

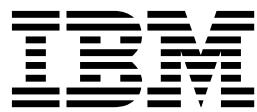
IBM Spectrum Protect
for Linux
バージョン **8.1.5**

インストール・ガイド



IBM Spectrum Protect
for Linux
バージョン **8.1.5**

インストール・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、 191 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 5、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

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

原典： IBM Spectrum Protect
for Linux
Version 8.1.5
Installation Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

© Copyright IBM Corporation 1993, 2018.

目次

本書について	vii
本書の対象読者	vii
インストール可能コンポーネント	vii
資料	viii
このリリースの新機能	ix
第 1 部 サーバーのインストールおよびアップグレード	1
第 1 章 サーバーのインストール計画	3
インストールを開始する前の前提知識	3
最適なパフォーマンスのための計画	3
サーバーのハードウェアおよびオペレーティング・システムの計画	4
サーバー・データベース・ディスクの計画	7
サーバーの回復ログ・ディスクの計画	10
ディレクトリー・コンテナストレージ・プールとクラウド・コンテナー・ストレージ・プールの計画	12
DISK 装置クラスまたは FILE 装置クラスのストレージ・プールの計画	20
正しいタイプのストレージ・テクノロジーの計画	22
サーバー・インストールへのベスト・プラクティスの適用	24
最小システム要件	26
Linux x86_64 サーバーの最小要件	27
Linux on System z サーバーの最小要件	27
Linux on Power Systems (リトル・エンディアン) の最小サーバー要件	27
IBM Spectrum Protect サーバーとシステム上の他の DB2 製品との互換性	27
IBM Installation Manager	29
サーバーの詳細を計画するためのワークシート	30
キャパシティー計画	31
データベースのスペース所要量の見積もり	31
回復ログのスペース要件	35
データベースおよび回復ログのスペース使用率のモニター	49
インストール・ロールバック・ファイルの削除	50
サーバー名の命名のベスト・プラクティス	52
インストール・ディレクトリー	54
第 2 章 サーバー・コンポーネントのインストール	55
インストール・パッケージの入手	55
インストール・ウィザードを使用した IBM Spectrum Protect のインストール	57
コンソール・モードを使用した IBM Spectrum Protect のインストール	58
サイレント・モードで IBM Spectrum Protect をインストール	59
サーバー言語パッケージのインストール	60
サーバー言語のロケール	60
言語パッケージの構成	61
言語パッケージの更新	62
第 3 章 IBM Spectrum Protect のインストール後の最初のステップの実行	63
カーネル・パラメーターのチューニング	64
カーネル・パラメーターの更新	64
推奨値	64
サーバー・インスタンスのユーザー ID とディレクトリーの作成	65
IBM Spectrum Protect サーバーの構成	67
構成ウィザードを使用した IBM Spectrum Protect の構成	68
手動でのサーバー・インスタンスの構成	69
サーバー・データベース保守のためのサーバー・オプションの構成	78
サーバー・インスタンスの開始	80
アクセス権限およびユーザー制限の確認	81
インスタンス・ユーザー ID からのサーバーの始動	83
Linux システムでのサーバーの自動始動	83
保守モードでのサーバーの始動	85
サーバーの停止	86
ライセンスの登録	87
データベース・バックアップ操作のためのサーバーの準備	87
単一システムでの複数のサーバー・インスタンスの実行	88
サーバーのモニター	88
第 4 章 IBM Spectrum Protect サーバー・フィックスパックのインストール	91
第 5 章 V8.1 へのアップグレード	95
V8.1 へのアップグレード	96
アップグレードの計画	96
システムの準備	97
サーバーのインストールとアップグレードの検証	99
クラスター環境でのサーバーのアップグレード	102
クラスター環境における V8.1.5 への IBM Spectrum Protect のアップグレード	103
第 6 章 バージョン 8.1.5 から以前のサーバーへの復帰	105
以前のサーバー・バージョンに戻すための手順	105

新規ストレージ・プールを作成した場合またはデータ重複排除を使用可能にした場合の追加のリカバリ一手順.	107
第 7 章 リファレンス: IBM Spectrum Protect サーバー・データベースに使用する DB2 コマンド	109
第 8 章 IBM Spectrum Protect のアンインストール	113
グラフィカル・ウィザードを使用した IBM Spectrum Protect のアンインストール	113
コンソール・モードでの IBM Spectrum Protect のアンインストール	114
サイレント・モードでの IBM Spectrum Protect のアンインストール	114
IBM Spectrum Protect のアンインストールと再インストール	115
IBM Installation Manager のアンインストール	116
第 2 部 Operations Center のインストールおよびアップグレード	119
第 9 章 Operations Center のインストール計画	121
Operations Center のシステム要件	121
Operations Center のコンピューターの要件 .	122
ハブ・サーバーおよびスポーク・サーバーの要件	122
オペレーティング・システム要件	126
Web ブラウザーの要件	127
言語要件	127
IBM Spectrum Protect クライアント管理サービスの要件と制限.	128
Operations Center に必要な管理者 ID.	130
IBM Installation Manager	131
インストール・チェックリスト	132
第 10 章 Operations Center のインストール	135
Operations Center インストール・パッケージの入手	135
グラフィカル・ウィザードを使用した Operations Center のインストール	136
コンソール・モードでの Operations Center のインストール	136
サイレント・モードでの Operations Center のインストール	136
第 11 章 Operations Center のアップグレード	139
第 12 章 Operations Center の概要	141
Operations Center の構成	141
ハブ・サーバーの指定	142
スポーク・サーバーの追加	143
メール・アラートの管理者への送信	143
ログイン画面へのカスタマイズ・テキストの追加	146
REST サービスの有効化	147
セキュア通信の構成	148
Operations Center とハブ・サーバー間のセキュア通信	148
ハブ・サーバーとスポーク・サーバー間の通信の保護	151
Operations Center のトラストストア・ファイルのパスワードのリセット	153
Web サーバーの開始と停止	155
Operations Center の開始	155
IBM Spectrum Protect クライアント管理サービスでの診断情報の収集	156
グラフィカル・ウィザードを使用したクライアント管理サービスのインストール	156
サイレント・モードでの クライアント管理サービス のインストール	158
クライアント管理サービスが正しくインストールされていることの確認	159
クライアント管理サービスを使用するための Operations Center の構成	160
クライアント管理サービス の始動と停止	161
クライアント管理サービス のアンインストール .	162
カスタム・クライアント・インストールのための クライアント管理サービスの構成.	163
第 13 章 Operations Center のインストールのトラブルシューティング	179
日本語、中国語、または韓国語のフォントが正しく表示されない	179
第 14 章 Operations Center のアンインストール	181
グラフィカル・ウィザードを使用した Operations Center のアンインストール	181
コンソール・モードでの Operations Center のアンインストール	181
サイレント・モードでの Operations Center のアンインストール.	182
第 15 章 Operations Center の前のバージョンへのロールバック	183
第 3 部 付録	185

付録 A. インストール・ログ・ファイル 187

付録 B. IBM Spectrum Protect 製品フ
アミリーのアクセシビリティ機能 . . . 189

特記事項. 191

用語集. 195

索引 197

本書について

本書には、IBM Spectrum Protect™ サーバー、サーバー言語、ライセンス、およびデバイス・ドライバーのインストール手順と構成手順が記載されています。

本書には Operations Center のインストールの手順も記載されています。

本書の対象読者

本書は、IBM Spectrum Protect サーバーあるいは Operations Center をインストール、構成、またはアップグレードするシステム管理者を対象としています。

インストール可能コンポーネント

IBM Spectrum Protect サーバーおよびライセンスは必須コンポーネントです。

表 1では、すべてのインストール可能コンポーネントについて説明しています。これらのコンポーネントは、複数の異なるインストール・パッケージにあります。

表 1. IBM Spectrum Protect インストール可能コンポーネント

IBM Spectrum Protect コンポーネント	説明	追加情報
サーバー (必須)	データベース、Global Security Kit (GSKit)、IBM® Java™ ランタイム環境 (JRE)、およびサーバーの構成と管理に役立つツールが含まれています。	55 ページの『第 2 章 サーバー・コンポーネントのインストール』を参照してください。
言語パッケージ (オプション)	それぞれの言語パッケージ (各言語ごとに 1 つ) には、サーバーの言語に特有の情報が含まれています。	60 ページの『サーバー言語パッケージのインストール』を参照してください。
ライセンス (必須)	すべてのライセンス機能のサポートが含まれています。このパッケージをインストールした後、購入したライセンスを登録する必要があります。	REGISTER LICENSE コマンドを使用します。
デバイス (オプション)	メディアの管理機能を拡張します。	このドライバーでサポートされる装置のリストは、IBM サポート・ポータルから入手できます。

表 1. IBM Spectrum Protect インストール可能コンポーネント (続き)

IBM Spectrum Protect コンポーネント	説明	追加情報
ストレージ・エージェント (オプション)	<p>クライアント・システムが、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・デバイスに直接データを書き込んだり、そのデバイスから直接データを読み取ったりできるようにするコンポーネントをインストールします。</p> <p>要確認: IBM Spectrum Protect for Storage Area Networks は、個別にライセンス交付を受けた製品です。</p>	ストレージ・エージェントについて詳しくは、Tivoli Storage Manager for Storage Area Networks (V7.1.1)を参照してください。
Operations Center (オプション)	Operations Center をインストールします。これは、ストレージ環境を管理するための Web ベースのインターフェースです。	119 ページの『第 2 部 Operations Center のインストールおよびアップグレード』を参照してください。

資料

IBM Spectrum Protect 製品ファミリーには、IBM Spectrum Protect Snapshot、IBM Spectrum Protect for Space Management、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。

新機能および更新内容のリストについては、新機能を参照してください。

第 1 部 サーバーのインストールおよびアップグレード

IBM Spectrum Protect サーバーをインストールしてアップグレードします。

第 1 章 サーバーのインストール計画

サーバー・ソフトウェアを、ストレージ装置を管理するコンピューターにインストールし、クライアント・ソフトウェアを IBM Spectrum Protect サーバーが管理するストレージにデータを転送するすべてのワークステーションにインストールします。

インストールを開始する前の前提知識

IBM Spectrum Protect をインストールする前に、ご使用のオペレーティング・システム、ストレージ装置、通信プロトコル、およびシステム構成をよく理解してください。

サーバー保守リリース、クライアント・ソフトウェア、および資料は、IBM サポート・ポータルから入手できます。

制約事項: DB2® が既にインストールされているシステムに、いくつかの制限付きで、バージョン 8.1.5 のサーバーをインストールして実行することができます。この場合、DB2 が単独でインストールされているか、または他のアプリケーションの一部としてインストールされているかは関係ありません。詳細については、27 ページの『IBM Spectrum Protect サーバーとシステム上の他の DB2 製品との互換性』を参照してください。

経験豊かな DB2 管理者は、拡張 SQL 照会を実行したり、DB2 ツールを使用してデータベースをモニターしたりすることができます。ただし、DB2 ツールを使用して、IBM Spectrum Protect によって事前設定されている DB2 構成設定を変更したり、別の方で（例えば他の製品を使用して）IBM Spectrum Protect の DB2 環境を変更したりしないでください。V8.1.5 サーバーは、サーバーがデプロイするデータ定義言語 (DDL) およびデータベース構成を使用して構築され、幅広くテストが行われています。

重要: IBM Spectrum Protect インストール・パッケージおよびフィックスパックとともにインストールされている DB2 ソフトウェアは変更しないでください。別のバージョン、リリース、またはフィックスパックの DB2 ソフトウェアをインストールしたり、それらにアップグレードしたりしないでください。データベースが損傷する可能性があります。

最適なパフォーマンスのための計画

IBM Spectrum Protect サーバーのインストール前に、システムの特性および構成を評価し、最適なパフォーマンスを得るためにサーバーをセットアップします。

手順

1. 『インストールを開始する前の前提知識』を確認します。
2. 以下の各サブセクションを確認します。

IBM Spectrum Protect サーバーのインストール

サーバーのハードウェアおよびオペレーティング・システムの計画

チェックリストを使用して、サーバーがインストールされているシステムが、ハードウェアおよびソフトウェア構成の要件を満たしているかを確認します。

質問	タスク、特性、オプション、または設定	詳細情報
オペレーティング・システムおよびハードウェアが要件を満たしているか上回っていますか？ <ul style="list-style-type: none">• プロセッサーの数と速度• システム・メモリー• サポートされるオペレーティング・システム・レベル	<p>必須メモリーの最小容量を使用している場合、最小の作業負荷をサポートすることができます。</p> <p>システム・メモリーを追加することでパフォーマンスが向上するかを実験することができます。その後、そのシステム・メモリーをサーバー専用にしたままにするかを決定します。毎日のサーバー作業負荷のサイクル全体を使用して、メモリーのバリエーションをテストします。</p> <p>システム上で複数のサーバーを稼働させる場合、システムの要件を満たすように各サーバーの要件を追加します。</p>	<p>オペレーティング・システムの要件は、技術情報 1243309で参照してください。</p> <p>さらに、オペレーティング・システムおよびその他のアプリケーションのタスクのチューニングのガイダンスも確認します。</p> <p>これらの機能を使用している場合の要件について詳しくは、以下のトピックを参照してください。</p> <ul style="list-style-type: none">• データ重複排除のチェックリスト• ノード複製のチェックリスト <p>サーバーとストレージのサイズ設定の要件については、IBM Spectrum Protect Blueprintを参照してください。</p>
最適なパフォーマンスを得るためにディスクが構成されていますか？	各種ディスク・システムで実行可能なチューニングの量は、それぞれ異なります。適切なキュー項目数とその他のディスク・システム・オプションが設定されていることを確認してください。	詳細については、以下のトピックを参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
サーバーに十分なメモリーがありますか？	<p>作業負荷が大きい場合やデータ重複排除やノード複製などの拡張機能を使用する場合、システム要件の資料で示されている最小システム・メモリーより多くのメモリーが必要になります。</p> <p>データ重複排除が有効にされていないデータベースでは、以下のガイドラインを使用してメモリー要件を指定してください。</p> <ul style="list-style-type: none"> • 500 GB 未満のデータベースの場合、16 GB のメモリーが必要です。 • サイズが 500 GB から 1 TB のデータベースの場合、24 GB のメモリーが必要です。 • サイズが 1 TB から 1.5 TB のデータベースの場合、32 GB のメモリーが必要です。 • 1.5 TB より大きいデータベースの場合、40 GB のメモリーが必要です。 <p>複製処理のための活動ログおよびアーカイブ・ログ用に追加のスペースを割り振るようにしてください。</p>	<p>これらの機能を使用している場合の要件について詳しくは、以下のトピックを参照してください。</p> <ul style="list-style-type: none"> • データ重複排除のチェックリスト • ノード複製のチェックリスト • メモリー所要量

