアクセスを制御することができます。

### 手順

ボリュームへのアクセスを制御するには、以下のいずれかのアクションを実行します。

- サーバーがボリュームをマウントできないようにするには、**UPDATE VOLUME** コマンドを発行して、**ACCESS=UNAVAILABLE** パラメーターを指定します。
- ボリュームを使用不可にして、保護するためのオフサイトに送るには、コピー・ストレージ・プールまたは活動データ・ストレージ・プールを使用します。
- まず、1 次ストレージ・プールをコピー・ストレージ・プールにバックアップし、次にそのコピー・ストレージ・プール・ボリュームをオフサイトに送ります。
- 活動バージョンのクライアント・バックアップ・データを活動データ・ストレージ・プールにコピーした後、ボリュームをオフサイトに送信することができます。
- コピー・ストレージ・プール・ボリュームおよび活動データ・プール・ボリュームは、そのアクセス・モードをオフサイトに変更し、そのボリューム・ヒストリーをそのロケーションが分かるように更新することによって、トラッキングできます。

### 関連情報

[UPDATE VOLUME \(ストレージ・プール・ボリュームの更新\)](#)

## テープの再利用

十分なテープ供給ができるように、古いファイルを期限切れにする、ボリュームをレクラメーション処理する、寿命に達したボリュームを削除するなどの作業を行うことができます。また、スクラッチ・ボリュームの供給を維持することも可能です。

## このタスクについて

時間の経過とともに、メディアは古くなり、メディア上に保管されているバックアップ・データの一部が不要になる場合があります。サーバー・ポリシーを定義して、保存するバックアップ・バージョンの数およびそれらの保存期間を決定することができます。満了処理を使用すると、不要になったファイルを削除することができます。必要なデータは、メディア上に保持することができます。データが不要になったら、メディアをレクラメーション処理して再使用することができます。

### 手順

1. 定期的に満了処理を実行して、不要なクライアント・データを削除します。期限切れプロセスにより、ポリシーでの保持指定を超えたか、あるいはユーザーまたは管理者がデータの活動バージョンを削除したという理由で有効でなくなったデータが削除されます。
2. レクラメーション処理を実行して、ストレージ・プール内のボリュームを再利用します。  
レクラメーション処理により、期限の切れていないデータが複数のボリュームから移動されてもっと少数のボリュームに統合されます。メディアは、その後ストレージ・プールに戻され、再利用されます。
3. ボリューム・ヒストリーを削除して、不要になった期限切れのデータベース・バックアップやエクスポート・データを含むボリュームを再利用します。



ボリューム・ヒストリー内の追跡対象ボリュームをサーバーで再利用するには、その前に、**DELETE VOLHISTORY** コマンドを発行してボリューム・ヒストリー・ファイルからボリューム情報を削除する必要があります。

**ヒント:**サーバーが災害復旧管理機能 (DRM) 機能を使用する場合、ボリューム情報は **MOVE DRMEDIA** コマンド処理時に自動的に削除されます。

4. テープ・ボリュームが寿命に達する時期を判別します。サーバーを使用して、メディアに対して実行された書き込み操作の回数および書き込みエラーの数などの、ボリュームについての統計情報を表示することができます。専用ボリュームおよびスクラッチ・ボリュームは、以下の統計データを表示します。

#### 専用ボリューム

最初に専用ボリュームとして定義されたメディアの場合、ボリュームがレクラメーション処理される時に、サーバーによりこの統計データが保守されます。この情報を、製造元が推奨する書き込み操作回数および書き込みエラー回数と比較できます。

#### スクラッチ・ボリューム

最初にスクラッチ・ボリュームとして定義されたメディアの場合、ボリュームがレクラメーション処理されるたびに、サーバーにより統計データが上書きされます。

5. 寿命に達したボリュームから、有効なデータをレクラメーション処理します。ボリュームが自動ライブラリー内にある場合は、ボリューム・インベントリーから出してチェックします。**DELETE VOLUME** コマンドによってデータベースから専用ボリュームを削除します。
6. ボリュームがテープ・ローテーションに必ず使用可能になるようにし、ストレージ・プールがスペース不足にならないようにします。Operations Center を使用して、スクラッチ・ボリュームの使用可能性をモニターすることができます。スクラッチ・ボリュームが、要求を満たすのに十分な数であることを確認してください。詳細については、[190 ページの『WORM メディアを含むライブラリーにおけるボリューム提供の維持』](#)を参照してください。

**WORM メディア:** Write Once Read Many (WORM) ドライブでは、バックアップ操作を完了させるためにボリュームを使用できないことが原因でサーバーでトランザクションが取り消されると、メディアが無駄になる可能性があります。サーバーが WORM ボリュームへの書き込みを行った後は、トランザクションが取り消された場合 (装置内のメディア不足のためにバックアップが取り消された場合など) でも、そのボリューム上のスペースは再利用できません。無駄になる WORM メディアを最小限に抑えるには、以下のアクションを実行します。

- a. 装置ストレージ・プール用のスクラッチ・ボリュームの最大数が、少なくとも、ライブラリー内のストレージ・スロットの数と同じになるようにします。
- b. 予想されるロードに対して十分な数のボリュームを、装置のボリューム・インベントリーにチェックインします。

ほとんどのバックアップ操作が小さいサイズのファイルの場合、トランザクション・サイズの制御によって、WORM プラッターの使用法に影響を与えることができます。トランザクションが小さくなれば、バックアップ操作などのトランザクションが取り消されることになっても、無駄になるスペースは少なくなります。トランザクション・サイズは、サーバー・オプション TXNGROUPMAX、およびクライアント・オプション TXNBYTELIMIT によって制御されます。

## 関連タスク

### アップグレードされたドライブへのデータのマイグレーション

ライブラリー内のすべての磁気テープ・ドライブをアップグレードする場合、既存のデータのマイグレーションおよび満了処理を行うために既存のポリシー定義を保存して、新規ドライブをデータの保管に使用することができます。

### サーバーによるボリューム要求の管理

IBM Spectrum Protect は、コンソール・モードで開始した管理コマンド・ライン・クライアントのすべてに対し、要求および状況メッセージを表示します。これらの要求メッセージには、しばしば時間制限が付きます。指定された時間制限内にサーバー操作が正常に完了する必要があります。完了しない場合、操作はタイムアウトになります。

## 関連情報

[DELETE VOLHISTORY \(順次ボリューム・ヒストリー情報の削除\)](#)

[DELETE VOLUME \(ストレージ・プール・ボリュームの削除\)](#)

[EXPIRE INVENTORY \(インベントリ満了処理の手動による開始\)](#)

[RECLAIM STGPOOL \(順次アクセス・ストレージ・プール内のボリュームのレクラメーション\)](#)

[Txnbytelimit オプション](#)

[TXNGROUPMAX サーバー・オプション](#)

## スクラッチ・ボリュームの提供の維持

ストレージ・プール用のスクラッチ・ボリュームの最大数は、予想される使用量に見合った十分な数に設定する必要があります。

### このタスクについて

ストレージ・プールを定義するときは、そのストレージ・プールが使用できる スクラッチ・ボリュームの最大数を指定する必要があります。サーバーは、必要になると、自動的にスクラッチ・ボリュームを要求します。サーバーがストレージ・プールに使用しているスクラッチ・ボリュームの数が、指定されている最大数を超えると、ストレージ・プールのスペースが不足する可能性があります。

### 手順

スクラッチ・ボリュームの最大数を超えるストレージ・プールが必要な場合は、以下のいずれかまたは両方のアクションを実行することができます。

1. **UPDATE STGPOOL** コマンドを発行して **MAXSCRATCH** パラメーターを指定することで、スクラッチ・ボリュームの最大数を増やします。
2. より少数のボリュームにデータを統合するために、満了処理とレクラメーション処理を実行して、ボリュームを再利用可能にします。
  - a) **EXPIRE INVENTORY** コマンドを発行して、満了処理を実行します。

**ヒント:** デフォルトでは、このプロセスは毎日自動的に実行されます。サーバー・オプション・ファイル `dsmserv.opt` で **EXPINTERVAL** サーバー・オプションを指定して、自動的に満了処理を実行することもできます。値 0 は、**EXPIRE INVENTORY** コマンドを使用して満了処理を実行する必要があることを意味します。

- b) **RECLAIM STGPOOL** コマンドを発行して、レクラメーション処理を実行します。

**ヒント:** ストレージ・プールを定義する際に **DEFINE STGPOOL** コマンドを使用して **RECLAIMPROCESS** パラメーターを指定することで、レクラメーションしきい値を指定することもできます。

### 次のタスク

将来のバックアップ操作に追加ボリュームが必要な場合は、**LABEL LIBVOLUME** コマンドを使用して追加のスクラッチ・ボリュームにラベルを付けます。

#### 関連タスク

[自動ライブラリー内でのスクラッチ・ボリューム提供の維持](#)

自動ライブラリーに関連付けられるストレージ・プールを定義するときは、ライブラリーの物理容量に等しいスクラッチ・ボリューム最大数を指定できます。サーバーが、ストレージ・プールでそれより多くのスクラッチ・ボリュームを使用している場合、十分なボリュームが使用可能であることを確認する必要があります。

#### 関連情報

[EXPIRE INVENTORY \(インベントリ満了処理の手動による開始\)](#)

[LABEL LIBVOLUME \(ライブラリー・ボリュームのラベル付け\)](#)

[RECLAIM STGPOOL \(順次アクセス・ストレージ・プール内のボリュームのレクラメーション\)](#)

[UPDATE STGPOOL \(ストレージ・プールの更新\)](#)

## WORM メディアを含むライブラリーにおけるボリューム提供の維持

Write Once Read Many (WORM) メディアを含むライブラリーでは、スクラッチ・ボリュームまたは新しい専用ボリュームがそのライブラリーで常に提供されるように図り、データ・ストレージ・トランザクションの取り消しが起こらないようにすることができます。トランザクションを取り消すと、WORM メディアが無駄に使用される原因になります。

### このタスクについて

データ・ストレージ操作を完了するためのボリュームが専用ボリュームであれ、スクラッチ・ボリュームであれ、使用できない場合は、IBM Spectrum Protect はトランザクションを取り消します。IBM Spectrum Protect が WORM ボリュームへの書き込みによってトランザクションを開始した後は、そのトランザクションが取り消されても、ボリューム上の書き込み済みのスペースは再利用できません。

例えば、それぞれ 2.6 GB を保持する WORM ボリュームがあり、クライアントが 12 GB のファイルのバックアップを開始したとします。IBM Spectrum Protect が 4 つのボリュームに書き込んだ後、5 番目のスクラッチ・ボリュームを取得できなかった場合、IBM Spectrum Protect はこのバックアップ操作を取り消します。IBM Spectrum Protect が既に書き込んだ 4 つのボリュームは、再利用できません。

トランザクションの取り消しを最小限に抑えるには、バックアップなどの予期されるクライアント操作に対応するために十分なボリュームがライブラリー内になければなりません。

### 手順

1. ライブラリーに関連付けられているストレージ・プールに十分なスクラッチ・ボリュームがあることを確認します。**UPDATE STGPOOL** コマンドを発行して、**MAXSCRATCH** パラメーターを指定します。
2. 予想される負荷に対応するためには、**CHECKIN LIBVOLUME** コマンドを発行することで、十分な数のスクラッチ・ボリュームまたは専用ボリュームをライブラリーにチェックインしてください。
3. トランザクション・サイズを制御するには、TXNGROUPMAX サーバー・オプションおよび TXNBYTELIMIT クライアント・オプションを指定します。クライアントが小さいサイズのファイルを保管することが多い場合は、トランザクション・サイズの制御によって、WORM ボリュームの使用方法に影響を与えることができます。トランザクションが小さければ、バックアップなどのトランザクションが取り消されることになっても、無駄になるスペースは少なく済みます。

### 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[UPDATE STGPOOL \(ストレージ・プールの更新\)](#)

[Txnbytelimit オプション](#)

[TXNGROUPMAX サーバー・オプション](#)

## 自動ライブラリー内のボリューム・インベントリーの管理

IBM Spectrum Protect サーバーは、ライブラリー・ボリューム・インベントリーを使用して、自動ライブラリーで使用可能なスクラッチ・ボリュームおよび専用ボリュームを追跡します。このインベントリーがライブラリーに実際に存在するボリュームと整合していることを確認する必要があります。

ライブラリー・ボリューム・インベントリーは、各ストレージ・プール用のボリューム・インベントリーとは別個のものです。ライブラリーのボリューム・インベントリーにボリュームを追加するには、その IBM Spectrum Protect ライブラリーにボリュームをチェックインします。

ライブラリー・ボリューム・インベントリー内のボリューム・リストは、装置のストレージ・プール・インベントリー内のボリューム・リストと同じではない場合があります。例えば、ライブラリーにはスクラッチ・ボリュームをチェックインできますが、ストレージ・プールにスクラッチ・ボリュームを定義することはできません。バックアップ操作でスクラッチ・ボリュームが選択されていない場合、ストレージ・プールに対して専用ボリュームを定義することができますが、それらのボリュームを装置のボリューム・インベントリーにチェックインすることはできません。

サーバー・ライブラリーのボリューム・インベントリーが正確さを保つようにするには、ボリュームをチェックアウトして、SCSI ライブラリーからボリュームを物理的に除去します。ストレージ・プールによって使用されているボリュームをチェックアウトすると、そのボリュームは、ストレージ・プールの中に残

ります。チェックアウトされているボリュームをマウントする必要がある場合は、そのボリュームをチェックインするように要求するメッセージが、マウント・オペレーターのコンソールに表示されます。チェックイン操作が失敗した場合、サーバーはそのボリュームに使用不可のマークを付けます。

ボリュームがライブラリー・ボリューム・インベントリー内にある場合、ボリュームの状況をスクラッチから専用に変更することができます。

サーバー・ライブラリーのボリューム・インベントリーがライブラリー内に実際に存在するボリュームと整合しているかどうかを確認するために、ライブラリーを監査できます。ボリュームのチェックイン操作またはチェックアウト操作を使用してサーバーに通知せずにライブラリーにボリュームを出し入れした場合は、インベントリーが不正確になるおそれがあります。

## 関連タスク

[自動ライブラリーへのボリュームのチェックイン](#)

**CHECKIN LIBVOLUME** コマンドを使用して、ボリュームを自動ライブラリーにチェックインすることができます。

## 関連情報

[AUDIT LIBRARY \(自動化ライブラリーにあるボリューム・インベントリーの監査\)](#)

## 自動ライブラリーのボリュームの状況の変更

ボリュームの状況を専用からスクラッチへ、またはスクラッチから専用へ変更することができます。

## 手順

ボリュームの状況を変更するには、**UPDATE LIBVOLUME** コマンドを発行します。

例えば、VOL1 という名前のボリュームの状況を専用ボリュームに変更するには、次のコマンドを発行します。

```
update libvolume lib1 vol1 status=private
```

## 制約事項:

- ボリュームがストレージ・プールに属している場合、またはボリューム・ヒストリー・ファイルに定義されている場合は、そのボリュームの状況を専用からスクラッチに変更することはできません。
- 専用ボリュームは、管理者が定義したボリュームで、データがないか、無効なデータを持つものです。活動データを含む部分的に書き込まれたボリュームにすることはできません。ボリューム状況が変更されると、ボリューム統計は失われます。

## 自動ライブラリーからのボリュームの除去

ボリュームにデータをエクスポートした場合や、別のシステムにデータをインポートする場合は、自動ライブラリーからボリュームを除去することができます。また、ボリュームを除去して、新規ボリューム用のスペースを作成することもできます。

## このタスクについて

デフォルトでは、サーバーは、チェックアウトするボリュームをマウントし、その内部ラベルを検査します。ラベルを検査すると、サーバーはライブラリー・ボリューム・インベントリーからボリュームを除去した後、そのボリュームをライブラリーの入り口ポートと出口ポートまたは都合のよい入出力装置に移動します。ライブラリーに入り口ポートと出口ポートがない場合、サーバーはライブラリー内のスロットまたは装置からボリュームを除去するようにマウント・オペレーターに要求します。

## 手順

- ボリュームを自動ライブラリーから除去するには、**CHECKOUT LIBVOLUME** コマンドを発行します。
- 自動ライブラリーに複数の入り口ポートと出口ポートがある場合は、**CHECKOUT LIBVOLUME** コマンドを発行して **REMOVE=BULK** パラメーターを指定します。サーバーは、ボリュームを次に使用可能な入り口ポートと出口ポートに排出します。



## 次のタスク

ストレージ・プールに定義されているボリュームをチェックアウトした後、サーバーがそのボリュームにアクセスする必要があると、サーバーはボリュームのチェックインを要求します。ボリュームをライブラリーに戻すには、**CHECKIN LIBVOLUME** コマンドを発行します。

### 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[CHECKOUT LIBVOLUME \(ストレージ・ボリュームのライブラリーからのチェックアウト\)](#)

## 自動ライブラリー内でのスクラッチ・ボリューム提供の維持

自動ライブラリーに関連付けられるストレージ・プールを定義するときは、ライブラリーの物理容量に等しいスクラッチ・ボリューム最大数を指定できます。サーバーが、ストレージ・プールでそれより多くのスクラッチ・ボリュームを使用している場合、十分なボリュームが使用可能であることを確認する必要があります。

### 手順

サーバーがそのストレージ・プールで使用しているスクラッチ・ボリュームの数が、ストレージ・プール定義に指定された数を超えたときは、次のステップを実行してください。

1. **CHECKIN LIBVOLUME** コマンドを発行して、ライブラリーにスクラッチ・ボリュームを追加します。

**ヒント:** それらのスクラッチ・ボリューム用のロケーションを確保する目的で、ライブラリーからボリュームを移動するために、オーバーフロー・ロケーションを使用する必要があることもあります。詳細については、192 ページの『オーバーフロー・ロケーションを使用した満杯のライブラリーの管理』を参照してください。

2. **UPDATE STGPOOL** コマンドを発行して **MAXSCRATCH** パラメーターを指定することで、ストレージ・プールに追加可能なスクラッチ・ボリュームの最大数を増やします。

## 次のタスク

将来のリカバリー操作に追加のボリュームが必要になる可能性があるため、予備のスクラッチ・ボリュームにラベル付けをして、準備しておくことを検討してください。

### 関連タスク

スクラッチ・ボリュームの提供の維持

ストレージ・プール用のスクラッチ・ボリュームの最大数は、予想される使用量に見合った十分な数に設定する必要があります。

## オーバーフロー・ロケーションを使用した満杯のライブラリーの管理

ストレージの要求が増えるに従って、ストレージ・プールに必要なボリューム数が自動ライブラリーの物理容量を超えることがあります。新規ボリュームがスペースを使用できるようにする場合、および既存のボリュームをモニターする場合には、ストレージ・プールのオーバーフロー・ロケーションを定義することができます。

## このタスクについて

サーバーは、オーバーフロー域に移動されたボリュームを追跡し、新規ボリュームがストレージ・スロットを使用できるようにします。

### 手順

1. ボリューム・オーバーフロー・ロケーションを作成します。**DEFINE STGPOOL** コマンドまたは **UPDATE STGPOOL** コマンドを発行して **OVFLOCATION** パラメーターを指定することで、自動ライブラリーに関連付けられているストレージ・プールを定義または更新します。

例えば、ARCHIVEPOOL という名前のストレージ・プールに ROOM2948 という名前のオーバーフロー・ロケーションを作成するには、次のコマンドを発行します。

```
update stgpool archivepool ovflocation=Room2948
```

2. ライブラリー内にスクラッチ・ボリューム用のスペースを作成する必要がある場合は、**MOVE MEDIA** コマンドを発行して、いっぱいになったボリュームをオーバーフロー・ロケーションに移動します。  
例えば、指定されたストレージ・プールの中のいっぱいのボリュームをすべてライブラリーから移動するには、次のコマンドを発行します。

```
move media * stgpool=archivepool
```

3. 必要に応じてスクラッチ・ボリュームをチェックインします。

**制約事項:** ボリュームがボリューム・ヒストリー・ファイル内に項目を持っている場合は、そのボリュームをスクラッチ・ボリュームとしてチェックインできません。詳細については、[181 ページの『自動ライブラリーへのボリュームのチェックイン』](#)を参照してください。

4. **QUERY MEDIA** コマンドを発行して、オーバーフロー・ロケーション内の空のスクラッチ・テープを識別します。  
例えば、次のコマンドを出します。

```
query media * stg=* whereovflocation=Room2948 wherestatus=empty
```

5. サーバーが追加ボリュームを要求する場合、オーバーフロー・ロケーションからボリュームを見つけてチェックインします。

オーバーフロー・ロケーション内のボリュームを検出するには、**QUERY MEDIA** コマンドを発行します。また、**QUERY MEDIA** コマンドを使用して、ボリュームをチェックインすることでコマンドを生成することもできます。

例えば、オーバーフロー・ロケーションにあるボリュームをリストし、同時にそれらのボリュームをライブラリーにチェックインするコマンドを生成するには、以下の例のようなコマンドを発行します。

```
query media format=cmd stgpool=archivepool whereovflocation=Room2948  
cmd="checkin libvol autolib &vol status=private"  
cmdfilename="%storage%move%media%checkin.vols"
```

#### ヒント:

- サーバーからのマウント要求には、ボリュームのロケーションが含まれます。
- ボリュームを処理に使用できるようになるまでの経過日数を指定するには、**UPDATE STGPOOL** コマンドを発行して **REUSEDELAY** パラメーターを指定します。
- 生成されたコマンドが入っているファイルは、IBM Spectrum Protect **MACRO** コマンドを使用して実行することができます。

#### 関連情報

[MOVE MEDIA \(順次アクセス・ストレージ・プール・メディアの移動\)](#)

[QUERY MEDIA \(順次アクセス・ストレージ・プール・メディアの照会\)](#)

[UPDATE STGPOOL \(ストレージ・プールの更新\)](#)

## ライブラリー内のボリューム・インベントリーの監査

自動ライブラリーを監査して、ライブラリー・ボリューム・インベントリーがライブラリーに実際に存在するボリュームと整合していることを確認することができます。ライブラリー内のボリュームを手動で移動したりデータベースに問題が発生したりしたためにライブラリー・ボリューム・インベントリーが正常な状態ではなくなった場合、ライブラリーを監査することが推奨されます。



## 手順

1. ライブラリー・ドライブにボリュームがマウントされていないことを確認します。IDLE 状態でマウントされたボリュームがある場合は、**DISMOUNT VOLUME** コマンドを発行してそのボリュームをマウント解除します。
2. **AUDIT LIBRARY** コマンドを発行して、ボリューム・インベントリーを監査します。以下のいずれかのアクションを実行します。
  - ライブラリーにバーコード・リーダーがある場合、ボリュームの識別のためにバーコード・リーダーを使用することにより、時間を節約できます。例えば、バーコード・リーダーを使用して TAPELIB ライブラリーを監査するには、次のコマンドを発行します。

```
audit library tapelib checklabel=barcode
```

- ライブラリーにバーコード・リーダーがない場合は、**CHECKLABEL=BARCODE** を指定せずに **AUDIT LIBRARY** コマンドを発行します。サーバーは、各ボリュームをマウントしてラベルを確認します。ラベルを確認した後、サーバーは残りのすべてのボリュームの監査を完了します。

## タスクの結果

サーバーは、欠落したボリュームをインベントリーから削除し、最後の監査以降に移動されたボリュームの位置を更新します。

**制約事項:**サーバーは、監査操作中に新規ボリュームをインベントリーに追加することはできません。

### 関連タスク

[テープ・ボリュームのラベル付け](#)

サーバーでテープ・ボリュームを使用するには、その前に、テープ・ボリュームにラベルを付ける必要があります。

### 関連情報

[AUDIT LIBRARY \(自動化ライブラリーにあるボリューム・インベントリーの監査\)](#)

[DISMOUNT VOLUME \(ボリューム名によるボリュームのマウント解除\)](#)

## 部分的に書き込まれているボリューム

部分的に書き込まれているボリュームは、サーバーがそれらのボリュームをマウントする前に状況がスクラッチであった場合でも、常に専用ボリュームになります。サーバーは、スクラッチ・ボリュームの元の状況を追跡し、空になるとスクラッチ状況に戻します。

サーバーは、ボリュームがマウントされるまで、自動ライブラリー内のボリューム以外のスクラッチ・ボリュームを認識していません。ボリュームがマウントされると、そのボリューム状況は専用に変更され、ボリュームは、マウント要求が出されたストレージ・プールの一部として自動的に定義されます。

### 関連タスク

[自動ライブラリーのボリュームの状況の変更](#)

ボリュームの状況を専用からスクラッチへ、またはスクラッチから専用へ変更することができます。

## 共有ライブラリーでの操作

共有ライブラリーは、SCSI ライブラリーによって物理的に表される論理ライブラリーです。物理ライブラリーは、ライブラリー・マネージャーとして構成された IBM Spectrum Protect サーバーによって制御されます。SHARED ライブラリー・タイプを使用する IBM Spectrum Protect サーバーは、IBM Spectrum Protect ライブラリー・マネージャー・サーバーに対するライブラリー・クライアントです。

ライブラリー・マネージャーが開始し、ストレージ装置が初期化されたとき、あるいはライブラリー・マネージャーがライブラリー・クライアントに定義された後に、ライブラリー・クライアントはそのライブラリー・マネージャーに接触します。ライブラリー・クライアントは、接続したサーバーが指定したライブラリー装置に対するライブラリー・マネージャーであることを確認します。また、ライブラリー・クラ

イアントは、ライブラリー・マネージャーのドライブ定義との整合性の比較も行います。ライブラリー・クライアントは、次のそれぞれの操作ごとにライブラリー・マネージャーに 接続します。

#### ボリューム・マウント

ライブラリー・クライアントは、共有ライブラリー装置の特定のボリュームへの アクセス要求をライブラリー・マネージャーに送ります。スクラッチ・ボリュームの場合、ライブラリー・クライアントはボリューム名を指定しません。ライブラリー・マネージャーが要求されたボリュームにアクセスできない場合、あるいはスクラッチ・ボリュームが使用できない場合、ライブラリー・マネージャーはそのマウント要求を拒否します。マウントが正常に行われると、ライブラリー・マネージャーはそのボリュームがマウントされるドライブの名前を戻します。

#### ボリュームの解放

ライブラリー・クライアントは、ボリュームへのアクセスを必要としなくなった時点で、そのボリュームをスクラッチに戻すことができることをライブラリー・マネージャーに通知します。ライブラリー・マネージャー・データベースは、ライブラリー・サーバーのインベントリーに入ったボリュームの新しい位置で更新されます。そのボリュームは、ライブラリー・クライアントの ボリューム・インベントリーから削除されます。

195 ページの表 35 に、IBM Spectrum Protect 操作の処理における、ライブラリー・クライアントとライブラリー・マネージャー間の相互作用を示します。

表 35. SAN 対応サーバーが IBM Spectrum Protect 操作を処理する方法		
操作 (コマンド)	ライブラリー・マネージャー	ライブラリー・クライアント
ライブラリー・ボリュームの照会 ( <b>QUERY LIBVOLUME</b> )	ライブラリーにチェックインされているボリュームを表示する。 専用ボリュームの場合、そのオーナー・サーバーも表示される。	適用されない。
ライブラリー・ボリュームのチェックインおよびチェックアウト ( <b>CHECKIN LIBVOLUME</b> 、 <b>CHECKOUT LIBVOLUME</b> )	ライブラリー装置にコマンドを送信する。	適用外。 クライアント・リストア操作のためにチェックイン操作が必要な場合に、ライブラリー・マネージャー・サーバーに要求が送信される。
メディアの移動および DRM メディアの移動 ( <b>MOVE MEDIA</b> 、 <b>MOVE DRMEDIA</b> )	ライブラリー・マネージャー・サーバーが使用するボリュームに対してのみ有効。	ライブラリー・マネージャー・サーバーが操作を実行するように要求する。そのライブラリー・マネージャー・サーバーでチェックアウト・プロセスを生成する。
ライブラリー・インベントリーの監査 ( <b>AUDIT LIBRARY</b> )	インベントリーをライブラリー装置と同期させる。	インベントリーをライブラリー・マネージャー・サーバーと同期させる。
ライブラリー・ボリュームへのラベル付け ( <b>LABEL LIBVOLUME</b> )	ボリュームにラベルを付けてチェックインする。	適用されない。
ボリュームの取り外し ( <b>DISMOUNT VOLUME</b> )	ライブラリー装置に要求を送信する。	ライブラリー・マネージャー・サーバーが操作を実行するように要求する。

表 35. SAN 対応サーバーが IBM Spectrum Protect 操作を処理する方法 (続き)

操作 (コマンド)	ライブラリー・マネージャー	ライブラリー・クライアント
ボリュームの照会 ( <b>QUERY VOLUME</b> )	ボリュームが要求元のライブラリー・クライアントに所有されているかどうか、およびボリュームがライブラリー装置にあるかどうかを検査する。	ライブラリー・マネージャー・サーバーが操作を実行するように要求する。

## サーバーによるボリューム要求の管理

IBM Spectrum Protect は、コンソール・モードで開始した管理コマンド・ライン・クライアントのすべてに対し、要求および状況メッセージを表示します。これらの要求メッセージには、しばしば時間制限が付きます。指定された時間制限内にサーバー操作が正常に完了する必要があります。完了しない場合、操作はタイムアウトになります。

### このタスクについて

自動ライブラリーの場合は、**CHECKIN LIBVOLUME** コマンドおよび **LABEL LIBVOLUME** コマンドを使用して、カートリッジをスロットに挿入します。**WAITTIME** パラメーターの値を指定すると、応答メッセージが表示されます。このパラメーターの値が 0 の場合は、応答は不要です。**CHECKOUT LIBVOLUME** コマンドを発行した場合は、スロットにカートリッジを挿入する必要があり、すべての場合に応答メッセージが表示されます。

### 手順

- 次の表は、さまざまなサーバー・メディア・タスクの処理方法について説明しています。

タスク	詳細
マウント・メッセージのための管理クライアントの使用	サーバーは、マウント要求状況メッセージを、サーバー・コンソール、およびマウント・モードまたはコンソール・モードのすべての管理コマンド・ライン・クライアントに送信します。  マウント・モードで管理コマンド・ライン・クライアントを開始するには、管理コマンド・ライン・クライアントで <b>dsmadm -mountmode</b> コマンドを発行します。
自動ライブラリーに関するメッセージの受信	マウント・メッセージ、および自動ライブラリーに関するエラー・メッセージは、マウント・モードまたはコンソール・モードの管理コマンド・ライン・クライアントで表示できます。マウント・メッセージはライブラリーに送られ、オペレーターには送られません。ライブラリーの問題に関するメッセージは、マウント・メッセージ・キューに送られます。
保留中のオペレーター要求に関する情報の取得	保留中のオペレーター要求に関する情報を取得するには、マウント・モードで開始した管理コマンド・ライン・クライアントで <b>QUERY REQUEST</b> コマンドを発行するか、またはマウント・メッセージ・キューを確認します。 <b>QUERY REQUEST</b> コマンドを出すと、サーバーは、要求されたアクションと、その要求がタイムアウトになるまでに残されている時間を表示します。
オペレーター要求に対する応答	サーバーでマウント要求の完了に対する明示的な応答が必要な場合は、 <b>REPLY</b> コマンドを使用します。  <i>request_number</i> パラメーターは、要求識別番号を指定します。この番号を使用して、どの保留中のオペレーター要求が完了したかをサーバーに通知します。この 3 桁の数字は常に要求メッセージの一部として表示されます。