IBM Spectrum Protect サーバーのインストール

質問	タスク、特性、オプション、または設定	詳細情報
システムには、IBM Spectrum Protect サーバーが同時に実行する必要があるデータ操作を処理するのに十分なホスト・バス・アダプター (HBA) がありますか？	<p>どの操作が同時に HBA を使用する必要があるかを理解します。</p> <p>例えば、サーバーは、ストレージ・プール・マイグレーションを 0.5 GB/秒の容量で完了する必要があると同時に、1 GB/秒のバックアップ・データを保管する必要があるとします。HBA は、必要な速度ですべてのデータを処理できなければなりません。</p>	HBA キャパシティーのチューニングを参照してください。
ネットワーク帯域幅は、予定されているバックアップの最大スループットより大きいですか？	<p>ネットワーク帯域幅は、システムがバックアップなどの操作を許可された時間内あるいはサービス・レベル・コミットメントを満たす時間内に完了できるものでなければなりません。</p> <p>ノード複製の場合、ネットワーク帯域幅は、予定されている最大スループットより大きくなければなりません。</p>	<p>詳細については、以下のトピックを参照してください。</p> <ul style="list-style-type: none"> ネットワーク・パフォーマンスのチューニング ノード複製のチェックリスト
IBM Spectrum Protect サーバー・ファイルに推奨されるファイル・システムを使用していますか？	最適なパフォーマンスとデータ可用性を確実に得るために、ファイル・システムを使用してください。サーバーは、その機能をサポートするファイル・システムとの直接入出力を使用します。直接入出力を使用することで、スループットを向上させ、プロセッサーの使用を削減することができます。ご使用のオペレーティング・システムに合う推奨ファイル・システムについて詳しくは、IBM Spectrum Protect server-supported file systemsを参照してください。	詳しくは、ディスク・パフォーマンスのためのオペレーティング・システムの構成を参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
十分なページング・スペースの構成を計画していますか？	<p>ページ・スペースあるいはスワップ・スペースは、処理に使用可能なメモリーを拡張します。システム内の RAM の空き容量が少ない場合、使用していないプログラムやデータは、メモリーからページング・スペースに移動されます。このアクションにより、メモリーがデータベース操作などの他の活動用に解放されます。</p> <p>最小 32 GB のページング・スペースまたはご使用の RAM の 50% のいずれか大きいほうの値を使用します。</p>	
サーバーのインストール後にカーネル・パラメーターのチューニングを計画していますか？	カーネル・パラメーターをチューニングする必要があります。	カーネル・パラメーターのチューニングについては、Linux: Linux システムのカーネル・パラメーターのチューニングを参照してください。

サーバー・データベース・ディスクの計画

チェックリストを使用して、サーバーがインストールされているシステムが、ハードウェアおよびソフトウェア構成の要件を満たしているかを確認します。

IBM Spectrum Protect サーバーのインストール

質問	タスク、特性、オプション、または設定	詳細情報
データベースは、高速で待ち時間が短いディスク上にありますか？	<p>IBM Spectrum Protect データベースには、以下のドライブを使用しないでください。</p> <ul style="list-style-type: none"> • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) <p>ほとんどのサーバー・ハードウェアにデフォルトで組み込まれている内蔵ディスクは使用しないでください。</p> <p>ファイバー・チャネルまたは SAS インターフェースを備えたエンタープライズ・レベルのソリッド・ステート・ディスク (SSD) は、最高のパフォーマンスを提供します。</p> <p>IBM Spectrum Protect のデータ重複排除機能を使用する予定の場合は、1 秒あたりの入出力操作 (IOPS) の観点からディスク・パフォーマンスに焦点を置いてください。</p>	詳しくは、データ重複排除のチェックリストを参照してください。
データベースは、活動ログ、アーカイブ・ログ、およびストレージ・プール・ボリュームに使用されているディスクあるいは LUN とは別のディスクまたは LUN に保管されていますか？	<p>サーバー・データベースを他のサーバー・コンポーネントと分離することで、同時に実行する必要があるさまざまな操作による同じリソースの競合を減らすことができます。</p> <p>ヒント：ソリッド・ステート・ドライブ (SSD) テクノロジーを使用する場合、データベースとアーカイブ・ログはアレイを共有できます。</p>	
RAID を使用している場合、システムに最適な RAID レベルを選択する方法を知っていますか？すべての LUN を同じサイズとタイプの RAID を使用して定義していますか？	<p>システムで非常に多くの書き込みを行う必要がある場合、RAID 10 は RAID 5 より優れたパフォーマンスを提供します。ただし、RAID 10 では、同じ容量の使用可能なストレージを確保するために RAID 5 より多くのディスクが必要です。</p> <p>ご使用のディスク・システムが RAID の場合、すべての LUN を同じサイズとタイプの RAID を使用して定義してください。例えば、4+1 RAID 5 と 4+2 RAID 6 を混用しないでください。</p>	

質問	タスク、特性、オプション、または設定	詳細情報
ストリップ・サイズまたはセグメント・サイズを設定するオプションが使用可能な場合、ディスク・システムを構成する時にそのサイズを最適化するように計画していますか？	ストリップ・サイズまたはセグメント・サイズを設定できる場合、データベース用のディスク・システムでは 64 KB または 128 KB のサイズを使用してください。	データベースに使用するブロック・サイズは、表スペースに応じて変化します。ほとんどの表スペースでは、8 KB のブロックを使用しますが、一部では 32 KB のブロックを使用します。
データベース用に少なくとも 4 つのディレクトリー（ストレージ・パスとも呼ばれる）を 4 つの異なる LUN 上に作成するように計画していますか？ サブシステム上の個別のアレイごとに、1 つのディレクトリーを作成します。アレイの数が 3 つに満たない場合、アレイ内に個別の LUN ボリュームを作成します。	<p>作業負荷が大きくなったり、一部のフイーチャーを使用することで、最小要件より多くのデータベース・ストレージ・パスが必要になります。</p> <p>データ重複排除のようなサーバー操作は、データベースに対する 1 秒当たりの入出力操作 (IOPS) の駆動回数が高くなります。このような操作は、データベースに多くのディレクトリーがある場合、パフォーマンスが向上します。</p> <p>2 TB より大きい、あるいはそのサイズまで増大することが予想されるサーバー・データベースの場合、8 つのディレクトリーを使用してください。</p> <p>作成するストレージ・パス数を決定する際には、予定されているシステムの増大量を考慮してください。サーバーが最初に作成されたときにストレージ・パスが存在している場合、サーバーは、より多くのストレージ・パスをより効率的に使用します。</p> <p><i>DB2_PARALLEL_IO</i> 変数を使用すると、1 つのコンテナーが含まれる表スペース、または複数の物理ディスクにコンテナーが含まれる表スペースで、強制的に並列入出力が行われます。 <i>DB2_PARALLEL_IO</i> 変数を設定しない場合、入出力並列処理は、表スペースに使用されるコンテナー数と等しくなります。例えば、表スペースに 4 つのコンテナーが含まれる場合、使用される入出力並列処理のレベルは 4 になります。</p>	<p>詳細については、以下のトピックを参照してください。</p> <ul style="list-style-type: none"> • データ重複排除のチェックリスト • ノード複製のチェックリスト <p>サーバーがデータを重複排除する場合の増大量を予測するには、技術情報 1596944 を参照してください。</p> <p>IBM Spectrum Protect サーバーのデータベース・サイズ、データベース再編成、およびパフォーマンスの考慮事項に関する最新情報については、技術情報 1683633 を参照してください。</p> <p><i>DB2_PARALLEL_IO</i> 変数の設定については、IBM DB2 レジストリー変数の推奨設定を参照してください。</p>

IBM Spectrum Protect サーバーのインストール

質問	タスク、特性、オプション、または設定	詳細情報
データベース用のディレクトリーはすべて同じサイズですか？	<p>すべてのディレクトリーのサイズを同一にすることで、データベース操作の並列処理の度合いが確実に一貫性のあるものになります。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、並列プリフェッヂが最適化される可能性が低下します。</p> <p>この指針は、サーバーの初期構成の後にストレージ・パスを追加する必要がある場合にも適用されます。</p>	
AIX® システム上のデータベース LUN のキュー項目数を増やすように計画していますか？	多くの場合、デフォルトのキュー項目数は少なすぎます。	ディスク・パフォーマンスのための AIX システムの構成を参照してください。

サーバーの回復ログ・ディスクの計画

チェックリストを使用して、サーバーがインストールされているシステムが、ハードウェアおよびソフトウェア構成の要件を満たしているかを確認します。

質問	タスク、特性、オプション、または設定	詳細情報
活動ログとアーカイブ・ログは、データベースおよびストレージ・プール・ボリュームに使用されているディスクあるいは LUN とは別のディスクまたは LUN に保管されていますか？	活動ログを配置するディスクが、他のサーバーあるいはシステムの目的で使用されていないことを確認してください。活動ログは、サーバー・データベース、アーカイブ・ログ、あるいはシステム・ファイル (ページまたはスワップ・スペースなど) を含むディスク上に配置しないでください。	サーバー・データベース、活動ログ、およびアーカイブ・ログを分離することで、同時に実行する必要があるさまざまな操作による同じリソースの競合を減らすことができます。
ログは、不揮発性書き込みキャッシュを備えたディスク上にありますか？	不揮発性書き込みキャッシュを使用することで、データを可能な限り速くログに書き込むことができます。ログの書き込み操作が高速になると、サーバー操作のパフォーマンスを向上させることができます。	

質問	タスク、特性、オプション、または設定	詳細情報
ログは、作業負荷に十分に対応するサイズに設定するよう計画していますか？	<p>作業負荷が不明な場合は、できるだけ大きなサイズを使用してください。</p> <p>活動ログ</p> <p>最大サイズは 512 GB です。 ACTIVELOGSIZE サーバー・オプションを使用して設定します。</p> <p>固定サイズの活動ログが作成された後に、活動ログ・ファイル・システム上に少なくとも 8 GB のフリー・スペースがあることを確認します。</p> <p>アーカイブ・ログ</p> <p>アーカイブ・ログのサイズは、サーバー・オプションではなく、ログが配置されているファイル・システムのサイズによって制限されます。アーカイブ・ログは、少なくとも活動ログと同じ容量にします。</p>	<ul style="list-style-type: none"> ログのサイズ設定について詳しくは、技術情報 1421060 のリカバー・ログ情報を参照してください。 データ重複排除を使用する場合のサイズ設定について詳しくは、データ重複排除のチェックリストを参照してください。
アーカイブ・フェイルオーバー・ログを定義していますか？そのログは、アーカイブ・ログとは別のディスク上に配置するよう計画していますか？	<p>アーカイブ・フェイルオーバー・ログは、アーカイブ・ログが満杯になったときに、サーバーが緊急で使用するためのものです。アーカイブ・フェイルオーバー・ログには、低速なディスクを使用しても構いません。</p>	<p>ARCHFAILOVERLOGDIRECTORY サーバー・オプションを使用して、アーカイブ・フェイルオーバー・ログの配置場所を指定します。</p> <p>アーカイブ・フェイルオーバー・ログのディレクトリーの使用量をモニターしてください。サーバーがアーカイブ・フェイルオーバー・ログを使用する必要がある場合、アーカイブ・ログのスペースが不足しています。</p>
活動ログをミラーリングしている場合、1 つのタイプのミラーリングのみを使用していますか？	<p>以下のいずれかの方法を使用して、ログをミラーリングすることができます。ログのミラーリングには、1 つのタイプのみを使用してください。</p> <ul style="list-style-type: none"> IBM Spectrum Protect サーバーで使用可能な MIRRORLOGDIRECTORY オプションを使用して、ミラーリングする場所を指定する。 ソフトウェア・ミラーリング (Logical Volume Manager (LVM) on AIX など) を使用する。 ディスク・システム・ハードウェア内のミラーリングを使用する。 	<p>活動ログをミラーリングする場合、活動ログとミラー・コピーに使用するディスクの両方が同じ速度と信頼性を備えている必要があります。</p> <p>詳しくは、回復ログの構成およびチューニングを参照してください。</p>

ディレクトリー・コンテナーストレージ・プールとクラウド・コンテナー・ストレージ・プールの計画

最適なパフォーマンスを得るために、ディレクトリー・コンテナーストレージ・プールとクラウド・コンテナー・ストレージ・プールのセットアップ方法を確認します。

質問	タスク、特性、オプション、または設定	詳細情報
1 秒当たりの入出力操作 (IOPS) を単位として測定する際、IBM Spectrum Protect データベースに高速ディスク・ストレージを使用していますか？	<p>データベースには、高パフォーマンス・ディスクを使用します。データ重複排除処理のために、ソリッド・ストート・ドライブ・テクノロジーを使用します。</p> <p>データベースには最小で 3000 IOPS の処理能力があることを確認してください。日次バックアップのデータ量 (データ重複排除前) 1 TBにつき 1000 IOPS をこの最小値に追加してください。</p> <p>例えば、毎日 3 TB のデータを取り込む IBM Spectrum Protect サーバーでは、データベース・ディスクに 6000 IOPS の処理能力が必要です。</p> $3000 \text{ IOPS minimum} + 3000 \text{ (3 TB} \times 1000 \text{ IOPS)} = 6000 \text{ IOPS}$	<p>ディスク選択の際の推奨事項は、「サーバー・データベース・ディスクの計画」を参照してください。</p> <p>IOPS の詳細については、「IBM Spectrum Protect Blueprints」を参照してください。</p>

質問	タスク、特性、オプション、または設定	詳細情報
データベースのサイズに対して十分なメモリーがありますか？	<p>データベース・サイズが 100 GB でデータの重複排除を行う IBM Spectrum Protect サーバーでは、最小で 40 GB のシステム・メモリーを使用してください。バックアップ・データの保存容量が増える場合、メモリー所要量を増やすことが必要な場合があります。</p> <p>定期的にメモリー使用量をモニターし、追加のメモリーが必要かどうかを判別してください。</p> <p>データベース・ページのキャッシング機能を向上させるために、追加システム・メモリーを使用してください。以下のメモリー・サイズのガイドラインは、バックアップする新規データの日次量に基づいています。</p> <ul style="list-style-type: none"> • データの日次バックアップ用に 128 GB システム・メモリー（ここでデータベース・サイズは 1 TB から 2 TB） • データの日次バックアップ用に 192 GB システム・メモリー（ここでデータベース・サイズは 2 TB から 4 TB） 	メモリー所要量