タスク	詳細
オペレーター要求の取り消し	<p>ライブラリーのマウント要求を取り消すには、<b>CANCEL REQUEST</b> コマンドを発行します。自動 SCSI ライブラリーに関連した大部分の要求では、要求されたマウントを取り消すには、オペレーターがハードウェア・アクションまたはシステム・アクションを実行する必要があります。このような要求では、サーバーは <b>CANCEL REQUEST</b> コマンドを受け付けません。</p> <p><b>CANCEL REQUEST</b> コマンドには、要求識別番号を含める必要があります。この番号は要求メッセージに入っています。</p> <p>要求されたボリュームに <b>UNAVAILABLE</b> のマークを付けるには、<b>CANCEL REQUEST</b> コマンドを発行して <b>PERMANENT</b> パラメーターを指定します。<b>PERMANENT</b> パラメーターを指定した場合、サーバーは、要求されたボリュームのマウントを再試行しません。これは、例えば、ボリュームがリモート・サイトにある場合や、使用不可の場合に役立ちます。</p>
ボリューム・チェックイン要求に対する応答	<p>サーバーは、マウントする特定のボリュームを自動ライブラリーで見つけれない場合は、そのボリュームをチェックインするようにオペレーターに要求します。</p> <p>要求されたボリュームが使用可能である場合、ライブラリー内にそのボリュームを入れ、チェックインします。詳細については、<a href="#">181 ページの『自動ライブラリーへのボリュームのチェックイン』</a>を参照してください。</p> <p>要求されたボリュームが使用不可の場合は、<b>UPDATE VOLUME</b> コマンドを発行して <b>ACCESS=UNAVAILABLE</b> パラメーターを指定することによって、ボリュームのアクセス・モードを更新します。次に、<b>CANCEL REQUEST</b> コマンドを使用してチェックイン要求を取り消します。この要求を行ったクライアント・プロセスは取り消さないでください。取り消す要求の ID を取得するには、<b>QUERY REQUEST</b> コマンドを使用します。</p> <p>ストレージ・プールの装置クラスに指定されたマウント待機時間内にサーバーからのチェックイン要求に応答しないと、サーバーはそのボリュームに使用不可のマークを付けます。</p>
マウントされているボリュームの判別	<p>サーバーで使用するために現在マウントされているすべてのボリュームに関するレポートが必要な場合は、<b>QUERY MOUNT</b> コマンドを発行します。このレポートには、どのボリュームがマウントされているか、どのドライブがそれらにアクセスしているか、およびボリュームが現在使用中かどうかを示されます。</p>
アイドル・ボリュームの取り外し	<p>ボリュームがアイドルになると、サーバーは、その装置クラスのためのマウント保存期間パラメーターに指定された時間だけ、そのボリュームをマウントしたままにします。ボリュームを繰り返し使用する場合は、マウント保存値を使用するとアクセス時間を短縮できます。</p> <p>使用されていないボリュームをマウントされているドライブから取り外すには、<b>DISMOUNT VOLUME</b> コマンドを発行します。</p> <p>マウント保存期間の設定については、<a href="#">128 ページの『ボリュームのマウント保存期間の制御』</a>を参照してください。</p>

## 関連情報

[QUERY REQUEST \(1 つ以上の保留中のマウント要求の照会\)](#)

## 磁気テープ・ドライブの管理

磁気テープ・ドライブを照会、更新、および削除することができます。磁気テープ・ドライブをクリーニングしたり、磁気テープ・ドライブの暗号化とデータ検証を構成したりすることもできます。

### ドライブの更新

ドライブ定義の属性を変更して、ドライブをオフラインにしたり再構成したりすることができます。

#### このタスクについて

ドライブの以下の属性を変更することができます。

- エレメント・アドレス (ドライブが SCSI 内にある場合)
- クリーニング頻度
- ドライブ状況: オンラインまたはオフライン

**制約事項:** ドライブを使用中の場合、エレメント番号および装置名を変更することはできません。ドライブをオフラインにする手順については、[199 ページの『テープ装置のオフラインでの使用』](#)を参照してください。

ボリュームは、ドライブにマウントされている場合でも、アイドル状態であれば明示的にマウント解除することができます。アイドル状態のボリュームをマウント解除する手順については、[196 ページの『サーバーによるボリューム要求の管理』](#)を参照してください。

#### 手順

- **UPDATE DRIVE** コマンドを発行して、ドライブのエレメント・アドレスを変更します。  
例えば、AUTO という名前のライブラリー内で、DRIVE3 のエレメント・アドレスを 119 に変更するには、次のコマンドを発行します。

```
update drive auto drive3 element=119
```

- **UPDATE PATH** コマンドを発行して、ドライブの装置名を変更します。  
例えば、DRIVE3 という名前のドライブの装置名を変更するには、次のコマンドを実行します。

```
AIX update path server1 drive3 srctype=server desttype=drive library=scsilib  
device=/dev/rmt0
```

```
Linux update path server1 drive3 srctype=server desttype=drive library=scsilib  
device=/dev/IBMtape0
```

```
Windows update path server1 drive3 srctype=server desttype=drive library=scsilib  
device=mt3.0.0.0
```

#### 関連情報

[UPDATE DRIVE \(ドライブの更新\)](#)

[UPDATE PATH \(パスの変更\)](#)



## テープ装置のオフラインでの使用

テープ装置が使用中のときは、オフラインで 사용할 수 있습니다。例えば、保守を実行するためにドライブをオフラインにすることがあります。

### このタスクについて

ドライブの使用中にそのドライブの状況をオフラインに変更すると、サーバーはドライブ内のテープの処理を終了し、その後にドライブの使用を停止します。ただし、使用していたテープが単一トランザクションの一連のテープの一部であった場合、そのドライブではその一連のテープの処理を完了することができません。使用可能なドライブが他にない場合、そのトランザクションは失敗します。

### 手順

- ドライブの状況を変更するには、**UPDATE DRIVE** コマンドを発行して **ONLINE** パラメーターを指定します。例えば、ライブラリー MANLIB 内のドライブ DRIVE3 を更新してドライブをオフラインにするには、次のコマンドを発行します。

```
update drive manlib drive3 online=no
```

**制約事項:** **ONLINE** パラメーターを指定する場合は、他のオプション・パラメーターを指定しないでください。指定すると、ドライブは更新されず、ドライブが使用中のときはコマンドは失敗します。

### タスクの結果

ライブラリー内のすべてのドライブをオフライン状況に更新すると、ライブラリー・マウント・ポイントを必要とするプロセスは失敗します。

更新されたドライブの状態は、サーバーを停止および再始動しても保持されます。サーバーの再始動時にドライブにオフラインにマークが付いていると、ドライブを手動でオンラインにする必要があることを示す警告が発行されます。

### 関連情報

[UPDATE DRIVE \(ドライブの更新\)](#)

## テープに対する読み取り/書き込み操作中のデータ検証

データを検証して破損したデータを識別するために、論理ブロック保護と呼ばれる機能を使用できます。論理ブロック保護を使用する場合、IBM Spectrum Protect は、データをテープに書き込む際に、そのデータの各論理ブロックの最後に巡回冗長検査 (CRC) 値を挿入します。

論理ブロック保護を使用すると、テープへのデータの書き込み時、およびストレージ・エリア・ネットワーク経由での磁気テープ・ドライブから IBM Spectrum Protect へのデータ転送時に発生するエラーを識別することができます。論理ブロック保護をサポートするドライブは、読み取り操作と書き込み操作の実行中にデータを検証します。IBM Spectrum Protect サーバーは、読み取り操作の実行中にデータを検証します。

書き込み操作中にドライブによる検証が失敗した場合、テープへの転送時にデータが破損したことを示している可能性があります。この場合、IBM Spectrum Protect サーバーは、書き込み操作に失敗します。操作を続けるには、操作を再始動する必要があります。読み取り操作中にドライブによる検証が失敗した場合、テープ・メディアが破損していることを示している可能性があります。読み取り操作中に IBM Spectrum Protect サーバーによる検証が失敗した場合、磁気テープ・ドライブからの転送時にデータが破損したことを示している可能性があります。サーバーは操作を再実行します。検証が連続して失敗する場合、IBM Spectrum Protect サーバーはハードウェアまたは接続の問題を示すエラー・メッセージを発行します。

論理ブロック保護が磁気テープ・ドライブ上で無効になっている場合、またはドライブが論理ブロック保護をサポートしない場合は、IBM Spectrum Protect サーバーは保護データを読み取ることができます。ただし、データは検証されません。



論理ブロック保護は、ストレージ・プールを定義または更新するときに指定できる CRC 検証より優れています。ストレージ・プールに対して CRC 検証を指定すると、データはボリューム監査操作時にのみ検証されます。エラーは、データがテープに書き込まれた後で認識されます。

#### 制約事項:

- バックアップ・セットやデータベース・バックアップなど、順次データに対して論理ブロック保護を使用することはできません。
- CRC 検査を行うと、CRC 値を計算して比較するためにクライアントとサーバーの両方で必要なプロセッサ使用量が増加するため、パフォーマンスに影響します。
- スクラッチ・ボリュームでは、読み取り/書き込み操作に対する論理ブロック保護 (LBPROTECT=READWRITE) を指定する場合、データがボリュームに書き込まれた後にはパラメーター値を変更しないでください。IBM Spectrum Protect サーバー上のボリュームの存続中にパラメーター値を変更することはサポートされません。

## 論理ブロック保護をサポートするドライブ

論理ブロック保護は、3592、LTO、および ECARTRIDGE の各装置タイプでのみ使用可能です。対応する 3592 ドライブには、IBM TS1130、TS1140、およびそれ以降の世代が含まれます。対応する LTO ドライブには、IBM LTO-5 およびサポートされる LTO-6 ドライブが含まれます。対応する Oracle StorageTek ドライブには、T10000C および T10000D フォーマットを使用するドライブが含まれます。

次の表に、論理ブロック保護をサポートするドライブで使用できるメディアとフォーマットを示します。

ドライブ	磁気テープ・メディア	ドライブ・フォーマット
IBM TS1130	3592 第 2 世代	3592-3 および 3592-3C
IBM TS1140	3592 第 2 世代 3592 第 3 世代	第 2 世代: 3592-3 および 3592-3C 第 3 世代: 3592-4 および 3592-4C
IBM TS1150	3592 第 3 世代 3592 第 4 世代	第 4 世代: 3592-5 および 3592-5C
IBM LTO-5	LTO-5	Ultrium 5 および Ultrium 5C
IBM LTO-6	LTO-6 LTO-5	Ultrium 6 および Ultrium 6C Ultrium 5 および Ultrium 5C
IBM LTO-7	LTO-7 LTO-6	Ultrium 7 および Ultrium 7C Ultrium 6 および Ultrium 6C
Oracle T10000C	Oracle StorageTek T10000 T2	T10000C および T10000C-C
Oracle T10000D	Oracle StorageTek T10000 T2	T10000D および T10000D-C

#### ヒント:

- テープ・ボリュームの論理ブロック保護を有効にし、データのバックアップにボリュームを再使用するには、装置クラスおよびドライブの論理ブロック保護を有効にする必要があります。
- 論理ブロック保護に対応していない 3592 ドライブ、LTO ドライブ、または Oracle StorageTek ドライブを使用している場合は、論理ブロック保護機能を提供するファームウェアを使用してドライブをアップグレードできます。

SCSI ライブラリー内のドライブでは、論理ブロック保護が使用可能です。論理ブロック保護のサポートに関する最新情報については、[技術情報 1568108](#) を参照してください。

書き込み操作のために論理ブロック保護を使用するには、ライブラリー内のすべてのドライブが論理ブロック保護をサポートしている必要があります。ドライブが論理ブロック保護に対応していない場合、読み取り/書き込みアクセスが可能なボリュームはマウントされません。ただし、サーバーはそのドライブを使

用して、読み取り専用アクセスが可能なボリュームをマウントできます。読み取り/書き込み操作に対して論理ブロック保護が有効になっている場合は、IBM Spectrum Protect サーバーによって保護データが読み取られ、検証されます。

## 論理ブロック保護の有効化および無効化

論理ブロック保護は、読み取り操作と書き込み操作に対して指定することも、書き込み操作のみにに対して指定することもできます。論理ブロック保護を無効にすることもできます。デフォルトでは、サーバーおよび磁気テープ・ドライブ上で巡回冗長検査 (CRC) 検証によってパフォーマンス上の影響が生じるため、論理ブロック保護は無効になっています。

### このタスクについて

空のボリュームまたは充てん中のボリュームに対する読み取り/書き込みの操作は、そのボリュームに論理ブロック保護が設定されているかどうかによって異なります。保護データ・ブロックと無保護データ・ブロックを同一ボリューム上に混在させることはできません。論理ブロック保護の設定を変更した場合、その変更は空のボリュームのみに適用されます。充てん中のボリュームおよび満杯のボリュームは、それらが空になって、再び書き込まれる準備ができるまで、それらの論理ブロック保護の状況を維持します。例えば、論理ブロック保護が無効にされており、サーバーが、論理ブロック保護がある装置クラスに関連付けられたボリュームを選択した場合、サーバーはそのボリュームへの保護データの書き込みを続行します。

**制約事項:** 論理ブロック保護は、特定の装置タイプでのみ使用可能です。詳細については、[200 ページの『論理ブロック保護をサポートするドライブ』](#)を参照してください。

### 手順

1. 3592、LTO、および ECARTRIDGE の装置タイプの論理ブロック保護を有効にするには、**DEFINE DEVCLASS** コマンドまたは **UPDATE DEVCLASS** コマンドを発行して、**LBPROTECT** パラメーターを指定します。  
例えば、3592\_lbprotect という名前の 3592 装置クラスに対して、読み取り操作および書き込み操作の実行中の論理ブロック保護を指定するには、次のコマンドを発行します。

```
define devclass 3592_lbprotect library=3594 lbprotect=readwrite
```

#### ヒント:

- **LBPROTECT** パラメーターの値を NO から READWRITE または WRITEONLY に更新し、サーバーが、書き込み操作の論理ブロック保護の設定されていない充てん中のボリュームを選択すると、サーバーはそのボリュームがマウントされるたびにメッセージを出します。このメッセージは、論理ブロック保護を使用しないボリュームにデータが書き込まれることを示しています。このメッセージが表示されないようにするか、IBM Spectrum Protect が論理ブロック保護を使用したデータ書き込みのみを行うようにするには、論理ブロック保護のない充てん中のボリュームのアクセス権を、読み取り専用に更新してください。
  - パフォーマンスを改善するために、**DEFINE STGPOOL** コマンドおよび **UPDATE STGPOOL** コマンドでは **CRCDATA** パラメーターを指定しないでください。
  - ドライブと IBM Spectrum Protect サーバーの両方での読み取り操作中にデータが検証される場合は、リストア操作とリトリブ操作の際にサーバーのパフォーマンスが低下する可能性があります。リストア操作およびリトリブ操作に必要な時間を削減するには、**LBPROTECT** パラメーターの設定を READWRITE から WRITEONLY に変更します。データがリストアまたは取得された後に、**LBPROTECT** パラメーターを READWRITE にリセットすることができます。
2. 論理ブロック保護を無効にするには、**DEFINE DEVCLASS** コマンドまたは **UPDATE DEVCLASS** コマンドを発行して、**LBPROTECT=NO** パラメーターを指定します。

**制約事項:** 論理ブロック保護を無効にした場合、サーバーは論理ブロック保護を使用する空のテープに対して書き込みを行いません。ただし、論理ブロック保護を使用する充てん中のボリュームを選択した場合、サーバーは論理ブロック保護を使用してボリュームへの書き込みを続行します。サーバーが論理ブロック保護を使用するテープへの書き込みを行わないようにするには、論理ブロック保護を使用する

充てん中のボリュームのアクセス権限を読み取り専用に変更します。データを読み取る際に、ドライブおよびサーバーのいずれも CRC の結果を検査しません。

災害が発生し、災害復旧サイトに論理ブロック保護をサポートするドライブがない場合、**LBPROTECT=NO** パラメーターを指定する必要があります。書き込み操作に磁気テープ・ドライブが使用されている場合は、保護データを含むボリュームのボリューム・アクセス権を読み取り専用に変更して、サーバーがそれらのボリュームを使用するのを防ぐ必要があります。

サーバーが論理ブロック保護を有効にする必要がある場合、サーバーは、ドライブが論理ブロック保護をサポートしていないことを示すエラー・メッセージを発行します。

## 次のタスク

ボリュームに論理ブロック保護があるかどうかを判別するには、**QUERY VOLUME** コマンドを発行し、「論理ブロック保護」フィールドの値を確認します。

### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[DEFINE STGPOOL \(ストレージ・プール内のボリュームの定義\)](#)

[QUERY VOLUME \(ストレージ・プール・ボリュームの照会\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

[UPDATE STGPOOL \(ストレージ・プールの更新\)](#)

## 論理ブロック保護を使用するボリュームに対する読み取り/書き込み操作

空のボリュームまたは充てん中のボリュームに対する読み取り/書き込みの操作は、そのボリュームに論理ブロック保護が設定されているかどうかによって異なります。保護データ・ブロックと無保護データ・ブロックを同一ボリューム上に混在させることはできません。

**UPDATE DEVCLASS** コマンドを使用して論理ブロック保護の設定を変更した場合、その変更は、空のボリュームのみに適用されます。充てん中のボリュームおよび満杯のボリュームは、それらが空になって、再び書き込まれる準備ができるまで、それらの論理ブロック保護の状況を維持します。

例えば、**LBPROTECT** パラメーターの値を **READWRITE** から **NO** に変更すると想定します。装置クラスに関連付けられており、論理ブロック保護があるボリュームをサーバーが選択した場合、サーバーは、そのボリュームへの保護データの書き込みを続行します。

### ヒント:

- ドライブが論理ブロック保護をサポートしていない場合、書き込み操作に論理ブロック保護が使用されたボリュームはマウントすることができません。サーバーが書き込み操作のために保護ボリュームをマウントしないようにするには、ボリュームのアクセス権限を読み取り専用に変更してください。また、サーバーが磁気テープ・ドライブ上で論理ブロック保護機能を有効にしないように、論理ブロック保護を無効にしてください。
- ドライブが論理ブロック保護をサポートしておらず、論理ブロック保護が無効になっている場合、サーバーは保護ボリュームからデータを読み取ります。ただし、データはサーバーと磁気テープ・ドライブによって検証されません。

### 関連情報

[QUERY VOLUME \(ストレージ・プール・ボリュームの照会\)](#)

[UPDATE DEVCLASS \(装置クラスの更新\)](#)

## テープ・ライブラリー内のストレージ・プール管理

保護データと無保護データを混合してライブラリーに保管するには、データを分離するために別々の装置クラスと別々のストレージ・プールを作成する必要があります。装置クラスが保護データに関連付けられている場合、読み取り操作と書き込み操作に対して、あるいは書き込み操作のみに対して、論理ブロック保護を指定することができます。

保護データおよび無保護データについて、LTO-5 ドライブを使用する TS3500 ライブラリーの装置クラスおよびストレージ・プールを定義するには、次の例に示すように一連のコマンドを発行します。

```
define library 3584 libtype=scsi
define devclass lbprotect library=3584 devicetype=lto lbprotect=readwrite
define devclass normal library=3584 devicetype=lto lbprotect=no
define stgpool lbprotect_pool lbprotect maxscratch=10
define stgpool normal_pool normal maxscratch=10
```

#### 関連情報

[DEFINE DEVCLASS \(装置クラスの定義\)](#)

[DEFINE LIBRARY \(ライブラリーの定義\)](#)

[DEFINE STGPOOL \(ストレージ・プール内のボリュームの定義\)](#)

## 磁気テープ・ドライブのクリーニング

サーバーを使用して磁気テープ・ドライブ・クリーニングを管理することができます。サーバーは、SCSI ライブラリーの磁気テープ・ドライブのクリーニング方法を管理することができます。

### このタスクについて

磁気テープ・ドライブをクリーニングするには、システム特権または無制限のストレージ特権が必要です。自動ライブラリーの場合、クリーニング操作の頻度を指定し、ライブラリー・ボリューム・インベントリにクリーナー・カートリッジを入れることにより、クリーニングを自動化することができます。IBM Spectrum Protect は、指定されたとおりにクリーナー・カートリッジをマウントします。SCSI ライブラリーで、その装置のハードウェアにおいて自動ドライブ・クリーニング・サポートを提供する、サーバー制御のドライブ・クリーニングの使用を計画する場合は、特別な考慮事項があります。

**ヒント:** 自動テープ・ライブラリーがライブラリー・ドライブのクリーニングをサポートする場合、その機能が有効にされていることを確認してください。

ご使用の装置の製造元が提供するライブラリー・クリーニング機能を使用することで、ドライブの読み取り/書き込みヘッドが早く摩耗するのを防ぐことができます。

メーカーの異なるドライブおよびライブラリーは、クリーナー・カートリッジの管理方法や、ドライブにクリーナー・カートリッジが有るかどうかの報告方法が異なります。デバイス・ドライバーは、クリーナー・カートリッジが入っているドライブを オープンできない場合があります。ドライブ・クリーニングに関して装置によって出されるセンス・コードとエラー・コードは異なります。通常、ライブラリー・ドライブのクリーニングは、アプリケーションから認識されません。したがって、IBM Spectrum Protect によって常に、ドライブのクリーナー・カートリッジが検出されるわけではなく、また、クリーニングがいつ開始されるかが判別されるわけではありません。

装置によっては、ドライブ・クリーニングを開始する次のマウント要求までに短いアイドル時間を必要とするものもあります。しかし、IBM Spectrum Protect は、ドライブのアイドル時間を最小化しようとしています。結果として、ライブラリーのドライブ・クリーニングが効果的に機能するのを妨げられることがあります。このようになった場合は、IBM Spectrum Protect を使用してドライブ・クリーニングを制御してください。頻度を、メーカーのクリーニング推奨値に合うように設定できます。

## 磁気テープ・ドライブのクリーニング方法

時間の経過につれて、テープ上の読み取りヘッドが汚れて、読み取り操作や書き込み操作が失敗する可能性があります。このような問題を防止するために、テープ・クリーニングを有効にします。テープ・クリーニングは、ドライブまたは IBM Spectrum Protect から有効にすることができます。

ライブラリー・ドライブ・クリーニング方式、または IBM Spectrum Protect ドライブ・クリーニング方式を使用することを選択できますが、両方を使用することはできません。一部の SCSI ライブラリーには、自動ドライブ・クリーニング機能があります。ライブラリー・ドライブ・クリーニング方式を選択します (使用可能な場合)。使用できない場合や問題が発生する場合は、IBM Spectrum Protect を使用してライブラリー・ドライブ・クリーニングを制御します。



## ライブラリー・ドライブ・クリーニング方式

ライブラリー・ドライブ・クリーニング方式には、この機能を使用する自動テープ・ライブラリーにとっていくつかの利点があります。

- IBM Spectrum Protect 管理者がカートリッジ・クリーニングを物理的に管理する負担を軽減します。
- クリーニング・カートリッジの使用率を改善させます。大部分のテープ・ライブラリーは、ハードウェアの標識に基づいてドライブをクリーニングする回数を追跡します。IBM Spectrum Protect では、未加工のカウントが使用されます。
- 不要なクリーニングを減らします。最新の磁気テープ・ドライブは固定間隔でのクリーニングを必要とせず、クリーニングが必要な時にそれを検出して要求することができます。

ライブラリー・ドライブ・クリーニング方式を提供する製造元は、ドライブの読み取り/書き込みヘッドの摩耗を遅らせるために、ライブラリー・ドライブ・クリーニングの使用を推奨しています。メーカーの異なるドライブおよびライブラリーは、クリーナー・カートリッジの管理方法や、ドライブにクリーナー・カートリッジが存在しているかどうかの報告方法が異なります。デバイス・ドライバーは、クリーナー・カートリッジが入っているドライブをオープンできない場合があります。ドライブ・クリーニングに関して装置によって出されるセンス・コードとエラー・コードは異なります。通常、ライブラリー・ドライブ・クリーニングはすべてのアプリケーションから認識されません。ただし、IBM Spectrum Protect がドライブ内のクリーナー・カートリッジを常に検出するわけではなく、いつクリーニングが開始されたかを判別できない場合があります。

## IBM Spectrum Protect ドライブ・クリーニング方式

装置によっては、ドライブ・クリーニングを開始する次のマウント要求までに短いアイドル時間を必要とするものもあります。しかし、IBM Spectrum Protect は、ドライブのアイドル時間を最小化しようとしています。結果として、ライブラリーのドライブ・クリーニングが効果的に機能するのを妨げられることがあります。このようになった場合は、ドライブ・クリーニングを制御するために、IBM Spectrum Protect を使用してみてください。頻度を、メーカーのクリーニング推奨値に合うように設定します。

IBM Spectrum Protect がドライブ・クリーニング・プロセスを制御する場合は、問題を回避するためにライブラリー・ドライブ・クリーニング機能を無効にします。ライブラリー・ドライブ・クリーニング機能が有効にされている場合、一部の装置では、ライブラリー内で検出されたすべてのクリーナー・カートリッジを、ライブラリー内のクリーナー・カートリッジ専用スロットに自動的に移動します。ライブラリーのドライブ・クリーニング機能を無効にするまでは、クリーナー・カートリッジを IBM Spectrum Protect のライブラリー・インベントリにチェックインすることはできません。

ドライブからのクリーニングを有効にするには、ドライブの製造元が提供する手順に従います。IBM Spectrum Protect を使用してクリーニングを有効にするには、204 ページの『自動ライブラリーでドライブ・クリーニングを行うためのサーバーの構成』を参照してください。

## 自動ライブラリーでドライブ・クリーニングを行うためのサーバーの構成

自動ライブラリーのサーバー制御ドライブ・クリーニングを構成するときに、ドライブのクリーニング頻度を指定することができます。

### 始める前に

ドライブをクリーニングする必要がある頻度を判別します。**DEFINE DRIVE** コマンドまたは **UPDATE DRIVE** コマンドの **CLEANFREQUENCY** パラメーターに適切な値を指定できるようにするためには、このステップが必要です。例えば、ドライブ上で 100 GB のデータが処理された後にドライブをクリーニングするには、**CLEANFREQUENCY=100** を指定します。

クリーニング頻度のガイドラインについては、ドライブ製造元の資料を参照してください。資料で示されたクリーニング頻度のガイドラインが使用時間で指定されている場合は、以下のステップを実行して、その値をギガバイト値に変換します。

1. ドライブの「バイト/秒」値を使用して「ギガバイト/時間」値を判別します。
2. ギガバイト/時間の値に、推奨クリーニング頻度 (使用時間数) を掛けます。
3. その結果をクリーニング頻度値として使用します。

**CLEANFREQUENCY** パラメーターの値を指定するか、必要に応じてドライブをクリーニングするための **ASNEEDED** を指定します。

#### 制約事項:

1. IBM 3592 ドライブの場合、**CLEANFREQUENCY** パラメーターに数値を指定する必要があります。製品資料にリストされたクリーニング頻度を使用することで、過度にドライブをクリーニングすることがなくなります。
2. **CLEANFREQUENCY=ASNEEDED** パラメーター値は、すべての磁気テープ・ドライブで機能するわけではありません。ドライブがこの機能をサポートしているかを判別するには、ご使用のオペレーティング・システムに関する情報を参照してください。

Windows	AIX	AIX および Windows でサポートされるデバイス
Linux		Linux でサポートされるデバイス

技術情報で、ドライブ名をクリックして詳細情報を表示します。ASNEEDED 値がサポートされていない場合は、ギガバイト数を指定します。

## 手順

**DEFINE DRIVE** または **UPDATE DRIVE** コマンドで **CLEANFREQUENCY** パラメーターを使用して、ライブラリーのドライブを定義または更新します。

例えば、100 GB のデータが処理された後に DRIVE1 という名前のドライブをクリーニングするには、次のコマンドを発行します。

```
update drive autolib1 drive1 cleanfrequency=100
```

## タスクの結果

クリーナー・カートリッジがチェックインされると、サーバーはドライブがクリーニングを必要とする時点でそのドライブにクリーナー・カートリッジをマウントします。サーバーは、指定されたクリーニングの回数だけ、そのクリーナー・カートリッジを使用します。詳細については、[155 ページの『クリーナー・カートリッジでの操作』](#)を参照してください。

## 次のタスク

205 ページの『クリーナー・カートリッジのライブラリーへのチェックイン』の手順に従って、クリーナー・カートリッジをライブラリー・ボリューム・インベントリーにチェックインします。

#### 関連情報

[DEFINE DRIVE \(ドライブのライブラリーへの定義\)](#)

[UPDATE DRIVE \(ドライブの更新\)](#)

## クリーナー・カートリッジのライブラリーへのチェックイン

磁気テープ・ドライブの自動クリーニングを有効にするには、クリーナー・カートリッジを自動ライブラリーのボリューム・インベントリーにチェックインする必要があります。

## このタスクについて

ライブラリーにクリーナー・カートリッジをチェックインし、サーバーがクリーナー・カートリッジとして正しく識別していることを確認します。クリーナー・カートリッジが、検索プロセスで検出されるスロットに入っていないことを確認します。エラーまたは 15 分以上の遅延が発生する場合、クリーナー・カートリッジが正しく配置されていないことを示している可能性があります。

推奨される方法は、クリーナー・カートリッジを個別にチェックインする方法です。データ・カートリッジとクリーナー・カートリッジの両方をチェックインする必要がある場合、まずデータ・カートリッジをライブラリーに置いて、チェックインします。その後、クリーナー・カートリッジをライブラリーにチェックインします。



## 手順

クリーナー・カートリッジをライブラリーにチェックインするには、**CHECKIN LIBVOLUME** コマンドを発行します。

例えば、AUTOLIB1 という名前のクリーナー・カートリッジをチェックインするには、次のコマンドを発行します。

```
checkin libvolume autolib1 cleanv status=cleaner cleanings=10  
checklabel=no
```

サーバーは、カートリッジを出入り口ポートまたは特定のスロットに配置するように要求します。

## 関連情報

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

## クリーナー・カートリッジでの操作

磁気テープ・ドライブが必要なときに確実にクリーニングされるようにし、磁気テープ・ストレージの問題を防止するには、次のガイドラインに従います。

### クリーニング・プロセスのモニター

クリーナー・カートリッジがライブラリーにチェックインされており、ドライブをクリーニングする必要がある場合、サーバーは、データ・ボリュームをマウント解除してクリーニング操作を実行します。クリーニング操作が失敗あるいは取り消されるか、使用可能なクリーナー・カートリッジがない場合、ドライブをクリーニングする必要があることに気付かない可能性があります。このような問題に関するクリーニング・メッセージをモニターして、ドライブが必要時にクリーニングされていることを確認してください。必要に応じて、**CLEAN DRIVE** コマンドを発行してサーバーに再度クリーニングを試行させるか、またはクリーナー・カートリッジを手操作でドライブにロードしてください。

### 複数のクリーナー・カートリッジの使用

1つのクリーナー・カートリッジをチェックインすると、サーバーはそのクリーナー・カートリッジを指定されたクリーニング回数だけ使用します。複数のクリーナー・カートリッジをチェックインすると、そのカートリッジに指定されたクリーニング回数に達するまで、サーバーは1つのカートリッジのみを使用します。その後、サーバーは次のクリーナー・カートリッジを使用します。複数のクリーナー・カートリッジをチェックインして、複数の**CLEAN DRIVE** コマンドを同時に発行すると、サーバーは同時に複数のカートリッジを使用して、各カートリッジの残りのクリーニング回数を減らします。

## 関連情報

[AUDIT LIBRARY \(自動化ライブラリーにあるボリューム・インベントリーの監査\)](#)

[CHECKIN LIBVOLUME \(ストレージ・ボリュームのライブラリーへのチェックイン\)](#)

[CLEAN DRIVE \(ドライブのクリーニング\)](#)

[LABEL LIBVOLUME \(ライブラリー・ボリュームのラベル付け\)](#)

[QUERY LIBVOLUME \(ライブラリー・ボリュームの照会\)](#)

## ドライブ・クリーニングに関連するエラーの解決

ライブラリー内のカートリッジを移動する際に、クリーナー・カートリッジを入れるべき場所にデータ・カートリッジが入る場合があります。サーバーが実行するプロセスと発行されるメッセージを確認することで、問題を解決することができます。

ドライブのクリーニングが必要になると、サーバーは、データベースでクリーナー・カートリッジとして表示されるカートリッジをドライブにロードします。ドライブは、その後 **READY** 状態に移り、**IBM Spectrum Protect** は、カートリッジがデータ・カートリッジであることを検出します。サーバーは、以下のステップを実行します。