IBM Spectrum Protect サーバーのインストール

質問	タスク、特性、オプション、または設定	詳細情報
データベース活動ログとアーカイブ・ログのストレージ容量のサイズを適切に設定していますか？	<p>ACTIVELOGSIZE サーバー・オプションの値を 131072 に設定して、サーバーの最小活動ログ・サイズが 128 GB になるように構成します。</p> <p>アーカイブ・ログの推奨開始サイズは 1 TB です。アーカイブ・ログのサイズは、サーバー・オプションではなく、ログが配置されているファイル・システムのサイズによって制限されます。ファイル・システムでは、アーカイブ・ログのサイズより最低でも 10% 余分にディスク・スペースを確保するようにしてください。</p> <p>データベース・アーカイブ・ログには、少なくとも 1 TB の初期空き容量があるディレクトリーを使用します。ARCHLOGDIRECTORY サーバー・オプションを使用してディレクトリーを指定します。</p> <p>ARCHFAILOVERLOGDIRECTORY サーバー・オプションを使用して、アーカイブ・フェイルオーバー・ログ用のスペースを定義します。</p>	システムのサイズ設定について詳しくは、「IBM Spectrum Protect Blueprints」を参照してください。
アーカイブ・ログとデータベース・バックアップに対して圧縮は使用可能ですか？	<p>ARCHLOGCOMPRESS サーバー・オプションを有効にすると、ストレージ・スペースが節約されます。</p> <p>この圧縮オプションは、インライン圧縮とは異なります。インライン圧縮は、IBM Spectrum Protect V7.1.5 以降ではデフォルトで使用可能になっています。</p> <p>制約事項: バックアップされるデータの量が 1 日に 6 TB を超える場合はこのオプションを使用しないでください。</p>	システムの圧縮について詳しくは、「IBM Spectrum Protect Blueprints」を参照してください。
IBM Spectrum Protect データベースとログは別個のディスク・ボリューム (LUN) 上にありますか？	データベースは、IBM Spectrum Protect データベースのログやストレージ・プール、あるいはその他のアプリケーションやファイル・システムとの間でディスク・ボリュームを共有しません。	サーバー・データベースおよびリカバリー・ログの構成について詳しくは、サーバー・データベースおよび回復ログの構成とチューニングを参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
データ重複排除で使用する予定の IBM Spectrum Protect サーバーごとに、最小で 8 個 (2.2 GHz またはそれと同等) のプロセッサー・コアを使用していますか？	クライアント・サイド・データ重複排除を使用する計画の場合は、データ重複排除処理の実行に使用できる十分なリソースがバックアップ操作時にクライアント・システムにあることを確認してください。クライアント・サイド・データ重複排除では、バックアップ・プロセス当たり少なくとも 1 つの 2.2 GHz プロセッサー・コアに相当するプロセッサーを使用してください。	<ul style="list-style-type: none"> 重複排除の効果的な計画と使用 IBM Spectrum Protect Blueprints
データベース用に十分なストレージ・スペースを割り振りましたか？	<p>大まかな見積もりとして、重複排除ストレージ・プールで保護される 50 TB のデータごとに、100 GB のデータベース・ストレージを計画してください。「保護データ」とは、データ重複排除を行う前のデータ量で、保管されているすべてのバージョンのオブジェクトが含まれます。</p> <p>ベスト・プラクティスとしては、データ重複排除に専用の新規コンテナー・ストレージ・プールを定義してください。データ重複排除はストレージ・プール・レベルで行われ、暗号化データを除くストレージ・プール内のすべてのデータが重複排除されます。</p>	
ご使用の環境のサイズに十分なスペースを構成するために、ストレージ・プール容量を見積もりましたか？	<p>以下の方法を使用して、重複排除に必要なストレージ・プール容量を見積もることができます。</p> <ol style="list-style-type: none"> ソース・データのベース・サイズを見積もる。 見積もられた変更率および成長率を使用して、毎日のバックアップ・サイズを見積もる。 保存要件を決定する。 ベース・サイズ、毎日のバックアップ・サイズ、および保存要件を因数処理することで、ソース・データの総量を見積もる。 重複排除の比率因数を適用する。 圧縮の比率因数を適用する。 一時的なストレージ・プールの使用を考慮するために、見積もり値を切り上げる。 	この手法の使用例については、重複排除の効果的な計画と使用を参照してください。

IBM Spectrum Protect サーバーのインストール

質問	タスク、特性、オプション、または設定	詳細情報
ディスク入出力を多くのディスク装置およびコントローラーに分散させていますか？	<p>できるだけ多くのディスクから構成されたアレイを使用してください（ワイド・ストライピングと呼ばれることもあります）。サブシステム上の個別のアレイごとに、1 つのデータベース・ディレクトリリーを使用するようにしてください。</p> <p>表スペース内のコンテナーが複数の物理ディスクにまたがる場合に、使用される表スペースごとの並列入出力を可能にするため、DB2_PARALLEL_IO レジストリー変数を設定してください。</p> <p>入出力帯域幅が使用可能で、かつファイルのサイズが大きい（例えば、1 MB）場合は、プロセッサー全体のリソースが、重複の検出処理に占有される可能性があります。ファイルのサイズが小さい場合は、その他のボトルネックが発生する可能性があります。</p> <p>重複排除ストレージ・プール・デバイス・クラスに 8 個以上のファイル・システムを指定し、入出力ができるだけ多くの LUN および物理装置に分散されるようにします。</p>	<p>ストレージ・プールをセットアップするためのガイドラインとしては、「DISK 装置クラスまたは FILE 装置クラスのストレージ・プールの計画」を参照してください。</p> <p>DB2_PARALLEL_IO 変数の設定については、IBM DB2 レジストリー変数の推奨設定を参照してください。</p>
バックアップ・ストラテジーに基づいて日次操作をスケジュールしていますか？	<p>操作の最適な順序は、以下の順番です。</p> <ol style="list-style-type: none"> 1. クライアント・バックアップ 2. ストレージ・プールの保護 3. ノード複製 4. データベース・バックアップ 5. インベントリーの期限切れ 	<ul style="list-style-type: none"> • データ重複排除およびノード複製プロセスのスケジューリング • ディレクトリー・コンテナー・ストレージ・プールの日次操作

IBM Spectrum Protect サーバーのインストール

質問	タスク、特性、オプション、または設定	詳細情報
DB2 ロック・リストを管理するためには十分なストレージがありますか？	<p>ラージ・ファイルまたは多数のファイルを同時に含むデータを重複排除する場合、プロセスによってストレージ・スペースの容量が不十分になる可能性があります。ロック・リスト・ストレージの容量が不十分な場合、バックアップの失敗、データ管理プロセスの失敗、またはサーバーの停止が発生する可能性があります。</p> <p>データ重複排除で処理されるファイルのサイズが 500 GB を超えている場合は、ストレージ・スペースを使い切る可能性が高くなります。ただし、クライアント・サイド・データ重複排除を使用しているバックアップ操作の数が多い場合は、それより小さいサイズのファイルでもこの問題が発生する可能性があります。</p>	DB2 LOCKLIST パラメーターのチューニングについて詳しくは、サーバー・サイドのデータ重複排除のチューニングを参照してください。
IBM Spectrum Protect サーバーにデータを転送できる十分な帯域幅が使用可能ですか？	<p>データを IBM Spectrum Protect サーバーに転送する場合、必要な帯域幅を減らすために、クライアント・サイドまたはサーバー・サイドのデータ重複排除と圧縮を使用します。</p> <p>オンライン圧縮を使用するには V7.1.5 以上のサーバーを使用して、拡張圧縮処理を有効にするには V7.1.6 以降のクライアントを使用します。</p>	詳細については、 enablededup クライアント・オプションを参照してください。
各ストレージ・プールに割り当てるストレージ・プール・ディレクトリーの数を決定しましたか？	<p>DEFINE STGPOOLDIRECTORY コマンドを使用して、ディレクトリーをストレージ・プールに割り当てます。</p> <p>複数のストレージ・プール・ディレクトリーを作成し、各ディレクトリーが個別のディスク・ボリューム (LUN) にバックアップされるようにします。</p>	

IBM Spectrum Protect サーバーのインストール

質問	タスク、特性、オプション、または設定	詳細情報
クラウド・コンテナー・ストレージ・プールで十分なディスク・スペースを割り振りましたか？	<p>バックアップの失敗を回避するには、ローカル・ディレクトリーに十分なスペースが必要です。以下のリストを最適なディスク・スペースのガイドとして使用してください。</p> <ul style="list-style-type: none">シリアル接続 SCSI (SAS) および回転ディスクの場合、毎日のデータ削減（圧縮およびデータ重複排除）の後に予想される新規データ量を計算します。その量の最大 100 パーセント（テラバイト単位）をディスク・スペース用に割りります。オンプレミスのハイパフォーマンス・クラウド・システムに高速ネットワーク接続されているフラッシュ・ベース・ストレージ・システムの場合は、3 TB を提供します。ハイパフォーマンス・クラウド・システムに高速ネットワーク接続されているソリッド・ステート・ドライブ (SSD) システムの場合は、5 TB を提供します。	

質問	タスク、特性、オプション、または設定	詳細情報
適切なタイプのローカル・ストレージを選択しましたか？	<p>ローカル・ストレージからクラウドへのデータ転送が、次のバックアップ・サイクルが開始される前に完了することを確認してください。</p> <p>ヒント: データは、クラウドに移動された直後にローカル・ストレージから削除されます。</p> <p>以下のガイドラインを使用します。</p> <ul style="list-style-type: none"> • ハイパフォーマンス・クラウド・システムを備えた大規模システムでは、フラッシュまたは SSD を使用します。オブジェクト・ストレージへの高速接続を備えた、専用の 10 GB 広域ネットワーク (WAN) リンクが必要です。例えば、専用の 10 GB WAN リンクと、IBM Cloud Object Storage ポートケーションまたは Amazon Simple Storage Service (Amazon S3) データ・センターへの高速接続がある場合は、フラッシュまたは SSD を使用します。 • 以下のシナリオでは、より大容量の 15000 rpm SAS ディスクを使用します。 <ul style="list-style-type: none"> - 中規模のシステム - 低速なクラウド接続 (例えば、1 GB) - 複数の地域にまたがるサービス・プロバイダーとして IBM Cloud Object Storage を使用する場合 • SAS または回転ディスクの場合、毎日のデータ削減 (圧縮およびデータ重複排除) の後に予想される新規データ量を計算します。その量の最大 100 パーセント (テラバイト単位) をディスク・スペース用に割り振ります。 	

DISK 装置クラスまたは FILE 装置クラスのストレージ・プールの計画

チェックリストを使用して、ディスク・ストレージ・プールがどのようにセットアップされているかを確認します。このチェックリストには、DISK または FILE デバイス・クラスを使用するストレージ・プールに関するヒントも含まれています。

質問	タスク、特性、オプション、または設定	詳細情報
ストレージ・プールの LUN は、時間制約内にワークロードを適切に処理するために、256 KB の順次読み取りおよび書き込み用のスループット速度を維持できますか？	<p>ピークの負荷について計画する場合、サーバーがディスク・ストレージ・プールに対して同時に読み取りあるいは書き込みを行うすべてのデータを考慮してください。例えば、同時に実行されるクライアント・バックアップ操作とサーバーのデータ移動操作（マイグレーションなど）によって生じるデータの流れのピークについて考慮します。</p> <p>IBM Spectrum Protect サーバーは、ストレージ・プールに対して大部分は 256 KB のブロックで読み取りおよび書き込みを行います。</p> <p>ディスク・システムに処理能力がある場合は、ランダム読み取り/書き込み操作ではなく順次読み取り/書き込み操作を使用して、最適なパフォーマンスを得られるようにディスク・システムを構成します。</p>	詳しくは、ディスク・システムの基本パフォーマンスの分析を参照してください。
読み取りおよび書き込みキャッシュを使用するようにディスクが構成されていますか？	パフォーマンスを向上させるには、使用するキャッシュを増やします。	
FILE デバイス・クラスを使用するストレージ・プールの場合、ストレージ・プール・ボリュームを使用するのに適したサイズを判別しましたか？	ディスクを使用するストレージ・プールの最適なボリュームの数とサイズに記載されている情報を確認します。 FILE デバイス・クラス・ボリュームのサイズを推定するための情報がない場合は、50 GB のボリュームを使用して開始してください。	通常、ボリュームが小さすぎる場合、問題はより頻繁に発生します。ボリュームのサイズが必要なサイズより大きい場合は、問題が報告されることはありません。使用するボリューム・サイズを判別する場合、予防措置として、必要なサイズより大きいサイズを選択してください。
FILE デバイス・クラスを使用するストレージ・プールの場合、事前割り振りボリュームを使用していますか？	<p>スクラッチ・ボリュームを使用すると、ファイルがフラグメント化される場合があります。</p> <p>ストレージ・プールがボリュームを使い尽くしていないことを確認するには、MAXSCRATCH パラメーターをゼロより大きい値に設定します。</p>	<p>DEFINE VOLUME サーバー・コマンドを使用して、ストレージ・プールにボリュームを事前割り振りします。</p> <p>DEFINE STGPOOL または UPDATE STGPOOL サーバー・コマンドを使用して、MAXSCRATCH パラメーターを設定します。</p>

質問	タスク、特性、オプション、または設定	詳細情報
FILE デバイス・クラスを使用するストレージ・プールの場合、クライアント・セッションの最大数と定義済みのボリューム数を比較しましたか？	<p>同時に実行されるクライアント・セッションの予想ピーク数を処理できるよう、常にストレージ・プール内に十分な使用可能ボリュームを保持してください。ボリュームには、スクラッチ・ボリューム、空ボリューム、または部分的に使用されたボリュームがあります。</p>	FILE デバイス・クラスを使用するストレージ・プールの場合、一度にボリュームに書き込みを行えるのは 1 つのセッションまたはプロセスのみです。
FILE デバイス・クラスを使用するストレージ・プールの場合、デバイス・クラスの MOUNTLIMIT パラメーターを、並行してマウントされる可能性があるボリューム数を構成するのに十分な大きさの値に設定していますか？	<p>データ重複排除を使用するストレージ・プールの場合、通常、MOUNTLIMIT パラメーターの範囲は 500 から 1000 の間です。</p> <p>MOUNTLIMIT の値を、すべてのアクティブ・セッションで必要なマウント・ポイントの最大数に設定します。必要なマウント・ポイントの最大数に影響する以下のパラメーターを確認してください。</p> <ul style="list-style-type: none"> • MAXSESSIONS サーバー・オプション。このオプションは、並行して実行できる IBM Spectrum Protect セッションの最大数です。 • MAXNUMMP パラメーター。このパラメーターは、各クライアント・ノードが使用できるマウント・ポイントの最大数を設定します。 <p>例えば、クライアント・ノードのバックアップ・セッションの最大数が一般的に 100 で、各ノードで MAXNUMMP=2 が設定されている場合、100 個のノードに対してそれぞれ 2 個のマウント・ポイントを乗算することで、MOUNTLIMIT パラメーターの値 200 が得られます。</p>	<p>REGISTER NODE または UPDATE NODE サーバー・コマンドを使用して、クライアント・ノードの MAXNUMMP パラメーターを設定します。</p>

IBM Spectrum Protect サーバーのインストール

質問	タスク、特性、オプション、または設定	詳細情報
DISK デバイス・クラスを使用するストレージ・プールの場合、各ファイル・システムに配置するストレージ・プール・ボリュームの数を判別しましたか？	<p>DISK デバイス・クラスを使用するストレージ・プール用のストレージをどのように構成するかは、ディスク・システムに RAID を使用しているかどうかによって異なります。</p> <p>RAID を使用していない場合は、物理ディスクごとに 1 つのファイル・システムを構成し、各ファイル・システムに対して 1 つのストレージ・プール・ボリュームを定義します。</p> <p>$n+1$ 個のボリュームで RAID 5 を使用している場合は、以下のいずれかの方法でストレージを構成します。</p> <ul style="list-style-type: none">• LUN 上に n 個のファイル・システムを構成し、ファイル・システムごとに 1 つのストレージ・プール・ボリュームを定義する。• LUN に対して 1 つのファイル・システムと n 個のストレージ・プール・ボリュームを構成する。	この指針に従ったレイアウト例については、サーバー・ストレージ・プールのレイアウト例を参照してください。
複数のファイル・システム間で入出力が分散されるようにストレージ・プールを作成しましたか？	<p>必ず、各ファイル・システムをディスク・システム上の異なる LUN 上に配置してください。</p> <p>一般に 10 個から 30 個のファイル・システムを持つことが適切な目標ですが、それらのファイル・システムは確実に約 250 GB 以上になるようにしてください。</p>	詳細については、以下のトピックを参照してください。 <ul style="list-style-type: none">• サーバーのディスク・ストレージのチューニング• ストレージ・プールとボリュームのチューニングおよび構成

正しいタイプのストレージ・テクノロジーの計画

各ストレージ・デバイスには、異なる容量とパフォーマンスの特性があります。これらの特性は、どのデバイスが IBM Spectrum Protect での使用により適しているかに影響します。