1. サーバーは、データ・カートリッジの内部磁気テープ・ラベルを読み取ろうとします。
2. サーバーは、ドライブからカートリッジを排出し、カートリッジをライブラリー内のクリーナー・カートリッジのホーム・スロットに戻します。排出操作が失敗した場合、サーバーは、ドライブにオフラインのマークを付け、カートリッジがまだドライブにあることを示すメッセージを発行します。

3. サーバーは、クリーナー・カートリッジをチェックアウトして、他のドライブ・クリーニング要求でそれが選択されることを避けます。クリーナー・カートリッジはライブラリー内に残りますが、IBM Spectrum Protect ライブラリー・インベントリーにはもう現れません。
4. 内部磁気テープ・ラベルを使用することで、サーバーは、現行のライブラリー・インベントリー、ストレージ・プール・ボリューム、およびボリューム・ヒストリー・ファイルに対するボリューム名をチェックします。
  - ・ライブラリー・インベントリー内でボリューム名が見つからない場合、誤ってデータ・カートリッジがクリーナー・カートリッジとしてチェックインされる可能性があります。ボリュームがチェックアウトされたら、その他にアクションを実行する必要はありません。
  - ・ライブラリー・インベントリー内にボリューム名が見つかった場合、サーバーは、手操作による介入とライブラリー監査が必要であることを示すメッセージを発行します。問題を解決するには、[193 ページ](#)の『ライブラリー内のボリューム・インベントリーの監査』の手順に従います。

## 磁気テープ・ドライブの置換

IBM Spectrum Protect に定義されているテープ・ライブラリー内のドライブを置き換える場合は、旧ドライブおよびそのパス定義を削除し、新規ドライブおよびそのパスを定義する必要があります。

ドライブとパス定義の置き換えは、同じ論理アドレス、物理アドレス、SCSI ID、およびポート番号を使用して、あるドライブを同じタイプの別のドライブと交換する場合でも必要です。ドライブ接続を変更すると、装置の別名が変わる可能性があります。

新規ドライブが、新しいメディア・フォーマットをサポートするアップグレード・ドライブである場合は、新しい論理ライブラリー、装置クラス、およびストレージ・プールの定義が必要になる可能性があります。複数ドライブ・ライブラリー内の新規ドライブのポリシーをセットアップするための手順は、ライブラリー内のドライブおよびメディアのタイプによって異なります。

## 磁気テープ・ドライブの削除

ライブラリーから磁気テープ・ドライブを削除することができます。例えば、使用しなくなったドライブや、交換したいドライブを削除することができます。

### 手順

1. IBM Spectrum Protect サーバーを停止して、オペレーティング・システムをシャットダウンします。
2. 旧ドライブを除去し、製造元の指示に従って新規ドライブを取り付けます。
3. オペレーティング・システムと IBM Spectrum Protect サーバーを再始動します。
4. サーバーからドライブへのパスを削除します。  
例えば、SERVER1 から LIB1 へのパスを削除するには、次のコマンドを発行します。

```
delete path server1 lib1 srctype=server desttype=drive
```

5. ドライブ定義を削除します。  
例えば、DLT1 という名前のドライブを LIB1 という名前のライブラリー装置から削除するには、以下のコマンドを発行します。

```
delete drive lib1 dlt1
```

### 関連情報

[DELETE DRIVE \(ライブラリーからのドライブの削除\)](#)

[DELETE PATH \(パスの削除\)](#)

## ドライブを同じタイプの別のドライブと置換

置換するドライブと同じメディア・フォーマットをサポートするドライブを追加するには、新しいドライブとパスを定義する必要があります。

### このタスクについて

ライブラリーに 1 つのモデルのドライブのみが含まれており、ドライブを交換したい場合は、そのドライブを同じモデルのドライブと交換する必要があります。ライブラリー内で複数のモデルのドライブが混在しており、1 つのドライブを交換したい場合は、そのドライブをライブラリー内に存在する任意のモデルのドライブと交換することができます。

### 手順

1. 古いドライブに関するパスおよびドライブの定義を削除します。例えば、LIB1 という名前のライブラリーから DRIVE1 という名前のドライブを削除するには、次のコマンドを入力します。

```
delete path server2 drive1 srctype=server desttype=drive library=lib1
delete drive lib1 drive1
```

2. ライブラリーの電源をオフにし、元のドライブを取り外し、新規ドライブに交換して、ライブラリーの電源をオンにします。
3. ホスト・システムを最新表示して、システムが新規ドライブを検出したことを確認します。
4. 新しいドライブとパスを定義します。例えば、新規ドライブ DRIVE2 と SERVER2 からそのドライブへのパスを定義するには、IBM Spectrum Protect デバイス・ドライバーを使用している場合、次のコマンドを入力します。

```
AIX define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=/dev/mt0
```

```
Linux define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=/dev/tmscsi/mt0
```

```
Windows define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=mt3.0.0.1
```

**ヒント:** 既存のライブラリー、装置クラス、およびストレージ・プールの定義を使用することができます。

### 関連情報

[DELETE DRIVE \(ライブラリーからのドライブの削除\)](#)

[DELETE PATH \(パスの削除\)](#)

## アップグレードされたドライブへのデータのマイグレーション

ライブラリー内のすべての磁気テープ・ドライブをアップグレードする場合、既存のデータのマイグレーションおよび満了処理を行うために既存のポリシー定義を保存して、新規ドライブをデータの保管に使用することができます。

### 始める前に

以下のシナリオは、DISK 装置クラスの 1 次ストレージ・プール (POOL1 という名前) が既に準備されていることを前提としています。

## 手順

1. 新規ドライブ用に作成されたストレージ・プールにデータをマイグレーションするには、**NEXTSTGPOOL** パラメーターを指定します。例えば、既存のストレージ・プール (POOL1) から新規ストレージ・プール (POOL2) にデータをマイグレーションするには、次のコマンドを発行します。

```
update stgpool pool1 nextstgpool=pool2
```

2. **UPDATE MGMTCLASS** コマンドを使用して、管理クラス定義を更新し、DISK ディスク・ストレージ・プールにデータを保管します。

## 関連情報

[DEFINE STGPOOL \(ストレージ・プール内のボリュームの定義\)](#)

[UPDATE MGMTCLASS \(管理クラスの更新\)](#)

[UPDATE STGPOOL \(ストレージ・プールの更新\)](#)

# IBM Spectrum Protect サーバーの保護

サーバーおよびクライアント・ノードへのアクセスの制御、データの暗号化、およびセキュアなアクセス・レベルとパスワードの維持により、IBM Spectrum Protect サーバーおよびデータを保護します。

## 管理者の管理

システム権限を持つ管理者は、IBM Spectrum Protect サーバーを使用するすべてのタスク (他の管理者への権限レベルの割り当てを含む) を実行することができます。一部のタスクを実行するには、1 つ以上の権限レベルを割り当てられることによって権限を付与される必要があります。

## 手順

管理者の設定を変更するには、以下のタスクを実行します。

タスク	手順
管理者の追加	<p>システム権限を持つ管理者 (ADMIN1) を追加してパスワードを指定するには、以下の手順を実行します。</p> <ol style="list-style-type: none"><li>a. 以下のコマンドを発行して、管理者を登録し、パスワードとして <b>Pa\$#\$tw0</b> を指定します。</li></ol> <pre>register admin admin1 Pa\$#\$tw0</pre> <ol style="list-style-type: none"><li>b. 以下のコマンドを発行して、管理者にシステム権限を付与します。</li></ol> <pre>grant authority admin1 classes=system</pre>
管理権限の変更	<p>管理者 ADMIN1 の権限レベルを変更します。</p> <ul style="list-style-type: none"><li>• 以下のコマンドを発行して、管理者にシステム権限を付与します。</li></ul> <pre>grant authority admin1 classes=system</pre> <ul style="list-style-type: none"><li>• 次のコマンドを発行して、管理者のシステム権限を取り消します。</li></ul> <pre>revoke authority admin1 classes=system</pre>

タスク	手順
管理者の削除	<p>以下のコマンドを発行して、管理者 ADMIN1 を削除して IBM Spectrum Protect サーバーにアクセスできないようにします。</p> <pre>remove admin admin1</pre>
サーバーへのアクセスの一時停止	<p><b>LOCK ADMIN</b> コマンドまたは <b>UNLOCK ADMIN</b> コマンドを使用して、管理者をロックまたはアンロックします。</p>

#### 関連概念

##### 管理者役割の計画

IBM Spectrum Protect ソリューションにアクセスできる管理者に割り当てる権限レベルを定義します。

## パスワード要件の変更

最小パスワード限界、パスワード長、パスワードの有効期限を変更したり、IBM Spectrum Protect の認証を使用可能または使用不可にしたりすることができます。

### このタスクについて

パスワード認証を適用してパスワード制限を管理することにより、潜在的なセキュリティー・リスクからデータとサーバーを保護します。

### 手順

IBM Spectrum Protect サーバーのパスワード要件を変更するには、以下のタスクを実行します。

表 36. IBM Spectrum Protect サーバーの認証タスク	
タスク	手順
無効なパスワード試行の制限の設定。	<ol style="list-style-type: none"> <li>Operations Center の「サーバー」ページで、サーバーを選択します。</li> <li>「詳細」をクリックして、「プロパティ」タブをクリックします。</li> <li>「無効なサインオン試行数の限度」フィールドで、無効な試行回数を設定します。 インストール時のデフォルト値は 0 です。</li> </ol>
パスワードの最小長の設定。	<ol style="list-style-type: none"> <li>Operations Center の「サーバー」ページで、サーバーを選択します。</li> <li>「詳細」をクリックして、「プロパティ」タブをクリックします。</li> <li>「最小パスワード長」フィールドで、文字数を設定します。</li> </ol>
パスワードの満了期間の設定。	<ol style="list-style-type: none"> <li>Operations Center の「サーバー」ページで、サーバーを選択します。</li> <li>「詳細」をクリックして、「プロパティ」タブをクリックします。</li> <li>「パスワード共通の有効期限」フィールドで、日数を設定します。</li> </ol>

表 36. IBM Spectrum Protect サーバーの認証タスク (続き)

タスク	手順
デフォルトの認証方式の設定。	<p><b>SET DEFAULTAUTHENTICATION</b> コマンドを発行します。例えば、サーバーをデフォルトの認証方式として使用する場合、以下のコマンドを発行します。</p> <pre>set defaultauthentication local</pre> <p>サーバーを使用して認証を行うように 1 つのクライアント・ノードを更新するには、<b>UPDATE NODE</b> コマンドに <b>AUTHENTICATION=LOCAL</b> を組み込みます。</p> <pre>update node authentication=local</pre>

## システムでのサーバーの保護

不正アクセスを防止するために、IBM Spectrum Protect サーバーが稼働しているシステムを保護します。

### 手順

無許可のユーザーが、サーバー・データベースおよびサーバー・インスタンスのディレクトリーにアクセスできないようにします。実装時に構成したこれらのディレクトリーに対するアクセス設定を保持してください。

## サーバーへのユーザー・アクセスの制限

権限レベルによって、管理者が IBM Spectrum Protect サーバーで実行できる内容が決まります。システム権限を持つ管理者は、サーバーに対してすべてのタスクを実行できます。ポリシー権限、ストレージ権限、またはオペレーター権限を持つ管理者は、タスクのサブセットを実行できます。

### 手順

1. **REGISTER ADMIN** コマンドを使用して管理者を登録した後、**GRANT AUTHORITY** コマンドを使用して、管理者の権限レベルを設定します。  
権限の設定および変更について詳しくは、[209 ページの『管理者の管理』](#)を参照してください。
2. 一部のタスクを実行するための管理者の権限を制御するには、以下の 2 つのサーバー・オプションを使用します。
  - a) **QUERYAUTH** サーバー・オプションを使用して、**QUERY** コマンドと **SELECT** コマンドを発行するために管理者に必要な権限レベルを選択できます。デフォルトでは、権限レベルは不要です。この要件を、権限レベル (システムを含む) の 1 つに変更できます。
  - b) **REQSYSAUTHOUTFILE** サーバー・オプションを使用して、サーバーによる外部ファイルへの書き込みが行われるコマンドにはシステム権限が必要であることを指定できます。デフォルト解釈では、このようなコマンドにはシステム権限が必要です。
3. クライアント・ノードでのデータ・バックアップを、root ユーザー ID または許可ユーザーのみに制限できます。  
例えば、バックアップを root ユーザー ID に制限するには、**REGISTER NODE** コマンドまたは **UPDATE NODE** コマンドを発行して、**BACKUPINITIATION=root** パラメーターを指定します。

```
update node backupinitiation=root
```



# サーバーの停止および始動

保守タスクまたは再構成タスクを実行する前に、サーバーを停止します。次に、サーバーを保守モードで始動します。保守タスクまたは再構成タスクを終了したら、サーバーを実動モードで再始動します。

## 始める前に

IBM Spectrum Protect サーバーを停止および始動するには、システム特権またはオペレーター特権が必要です。

## サーバーの停止

サーバーを停止する前に、すべてのデータベース・バックアップ操作が完了していること、およびその他すべてのプロセスとセッションが終了していることを確認して、システムを準備します。こうすることで、サーバーを安全にシャットダウンして、データが保護されていることを確認できます。

### このタスクについて

**HALT** コマンドを発行してサーバーを停止すると、以下のアクションが行われます。

- すべてのプロセスおよびクライアント・ノード・セッションが取り消されます。
- すべての現行トランザクションが停止されます。(トランザクションは、サーバーの再始動時にロールバックされます。)

### 手順

システムを準備してサーバーを停止するには、以下の手順を実行します。

1. **DISABLE SESSIONS** コマンドを発行して、新規クライアント・ノード・セッションが開始しないようにします。

```
disable sessions all
```

2. 以下のステップを実行して、進行中のクライアント・ノード・セッションまたはプロセスがないかを判別します。
  - a. Operations Center の「概要」ページで「アクティビティ」領域を参照して、現在アクティブであるプロセスおよびセッションの総数を確認します。その数が毎日のストレージ管理の日常業務時に表示される通常の数と大幅に異なる場合は、Operations Center の他の状況標識を表示して、問題がないかを確認します。
  - b. 「アクティビティ」領域のグラフを参照して、以下の期間中のネットワーク・トラフィックの量を比較します。
    - 現在の期間 (直近 24 時間の間)
    - 直前の期間 (現在の期間の前の 24 時間)直前の期間のグラフが予想されるトラフィック量を表している場合、現在の期間のグラフで示される大幅な差異は、問題を示している可能性があります。
  - c. 「サーバー」ページで、プロセスおよびセッションを表示したいサーバーを選択して、「詳細」をクリックします。サーバーがハブ・サーバーまたはスポーク・サーバーとして Operations Center で登録されていない場合は、管理コマンドを使用して、プロセスに関する情報を取得します。 **QUERY PROCESS** コマンドを発行してプロセスを照会し、**QUERY SESSION** コマンドを発行してセッションに関する情報を取得します。
3. クライアント・ノード・セッションが完了するまで待つか、それらを取り消します。プロセスおよびセッションを取り消すには、以下のステップを実行します。
  - 「サーバー」ページで、プロセスおよびセッションを表示したいサーバーを選択して、「詳細」をクリックします。

- ・「**アクティブ・タスク**」タブをクリックして、キャンセルする 1 つ以上のプロセス、セッション、またはその両方の組み合わせを選択します。
- ・「**キャンセル**」をクリックします。
- ・サーバーがハブ・サーバーまたはスポーク・サーバーとして Operations Center で登録されていない場合は、管理コマンドを使用してセッションを取り消します。**CANCEL SESSION** コマンドを発行してセッションを取り消し、**CANCEL PROCESS** コマンドを使用してプロセスを取り消します。

**ヒント:** 取り消すプロセスがテープ・ボリュームがマウントされるのを待機している場合、そのマウント要求は取り消されます。例えば、**EXPORT**、**IMPORT**、または **MOVE DATA** コマンドを発行すると、コマンドにより、テープ・ボリュームのマウントを必要とするプロセスが開始される場合があります。ただし、自動化ライブラリーによってテープ・ボリュームがマウントされている場合は、マウント・プロセスが完了するまで、取り消し操作は有効になりません。システム環境によっては、数分かかる場合があります。

4. **HALT** コマンドを発行して、サーバーを停止します。

```
halt
```

## 保守または再構成のタスクのためのサーバーの始動

サーバーの保守タスクや再構成タスクを開始する前に、サーバーを保守モードで始動します。保守モードでサーバーを始動するときは、保守タスクや再構成タスクを中断する可能性がある操作を使用不可にします。

### このタスクについて

**MAINTENANCE** パラメーターを指定して **DSMSERV** ユーティリティーを実行し、サーバーを保守モードで始動します。

保守モードでは、以下の操作が使用不可になります。

- ・管理コマンド・スケジュール
- ・クライアント・スケジュール
- ・サーバー上のストレージ・スペースのレクラメーション
- ・インベントリーの有効期限
- ・ストレージ・プールのマイグレーション

さらに、クライアントがサーバーとのセッションを開始できなくなります。

**ヒント:**

- ・サーバーを保守モードで始動するために、サーバー・オプション・ファイル `dsmserve.opt` を編集する必要はありません。
- ・サーバーが保守モードで稼働している間、ストレージ・スペースのレクラメーション、インベントリー満了処理、およびストレージ・プールのマイグレーションのプロセスを手動で開始できます。

### 手順

- ・サーバーを保守モードで始動するには、次のコマンドを発行します。

```
dsmserve maintenance
```

**ヒント:** 保守モードでのサーバーの始動に関するビデオを見るには、[保守モードでのサーバーの始動](#)を参照してください。

### 次のタスク

サーバー操作を実動モードで再開するには、以下の手順を実行します。

1. **HALT** コマンドを発行し、サーバーをシャットダウンする。

```
halt
```

2. 実動モードで使用する的方法を使用して、サーバーを始動します。使用するオペレーティング・システムの指示に従って、以下を実行します。

- **AIX**
- **Linux**
- **Windows**

保守モード中に使用不可になっていた操作が再び使用可能になります。

## サーバーのアップグレード計画

フィックスパックまたは暫定修正が入手可能になると、製品の改善点を利用するために IBM Spectrum Protect サーバーをアップグレードすることができます。サーバーおよびクライアントは、さまざまな時点でアップグレードできます。サーバーをアップグレードする前に、必ず計画ステップを完了してください。

### このタスクについて

次のガイドラインに従ってください。

- サーバーをアップグレードするために、インストール・ウィザードを使用する方法をお勧めします。ウィザードを開始した後、「**IBM Installation Manager**」ウィンドウで、「**更新**」アイコンをクリックします。「**インストール**」または「**変更**」アイコンをクリックしないでください。
- サーバー・コンポーネントと Operations Center コンポーネントの両方のアップグレードが入手可能な場合、両方のコンポーネントをアップグレードするためのチェック・ボックスを選択します。

### 手順

1. フィックスパックおよび暫定修正のリストを確認します。[IBM Spectrum Protect のダウンロード - 最新のフィックスパックと暫定修正](#)を参照してください。
2. README ファイルに記載されている製品の改善点を確認します。  
**ヒント:** [サポート・サイト](#)からインストール・パッケージ・ファイルを入手すると、README ファイルにもアクセスできます。
3. サーバーのアップグレード先のバージョンが、他のコンポーネント (ストレージ・エージェントやライブラリー・クライアントなど) と互換性があることを確認します。[IBM Spectrum Protect サーバーとストレージ・エージェントおよびライブラリー・クライアントの互換性](#)を参照してください。
4. ソリューションに V7.1 より前のレベルのサーバーまたはクライアントが含まれている場合、ガイドラインを調べて、クライアント・バックアップおよびアーカイブの操作が中断されないようにしてください。[IBM Spectrum Protect のサーバーとクライアントの互換性とアップグレードの考慮事項](#)を参照してください。
5. アップグレード手順を確認します。サーバー・データベース、装置構成情報、およびボリューム・ヒストリー・ファイルをバックアップしたことを確認します。

### 次のタスク

フィックスパックまたは暫定修正をインストールするには、ご使用のオペレーティング・システム用の指示に従います。

- **AIX** [サーバー・フィックスパックのインストール](#)
- **Linux** [サーバー・フィックスパックのインストール](#)
- **Windows**

## 障害やシステム更新に対する準備

計画された停電やシステム更新の間にシステムが整合した状態を保持できるように、IBM Spectrum Protect を準備します。

### このタスクについて

サーバーを管理、保護、および保守するためのアクティビティを必ず定期的にスケジュールしてください。データベースのバックアップ、装置構成ファイルのバックアップ、ボリューム・ヒストリーのバックアップなどのアクティビティのスケジュールについては、[56 ページの『サーバー保守アクティビティのスケジュールの定義』](#)を参照してください。

### 手順

- 以下のステップを実行して、進行中のプロセスおよびセッションをキャンセルします。
  - Operations Center の「サーバー」ページで、プロセスおよびセッションを確認したサーバーを選択し、「詳細」をクリックします。
  - 「アクティブ・タスク」タブをクリックして、キャンセルする 1 つ以上のプロセス、セッション、またはその両方の組み合わせを選択します。
  - 「キャンセル」をクリックします。
- HALT** コマンドを発行して、サーバーを停止します。

```
halt
```

**ヒント：**halt コマンドを Operations Center から発行するには、「設定」アイコンの上にカーソルを移動し、「コマンド・ビルダー」をクリックします。次に、サーバーを選択し、halt を入力して **Enter** キーを押します。

### 関連情報

[HALT \(サーバーのシャットダウン\)](#)

## DRM を使用した災害に対する準備と災害からのリカバリー

IBM Spectrum Protect は、災害時にご使用のサーバーおよびクライアントのデータをリカバリーするための災害復旧管理機能 (DRM) 機能を提供します。

DRM は、オフサイト・メディアの移動を追跡し、その情報を IBM Spectrum Protect データベースに登録します。DRM は、計画、スクリプト、およびその他の情報を計画ファイルに統合します。このファイルは、災害や計画外の停止が発生した場合に、IBM Spectrum Protect サーバーを復旧するために必要です。ランサムウェアなど、潜在的なマルウェア攻撃が心配な場合は、DRM の使用を検討してください。これは攻撃後のサーバーをリカバリーする際に役に立ちます。

**制約事項：**DRM は、IBM Spectrum Protect Extended Edition 製品でのみ使用可能です。

## 災害時回復計画ファイル

災害時回復計画ファイルには、その計画が作成される前に完了した最後のデータベース・バックアップ時点まで IBM Spectrum Protect サーバーを復旧するために必要な情報が含まれます。

計画はスタンザとして編成され、複数のファイルに分割することができます。各スタンザには、開始ステートメントと終了ステートメントがあります。

表 37. 災害時回復計画ファイル内のスタンザ	
スタンザ	スタンザ内の情報
SERVER.REQUIREMENTS	サーバーのデータベースおよび回復ログのストレージ要件を識別します。
RECOVERY.INSTRUCTIONS.GENERAL	接頭部 RECOVERY.INSTRUCTIONS.GENERAL で識別されるファイルに管理者が入力するサイト固有の指示を識別します。この指示には、回復方法、主な連絡先、このサーバーがバックアップする重要なアプリケーションの概要、およびその他の関連する回復指示が含まれます。
RECOVERY.INSTRUCTIONS.OFFSITE	接頭部 RECOVERY.INSTRUCTIONS.OFFSITE で識別されるファイルに管理者が入力する指示が含まれます。これらの指示では、オフサイト・ボールドの名前とロケーション、およびボールド管理者との連絡方法 (例えば、名前と電話番号など) が示されます。
RECOVERY.INSTRUCTIONS.INSTALL	接頭部 RECOVERY.INSTRUCTIONS.INSTALL で識別されるファイルに管理者が入力する指示が含まれます。これらの指示では、基本サーバーの再作成方法が示され、システム・イメージ・バックアップ・コピーのロケーションを提供します。
RECOVERY.INSTRUCTIONS.DATABASE	接頭部 RECOVERY.INSTRUCTIONS.DATABASE で識別されるファイルに管理者が入力する指示が含まれます。これらの指示では、データベース・リカバリーの準備方法が示されます。例えば、自動ライブラリーのバックアップ・ボリュームを初期化またはロードする方法についての指示を入力できます。なお、このスタンザのサンプルはありません。
RECOVERY.INSTRUCTIONS.STGPOOL	接頭部 RECOVERY.INSTRUCTIONS.STGPOOL で識別されるファイルに管理者が入力する指示が含まれます。この指示には、ソフトウェア・アプリケーションの名前とそれらのアプリケーションのバックアップを含むコピー・ストレージ・プールの名前が含まれます。なお、このスタンザのサンプルはありません。
RECOVERY.VOLUMES.REQUIRED	サーバーのリカバリーに必要なデータベース・バックアップ・ボリュームとコピー・ストレージ・プール・ボリュームのリストを提供します。データベース・バックアップ・ボリュームは、それが最新のデータベース・バックアップの集合の一部である場合に組み込まれます。コピー・ストレージ・プール・ボリュームは、空ではなく、破損としてマークもされていない場合に組み込まれます。
RECOVERY.DEVICES.REQUIRED	バックアップ・ボリュームを読むのに必要な装置についての詳細を提供します。
RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE	サーバーを復旧するために必要なコマンドを指定したスクリプトが含まれます。
RECOVERY.SCRIPT.NORMAL.MODE	サーバーの 1 次ストレージ・プールをリストアするために必要なコマンドを指定したスクリプトが含まれます。
DB.STORAGEPATHS	IBM Spectrum Protect データベースのディレクトリーを識別します。
LICENSE.REGISTRATION	サーバー・ライセンスを登録するためのマクロが含まれます。
COPYSTGPOOL.VOLUMES.AVAILABLE	オフサイトに移動され、その後にオンサイトに戻されたコピー・ストレージ・プール・ボリュームをマークするためのマクロが含まれます。この情報をガイドとして使用し、管理コマンドを発行することができます。あるいは、ファイルに対してマクロをコピー、変更、および実行します。このマクロは、RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE スクリプトによって開始されます。
COPYSTGPOOL.VOLUMES.DESTROYED	災害時にコピー・ストレージ・プール・ボリュームがオンサイトにあった場合に、そのボリュームに使用不可のマークを付けるためのマクロが含まれます。これらのボリュームは、オフサイトにありと考えられ、したがって災害で破壊されていないと見なされます。この情報をガイドとして使用してコマンド行から管理コマンドを実行するか、またはマクロをファイルにコピーし、変更して実行することができます。このマクロは、RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE スクリプトによって開始されます。

表 37. 災害時回復計画ファイル内のスタンザ (続き)	
スタンザ	スタンザ内の情報
PRIMARY.VOLUMES.DESTROYED	災害時に 1 次ストレージ・プール・ボリュームがオンサイトにあった場合、そのボリュームを 破棄 としてマークするマクロが含まれています。この情報をガイドとして使用してコマンド・ラインから管理コマンドを実行するか、またはマクロをファイルにコピーし、変更して実行することができます。このマクロは、RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE スクリプトによって開始されます。
PRIMARY.VOLUMES.REPLACEMENT	置換用の 1 次ストレージ・プール・ボリュームを識別するためのマクロが含まれます。この情報をガイドとして使用してコマンド・ラインから管理コマンドを実行するか、またはマクロをファイルにコピーし、変更して実行することができます。このマクロは、RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE スクリプトによって開始されます。
STGPOOLS.RESTORE	1 次ストレージ・プールをリストアするためのマクロが含まれます。ガイドとしてスタンザを使用し、コマンド・ラインから管理コマンドを実行できます。また、これをファイルにコピーし、変更して実行することもできます。このマクロは、RECOVERY.SCRIPT.NORMAL.MODE スクリプトによって開始されます。
VOLUME.HISTORY.FILE	リカバリー計画を作成した時点のボリューム・ヒストリー情報のコピーが含まれます。 <b>DSMSERV RESTORE DB</b> ユーティリティは、このボリューム・ヒストリー・ファイルを使用してデータベースをリストアする必要があるボリュームを判別します。ボリューム・ヒストリー・ファイルは、RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE スクリプトによって使用されます。
DEVICE.CONFIGURATION.FILE	回復計画が作成されたときのサーバー装置の構成情報のコピーが含まれます。 <b>DSMSERV RESTORE DB</b> ユーティリティは、この装置構成ファイルを使用して、データベース・バックアップ・ボリュームを読み取ります。装置構成ファイルは、RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE スクリプトによって使用されます。
DSMSERV.OPT.FILE	サーバー・オプション・ファイルのコピーが入っています。このスタンザは、RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE スクリプトによって使用されます。
LICENSE.INFORMATION	最新のライセンス監査結果とサーバー・ライセンス条件のコピーが含まれます。
MACHINE.GENERAL.INFORMATION	サーバー・マシンを再構築するために必要な、サーバー・マシンに関する情報 (ロケーションなど) を提供します。このスタンザは、 <b>DEFINE MACHINE</b> コマンドを使用して <b>ADMSERVER=YES</b> を指定することでマシン情報がデータベース内に保存されている場合に、計画ファイルに含まれます。
MACHINE.RECOVERY.INSTRUCTIONS	サーバー・マシンに関するリカバリー手順を提供します。このスタンザは、マシンのリカバリー手順をデータベースに保存した場合に、計画ファイルに組み込まれます。
MACHINE.RECOVERY.CHARACTERISTICS	サーバー・マシンのハードウェアおよびソフトウェアの特性が含まれています。このスタンザは、マシン特性をデータベースに保存した場合に、計画ファイルに組み込まれます。
MACHINE.RECOVERY.MEDIA	サーバーを含むマシンの再構築に必要なメディアに関する情報を提供します。このスタンザは、回復メディア情報をデータベースに保存し、それをサーバーを含むマシンに関連付けた場合に、計画ファイルに組み込まれます。



# DRM を使用したサーバーおよびクライアントのデータのリカバリ

災害復旧管理機能 (DRM) 機能を使用して、災害発生時に IBM Spectrum Protect サーバーおよびクライアントのデータを復旧します。

## 始める前に

IBM Spectrum Protect は、クライアント/サーバー認証に Secure Sockets Layer (SSL) プロトコルを使用するようにセットアップされています。サーバーを始動すると、デジタル証明書ファイル `cert.kdb` がプロセスの一環として作成されます。このファイルには、サーバーの公開鍵が含まれており、クライアントはそれを使用してデータを暗号化することができます。Global Security Kit (GSKit) は特定フォーマットで別個のファイルにする必要があるため、デジタル証明書ファイルをサーバーのデータベースに保管することはできません。

1. `cert.kdb`、`cert.sth`、および `cert256.arm` の各ファイルのバックアップ・コピーを保持しておいてください
2. オリジナルの証明書ファイルとコピーの両方が失われたり破損したりした場合は、新規の証明書ファイルを生成します。

マスター暗号鍵は、GSKit 管理の新しい鍵データベース `dsmkeydb.kdb` に保管されます。サーバーに既存のマスター暗号鍵がある場合、そのマスター暗号鍵は `dsmserve.pwd` ファイルから鍵データベース `dsmkeydb.kdb` にマイグレーションされます。`dsmkeydb.kdb` ファイルと `dsmkeydb.sth` ファイルのバックアップ・コピーを保持しておいてください。マスター暗号鍵をバックアップするように **BACKUP DB** コマンドを構成できます。または自分で `dsmkeydb.kdb` ファイルと `dsmkeydb.sth` ファイルを手動でバックアップすることも可能です。マスター暗号鍵がないと、災害から復旧することができません。