手順

次の表を確認し、サーバーが必要とするストレージ・リソースを提供するのに適したストレージ・テクノロジーを選択してください。

表 2. IBM Spectrum Protect 要件を提供するためのストレージ・テクノロジー・タイプ

ストレージ・テクノロジー・タイプ	データベース	活動ログ	アーカイブ・ログとフェイルオーバー・アーカイブ・ログ	ストレージ・プール
ソリッド・ステート・ディスク (SSD)	<p>次の状況の場合は、データベースを SSD に配置します。</p> <ul style="list-style-type: none"> IBM Spectrum Protect データ重複排除を使用している場合。 毎日 8 TB を超える新規データをバックアップする場合。 	<p>IBM Spectrum Protect データベースを SSD に配置する場合、ベスト・プラクティスとしては、活動ログを SSD に配置します。使用可能なスペースがない場合は、代わりに高パフォーマンス・ディスクを使用してください。</p>	<p>SSD は、データベースおよび活動ログに使用するために節約してください。アーカイブ・ログとフェイルオーバー・アーカイブ・ログは、低速なストレージ・テクノロジー・タイプに配置することができます。</p>	<p>SSD は、データベースおよび活動ログに使用するために節約してください。ストレージ・プールは、低速なストレージ・テクノロジー・タイプに配置することができます。</p>
高パフォーマンス・ディスクは、以下の特性を備えています。	<p>高パフォーマンス・ディスクは、以下の状況で使用します。</p> <ul style="list-style-type: none"> サーバーがデータ重複排除を行わない場合。 サーバーがノード複製を行わない場合。 <p>サーバー・データベースは、そのログとストレージ・プール、および他のアプリケーションのデータから切り離してください。</p>	<p>高パフォーマンス・ディスクは以下の状況で使用します。</p> <ul style="list-style-type: none"> サーバーがデータ重複排除を行わない場合。 サーバーがノード複製を行わない場合。 <p>パフォーマンスと可用性を確保するために、活動ログはサーバー・データベース、アーカイブ・ログ、およびストレージ・プールから切り離してください。</p>	<p>アーカイブ・ログおよびフェイルオーバー・アーカイブ・ログに高パフォーマンス・ディスクを使用することができます。可用性を確保するために、これらのログはデータベースおよび活動ログから切り離してください。</p>	<p>ストレージ・プール用の高パフォーマンス・ディスクは、以下の状況で使用します。</p> <ul style="list-style-type: none"> データが頻繁に読み取られる場合。 データが頻繁に書き込まれる場合。 <p>パフォーマンスと可用性を確保するために、ストレージ・プール・データはサーバー・データベースとログ、および他のアプリケーションのデータから切り離してください。</p>
中パフォーマンス・ディスクまたは高パフォーマンス・ディスクは、以下の特性を備えています。	<p>ディスク・システム内で異なるディスク・テクノロジーを混用する場合は、高速なディスクをデータベースおよび活動ログに使用します。サーバー・データベースは、そのログとストレージ・プール、および他のアプリケーションのデータから切り離してください。</p>	<p>ディスク・システム内で異なるディスク・テクノロジーを混用する場合は、高速なディスクをデータベースおよび活動ログに使用します。パフォーマンスと可用性を確保するために、活動ログはサーバー・データベース、アーカイブ・ログ、およびストレージ・プールから切り離してください。</p>	<p>アーカイブ・ログおよびフェイルオーバー・アーカイブ・ログに中パフォーマンスまたは高パフォーマンス・ディスクを使用することができます。可用性を確保するために、これらのログはデータベースおよび活動ログから切り離してください。</p>	<p>ストレージ・プール用の中パフォーマンス・ディスクまたは高パフォーマンス・ディスクは以下の状況で使用します。</p> <ul style="list-style-type: none"> データが頻繁に読み取られる場合。 データが頻繁に書き込まれる場合。 <p>パフォーマンスと可用性を確保するために、ストレージ・プール・データはサーバー・データベースとログ、および他のアプリケーションのデータから切り離してください。</p>

IBM Spectrum Protect サーバーのインストール

表 2. IBM Spectrum Protect 要件を提供するためのストレージ・テクノロジー・タイプ (続き)

ストレージ・テクノロジー・タイプ	データベース	活動ログ	アーカイブ・ログとフェイルオーバー・アーカイブ・ログ	ストレージ・プール
SATA、Network Attached Storage	データベースにはこのストレージを使用しないでください。XIV ストレージ・システムにはデータベースを配置しないでください。	活動ログにはこのストレージを使用しないでください。	これらのログは一度だけ書き込みが行われ、読み取りも頻繁に行われないため、この低速なストレージ・テクノロジーを使用することができます。	低速ストレージ・テクノロジーは、以下の状況で使用します。 <ul style="list-style-type: none"> データが頻繁に書き込まれない場合 (一度だけの書き込みなど)。 データが頻繁に読み取られない場合。
テープおよび仮想テープ				長期間保存する場合、あるいはデータを頻繁に使用しない場合に使用します。

サーバー・インストールへのベスト・プラクティスの適用

通常、ハードウェアの構成と選択は、IBM Spectrum Protect ソリューションのパフォーマンスに最も顕著に影響します。パフォーマンスに影響するその他の要因には、オペレーティング・システムの選択と構成、および IBM Spectrum Protect の構成があります。

手順

- 以下のベスト・プラクティスは、最適なパフォーマンスを得るために、および問題を回避するために最も重要なものです。
- ご使用の環境に適用される構成のベスト・プラクティスを判別するため、以下の表を参照してください。

ベスト・プラクティス	詳細情報
サーバー・データベースには高速のディスクを使用します。ファイバー・チャネルまたは SAS インターフェースを備えたエンタープライズ・レベルのソリッド・ステート・ディスク (SSD) は、最高のパフォーマンスを提供します。	データベースには高速で待ち時間が短いディスクを使用します。データ重複排除およびノード複製を使用する場合は、SSD を使用することが基本です。 Serial Advanced Technology Attachment (SATA) および Parallel Advanced Technology Attachment (PATA) ディスクは使用しないでください。詳細およびヒントについては、以下のトピックを参照してください。 <ul style="list-style-type: none"> サーバー・データベース・ディスクの計画 正しいタイプのストレージ・テクノロジーの計画

ベスト・プラクティス	詳細情報
サーバー・システムに十分なメモリーがあることを確認してください。	<p>オペレーティング・システムの要件は、技術情報 1243309で参照してください。作業負荷が大きくなると、最小要件より多くのリソースが必要になります。データ重複排除やノード複製などの拡張機能を使用すると、システム要件の資料で示されている最小メモリーよりも多くのメモリーが必要になる可能性があります。</p> <p>複数のインスタンスを実行する予定の場合、各インスタンスごとに、1つのサーバー用にリストされているメモリーが必要です。1つのサーバーで必要なメモリーに、システムで計画しているインスタンスの数を乗算します。</p>
サーバー・データベース、活動ログ、アーカイブ・ログ、およびディスク・ストレージ・プールを相互に分離して配置します。	<p>すべての IBM Spectrum Protect ストレージ・リソースを別のディスク上に保持します。ストレージ・プール・ディスクを、サーバー・データベースおよびログのディスクから分離して保持します。ストレージ・プールとデータベースの両方が同じディスク上にあると、ストレージ・プール操作がデータベース操作を妨害する可能性があります。理想的には、サーバー・データベースとログも相互に分離してください。詳細およびヒントについては、以下のトピックを参照してください。</p> <ul style="list-style-type: none"> • サーバー・データベース・ディスクの計画 • サーバー・リカバリー・ログ・ディスクの計画 • DISK 装置クラスまたは FILE 装置クラスのストレージ・プールの計画
サーバー・データベースには、少なくとも 4 つのディレクトリーを使用します。大規模なサーバーや拡張機能を使用するサーバーの場合は、8 つのディレクトリーを使用します。	<p>各ディレクトリーを他の LUN および他のアプリケーションから分離された LUN 上に配置します。</p> <p>サーバーのデータベースが 2 TB より大きい場合、あるいはそのサイズより大きくなると予想される場合、そのサーバーは大規模なサーバーとして考慮してください。そのようなサーバーでは、8 つのディレクトリーを使用します。</p> <p>「サーバー・データベース・ディスクの計画」を参照してください。</p>
データ重複排除、ノード複製、あるいはその両方を使用している場合は、データベース構成およびその他の項目に関する指針に従ってください。	<p>これらの機能が使用されている場合に、サーバーがどの程度の処理能力で稼働できるかという点で非常に重要であるため、サーバー・データベースは指針に従って構成してください。詳細およびヒントについては、以下のトピックを参照してください。</p> <ul style="list-style-type: none"> • データ重複排除のチェックリスト • ノード複製のチェックリスト

IBM Spectrum Protect サーバーのインストール

ベスト・プラクティス	詳細情報
FILE タイプのデバイス・クラスを使用するストレージ・プールの場合、ストレージ・プール・ボリュームのサイズに関する指針に従ってください。通常、50 GB のボリュームが最適です。	<p>ボリューム・サイズを判別するには、ディスクを使用するストレージ・プールの最適なボリュームの数とサイズの情報を参照してください。</p> <p>キャパシティー要件だけではなく、スループット要件にも基づいて、ストレージ・プール装置およびファイル・システムを構成します。</p> <p>IBM Spectrum Protect で使用するストレージ・デバイスは、入出力が多い他のアプリケーションから分離し、そのストレージで十分なスループットが得られるようにしてください。</p> <p>詳細については、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。</p>
IBM Spectrum Protect クライアント操作とサーバー保守活動をスケジュールし、それらの操作のオーバーラップを回避または最小化します。	詳細については、以下のトピックを参照してください。 <ul style="list-style-type: none">日次操作のスケジュールのチューニングサーバー構成のチェックリスト
継続的に操作をモニターします。	モニタリングを行うことで、問題を早期に発見することができ、原因の特定も容易になります。最大 1 年間モニタリング・レポートの記録を保持することで、増大の傾向を把握し、増大に備えて計画することができます。パフォーマンスのための環境のモニタリングおよび保守を参照してください。

最小システム要件

IBM Spectrum Protect サーバーを Linux システムにインストールするには、通信方式および最新のデバイス・ドライバーなどの、最低レベルのハードウェアおよびソフトウェアを持つ必要があります。

IBM Spectrum Protect Blueprints を使用することで、最適な IBM Spectrum Protect 環境がデータ重複排除を使用してセットアップされます。

IBM Spectrum Protect デバイス・ドライバー・パッケージには、このオペレーティング・システム用のデバイス・ドライバーは含まれません。SCSI 汎用デバイス・ドライバーが使用されるからです。磁気テープ装置と一緒に IBM Spectrum Protect サーバーを使用する前に、デバイス・ドライバーを構成します。IBM Spectrum Protect ドライバー・パッケージには、ドライバー・ツールと ACSLS デーモンが含まれています。IBM ドライバー・パッケージは、Fix Central Web サイトで入手できます。

要件、サポートされるデバイス、クライアント・インストール・パッケージ、および修正については、IBM Support Portal for IBM Spectrum Protect を参照してください。IBM Spectrum Protect 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、Web サイトにアクセスして、該当するフィックスをダウンロードし適用してください。

Linux x86_64 サーバーの最小要件

IBM Spectrum Protect サーバーを Linux x86_64 オペレーティング・システムにインストールする前に、ハードウェアとソフトウェアの要件を確認してください。

IBM Spectrum Protect サーバーのインストールのためのハードウェア要件およびソフトウェア要件

IBM Spectrum Protect のシステム要件に関する最新の情報は、技術情報 1243309 を参照してください。

Linux on System z サーバーの最小要件

IBM Spectrum Protect サーバーを Linux on System z® オペレーティング・システムにインストールする前にハードウェアとソフトウェアの要件を確認してください。

IBM Spectrum Protect サーバーのインストールのためのハードウェア要件およびソフトウェア要件

IBM Spectrum Protect のシステム要件に関する最新の情報は、技術情報 1243309 を参照してください。

Linux on Power Systems™ (リトル・エンディアン) の最小サーバー要件

IBM Spectrum Protect サーバーを Linux on Power Systems (リトル・エンディアン) オペレーティング・システムにインストールする前に、ハードウェアとソフトウェアの要件を確認してください。

IBM Spectrum Protect サーバーのインストールのためのハードウェア要件およびソフトウェア要件

IBM Spectrum Protect のシステム要件に関する最新の情報は、技術情報 1243309 を参照してください。

IBM Spectrum Protect サーバーとシステム上の他の DB2 製品との互換性

IBM Spectrum Protect バージョン 8.1.5 サーバーと同じシステムに DB2 製品をデプロイして使用する他の製品を、いくつかの制限付きでインストールすることができます。

IBM Spectrum Protect サーバーと同じシステムに DB2 製品を使用する他の製品をインストールして使用するためには、必ず次の基準が満たされていることを確認してください。

IBM Spectrum Protect サーバーのインストール

表 3. IBM Spectrum Protect サーバーとシステム上の他の DB2 製品との互換性

基準	説明
バージョン・レベル	DB2 製品を使用する他の製品は、DB2 バージョン 9 以降を使用する必要があります。DB2 製品では、バージョン 9 から製品のカプセル化と分離がサポートされます。このバージョンから、コード・レベルが異なる複数の DB2 製品のコピーを同一システム上で実行することができます。 詳細については、複数の DB2 コピーに関する情報 (DB2 製品情報) を参照してください。
ユーザー ID とディレクトリー	ユーザー ID、フェンス・ユーザー ID、インストールの場所、その他のディレクトリー、および関連情報が複数の DB2 のインストールにおいて共有されていないことを確認してください。ご使用の指定は、IBM Spectrum Protect サーバーのインストールと構成に使用した ID と場所とは異なっていなければなりません。 <code>dsmicfgx</code> ウィザードを使用してサーバーを構成した場合、これらはウィザードの実行時に入力した値です。手動での構成方法を使用した場合、使用した手順を必要に応じて見直し、そのサーバーに使用した値を思い出してください。
リソース割り振り	IBM Spectrum Protect サーバーと、DB2 製品を使用する他のアプリケーション両方の要件と比較して、システムのリソースと機能を検討してください。他の DB2 アプリケーションに十分なリソースを提供するためには、IBM Spectrum Protect サーバーの設定を変更して、サーバーが使用するシステム・メモリーおよびリソースを削減する必要がある場合があります。 同様に、プロセッサーまたはメモリーのリソースの獲得において、他の DB2 アプリケーション作業負荷が IBM Spectrum Protect サーバーと競合している場合は、予期されるクライアント作業負荷または他のサーバー操作の処理で、サーバーのパフォーマンスに悪影響がある場合があります。 リソースを分離して、複数のアプリケーションでのプロセッサー、メモリー、および他のシステム・リソースの調整と割り振りにより多くの能力を提供するには、ロジカル・パーティション (LPAR)、ワークロード・パーティション (WPAR)、または他の仮想ワークステーション・サポートを使用することを検討してください。 例えば、DB2 アプリケーションを独自の仮想システムで実行します。

IBM Installation Manager

IBM Spectrum Protect は、IBM Installation Manager を使用します。これは、リモートまたはローカルのソフトウェア・リポジトリを使用して多くの IBM 製品をインストールまたは更新することができるインストール・プログラムです。

IBM Installation Manager の必要なバージョンがまだインストールされていない場合、IBM Spectrum Protect をインストールすると自動的にインストールまたはアップグレードされます。これは、後に必要に応じて IBM Spectrum Protect を更新またはアンインストールできるように、システムにインストールしたままにしておく必要があります。

IBM Installation Manager で使用される一部の用語の説明を以下にリストします。

オファリング

ソフトウェア製品のインストール可能単位。

IBM Spectrum Protect オファリングには、IBM Installation Manager が IBM Spectrum Protect をインストールするために必要なすべてのメディアが含まれています。

パッケージ

オファリングをインストールするために必要なソフトウェア・コンポーネントのグループ。

IBM Spectrum Protect パッケージには、以下のコンポーネントが含まれています。

- IBM Installation Manager インストール・プログラム
- IBM Spectrum Protect オファリング

パッケージ・グループ

共通親ディレクトリーを共有するパッケージのセット。

IBM Spectrum Protect パッケージのデフォルト・パッケージ・グループは、IBM Installation Manager です。

リポジトリ

データおよびその他のアプリケーション・リソース用のリモート・ストレージまたはローカル・ストレージのエリア。

IBM Spectrum Protect パッケージは、IBM Fix Central 上のリポジトリに保管されています。

共有リソース・ディレクトリー

パッケージで共有されるソフトウェア・ファイルまたはプラグインが含まれるディレクトリー。

IBM Installation Manager は、インストール関連のファイルを共有リソース・ディレクトリーに保管します。これには、IBM Spectrum Protect の前のバージョンにロールバックするために使用されるファイルが含まれます。

サーバーの詳細を計画するためのワークシート

このワークシートを使用すると、IBM Spectrum Protect サーバーに必要なストレージの量とロケーションの計画に役立ちます。また、これを使用して名前とユーザー ID を追跡することもできます。

項目	必要なスペース	ディレクトリー数	ディレクトリーのロケーション
データベース			
活動ログ			
アーカイブ・ログ			
オプション: 活動ログのログ・ミラー			
オプション: 2 次アーカイブ・ログ (アーカイブ・ログのフェイルオーバー・ロケーション)			

項目	名前とユーザー ID	ロケーション
IBM Spectrum Protect サーバーの始動と実行に使用する ID である、サーバーのインスタンス・ユーザー ID		
インスタンス・ユーザー ID を含むディレクトリーである、サーバーのホーム・ディレクトリー		
データベース・インスタンス名		
サーバーのインスタンス・ディレクトリー。これは、特にこのサーバー・インスタンス用のファイル (サーバー・オプション・ファイルおよびその他のサーバー特有のファイル) を含むディレクトリーです。		
サーバー名。サーバーごとに固有の名前を使用してください。		

キャパシティー計画

IBM Spectrum Protect のキャパシティー計画には、データベース、リカバリー・ログ、および共有リソース域などのリソースの管理が含まれます。キャパシティー計画の一部としてリソースを最大化するために、データベースおよび回復ログのスペース所要量を見積もる必要があります。共有リソース域には、各インストールまたはアップグレードで使用可能な十分なスペースがなければなりません。

データベースのスペース所要量の見積もり

データベースのスペース所要量を見積もるには、サーバー・ストレージに同時に置くことができるファイルの最大数を使用するか、ストレージ・プール・キャパシティーを使用することができます。

このタスクについて

初期のデータベース・スペースに 25 GB 以上を使用することを検討してください。ファイル・システムのスペースを適切にプロビジョンしてください。テスト環境またはライブラリー・マネージャーのみの環境には、データベース・サイズ 25 GB で十分です。クライアントの作業負荷をサポートする実動サーバーの場合、データベース・サイズはもっと大きいサイズであることが必要です。ランダム・アクセス・ディスク (DISK) ストレージ・プールを使用する場合は、順次アクセス・ストレージ・プールよりも多くのデータベースおよびログ・ストレージ・スペースが必要になります。

IBM Spectrum Protect データベースの最大サイズは 6 TB です。

ファイル数およびストレージ・プールのサイズに基づく、本番環境におけるデータベースのサイズ見積もりについては、以下のトピックを参照してください。

ファイル数に基づくデータベース・スペース所要量の見積もり

ある時刻にサーバー・ストレージに入っているファイルの最大数を予想できる場合は、その数を使用してデータベースのスペース所要量を見積もることができます。

このタスクについて

サーバー・ストレージ内のファイルの最大数に基づいて、スペース所要量を見積もるには、以下のガイドラインを使用してください。

- イメージ・バックアップを含め、ファイルの保管済みの各バージョン用に 600 から 1000 バイト。

制約事項: このガイドラインには、データ重複排除中に使用されるスペースは含まれていません。

- キャッシュ・ファイル、コピー・ストレージ・プール・ファイル、活動データ・プール・ファイル、および重複排除されたファイルごとに、100 から 200 バイト。
- さまざまなデータ・アクセス・パターンや、データのサーバー・バックエンド・プロセスをサポートするには、データベースの最適化のために追加のスペースが必要です。余分なスペース量は、ファイル・オブジェクトの合計バイト数の見積もりの 50% に相当します。

IBM Spectrum Protect サーバーのインストール

以下の單一クライアントの例では、上記のガイドラインの最大値に基づいて計算が行われます。これらの例では、ファイル集約が使用される可能性については考慮されていません。一般に、小さいファイルを集約すると、必要なデータベース・スペースの量が削減されます。ファイルの集合は、スペース管理ファイルに影響を与えません。

手順

1. ファイル・バージョン数を計算します。ファイル・バージョン数を求めるために、以下の各値を加算してください。
 - a. バックアップ・ファイルの数を計算します。例えば、500,000 個ものクライアント・ファイルが同時にバックアップされる可能性があります。この例では、ストレージ・ポリシーは、最大 3 個のバックアップ・ファイル・コピーを保持するように設定されています。
$$500,000 \text{ files} * 3 \text{ copies} = 1,500,000 \text{ files}$$
 - b. アーカイブ・ファイル数を計算します。例えば、100,000 個ものクライアント・ファイルが、アーカイブ・コピーである場合があります。
 - c. スペース管理対象ファイルの数を計算します。例えば、200,000 個ものクライアント・ファイルが、クライアント・ワークステーションからマイグレーションされる場合があります。

ファイルごとに 1000 バイトを使用すると、クライアントに属するファイルに必要なデータベース・スペースの合計量は 1.8 GB です。

- $$(1,500,000 + 100,000 + 200,000) * 1000 = 1.8 \text{ GB}$$
2. キャッシュ・ファイル、コピー・ストレージ・プール・ファイル、活動データ・プール・ファイル、および重複排除されたファイルの数を計算します。
 - a. キャッシュ・コピーの数を計算します。例えば、5 GB のディスク・ストレージ・プールでキャッシングが使用可能になっています。このプールのマイグレーションの高しきい値は 90% で、このプールのマイグレーションの低しきい値は 70% です。したがって、ディスク装置上のプールの 20% (すなわち、1 GB) がキャッシュ・ファイルに占有されます。

平均のファイル・サイズが約 10 KB である場合は、約 100,000 個のファイルがどの時点でもキャッシュに存在します。

- $$100,000 \text{ files} * 200 \text{ bytes} = 19 \text{ MB}$$
- b. コピー・ストレージ・プール・ファイルの数を計算します。すべての 1 次ストレージ・プールは、コピー・ストレージ・プールにバックアップされます。
$$(1,500,000 + 100,000 + 200,000) * 200 \text{ bytes} = 343 \text{ MB}$$
 - c. 活動ストレージ・プール・ファイルの数を計算します。1 次ストレージ・プールにあるすべての活動クライアント・バックアップ・データは、活動データ・ストレージ・プールにコピーされます。1 次ストレージ・プールで 1,500,000 個のバックアップ・ファイルの 500,000 個のバージョンが活動状態であると想定します。
$$500,000 * 200 \text{ bytes} = 95 \text{ MB}$$
 - d. 重複排除されたファイルの数を計算します。重複排除されたストレージ・プールに、50,000 個のファイルが含まれていると想定します。

$$50,000 * 200 \text{ bytes} = 10 \text{ MB}$$

上記の計算に基づいて、クライアントのキャッシュ・ファイル、コピー・ストレージ・プール・ファイル、活動データ・プール・ファイル、および重複排除されたファイルには、約 0.5 GB の余分なデータベース・スペースが必要です。

3. データベースの最適化に必要な余分なスペース量を計算します。サーバーによる最適なデータ・アクセスと管理を行うには、余分なデータベース・スペースが必要です。余分なデータベース・スペース量は、ファイル・オブジェクトの合計スペース所要量の 50% に相当します。

$$(1.8 + 0.5) * 50\% = 1.2 \text{ GB}$$

4. クライアントに必要なデータベース・スペースの合計量を計算します。合計は、約 3.5 GB です。

$$1.8 + 0.5 + 1.2 = 3.5 \text{ GB}$$

5. すべてのクライアントに必要なデータベース・スペースの合計量を計算します。例えば、上記の計算で使用されたクライアントが代表的であり、500 のクライアントがある場合、以下の計算式を使用して、すべてのクライアントに必要なデータベース・スペースの合計量を見積もることができます。

$$500 * 3.5 = 1.7 \text{ TB}$$

タスクの結果

ヒント: 上記の例の結果は、あくまでも見積もりです。データベースの実際のサイズは、ディレクトリーの数やパスとファイル名の長さなど、さまざまな要因のために見積もりとは異なる可能性があります。データベースを定期的にモニターして、必要に応じてサイズを調整してください。

次のタスク

通常の操作時に、IBM Spectrum Protect サーバーには一時的なデータベース・スペースが必要な場合があります。このスペースは次の理由で必要です。

- 保持と最適化がまだ行われていない、ソートや順序付けの結果をデータベースで直接保持するため。結果は処理のためにデータベースに一時的に保持されます。
- 次のいずれかの方式を使用して、データベースへの管理アクセス権を与えるため。
 - DB2 Open Database Connectivity (ODBC) クライアント
 - Oracle Java Database Connectivity (JDBC) クライアント
 - 管理クライアント・コマンド・ラインからサーバーへの構造化照会言語 (SQL)

ファイル・オブジェクトと最適化のために、500 GB のスペースごとに、余分な 50 GB の一時スペースを使用することを検討してください。以下の表のガイドラインを参照してください。前のステップで使用されている例では、500 個のクライアントのファイル・オブジェクトおよび最適化に、合計 1.7 TB のデータベース・スペースが必要です。その計算に基づいて、一時スペースに 200 GB が必要です。必要なデータベース・スペースの合計量は 1.9 TB です。

データベース・サイズ	最小の一時スペース所要量
< 500 GB	50 GB

IBM Spectrum Protect サーバーのインストール

データベース・サイズ	最小の一時スペース所要量
$\geq 500 \text{ GB} \text{ かつ } < 1 \text{ TB}$	100 GB
$\geq 1 \text{ TB} \text{ かつ } < 1.5 \text{ TB}$	150 GB
$\geq 1.5 \text{ TB} \text{ かつ } < 2 \text{ TB}$	200 GB
$\geq 2 \text{ TB} \text{ かつ } < 3 \text{ TB}$	250 - 300 GB
$\geq 3 \text{ TB} \text{ かつ } < 4 \text{ TB}$	350 - 400 GB

ストレージ・プールのキャパシティーに基づくデータベース・スペース所要量の見積もり

ストレージ・プールのキャパシティーに基づいてデータベース・スペース所要量を見積もるには、1% から 5% の比率を使用します。例えば、200 TB のストレージ・プール・キャパシティーが必要な場合、データベースのサイズは 2 から 10 TB であると予想されます。一般的に、スペースが不足しないように、データベースをできるだけ大きくしてください。データベース・スペースを使い尽くすと、サーバー操作およびクライアント保管操作が失敗する可能性があります。

データベース・マネージャーと一時スペース

IBM Spectrum Protect サーバーのデータベース・マネージャーは、データベースのシステム・メモリーおよびディスク・スペースの管理と割り振りを行います。必要なデータベース・スペースの量は、使用可能なシステム・メモリーの量およびサーバーのワーカロードに左右されます。

データベース・マネージャーは、データを要求するために発行された SQL ステートメントに従って、特定のシーケンスでデータをソートします。サーバーのワーカロードによっては、あるいはデータベース・マネージャーが管理できる量を超えるデータがある場合には、データ（順に並んでいる）は一時ディスク・スペースに割り振られます。結果セットが大きい場合、データは一時ディスク・スペースに割り振られます。データベース・マネージャーは、データが一時ディスク・スペースに割り振られる際に使用されるメモリーを動的に管理します。

例えば、期限切れ処理では結果セットが大きくなる可能性があります。結果セットを格納するために十分なシステム・メモリーがデータベースにない場合は、データの一部が一時ディスク・スペースに割り振られます。期限切れ処理中に、大きすぎて処理できないノードまたはファイル・スペースが選択された場合、データベース・マネージャーはメモリー内のデータをソートできません。データベース・マネージャーは、データをソートするために一時スペースを使用する必要があります。

データベース操作を実行するために、以下のようなシナリオの場合は、データベース・スペースの追加を検討してください。

- データベースに少量のスペースしかなく、一時スペースを必要とするサーバー操作によって、残りのフリー・スペースが使用される場合。
- ファイル・スペースが大きい、またはファイル・スペースに多数のファイル・バージョンを作成するポリシーが割り当てられている場合。
- 限られたメモリーで IBM Spectrum Protect サーバーを実行しなければならない場合。データベースは、IBM Spectrum Protect サーバーのメイン・メモリーを使用して、データベース操作を実行します。しかし、使用可能なメモリーが不足

している場合、IBM Spectrum Protect サーバーはデータベースに対してディスク上に一時スペースを割り振ります。例えば、10G のメモリーが使用可能で、データベース操作に 12G のメモリーが必要な場合、データベースは一時スペースを使用します。

- IBM Spectrum Protect サーバーをデプロイすると、「データベース・スペース不足 (out of database space)」エラーが表示される場合。サーバーのアクティビティー・ログをモニターして、データベース・スペースに関連したメッセージを調べてください。

重要: IBM Spectrum Protect インストール・パッケージおよびフィックスパックとともにインストールされている DB2 ソフトウェアは変更しないでください。データベースが損傷する可能性があるため、別のバージョン、リリース、またはフィックスパックの DB2 ソフトウェアをインストールしたり、それらにアップグレードしたりしないでください。

回復ログのスペース要件

IBM Spectrum Protect で、回復ログ という用語は、活動ログ、アーカイブ・ログ、活動ログ・ミラー、およびアーカイブ・フェイルオーバー・ログを含みます。回復ログに必要なスペースの量は、例えば、サーバーとやり取りするクライアントのアクティビティーなど、さまざまな要因によって異なります。

活動ログとアーカイブ・ログのスペース

活動ログとアーカイブ・ログのスペース所要量を見積もる場合は、ときどき発生する大量の作業負荷やフェイルオーバーなどの不測の事態用に余分なスペースを組み込んでください。

IBM Spectrum Protect サーバー V7.1 以降では、活動ログのサイズは最大 512 GB まで可能です。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。

活動ログのサイズを見積もる際に、以下の一般ガイドラインを使用してください。

- 活動ログの推奨開始サイズは 16 GB です。
- 活動ログを、サーバーが通常処理する並行アクティビティーの量に対して十分以上の大きさになるようにします。予防措置として、サーバーが 1 度に管理する最大の作業量を予期するようにしてください。活動ログに、必要に応じて使用できる余分のスペースをプロビジョンします。20% の追加スペースの使用を考慮してください。
- 使用済みおよび使用可能な活動ログ・スペースをモニターします。クライアントのアクティビティーやサーバー操作のレベルなどの要因によって、必要に応じて活動ログのサイズを調整します。
- 活動ログを保持するディレクトリーを、必ず活動ログのサイズ以上にします。活動ログより大きいディレクトリーは、フェイルオーバーが発生した場合、フェイルオーバーに対応することができます。
- 活動ログ・ディレクトリーを含むファイル・システムに、一時的なログの移動のために 8 GB 以上のフリー・スペースがあることを確認してください。