1. `dsmkeydb.kdb` ファイルと `dsmkeydb.sth` ファイルのバックアップ・コピーを保持しておいてください。

## 手順

1. 最新の復旧計画を取得します。
2. 計画の `RECOVERY.INSTRUCTIONS.GENERAL` スタンザに記述されている回復ステップを検討します。
3. 計画ファイルのスタンザを、一般準備手順を行うための個々のファイル、IBM Spectrum Protect サーバーの復旧スクリプト、およびクライアント復旧手順に分割します。
4. ボールトから必要なすべての (計画でリストされている) リカバリ・ボリュームをリトリブします。
5. 装置構成ファイルを検討し、回復サイトのハードウェア構成が元のサイトと同じであることを確認します。何らかの差異がある場合には、装置構成ファイルを更新する必要があります。次の構成変更例では、構成情報の更新が必要です。
  - 異なる装置名。
  - 自動ライブラリーの場合、自動ライブラリーへのデータベース・バックアップ・ボリュームの挿入、およびライブラリーのエレメントを識別するための構成情報の更新を手動で行うための要件。これにより、サーバーは必要なデータベース・バックアップ・ボリュームを見付けることができます。
6. 交換用のハードウェアで IBM Spectrum Protect サーバーをセットアップします (オペレーティング・システムおよび IBM Spectrum Protect 基本リリースのインストールを含む)。
7. 復旧計画の IBM Spectrum Protect サーバー復旧スクリプトを実行します。  
`RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE` スタンザおよび `RECOVERY.SCRIPT.NORMAL.MODE` スタンザには、実行可能なコマンド・ファイルが含まれます。これを使用して、計画内で生成された他のコマンド・ファイルを呼び出すことで、IBM Spectrum Protect サーバーの復旧を行うことができます。`RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE` スクリプトは、クライアントがコピー・ストレージ・プール・ボリュームから直接リストアを開始できる時点にサーバーを復旧します。
8. `RECOVERY.SCRIPT.NORMAL.MODE` スクリプトを使用して、1 次ストレージ・プールをリストアします。
9. 高度な計画で定義した優先度の高いものから順に、クライアント・リストア操作を開始します。

## 次のタスク

IBM Spectrum Protect サーバーは、通常のサーバー操作に使用できるようになりました。すべての必要な操作がスケジュールされていることを確認します。詳しくは、56 ページの『サーバー保守アクティビティのスケジュールの定義』および [バックアップおよびアーカイブの操作のスケジュール](#) を参照してください。

### 関連情報

[PREPARE \(回復計画ファイルの作成\)](#)

[ディレクトリー・コンテナー・ストレージ・プール内のデータの修復およびリカバリー](#)

## 災害復旧ドリルの実行

災害復旧ドリルをスケジュールして、IBM Spectrum Protect サーバーのリカバリー可能性を認定する監査を準備し、障害発生後にデータをリストアして操作を再開できることを確認します。ドリルは、重大な状況が発生する前にすべてのデータが復元されて操作が再開可能であることを確認する場合にも役立ちます。

### 始める前に

次のタスクを実行してください。

- サーバーを管理、保護、および保守するためのアクティビティを定期的にスケジュールします。アクティビティのスケジュールについて詳しくは、56 ページの『サーバー保守アクティビティのスケジュールの定義』を参照してください。以下のタスクをスケジュールする必要があります。
  - データベースのバックアップ。
  - オフサイトへのメディアの移動。
  - 装置構成ファイル、ボリューム・ヒストリー・ファイル、および `dsmserv.opt` サーバー・オプション・ファイルのバックアップ。
  - オプション: PREPARE** コマンドの発行による災害時回復計画ファイルの作成。

#### ヒント:

**PREPARE** コマンドを発行すると、IBM Spectrum Protect 災害復旧管理機能 (DRM) 機能は、災害時回復計画ファイルのコピーを 1 つ作成します。

DRM を使用せずにオフサイトの災害復旧を管理することはできますが、DRM は、災害復旧時に必要な計画、スクリプト、およびその他の情報を統合するのに役立ちます。

保管用に、計画の複数のコピーを作成してください。これらのコピーは、例えば、印刷物として、USB フラッシュ・ドライブ、オフサイトにあるディスク・スペース、あるいはリモート・サーバーに保管します。災害時回復計画ファイルは、テープを使用して毎日オフサイトに移動されます。DRM について詳しくは、215 ページの『[DRM を使用した災害に対する準備と災害からのリカバリー](#)』を参照してください。

- 災害復旧サイトで以下のリソースを構成します。
  - リカバリー IBM Spectrum Protect サーバー。災害復旧にあるサーバーは、実動サイトのサーバーと同じレベルでなければなりません。
  - 実動サイトから送られたメディアを保管するテープ・ライブラリー。オフサイト・リカバリーのロケーションについては、23 ページの『[オフサイト・データ・ストレージ](#)』を参照してください。
  - データベース、アーカイブ・ログ、活動ログ、およびストレージ・プール用のディスク・ストレージ・スペース。
  - リストア操作をテストするためのクライアント。

### このタスクについて

実動環境と同様の環境で、頻繁に災害復旧計画および IBM Spectrum Protect サーバーのリカバリー可能性をテストします。

## 手順

1. テープがオンサイトで使用可能であることを確認します。**QUERY LIBVOLUME** コマンドを発行し、自動ライブラリーにチェックインされるボリュームを識別します。
2. 以下のステップを実行して、データベースをオンサイト・テープにバックアップします。
  - a. Operations Center の「サーバー」ページで、データベースをバックアップするサーバーを選択します。
  - b. 「バックアップ」をクリックして、「データベースのバックアップ」ウィンドウの指示に従います。
3. リカバリー・サイトにあるサーバーのホーム・ディレクトリーに以下のファイルをコピーします。
  - ・災害時回復計画ファイル
  - ・ボリューム・ヒストリー・ファイル
  - ・装置構成ファイル
  - ・オプション: dsmserve.opt サーバー・オプション・ファイル
4. テープをオフサイトのリカバリー・ロケーションに移動します。
5. リカバリー・サーバー上で **DSMSERV RESTORE DB** ユーティリティーを使用して、サーバー・データベースをリストアします。
6. **ACCESS=DESTROYED** パラメーターを指定して **UPDATE VOLUME** コマンドを発行し、ボリューム全体をリストアする必要があることを示します。
7. リカバリー・サーバー上で、**RESTORE STGPOOL** コマンドを使用してストレージ・プール・ボリュームをリストアします。

## 次のタスク

リストアされたストレージ・プール内のテープ・ボリュームを監査してデータに整合性があることを検証することで、ライブラリー内のデータにアクセスできることを確認します。**AUDIT VOLUME** コマンドを発行して、テープ・ボリュームを監査します。パフォーマンスを向上させるために、リストアされたデータのみを監査します。

### 関連タスク

[ライブラリー内のボリューム・インベントリーの監査](#)

自動ライブラリーを監査して、ライブラリー・ボリューム・インベントリーがライブラリーに実際に存在するボリュームと整合していることを確認することができます。ライブラリー内のボリュームを手動で移動したりデータベースに問題が発生したりしたためにライブラリー・ボリューム・インベントリーが正常な状態ではなくなった場合、ライブラリーを監査することが推奨されます。

### 関連情報

[AUDIT VOLUME \(ストレージ・プール・ボリュームのデータベース情報の検証\)](#)

[DSMSERV RESTORE DB \(データベースのリストア\)](#)

[RESTORE STGPOOL \(ストレージ・プール・データのリストア\)](#)

## データベースのリストア

災害復旧管理機能 (DRM) 機能を有効にしており、災害に対する準備を行う手順を実行した場合、災害の後にデータベースをリストアすることができます。DRM を構成していない場合でも、必要なバックアップ・ファイルがあれば、データベースをリストアすることができます。

### 始める前に

データベースおよび回復ログ・ディレクトリーが消失している場合は、それらをまず再作成してから、**DSMSERV RESTORE DB** サーバー・ユーティリティーを実行してください。

### このタスクについて

データベースを最新の状態または特定時点にリストアすることができます。データベースが消失した時点にデータベースをリカバリーするには、データベースを最新バージョンにリカバリーします。

### 制約事項:

- データベースを最新バージョンにリストアするには、アーカイブ・ログ・ディレクトリーを見つける必要があります。ディレクトリーが見つからない場合は、特定時点にのみデータベースをリストアできます。
- データベース・リストア操作に Secure Sockets Layer (SSL) プロトコルを使用することはできません。
- データベース・バックアップのリリース・レベルがリストア対象のサーバーのリリース・レベルと異なっている場合、サーバー・データベースをリストアすることはできません。例えば、バージョン 8.1 のサーバーを使用している場合に V7.1 データベースをリストアすると、エラーが発生します。

### 手順

**DSMSERV RESTORE DB** サーバー・ユーティリティーを使用して、データベースをリストアします。リストアするデータベースのバージョンに応じて、以下のいずれかの方法を選択します。

- データベースを最新バージョンにリストアします。例えば、次のコマンドを使用します。

```
dsmserv restore db
```

- データベースを特定時点にリストアします。例えば、2017 年 4 月 19 日に作成したバックアップの集合までデータベースをリストアするには、次のコマンドを使用します。

```
dsmserv restore db todate=04/19/2017
```

### 関連情報

[DSMSERV RESTORE DB \(データベースのリストア\)](#)



# 付録 A 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身体に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。

## 概要

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) を使用する操作

IBM Spectrum Protect ファミリー製品は、最新の W3C 標準 WAI-ARIA 1.0 ([www.w3.org/TR/wai-aria/](http://www.w3.org/TR/wai-aria/)) が、US Section 508 ([www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards)) および Web Content Accessibility Guidelines (WCAG) 2.0 ([www.w3.org/TR/WCAG20/](http://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、Accessibility section of the IBM Knowledge Center help ([www.ibm.com/support/knowledgecenter/about/releasesnotes.html?view=kc#accessibility](http://www.ibm.com/support/knowledgecenter/about/releasesnotes.html?view=kc#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 \(www.ibm.com/able\)](http://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認できません。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、このサンプル・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](http://ibm.com)<sup>®</sup> 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](http://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<sup>™</sup> 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 プライバシー・ステートメント」 (<http://www.ibm.com/privacy/jp/ja/>)、「IBM オンライン・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

---

IBM Spectrum Protect 製品ファミリーの用語と定義が記載されている用語集を使用できます。

[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]

アーカイブ操作  
    スケジューリング [114](#)  
    ルールの指定 [110](#)  
アーカイブ・ログ容量 [166](#)  
アクセシビリティ機能 [223](#)  
アップグレード  
    サーバー [214](#)  
暗号化  
    オプション [25](#)  
    方式 [122](#), [124](#)  
    DRIVEENCRYPTION パラメーター  
        3592 第 2 世代 [100](#)  
        LTO-4 以降 [97](#)  
インストール  
    クライアント [116](#)  
インベントリ容量 [166](#)  
エラー・チェック  
    ドライブのクリーニング [206](#)  
エラー・ログ  
    評価 [159](#)  
エレメント・アドレス [93](#), [186](#)  
オートチェンジャー [84](#)  
オフサイト・ストレージ [23](#)  
オフサイト・ボールド [23](#)  
オフサイト・ボリューム [62](#), [69](#)  
オプション  
    サーバー用に設定 [49](#)  
オプション、サーバー  
    NOPREEMPT [129](#)  
オペレーティング・システム  
    セキュリティ [211](#)  
        AIX サーバー・システムにインストール [31](#)  
        Linux サーバー・システムにインストール [33](#)  
        Windows サーバー・システムにインストール [37](#)  
オペレーティング・システムのインストール  
    AIX サーバー・システム [31](#)  
    Linux サーバー・システム [33](#)  
    Windows サーバー・システム [37](#)  
オンサイト・ボリューム [63](#), [71](#)

## [カ行]

カートリッジ  
    クリーナー・カートリッジ [155](#), [206](#)  
    複数世代のドライブの混合 [98](#)  
活動ログ容量 [166](#)  
監査  
    ライブラリー・ボリューム・インベントリ [193](#)  
管理  
    アクセス・レベル [211](#)  
    管理者 [209](#)  
    権限 [209](#)

管理コマンド  
    AUDIT LIBVOLUME [193](#)  
    CHECKIN LIBVOLUME [181](#), [183](#)  
    CHECKOUT LIBVOLUME [191](#)  
    CLEAN DRIVE [203](#)  
    DEFINE DEVCLASS  
        3592 [98](#)  
        LTO 装置クラス [95](#)  
    DEFINE DRIVE [93](#)  
    DEFINE LIBRARY [92](#)  
    UPDATE DRIVE [198](#), [199](#)  
    UPDATE LIBVOLUME [191](#)  
    UPDATE VOLUME [187](#)  
    VALIDATE LANFREE [121](#)  
キーボード [223](#)  
共用 SCSI ライブラリー [101](#)  
クライアント  
    アップグレード [162](#)  
    インストール [116](#)  
    構成 [116](#)  
    サーバーへの接続 [115](#)  
    スケジュール済み操作を実行するための構成 [117](#)  
    スケジュールの定義 [75](#)  
    操作の管理 [159](#)  
    ソフトウェアの選択 [109](#)  
    追加 [108](#)  
    登録 [115](#)  
    プロテクト [108](#)  
クライアント/サーバー通信  
    構成 [120](#)  
クライアント・アクセプター  
    構成 [117](#)  
    再始動 [160](#)  
    停止 [160](#)  
クライアント・ノード  
    実動からの除去 [163](#)  
    廃止 [163](#)  
クラス、装置  
    定義 [94](#)  
    FORMAT パラメーター [126](#)  
    LTO [95](#)  
グラフィカル・ウィザード  
    前提条件 RPM ファイル [46](#)  
クリーナー・カートリッジ  
    使用した操作 [155](#), [206](#)  
    チェックイン [205](#)  
計画ワークシート [8](#)  
権限レベル [209](#)  
構成  
    共用ライブラリー (shared library) [101](#)  
    クライアント [116](#)  
    変更 [160](#)  
コマンド  
    HALT [212](#)  
コマンド、管理  
    AUDIT LIBVOLUME [193](#)  
    CHECKIN LIBVOLUME [181](#), [183](#)

## コマンド、管理 (続き)

CHECKOUT LIBVOLUME [191](#)  
CLEAN DRIVE [203](#)  
DEFINE DEVCLASS  
3592 [98](#)  
LTO 装置クラス [95](#)  
DEFINE DRIVE [93](#)  
DEFINE LIBRARY [92](#)  
UPDATE DRIVE [198](#), [199](#)  
UPDATE LIBVOLUME [191](#)  
UPDATE VOLUME [187](#)  
VALIDATE LANFREE [121](#)

## コロケーション

計画 [177](#)  
効果の変更 [175](#)  
コロケーションを使用するかどうかの決定 [169](#)  
順次ストレージ・プールを使用可能にする [169](#)  
使用可能時のボリューム選択 [172](#)  
使用不可時のサーバーのボリューム選択方法 [174](#)  
操作への影響 [170](#)  
定義 [169](#)  
有効化 [177](#)

## [サ行]

### サーバー

オプションの設定 [49](#)  
計画、アップグレード [214](#)  
構成 [47](#)  
停止 [212](#)  
保守スケジュールの定義 [56](#)  
保守モードでの始動 [212](#), [213](#)  
ユーザー ID の作成 [41](#)

### サーバー・オプション

NOPREEMPT [129](#)

### サーバーの始動

保守モード [212](#)

### 災害

災害時回復管理機能 [215](#)  
災害時回復管理機能 [61-63](#), [215](#), [218-220](#)  
災害時回復計画ファイル [215](#)  
災害準備 [215](#)  
災害復旧 [61-63](#), [215](#), [218](#), [219](#)  
再構成タスク

保守モードでのサーバーの始動 [213](#)

時間間隔、ボリューム検査の設定 [129](#)

磁気テープ・ドライブ [2](#)

磁気テープ・ドライブ、置換 [207](#)

磁気テープ・ドライブのアップグレード [207](#)

磁気テープ・ドライブの置換 [207](#)

磁気テープ・ラベル

上書き [88](#)

### システム更新

prepare [215](#)

### システム状況

追跡 [157](#)

### システム要件

ハードウェア [3](#)

### 実装

テスト操作 [135](#)

### 自動ライブラリー

スクラッチ・ボリューム [192](#)

### 自動ライブラリー装置

監査 [193](#)

## 自動ライブラリー装置 (続き)

サーバーへの新規ボリュームに関する通知 [181](#)

磁気テープ・ドライブの置換 [207](#)

ボリューム・インベントリー [194](#)

ボリューム状況の変更 [191](#)

ボリュームの除去 [191](#)

ボリュームのチェックイン [181](#)

ボリュームへのラベル付け [180](#)

自動ライブラリー内でのボリュームのスワッピング [185](#)

### シャットダウン

サーバー [212](#)

順次モード、ライブラリーの [76](#)

### 障害

prepare [215](#)

### 状況レポート

入手 [157](#)

### シリアル番号

サーバーによる自動検出 [93](#), [131](#)