アーカイブ・ログの推奨開始サイズは 48 GB です。

IBM Spectrum Protect サーバーのインストール

アーカイブ・ログ・ディレクトリーは、直前のフルバックアップ以降に生成されるログ・ファイルを収容できる十分な大きさでなければなりません。例えば、データベースのフルバックアップを毎日実行する場合、アーカイブ・ログ・ディレクトリーは、24 時間で発生するすべてのクライアント・アクティビティーのログ・ファイルを保持できる十分な大きさが必要です。スペースをリカバリーするために、サーバーは、データベースのフルバックアップ後に古いアーカイブ・ログ・ファイルを削除します。アーカイブ・フェイルオーバー・ログ用のディレクトリーが存在しない場合、ログ・ファイルは活動ログ・ディレクトリーに残ります。この状態は、活動ログ・ディレクトリーが満杯になり、サーバーを停止させる原因になることがあります。サーバーが再始動すると、既存の活動ログ・スペースの一部が解放されます。

サーバーがインストールされた後は、アーカイブ・ログの使用率とアーカイブ・ログ・ディレクトリー内のスペースをモニターすることができます。アーカイブ・ログ・ディレクトリー内のスペースが満杯になると、以下の問題が発生する可能性があります。

- サーバーがフル・データベース・バックアップを実行できない。この問題を調べて解決してください。
- 他のアプリケーションがアーカイブ・ログ・ディレクトリーに書き込んで、アーカイブ・ログに必要なスペースを使い尽くす。他の IBM Spectrum Protect サーバーを始めとする他のアプリケーションと、アーカイブ・ログ・スペースを共有しないでください。必ずその特定サーバーが所有して管理する別個の保管場所があるようにします。

例: 基本クライアント保管操作の活動ログとアーカイブ・ログのサイズの見積もり:

基本クライアント保管操作には、バックアップ、アーカイブ、およびスペース管理があります。同時に進行中のすべての保管トランザクションを処理するのに十分なログ・スペースでなければなりません。

基本クライアント操作の活動ログとアーカイブ・ログのサイズを判別するには、以下の計算を使用してください。

number of clients x files stored during each transaction
x log space needed for each file

この計算は、以下の表の例で使用されます。

表 4. 基本クライアント保管操作

項目	値の例	説明
時間帯に関わらずファイルを同時にバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの最大数。	300	毎日夜間にファイルをバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの数。
各トランザクション中に保管されるファイル	4096	サーバー・オプション TXNGROUPMAX のデフォルト値は 4096 です。

表 4. 基本クライアント保管操作 (続き)

項目	値の例	説明
各ファイルに必要なログ・スペース	3053 バイト	<p>トランザクション内のファイルごとに 3053 バイトという値は、ファイル名が 12 から 120 バイトであるファイルを Windows クライアントからバックアップするときに必要なログ・バイト数を表しています。</p> <p>この値は、実験室条件下で実行されたテストの結果に基づきます。これらのテストは、ランダム・アクセス・ディスク (DISK) ストレージ・プールに対するバックアップ操作を実行するバックアップ/アーカイブ・クライアントで構成されました。DISK プールは、順次アクセス・ストレージ・プールよりも多くのログの使用量の増加をもたらします。保管するデータのファイル名が 12 から 120 バイトよりも長い場合は、3053 バイトより大きい値を使用することを検討してください。</p>
活動ログ: 推奨サイズ	19.5 GB ¹	<p>活動ログのサイズを判別するには、以下の計算を使用します。1 GB は 1,073,741,824 バイトに相当します。</p> $(300 \text{ クライアント} \times \text{各トランザクション時に保管される } 4096 \text{ ファイル} \times \text{ファイルごとに } 3053 \text{ バイト}) \div 1,073,741,824 \text{ バイト} = 3.5 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。</p> $3.5 + 16 = 19.5 \text{ GB}$
アーカイブ・ログ: 推奨サイズ	58.5 GB ¹	<p>3 つのサーバー・データベース・バックアップ・サイクル全体でアーカイブ・ログを保管できるという要件があるため、活動ログの見積もりに 3 を掛けて、アーカイブ・ログの合計所要量を見積もります。</p> $3.5 \times 3 = 10.5 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。</p> $10.5 + 48 = 58.5 \text{ GB}$

¹ この表内の値の例は、活動ログとアーカイブ・ログのサイズの計算方法を示すためにのみ使用しています。重複排除を使用しない本番環境では、活動ログの推奨される最小サイズは 16 GB です。重複排除を使用しない本番環境では、アーカイブ・ログの推奨される最小サイズは 48 GB です。ご使用の環境から値を補完し、その結果 16 GB および 48 GB より大きくなった場合は、その結果を使用して活動ログとアーカイブ・ログのサイズを調整します。

ログをモニターし、必要に応じてこれらのサイズを調整します。

IBM Spectrum Protect サーバーのインストール

例: 複数のセッションを使用するクライアントの活動ログとアーカイブ・ログのサイズの見積もり:

クライアント・オプション RESOURCEUTILIZATION が、デフォルトより大きい値に設定される場合、サーバーの並行作業負荷が増えます。

クライアントが複数のセッションを使用するときの活動ログとアーカイブ・ログのサイズを判別するには、以下の計算を使用してください。

$$\text{number of clients} \times \text{sessions for each client} \times \text{files stored during each transaction} \times \text{log space needed for each file}$$

この計算は、以下の表の例で使用されます。

表 5. 複数のクライアント・セッション

項目	値の例		説明
時間帯に関わらずファイルを同時にバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの最大数。	300	1000	毎日夜間にファイルをバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの数。
クライアントごとに可能なセッション数	3	3	クライアント・オプション RESOURCEUTILIZATION の設定は、デフォルトより大きくなります。各クライアント・セッションは、最大 3 つのセッションを並行して実行します。
各トランザクション中に保管されるファイル	4096	4096	サーバー・オプション TXNGROUPMAX のデフォルト値は 4096 です。
各ファイルに必要なログ・スペース	3053	3053	トランザクション内のファイルごとに 3053 バイトという値は、ファイル名が 12 から 120 バイトであるファイルを Windows クライアントからバックアップするときに必要なログ・バイト数を表しています。 この値は、実験室条件下で実行されたテストの結果に基づきます。テストは、ランダム・アクセス・ディスク (DISK) ストレージ・プールに対するバックアップ操作を実行するクライアントで構成されました。DISK プールは、順次アクセス・ストレージ・プールよりも多くのログの使用量の増加をもたらします。保管するデータのファイル名が 12 から 120 バイトよりも長い場合は、3053 バイトより大きい値を使用することを検討してください。

表 5. 複数のクライアント・セッション (続き)

項目	値の例		説明
活動ログ: 推奨サイズ	26.5 GB ¹	51 GB ¹	<p>300 のクライアントに以下の計算式が使用されました。1 GB は 1,073,741,824 バイトに相当します。</p> $(300 \text{ クライアント} \times \text{クライアントごとに 3 セッション} \times \text{各トランザクション時に保管される 4096 ファイル} \times \text{ファイルごとに 3053 バイト}) \div 1,073,741,824 = 10.5 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。</p> $10.5 + 16 = 26.5 \text{ GB}$ <p>1000 のクライアントに以下の計算式が使用されました。1 GB は 1,073,741,824 バイトに相当します。</p> $(1000 \text{ クライアント} \times \text{クライアントごとに 3 セッション} \times \text{各トランザクション時に保管される 4096 ファイル} \times \text{ファイルごとに 3053 バイト}) \div 1,073,741,824 = 35 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。</p> $35 + 16 = 51 \text{ GB}$
アーカイブ・ログ: 推奨サイズ	79.5 GB ¹	153 GB ¹	<p>3 つのサーバー・データベース・バックアップ・サイクル全体でアーカイブ・ログを保管できるという要件があるため、活動ログの見積もりに 3 を掛けます。</p> $10.5 \times 3 = 31.5 \text{ GB}$ $35 \times 3 = 105 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 48 GB を追加してこれらの量を増やします。</p> $31.5 + 48 = 79.5 \text{ GB}$ $105 + 48 = 153 \text{ GB}$

¹ この表内の値の例は、活動ログとアーカイブ・ログのサイズの計算方法を示すためにのみ使用しています。重複排除を使用しない本番環境では、活動ログの推奨される最小サイズは 16 GB です。重複排除を使用しない本番環境では、アーカイブ・ログの推奨される最小サイズは 48 GB です。ご使用の環境から値を補完し、その結果 16 GB および 48 GB より大きくなった場合は、その結果を使用して活動ログとアーカイブ・ログのサイズを調整します。

活動ログをモニターし、必要に応じてそのサイズを調整します。

IBM Spectrum Protect サーバーのインストール

例: 同時書き込み操作の活動ログとアーカイブ・ログのサイズの見積もり:

クライアント・バックアップ操作で、同時書き込み用に構成されるストレージ・プールを使用する場合、各ファイルに必要なログ・スペース量が増えます。

各ファイルに必要なログ・スペースは、同時書き込み操作に使用されるコピー・ストレージ・プールごとに約 200 バイト増えます。以下の表の例では、データは、1 次ストレージ・プールの他に、2 つのコピー・ストレージ・プールに保管されます。見積もられるログ・サイズは、ファイルごとに 400 バイト増えます。ファイルごとのログ・スペースの推奨値である 3053 バイトを使用する場合、必要な合計バイト数は 3453 です。

この計算は、以下の表の例で使用されます。

表 6. 同時書き込み操作

項目	値の例	説明
時間帯に関わらずファイルを同時にバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの最大数。	300	毎日夜間にファイルをバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの数。
各トランザクション中に保管されるファイル	4096	サーバー・オプション TXNGROUPMAX のデフォルト値は 4096 です。
各ファイルに必要なログ・スペース	3453 バイト	<p>3053 バイトに加えて、コピー・ストレージ・プールごとに 200 バイト。</p> <p>トランザクション内のファイルごとに 3053 バイトという値は、ファイル名が 12 から 120 バイトであるファイルを Windows クライアントからバックアップするときに必要なログ・バイト数を表しています。</p> <p>この値は、実験室条件下で実行されたテストの結果に基づきます。これらのテストは、ランダム・アクセス・ディスク (DISK) ストレージ・プールに対するバックアップ操作を実行するバックアップ/アーカイブ・クライアントで構成されました。DISK プールは、順次アクセス・ストレージ・プールよりも多くのログの使用量の増加をもたらします。保管するデータのファイル名が 12 から 120 バイトよりも長い場合は、3053 バイトより大きい値を使用することを検討してください。</p>
活動ログ: 推奨サイズ	20 GB ¹	<p>活動ログのサイズを判別するには、以下の計算を使用します。1 GB は 1,073,741,824 バイトに相当します。</p> <p>(300 クライアント × 各トランザクション時に保管される 4096 ファイル × ファイルごとに 3453 バイト) ÷ 1,073,741,824 バイト = 4.0 GB</p> <p>以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。</p> <p>4 + 16 = 20 GB</p>

表 6. 同時書き込み操作 (続き)

項目	値の例	説明
アーカイブ・ログ: 推奨サイズ	60 GB ¹	<p>3 つのサーバー・データベース・バックアップ・サイクル全体でアーカイブ・ログを保管できるという要件があるため、活動ログの見積もりに 3 を掛けて、アーカイブ・ログの所要量を見積もります。</p> $4 \text{ GB} \times 3 = 12 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。</p> $12 + 48 = 60 \text{ GB}$

¹ この表内の値の例は、活動ログとアーカイブ・ログのサイズの計算方法を示すためにのみ使用しています。重複排除を使用しない本番環境では、活動ログの推奨される最小サイズは 16 GB です。重複排除を使用しない本番環境では、アーカイブ・ログの推奨される最小サイズは 48 GB です。ご使用の環境から値を補完し、その結果 16 GB および 48 GB より大きくなった場合は、その結果を使用して活動ログとアーカイブ・ログのサイズを調整します。

ログをモニターし、必要に応じてこれらのサイズを調整します。

例: 基本クライアント保管操作とサーバー操作の活動ログとアーカイブ・ログのサイズの見積もり:

サーバー・ストレージ内のデータのマイグレーション、データ重複排除の識別プロセス、レクラメーション、および期限切れが、クライアント保管操作と同時に実行される場合があります。管理用タスク (管理クライアントからの管理コマンドや SQL 照会など) も、クライアント保管操作と同時に実行される場合があります。同時に実行されるサーバー操作と管理用タスクにより、必要な活動ログ・スペースが増える可能性があります。

例えば、ランダム・アクセス (DISK) ストレージ・プールから、順次アクセス・ディスク (FILE) ストレージ・プールへのファイルのマイグレーションでは、マイグレーションされるファイルごとに約 110 バイトのログ・スペースを使用します。例えば、300 個のバックアップ/アーカイブ・クライアントがあり、それぞれが毎晩 100,000 個のファイルをバックアップするとします。これらのファイルは最初に DISK に保管された後、FILE ストレージ・プールにマイグレーションされます。データ・マイグレーションに必要な活動ログ・スペース量を見積もるには、次の計算式を使用します。この計算のクライアント数は、時間帯に関わらずファイルを同時にバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの最大数を表します。

$$300 \text{ clients} \times 100,000 \text{ files for each client} \times 110 \text{ bytes} = 3.1 \text{ GB}$$

この値を、基本クライアント保管操作用に計算された活動ログ・サイズの見積もりに加算します。

IBM Spectrum Protect サーバーのインストール

例: 差異が大きい条件下での活動ログとアーカイブ・ログのサイズの見積もり:

迅速に完了するトランザクションが多数あり、完了にもっと時間がかかるトランザクションがいくつかある場合、活動ログ・スペースが不足する問題が生じる可能性があります。標準的な事例が発生するのは、ワークステーションまたはファイル・サーバーのバックアップ・セッションが多数アクティブであり、非常に大きいデータベース・サーバー・バックアップ・セッションがいくつかアクティブである場合です。この状態がご使用の環境に当てはまる場合は、作業が正常に完了するよう活動ログのサイズを増やす必要がある可能性があります。

例: フル・データベース・バックアップのアーカイブ・ログ・サイズの見積もり:

IBM Spectrum Protect サーバーがアーカイブ・ログから不要なファイルを削除するのは、フル・データベース・バックアップが行われるときのみです。したがって、アーカイブ・ログに必要なスペースを見積もる場合は、フル・データベース・バックアップの頻度も考慮する必要があります。

例えば、フル・データベース・バックアップが 1 週間に 1 回行われる場合、アーカイブ・ログのスペースは、1 週間の情報をアーカイブ・ログに入れることができなければなりません。

日次データベース・バックアップとフル・データベース・バックアップのアーカイブ・ログ・サイズの差が、次の表の例に示されています。

表 7. フル・データベース・バックアップ

項目	値の例	説明
時間帯に関わらずファイルを同時にバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの最大数。	300	毎日夜間にファイルをバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの数。
各トランザクション中に保管されるファイル	4096	サーバー・オプション TXNGROUPMAX のデフォルト値は 4096 です。
各ファイルに必要なログ・スペース	3453 バイト	ファイルごとの 3053 バイトに加えて、コピー・ストレージ・プールごとに 200 バイト。 トランザクション内のファイルごとに 3053 バイトという値は、ファイル名が 12 から 120 バイトであるファイルを Windows クライアントからバックアップするときに必要なログ・バイト数を表しています。 この値は、実験室条件下で実行されたテストの結果に基づきます。テストは、ランダム・アクセス・ディスク (DISK) ストレージ・プールに対するバックアップ操作を実行するクライアントで構成されました。DISK プールは、順次アクセス・ストレージ・プールよりも多くのログの使用量の増加をもたらします。保管するデータのファイル名が 12 から 120 バイトよりも長い場合は、3053 バイトより大きい値を使用することを検討してください。

表 7. フル・データベース・バックアップ (続き)

項目	値の例	説明
活動ログ: 推奨サイズ	20 GB ¹	<p>活動ログのサイズを判別するには、以下の計算を使用します。1 GB は 1,073,741,824 バイトに相当します。</p> $(300 \text{ クライアント} \times \text{トランザクションごとに } 4096 \text{ ファイル} \times \text{ファイルごとに } 3453 \text{ バイト}) \div 1,073,741,824 \text{ バイト} = 4.0 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。</p> $4 + 16 = 20 \text{ GB}$
アーカイブ・ログ: 毎日のフル・データベース・バックアップでの推奨サイズ	60 GB ¹	<p>3 つのバックアップ・サイクル全体でアーカイブ・ログを保管できるという要件があるため、活動ログの見積もりに 3 を掛けて、アーカイブ・ログの合計所要量を見積もります。</p> $4 \text{ GB} \times 3 = 12 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。</p> $12 + 48 = 60 \text{ GB}$
アーカイブ・ログ: 每週のフル・データベース・バックアップでの推奨サイズ	132 GB ¹	<p>3 つのサーバー・データベース・バックアップ・サイクル全体でアーカイブ・ログを保管できるという要件があるため、活動ログの見積もりに 3 を掛けて、アーカイブ・ログの合計所要量を見積もります。その結果に、フル・データベース・バックアップ間の日数を掛けます。</p> $(4 \text{ GB} \times 3) \times 7 = 84 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。</p> $84 + 48 = 132 \text{ GB}$

¹ この表内の値の例は、活動ログとアーカイブ・ログのサイズの計算方法を示すためにのみ使用しています。重複排除を使用しない本番環境では、活動ログの推奨される最小サイズは 16 GB です。重複排除を使用しない本番環境では、アーカイブ・ログの推奨される開始サイズは 48 GB です。ご使用の環境から値を補完し、その結果 16 GB および 48 GB より大きくなった場合は、その結果を使用して活動ログとアーカイブ・ログのサイズを調整します。

ログをモニターし、必要に応じてそれらのサイズを調整します。

例: データ重複排除操作の活動ログとアーカイブ・ログのサイズの見積もり:

データを重複排除する場合、活動ログとアーカイブ・ログのスペース所要量に対するその影響を考慮する必要があります。

活動ログとアーカイブ・ログのスペース所要量に影響を与える要因は次のとおりです。

重複排除されるデータの量

活動ログとアーカイブ・ログのスペースに対するデータ重複排除の影響は、

IBM Spectrum Protect サーバーのインストール

重複排除に適格なデータの割合に応じて異なります。重複排除できるデータの割合が比較的高い場合は、より多くのログ・スペースが必要です。

エクステントのサイズと数

重複識別プロセスによって識別されるエクステントごとに、約 1,500 バイトの活動ログ・スペースが必要です。例えば、重複識別プロセスによって 250,000 個のエクステントが識別される場合、活動ログの見積もりサイズは 358 MB です。

```
250,000 extents identified during each process x 1,500 bytes  
for each extent = 358 MB
```

以下のシナリオについて考えてみてください。300 個のバックアップ/アーカイブ・クライアントが、毎晩 100,000 個のファイルをバックアップします。このアクティビティーにより、30,000,000 ファイルの作業負荷が生じます。ファイルごとの平均エクステント数は 2 です。したがって、エクステントの総数は 60,000,000 になり、アーカイブ・ログのスペース所要量は 84 GB です。

```
60,000,000 extents x 1,500 bytes for each extent = 84 GB
```

重複識別プロセスは、ファイルの集合に対して作用します。集合は、TXNGROUPMAX サーバー・オプションで指定される、所定トランザクションに保管されるファイルで構成されます。TXNGROUPMAX サーバー・オプションがデフォルトの 4096 に設定されると想定します。ファイルごとの平均エクステント数が 2 である場合、各集合内のエクステントの総数は 8192 であり、活動ログに必要なスペースは 12 MB です。

```
8192 extents in each aggregate x 1500 bytes for each extent =  
12 MB
```

重複識別プロセスのタイミングと数

重複識別プロセスのタイミングと数も、活動ログのサイズに影響を与えます。上記の例で計算された 12 MB の活動ログ・サイズを使用すると、10 個の重複識別プロセスが並行して実行している場合、活動ログ上の並行負荷は 120 MB です。

```
12 MB for each process x 10 processes = 120 MB
```

ファイル・サイズ

重複識別のために処理されるラージ・ファイルも、活動ログのサイズに影響を与える場合があります。例えば、バックアップ/アーカイブ・クライアントが 80 GB のファイル・システム・イメージをバックアップすると思います。例えば、このファイル・システム・イメージに含まれているファイルが差分バックアップされる場合、このオブジェクトには、多くの重複エクステントがある可能性があります。例えば、ファイル・システム・イメージに 120 万個の重複エクステントがあるとします。このラージ・ファイル内の 120 万個のエクステントは、重複識別プロセスの単一のトランザクションを表します。この単一オブジェクトに必要な、活動ログ内の合計スペースは 1.7 GB です。

```
1,200,000 extents x 1,500 bytes for each extent = 1.7 GB
```

もっと小さい他の重複識別プロセスが、単一のラージ・オブジェクトの重複識別プロセスと同時に生じる場合、活動ログには十分なスペースがない可能性があります。例えば、ストレージ・プールの重複排除が使用可能であると

します。このストレージ・プールには、10 KB から数百 KB までの範囲にわたる、比較的小さい多数のファイルを含めて、データの混合があります。また、このストレージ・プールには、重複エクステントの割合が高い、ラージ・オブジェクトはほとんどありません。

スペース所要量だけでなく、並行トランザクションのタイミングと所要時間も考慮するには、活動ログの見積もりサイズを 2 倍に増やします。例えば、スペース所要量の計算が 25 GB (23.3 GB + 1.7 GB (ラージ・オブジェクトの重複排除用)) であるとします。重複排除プロセスが並行して実行される場合、活動ログの推奨サイズは 50 GB です。アーカイブ・ログの推奨サイズは 150 GB です。

次の表の例は、活動ログとアーカイブ・ログの計算を示しています。最初の表の例では、エクステントに平均サイズ 700 KB を使用します。2 番目の表の例では、平均サイズ 256 KB を使用します。これらの例が示すように、平均の重複排除エクステント・サイズ 256 KB の方が、活動ログの大きい見積もりサイズを示します。サーバーの作動上の問題を最小化または防止するために、本番環境における活動ログのサイズの見積もりには 256 KB を使用してください。

表 8. 平均の重複エクステント・サイズ 700 KB

項目	値の例		説明
重複排除対象の最大単一オブジェクトのサイズ	800 GB	4 TB	重複排除のための処理の細分性はファイル・レベルです。したがって、重複排除対象の最大の単一ファイルが、最大トランザクション、およびそれに応じた、活動ログとアーカイブ・ログ上の大きな負荷を表します。
エクステントの平均サイズ	700 KB	700 KB	重複排除アルゴリズムでは、可変ブロック方式を使用します。所定のファイルについて重複排除されるすべてのエクステントが同じサイズであるとは限らないので、この計算は、エクステントの平均サイズを前提としています。
所定ファイルのエクステント	1,198,372 ビット	6,135,667 ビット	これらの計算は、平均エクステント・サイズ (700 KB) を使用して、所定オブジェクトのエクステントの総数を表します。 800 GB のオブジェクトには、以下の計算式が使用されました。 $(800 \text{ GB} \div 700 \text{ KB}) = 1,198,372 \text{ bits}$ 4 TB のオブジェクトには、以下の計算式が使用されました。 $(4 \text{ TB} \div 700 \text{ KB}) = 6,135,667 \text{ bits}$
活動ログ: 単一の重複識別プロセス時に单一のラージ・オブジェクトの重複排除に必要な推奨サイズ	1.7 GB	8.6 GB	このトランザクションに必要な見積もり活動ログ・スペース。

IBM Spectrum Protect サーバーのインストール

表 8. 平均の重複エクステント・サイズ 700 KB (続き)

項目	値の例		説明
活動ログ: 推奨合計サイズ	66 GB ¹	79.8 GB ¹	<p>重複排除に加えてサーバーの作業負荷のその他の局面を検討した後、既存の見積もりに係数 2 を掛けます。これらの例では、単一のラージ・オブジェクトの重複排除に必要な活動ログ・スペースが、必要な活動ログ・サイズの前の見積もりと一緒に検討されます。</p> <p>複数のトランザクションと 800 GB のオブジェクトには、以下の計算式が使用されました。</p> $(23.3 \text{ GB} + 1.7 \text{ GB}) \times 2 = 50 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。</p> $50 + 16 = 66 \text{ GB}$ <p>複数のトランザクションと 4 TB のオブジェクトには、以下の計算式が使用されました。</p> $(23.3 \text{ GB} + 8.6 \text{ GB}) \times 2 = 63.8 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。</p> $63.8 + 16 = 79.8 \text{ GB}$
アーカイブ・ログ: 推奨サイズ	198 GB ¹	239.4 GB ¹	<p>活動ログの見積もりサイズに係数 3 を掛けます。</p> <p>複数のトランザクションと 800 GB のオブジェクトには、以下の計算式が使用されました。</p> $50 \text{ GB} \times 3 = 150 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。</p> $150 + 48 = 198 \text{ GB}$ <p>複数のトランザクションと 4 TB のオブジェクトには、以下の計算式が使用されました。</p> $63.8 \text{ GB} \times 3 = 191.4 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。</p> $191.4 + 48 = 239.4 \text{ GB}$

¹ この表内の値の例は、活動ログとアーカイブ・ログのサイズの計算方法を示すためにのみ使用しています。重複排除を使用する本番環境では、活動ログの推奨される最小サイズは 32 GB です。重複排除を使用する本番環境では、アーカイブ・ログの推奨される最小サイズは 96 GB です。ご使用の環境から値を補完し、その結果 32 GB および 96 GB より大きくなった場合は、その結果を使用して活動ログとアーカイブ・ログのサイズを調整します。

ログをモニターし、必要に応じてそれらのサイズを調整します。

表 9. 平均の重複エクステント・サイズ 256 KB

項目	値の例		説明
重複排除対象の最大単一オブジェクトのサイズ	800 GB	4 TB	重複排除のための処理の細分性はファイル・レベルです。したがって、重複排除対象の最大の単一ファイルが、最大トランザクション、およびそれに応じた、活動ログとアーカイブ・ログ上の大きな負荷を表します。
エクステントの平均サイズ	256 KB	256 KB	重複排除アルゴリズムでは、可変ブロック方式を使用します。所定のファイルについて重複排除されるすべてのエクステントが同じサイズであるとは限らないので、この計算は、エクステントの平均サイズを前提としています。
所定ファイルのエクステント	3,276,800 ビット	16,777,216 ビット	<p>これらの計算は、平均エクステント・サイズを使用して、所定オブジェクトのエクステントの総数を表します。</p> <p>複数のトランザクションと 800 GB のオブジェクトには、以下の計算式が使用されました。</p> $(800 \text{ GB} \div 256 \text{ KB}) = 3,276,800 \text{ bits}$ <p>複数のトランザクションと 4 TB のオブジェクトには、以下の計算式が使用されました。</p> $(4 \text{ TB} \div 256 \text{ KB}) = 16,777,216 \text{ bits}$
活動ログ: 単一の重複識別プロセス時に单一のラージ・オブジェクトの重複排除に必要な推奨サイズ	4.5 GB	23.4 GB	このトランザクションに必要な活動ログ・スペースの見積もりサイズ。
活動ログ: 推奨合計サイズ	71.6 GB ¹	109.4 GB ¹	<p>重複排除に加えてサーバーの作業負荷のその他の局面を検討した後、既存の見積もりに係数 2 を掛けます。これらの例では、单一のラージ・オブジェクトの重複排除に必要な活動ログ・スペースが、必要な活動ログ・サイズの前の見積もりと一緒に検討されます。</p> <p>複数のトランザクションと 800 GB のオブジェクトには、以下の計算式が使用されました。</p> $(23.3 \text{ GB} + 4.5 \text{ GB}) \times 2 = 55.6 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。</p> $55.6 + 16 = 71.6 \text{ GB}$ <p>複数のトランザクションと 4 TB のオブジェクトには、以下の計算式が使用されました。</p> $(23.3 \text{ GB} + 23.4 \text{ GB}) \times 2 = 93.4 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。</p> $93.4 + 16 = 109.4 \text{ GB}$

IBM Spectrum Protect サーバーのインストール

表 9. 平均の重複エクステント・サイズ 256 KB (続き)

項目	値の例		説明
アーカイブ・ログ: 推奨サイズ	214.8 GB ¹	328.2 GB ¹	<p>係数 3 を掛けた、活動ログの見積もりサイズ。</p> <p>800 GB のオブジェクトには、以下の計算式が使用されました。</p> $55.6 \text{ GB} \times 3 = 166.8 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。</p> $166.8 + 48 = 214.8 \text{ GB}$ <p>4 TB のオブジェクトには、以下の計算式が使用されました。</p> $93.4 \text{ GB} \times 3 = 280.2 \text{ GB}$ <p>以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。</p> $280.2 + 48 = 328.2 \text{ GB}$

¹ この表内の値の例は、活動ログとアーカイブ・ログのサイズの計算方法を示すためにのみ使用しています。重複排除を使用する本番環境では、活動ログの推奨される最小サイズは 32 GB です。重複排除を使用する本番環境では、アーカイブ・ログの推奨される最小サイズは 96 GB です。ご使用の環境から値を補完し、その結果 32 GB および 96 GB より大きくなった場合は、その結果を使用して活動ログとアーカイブ・ログのサイズを調整します。

ログをモニターし、必要に応じてそれらのサイズを調整します。

活動ログ・ミラー・スペース

活動ログ・ファイルを読み取れない場合にミラー・コピーを使用できるように、活動ログをミラーリングすることができます。存在することができる活動ログ・ミラーは 1 つのみです。

ログ・ミラーの作成が推奨オプションです。活動ログのサイズを増加すると、ログ・ミラーのサイズは自動的に増加します。ミラーの維持には 2 倍の入出力活動が必要なため、ログをミラーリングするとパフォーマンスに影響がある可能性があります。ログ・ミラーに必要な追加スペースが、ログ・ミラーを作成するかどうかを決める際のもう 1 つの考慮要因となります。

ミラー・ログ・ディレクトリーが満杯になると、サーバーは活動記録ログと db2diag.log にエラー・メッセージを発行します。サーバーのアクティビティーは続行します。