ドライブの [93](#)

ライブラリーの [93](#)

### 資料 vii

新規の磁気テープ・ドライブ [207](#)

身体障害 [223](#)

診断、装置の [131](#)

スクラッチ・ボリューム [189](#), [192](#)

スケール容量 [99](#)

### スケジュール

バックアップおよびアーカイブ操作 [114](#)

### スケジュール済み活動

チューニング [168](#)

### ストレージ

計画 [12](#), [14](#)

ストレージ・エージェント [15](#), [16](#)

### ストレージ構成

計画 [8](#)

ストレージ・スペース

解放 [165](#)

ストレージ装置 [94](#)

ストレージ・ハードウェア

構成 [30](#)

ストレージ・プール

コロケーションを使用するかどうかの決定 [169](#)

3592、特別な考慮事項 [98](#)

LTO Ultrium、特別な考慮事項 [95](#)

ストレージ・プール階層

計画 [20](#)

セットアップ [106](#)

ストレージ・プール容量 [2](#)

ストレージ・ボリューム

順次アクセスの準備 [179](#)

ラベル付け、順次アクセス [179](#)

### 制限

ユーザー・アクセス [211](#)

### 製品ライセンス

登録 [55](#)

### セキュア通信

SSL および TLS による構成 [52](#)

### セキュリティ

データ暗号化

3592 第 2 世代 [100](#)

IBM LTO 第 4 世代 [124](#)

IBM LTO 第 4 世代以降 [97](#)

Oracle StorageTek T10000C [124](#)

Oracle StorageTek T10000B [124](#)

- セキュリティー (続き)
  - データ暗号化 (続き)
    - Oracle StorageTek T10000D 124
    - データ暗号化、3592 第 2 世代、TS1120、TS1130、TS1140、TS1150 124
- セキュリティーの管理 50
- 設定
  - ボリュームへのチェックインの時間間隔 129
  - ライブラリー・モード 76
- 装置
  - 単一ライブラリーでの複数タイプ 17-19
  - 定義 92
  - 名前 78
  - zfc デバイス・ドライバー 87
- 装置、ストレージ
  - 磁気テープ・ドライブの置換 207
  - 装置情報 131
  - 必要な IBM Spectrum Protect 定義 19
- 装置クラス
  - LTO 95
- 装置クラス (device class)
  - 定義 94
  - FORMAT パラメーター 126
- 装置診断 131
- 装置タイプ
  - 単一ライブラリー内での複数 17, 19
  - LTO 95
- 装置の名前 78
- 装置のファイル名 78
- ソフトウェア
  - 選択 109
- ソフトウェア要件 6
- ソリューション
  - 拡張 108
- ソリューションの計画
  - テープ 1

## [タ行]

- タイプ、装置
  - 単一ライブラリー内での複数 17, 19
  - LTO 95
- 単一ライブラリーでの混合装置タイプ 17-19, 95, 98
- チェックイン
  - クリーナー・カートリッジ 205
  - ボリュームの時間間隔の設定 129
  - ライブラリー・ボリューム 181, 183
- 停止
  - サーバー 212
- データ
  - 非活動化 165
  - データ暗号化 122
  - データの移動 61
  - データの検証
    - 論理ブロック保護 199
  - データベースのリストア 220
  - データベース容量 166
  - データ保存ルール
    - 定義 56
  - データ・マイグレーション 2
  - データ・リカバリー
    - 戦略 219
- テープ
  - 回転 187

- テープ (続き)
  - 記録形式 126
  - ドライブ間の互換性 207
  - マウント保存期間の設定 128
  - capacity 125
- テープ・ソリューション
  - 計画 1
- テープ・デバイス・ドライバー
  - インストール 76
  - 要件 76
- テープへの保存のコピー 67, 74
- テープ要件 2
- デバイス・ドライバー
  - インストール 75, 79
  - 構成 85, 86, 89, 90
  - 自動ライブラリー装置の 75
  - 要件 75
  - IBM Spectrum Protect、インストール 75
- 電子的ボルト収容 23
- 登録
  - クライアント 115
- 特殊ファイル名 78
- 特権クラス (privilege class)
  - システム特権 209
- ドライバー、装置
  - インストール 75
  - 構成 85
  - 自動ライブラリー装置の 75
  - 要件 75
  - IBM Spectrum Protect、インストール 75
- ドライバー、テープ装置
  - インストール 76
  - 要件 76
- ドライブ
  - SAN での変更内容の検出 131
  - エレメント・アドレス 93
  - クリーニング 203, 206
  - 更新 198, 199
  - シリアル番号 93
  - 定義 93
  - ドライブ・クリーニング 203
  - ドライブの除去 207
  - ドライブの置換 208
  - ドライブの定義 208
  - ドライブのマイグレーション 208
  - トラブルシューティング
    - 管理者 ID 161
    - クライアント操作でのエラー 159
    - パスワードの問題 161
    - ロックされたクライアント・ノード 161

## [ナ行]

- ネットワーク帯域幅 2

## [ハ行]

- バーコード・リーダー
  - ライブラリー内のボリュームの監査 193
  - ライブラリー内のボリュームのラベル付け 181
  - ライブラリー用のボリュームのチェックイン 184
- ハードウェア要件 3
- 廃止プロセス

廃止プロセス (続き)  
クライアント・ノード (client node) [163](#)

パス  
定義 [92](#)

パスワード  
変更 [210](#)  
リセット [161](#)

パスワード要件  
LDAP [210](#)

バックアップ操作  
スケジューリング [114](#)  
適用範囲の変更 [113](#)  
ルールの指定 [110](#)

バックエンド・キャパシティー・ライセンス [156](#)

パフォーマンス  
ボリュームの使用頻度、長いマウント保存で改善 [128](#)

判別  
ボリューム・チェックインの時間間隔 [129](#)

非活動化プロセス  
バックアップ・データ [165](#)

ファイアウォール  
通信の構成 [120](#)

ファイバー・チャネル SAN 接続装置 [85](#)

ファイバー・チャネル装置 [83](#)

ファイル・システム  
計画 [8](#)  
準備、AIX サーバー・システムの [42](#)  
準備、Linux サーバー・システムの [43](#)  
準備、Windows サーバー・システムの [44](#)

プール、ストレージ  
コロケーションを使用するかどうかの決定 [169](#)  
[3592](#)、特別な考慮事項 [98](#)  
LTO Ultrium、特別な考慮事項 [95](#)

プロセッサ・パリユー・ユニット (PVU) ライセンス交付  
[156](#)

フロントエンド・キャパシティー・ライセンス [156](#)

保護、データ [132](#)

保守  
スケジュールの定義 [56](#)

保守タスク  
スケジューリング [168](#)  
保守モードでのサーバーの始動 [213](#)

保守モード  
サーバーの始動 [212](#)

保存ストレージ・プールのコロケーション [176](#)

保存ボリューム [67](#), [69](#), [71](#), [74](#)

ポリシー  
指定 [110](#)  
表示 [111](#)  
編集 [112](#)

ポリシー・ドメイン  
指定 [110](#)

ボリューム  
アクセス、制御 [187](#)  
アクセス優先使用 [130](#)  
インベントリーの維持管理 [186](#)  
監査 [193](#)  
管理 [190](#)  
更新 [191](#)  
自動ライブラリー・インベントリー [194](#)  
順次ストレージ・プール [179](#)  
スワッピング [185](#)  
チェックアウト [191](#)  
取り外し [196](#)

ボリューム (続き)  
マウント対象の決定 [196](#)  
マウント保存期間 [128](#)  
ライブラリーからの除去 [191](#)  
ライブラリーへの新規ボリュームのチェックイン [181](#)

ボリューム容量 [126](#)

本書について [vii](#)

## [マ行]

マウント  
限度 [127](#)  
操作 [196](#)  
保存期間 [128](#)  
待ち期間 [129](#)  
ライブラリー [127](#)  
query [196](#)

マウント・ポイント (mount point)  
装置クラスでのマウント・リミットとの関係 [127](#)  
優先使用 [129](#)

マルチパス入出力  
AIX システムの構成 [38](#)  
Linux システムの構成 [39](#)  
Windows システムの構成 [40](#)

無効なアクセス・モード  
PERMANENT パラメーターによるマーク付け [196](#)

メッセージ  
自動ライブラリー [196](#)

メディア  
テープの回転 [187](#)

メディアの移動 [61-63](#)

メディアの非互換性 [154](#)

メディア・ラベル  
記録 [179](#)  
検査 [184](#)  
テープ用 [179](#)

モニター  
タスク  
定期的なチェックリスト [147](#)  
日次チェックリスト [137](#)  
定期的なチェックリスト [147](#)  
日次チェックリスト [137](#)  
目的 [137](#)

モニター・タスクの定期的なチェックリスト [147](#)

モニター・タスクの日次チェックリスト [137](#)

問題  
診断 [137](#)

## [ヤ行]

ユーザー ID  
サーバー用に作成 [41](#)

優先使用  
ボリューム・アクセス [130](#)  
マウント・ポイント (mount point) [129](#)

容量、テープ [125](#)

## [ラ行]

ライセンス準拠  
検査 [156](#)

ライブラリー  
共有 [14](#)

## ライブラリー (続き)

- 構成 [90](#)
- サーバー間での共用 [101](#)
- 自動 [190](#)
- シリアル番号 [93](#)
- 装置タイプの混合 [17, 19, 95, 98](#)
- 定義 [92](#)
- 複数の装置タイプの構成 [17, 19](#)
- 変更内容の検出、SAN 上での [93, 131](#)
- ボリューム・インベントリー [194](#)
- ボリューム・インベントリーの監査 [193](#)
- ボリュームの追加 [181](#)
- モード、ランダムまたは順次 [76](#)
- SCSI [14](#)
- ライブラリー共有 [16](#)
- ライブラリー・クライアント、共有ライブラリー [15, 105](#)
- ライブラリー・ストレージ・スロット [183, 186](#)
- ライブラリーの構成
  - SCSI [90](#)
- ライブラリー・マネージャー、共有ライブラリー [15, 104](#)
- ラベル
  - 既存ラベルの上書き [179, 180](#)
  - 順次ストレージ・プール [179](#)
  - チェックイン [184](#)
  - バーコード・リーダー [184](#)
  - ボリューム例 [180](#)
  - メディアの検査 [184](#)
  - ライブラリー装置を使用したボリューム [180](#)
  - SCSI ライブラリーでの自動ラベル付け [181](#)
- ランダム・モード、ライブラリーの [76](#)
- リカバリー・ドリル [219](#)
- ルール
  - 指定
    - バックアップおよびアーカイブ操作 [110](#)
  - 表示 [111](#)
  - 編集 [112](#)
- レポート
  - E メール
    - 構成 [157](#)
- 論理ブロック保護
  - 概要 [199](#)
  - サポートされるドライブ [200](#)
  - ストレージ・プール管理 [202](#)
  - 有効化 [201](#)
  - 読み取り/書き込み操作 [202](#)

## [数字]

- 3590 磁気テープ・ドライブ
  - 装置クラスの定義 [19](#)
- 3592 ドライブおよびメディア
  - クリーニング [204](#)
  - 装置クラスの定義 [19](#)
  - データ暗号化 [100, 124](#)
  - 複数世代のドライブの混合 [98](#)
  - DEVICETYPE パラメーター [181](#)
  - WORM メディアの使用可能化 [132](#)

## A

- AUDIT LIBVOLUME コマンド [193](#)
- AUTOLABEL パラメーター、テープ・ボリュームの [181](#)

## C

- CHECKIN LIBVOLUME コマンド [181, 183](#)
- CHECKOUT LIBVOLUME コマンド [191](#)
- CLEAN DRIVE コマンド [203, 206](#)

## D

- DEFINE DRIVE コマンド [93](#)
- DEFINE LIBRARY コマンド [92](#)
- DELETE DRIVE [207](#)
- DISMOUNT VOLUME コマンド [196](#)
- DLT WORM メディア [132](#)
- DRIVEENCRYPTION パラメーター
  - 3592 装置クラス [100](#)
  - LTO 装置クラス [97](#)
- DRM [61-63, 215, 218-220](#)
- DSMSERV RESTORE DB [220](#)

## E

- E メール・レポート
  - 構成 [157](#)

## I

- IBM Knowledge Center [vii](#)
- IBM Spectrum Protect 災害時回復管理機能 [215, 218](#)
- IBM Spectrum Protect ディレクトリー
  - 計画 [8](#)
- IBM Spectrum Protect デバイス・ドライバー [76, 77](#)
- IBM Spectrum Protect のインストール
  - AIX システム [45](#)
  - Linux システム [45](#)
  - Windows システム [46](#)
- IBM テープ・デバイス・ドライバー [76](#)
- IBM デバイス・ドライバー
  - インストール [79](#)
  - 構成 [79](#)

## K

- Knowledge Center [vii](#)

## L

- LABEL LIBVOLUME コマンド
  - 既存のボリューム・ラベルの上書き [179](#)
  - 順次ストレージ・プール・ボリュームのラベル付け [179](#)
  - ドライブの識別 [179](#)
  - 取り外し可能メディア・ボリューム [179](#)
  - ボリュームへのラベル付けの例 [180](#)
  - ライブラリー装置の使用 [180](#)
- LAN フリー・データ移動 (LAN-free data movement)
  - description [15, 16](#)
- LDAP
  - パスワード要件 [210](#)
- LTO Ultrium 装置およびメディア
  - 暗号化 [97, 124](#)
  - 装置クラス、定義および更新 [95](#)
  - WORM [132](#)



## M

mode  
ライブラリー (ランダムまたは順次) [76](#)  
MOVE RETMEDIA [69](#), [71](#)

## N

NOPREEMPT サーバー・オプション [129](#)

## O

Operations Center  
構成 [53](#)  
セキュア通信 [54](#)

## P

passthru ドライバー [77](#)

## Q

QUERY SAN [131](#)

## R

RPM ファイル  
グラフィカル・ウィザード用のインストール [46](#)

## S

SAN (Storage Area Network)  
サーバー間でのライブラリーの共用 [15](#), [101](#)  
ストレージ・エージェントの役割 [15](#), [16](#)  
装置の変更、検出 [131](#)  
装置へのクライアント・アクセス [15](#), [16](#)  
LAN フリー・データ移動 (LAN-free data movement) [15](#), [16](#)

SCSI  
異なる磁気テープ・テクノロジーを持ったライブラリー  
[98](#)  
ボリュームの自動ラベル付け [181](#)

SCSI 装置 [83](#)

SCSI ライブラリー  
ライブラリー・クライアントの定義 [102](#), [103](#)  
ライブラリー・サーバーの定義 [102](#), [103](#)

Sony WORM メディア (AIT50 および AIT100) [132](#)

SSL [52](#)

Storage Area Network (SAN)  
サーバー間でのライブラリーの共用 [15](#), [101](#)  
ストレージ・エージェントの役割 [15](#), [16](#)  
装置の変更、検出 [131](#)  
装置へのクライアント・アクセス [15](#), [16](#)  
LAN フリー・データ移動 (LAN-free data movement) [15](#), [16](#)

## T

TLS [52](#)  
tsmdlst ユーティリティー [131](#)

## U

Ultrium、LTO 装置タイプ  
暗号化 [97](#), [124](#)  
装置クラス、定義および更新 [95](#)  
WORM [132](#)  
UPDATE DRIVE コマンド [198](#), [199](#)  
UPDATE LIBVOLUME コマンド [191](#)

## V

VALIDATE LANFREE コマンド [121](#)

## W

WORM 装置およびメディア  
ライブラリーにおけるボリュームの維持 [190](#)  
DLT WORM [132](#)  
IBM 3592 [132](#)  
LTO WORM [132](#)  
Oracle StorageTek T10000D ドライブ [133](#)  
Oracle StorageTek T10000B ドライブ [133](#)  
Oracle StorageTek T10000C ドライブ [133](#)  
Quantum LTO3 [132](#)  
Sony AIT50 および AIT100 [132](#)  
VolSafe  
メディアの考慮事項 [132](#)  
WORM メディアに関する特別な考慮事項 [132](#)  
WORM ボリューム [133](#)  
WORM メディアでのデータ保護 [132](#)





プログラム番号: 5725-W98  
5725-W99  
5725-X15