アーカイブ・フェイルオーバー・ログ・スペース

アーカイブ・フェイルオーバー・ログは、アーカイブ・ログ・ディレクトリーのスペースが使い尽くされた場合に、サーバーによって使用されます。

アーカイブ・フェイルオーバー・ログ・ディレクトリーを指定すると、アーカイブ・ログのスペースが使い尽くされた場合に生じる問題を防止することができます。アーカイブ・フェイルオーバー・ログ・ディレクトリーが置かれているアーカイブ・ログ・ディレクトリーとドライブの両方が、またはファイル・システムがフルになった場合、データは活動ログ・ディレクトリーに残ります。この状態は活動ログを満杯にする原因になり、これはサーバーを停止させる原因になります。

データベースおよび回復ログのスペース使用率のモニター

使用済みと使用可能な活動ログ・スペースの量を判別するには、**QUERY LOG** コマンドを発行します。データベースおよび回復ログ内のスペース使用率をモニターするために、メッセージがないか活動記録ログを調べることもできます。

活動ログ

使用可能な活動ログ・スペースの量が少なすぎる場合、活動記録ログに次のメッセージが表示されます。

ANR4531I:

IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER

活動ログ・スペースが指定の最大サイズを超えると、このメッセージが表示されます。IBM Spectrum Protect サーバーはフル・データベース・バックアップを開始します。

最大ログ・サイズを変更するには、サーバーを停止します。`dsmserv.opt` ファイルを開き、`ACTIVELOGSIZE` オプションに新しい値を指定します。終了したら、サーバーを再始動してください。

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP

活動ログ・スペースが指定の最大サイズを超えると、このメッセージが表示されます。手動でデータベースをバックアップする必要があります。

最大ログ・サイズを変更するには、サーバーを停止します。`dsmserv.opt` ファイルを開き、`ACTIVELOGSIZE` オプションに新しい値を指定します。終了したら、サーバーを再始動してください。

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER

使用可能な活動ログ・スペースに対する、使用済みの活動ログ・スペースの比率が、ログ使用率のしきい値を超えるました。フル・データベース・バックアップが少なくとも 1 回行われている場合、IBM Spectrum Protect サーバーは差分データベース・バックアップを開始します。そうでない場合、サーバーはフル・データベース・バックアップを開始します。

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION

使用可能な活動ログ・スペースに対する、使用済みの活動ログ・スペースの比率が、ログ使用率のしきい値を超えたしました。手動でデータベースをバックアップする必要があります。

アーカイブ・ログ

使用可能なアーカイブ・ログ・スペースの量が少なすぎる場合、活動記録ログに次のメッセージが表示されます。

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED

使用可能なアーカイブ・ログ・スペースに対する、使用済みのアーカイブ・ログ・スペースの比率が、ログ使用率のしきい値を超えるました。IBM Spectrum Protect サーバーは自動フル・データベース・バックアップを開始します。

データベース

データベース・アクティビティーに使用可能なスペースの量が少なすぎる場合、活動記録ログに次のメッセージが表示されます。

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2

使用済みのデータベース・スペースが、データベース・スペース使用率のしきい値を超えた。データベースのスペースを増やすには、**EXTEND DBSPACE** コマンド、**EXTEND DBSPACE** コマンド、または **DBDIR** パラメーターを指定した DSMSERV FORMAT ユーティリティーを使用してください。

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB

サーバー・データベース・ファイルが置かれているディレクトリー内の使用可能スペースが 1 GB 未満です。

DSMSERV FORMAT ユーティリティーまたは構成ウィザードを使用して IBM Spectrum Protect サーバーが作成されるときに、サーバー・データベースおよび回復ログも作成されます。そのほかに、データベース・マネージャーが使用するデータベース情報を保持するためのファイルが作成されます。このメッセージで指定されているパスは、データベース・マネージャーによって使用されるデータベース情報の場所を示します。このパスでスペースが使用可能でない場合、サーバーは機能できなくなります。

ファイル・システムにスペースを追加するか、ファイル・システムまたはディスク上のスペースを使用可能にする必要があります。

インストール・ロールバック・ファイルの削除

インストール処理中に保存された特定のインストール・ファイルを削除して、共有リソース・ディレクトリーのスペースを解放することができます。例えば、ロールバック操作に必要であった可能性があるファイルは、削除できるファイル・タイプです。

このタスクについて

不要になったファイルを削除するには、グラフィカル・インストール・ウィザードまたはコンソール・モードのコマンド・ラインのいずれかを使用します。

グラフィカル・ウィザードを使用したインストール・ロールバック・ファイルの削除

IBM Installation Manager ユーザー・インターフェースを使用して、インストール・プロセス中に保存されている特定のインストール・ファイルを削除することができます。

手順

1. IBM Installation Manager を開きます。

IBM Installation Manager がインストールされているディレクトリーで、
eclipse サブディレクトリー (例えば、/opt/IBM/InstallationManager/
eclipse) に移動し、次のコマンドを発行して IBM Installation Manager を開
始します。

```
./IBMMIM
```

2. 「ファイル」 > 「プリファレンス」をクリックします。
3. 「ロールバックのファイル」を選択します。
4. 「保存されたファイルの削除」をクリックし、「OK」をクリックします。

コマンド・ラインを使用したインストール・ロールバック・ファイル の削除

コマンド・ラインを使用してインストール・プロセス中に保存された特定のインス
トール・ファイルを削除することができます。

手順

1. IBM Installation Manager がインストールされているディレクトリーで、以下
のサブディレクトリーに移動します。

```
eclipse/tools
```

例えば次のとおりです。

```
/opt/IBM/InstallationManager/eclipse/tools
```

2. tools ディレクトリーから、IBM Installation Manager コマンド・ラインを開
始するために、以下のコマンドを発行します。

```
./imcl -c
```

3. 「プリファレンス」を選択するには P を入力します。
4. 「ロールバックのファイル」を選択するには 3 を入力します。
5. 「ロールバックのファイル」を削除するには D を入力します。
6. 変更を適用して「プリファレンス」メニューに戻るには A を入力します。
7. 「プリファレンス」メニューを終了するには C を入力します。
8. Installation Manager を終了するには X を入力します。

サーバー名の命名のベスト・プラクティス

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、以下の説明を参照してください。

インスタンス・ユーザー ID

インスタンス・ユーザー ID は、サーバー・インスタンスに関連する他の名前の基盤として使用されます。インスタンス・ユーザー ID はインスタンス所有者とも呼ばれます。

例えば次のとおりです: `tsminst1`

インスタンス・ユーザー ID は、データベースおよび回復ログ用に作成される全ディレクトリーの所有権または読み取り/書き込みアクセス権限を持っている必要があるユーザー ID です。サーバーを実行する場合の標準的な方法では、インスタンス・ユーザー ID の下で実行します。そのユーザー ID はすべての **FILE** 装置クラスに使用されるディレクトリーへの読み取り/書き込みアクセス権も持っている必要があります。

インスタンス・ユーザー ID のホーム・ディレクトリー

ホーム・ディレクトリーはインスタンス・ユーザー ID の作成時に作成できます。ホーム・ディレクトリーがまだない場合は、オプション (-m) を使用して作成します。ローカル設定に応じて、ホーム・ディレクトリーの形式は次のようになる可能性があります。`/home/instance_user_ID`

例: `/home/tsminst1`

ホーム・ディレクトリーは、ユーザー ID とセキュリティー設定用のプロファイルを収納するのに主に使用されます。

データベース・インスタンス名

データベース・インスタンス名は、サーバー・インスタンスの実行に使用するインスタンス・ユーザー ID と同じでなければなりません。

例: `tsminst1`

インスタンス・ディレクトリー

インスタンス・ディレクトリーは、特にサーバー・インスタンス用のファイル (サーバー・オプション・ファイルおよびその他のサーバー特有のファイル) を含むディレクトリーです。これには、任意の名前を付けることができます。簡単に識別できるようにするために、ディレクトリーをインスタンス名に結合する名前を使用してください。

インスタンス・ディレクトリーは、インスタンス・ユーザー ID のホーム・ディレクトリーのサブディレクトリーとして作成できます。例:

`/home/instance_user_ID/instance_user_ID`

次の例は、インスタンス・ディレクトリーをユーザー ID `tsminst1` のホーム・ディレクトリーに配置します: `/home/tsminst1/tsminst1`

別の場所にディレクトリーを作成することもできます。例:

`/tsmserver/tsminst1`

インスタンス・ディレクトリーには、サーバー・インスタンス用の次のファイルが保管されます。

- サーバー・オプション・ファイルの `dsmserv.opt`
- サーバーの鍵データベース・ファイル `cert.kdb`、および `.arm` ファイル（クライアントおよび他のサーバーが、サーバーの Secure Sockets Layer 証明書をインポートする際に使用します）
- `DEVCONFIG` サーバー・オプションが完全修飾名を指定していない場合、装置構成ファイル
- `VOLUMEHISTORY` サーバー・オプションが完全修飾名を指定していない場合、ボリューム・ヒストリー・ファイル
- 装置クラスのディレクトリーが完全に指定されていない場合、または完全修飾でない場合、`DEVTYPE=FILE` ストレージ・プール
- ユーザー出口
- トレース出力（完全修飾でない場合）

データベース名

データベース名は、どのサーバー・インスタンスでも常に `TSMDB1` です。この名前は変更できません。

サーバー名

サーバー名は IBM Spectrum Protect の内部名で、複数の IBM Spectrum Protect サーバー間の通信に関連した操作に使用されます。例としては、サーバー間通信およびライブラリーの共用などがあります。

またサーバー名は、Operations Centerにサーバーを追加するときにも使用されます。それにより、サーバーはそのインターフェースを使用して管理できます。各サーバーごとに固有の名前を使用してください。Operations Centerで（または `QUERY SERVER` コマンドから）簡単に識別できるようにするために、サーバーのロケーションまたは目的を反映する名前を使用してください。IBM Spectrum Protect サーバーをハブ・サーバーまたはスポーク・サーバーとして構成した後は、その名前を変更しないでください。

ウィザードを使用する場合、推奨されるデフォルト名は、使用しているシステムのホスト名です。ユーザーの使用環境で意味のある別の名前を使用することができます。システム上に複数のサーバーがあり、かつウィザードを使用する場合は、それらのサーバーのいずれか 1 つにのみデフォルト名を使用できます。サーバーごとに固有の名前を入力する必要があります。

例えば次のとおりです。

PAYROLL

SALES

データベース・スペースおよび回復ログ用のディレクトリー

これらのディレクトリーは、ユーザーの使用環境の慣例に従って命名できます。簡単に識別できるようにするために、そのディレクトリーをサーバー・インスタンスに結合する名前の使用を検討してください。

IBM Spectrum Protect サーバーのインストール

例えばアーカイブ・ログの場合、次のような名前を指定します。

```
/tsminst1_archlog
```

インストール・ディレクトリー

IBM Spectrum Protect サーバー用のインストール・ディレクトリーには、サーバー、DB2、デバイス、言語、およびその他のディレクトリーがあります。各ディレクトリーには、いくつかの追加のディレクトリーが含まれています。

(/opt/tivoli/tsm/server/bin) は、サーバー・コードとライセンスが含まれるデフォルト・ディレクトリーです。

IBM Spectrum Protect サーバーのインストールの一部としてインストールされる DB2 製品は、DB2 情報源に記載されているディレクトリー構造を持っています。サーバー・ディレクトリーと同様に、これらのディレクトリーおよびファイルを保護してください。デフォルト・ディレクトリーは /opt/tivoli/tsm/db2 です。

米国英語、ドイツ語、フランス語、イタリア語、スペイン語、ブラジル・ポルトガル語、韓国語、日本語、中国語（繁体字、簡体字、GBK、Big5）、およびロシア語がサポートされています。

第 2 章 サーバー・コンポーネントのインストール

バージョン 8.1.5 サーバー・コンポーネントをインストールするには、インストール・ウィザード、コンソール・モードでのコマンド・ライン、またはサイレント・モードを使用できます。

このタスクについて

IBM Spectrum Protect インストール・ソフトウェアを使用して、次のコンポーネントをインストールできます。

- サーバー

ヒント: サーバー・コンポーネントを選択するときに、データベース (DB2)、Global Security Kit (GSKit)、および IBM Java ランタイム環境 (JRE) が自動的にインストールされます。

- サーバー言語
- ライセンス
- 装置
- IBM Spectrum Protect for SAN
- Operations Center

本書を使用して V8.1.5 のサーバーをインストールする場合は、約 30 分から 45 分程度かかります。

インストール・パッケージの入手

IBM Spectrum Protect インストール・パッケージは、IBM ダウンロード・サイト (Passport Advantage® または IBM Fix Centralなど) から入手できます。

始める前に

ファイルのダウンロードを予定している場合、ファイルを正しくダウンロードできるように、最大ファイル・サイズに関するシステム・ユーザー制限を無制限に設定してください。

1. 最大ファイル・サイズ値を照会するには、次のコマンドを発行します。
`ulimit -Hf`
2. 最大ファイル・サイズのシステム・ユーザー制限が無制限に設定されていない場合、ご使用のオペレーティング・システムの資料の指示に従って、無制限に変更してください。

手順

1. 以下のいずれかの Web サイトから該当するパッケージ・ファイルをダウンロードします。
 - パスポート・アドバンテージ または Fix Central からサーバー・パッケージをダウンロードします。

IBM Spectrum Protect サーバーのインストール

- 最新情報、更新、および保守修正については、IBM サポート・ポータルにアクセスしてください。
2. IBM ダウンロード・サイトからパッケージをダウンロードした場合は、以下のステップを実行します。
- a. 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。スペース要件については、ダウンロード文書を参照してください。
 - IBM Spectrum Protect 技術情報 4042944
 - IBM Spectrum Protect Extended Edition 技術情報 4042945
 - IBM Spectrum Protect for Data Retention 技術情報 4042946
 - b. パッケージ・ファイルを、選択したディレクトリーにダウンロードします。パスに含める文字数は 128 文字以下でなければならない。必ず、インストール・ファイルを空のディレクトリーに抽出します。インストール・ファイルは、前に抽出したファイルやその他のファイルが含まれるディレクトリーには抽出しないでください。
 - c. 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、次のコマンドを発行してファイル許可を変更します。
`chmod a+x package_name.bin`
 - d. 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、次のようなダウンロード・ファイルの名前です。
- 8.1.x.000-IBM-SPSRV-Linuxx86_64.bin*
8.1.x.000-IBM-SPSRV-Linuxs390x.bin
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
3. IBM Spectrum Protect のインストール方式を次のの中から 1 つ選択します。
- 57 ページの『インストール・ウィザードを使用した IBM Spectrum Protect のインストール』
 - 58 ページの『コンソール・モードを使用した IBM Spectrum Protect のインストール』
 - 59 ページの『サイレント・モードで IBM Spectrum Protectをインストール』
4. IBM Spectrum Protect 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、IBM サポート・ポータル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。

インストール・ウィザードを使用した IBM Spectrum Protect 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、サーバーをインストールできます。

始める前に

インストールを始める前に、次のアクションを実行します。

- 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。オペレーティング・システムの言語が、デフォルトで、インストール・ウィザードの言語になります。

手順

以下の方法を使用して IBM Spectrum Protect をインストールします。

オプション	説明
ダウンロードしたパッケージからソフトウェアをインストールする場合:	<ol style="list-style-type: none"> パッケージをダウンロードしたディレクトリーに変更します。 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。 <code>./install.sh</code>

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。

インストール・ログ・ファイルは、Installation Manager ツールから「ファイル」>「ログの表示」をクリックすると表示できます。これらのログ・ファイルを収集するには、Installation Manager ツールから「ヘルプ」>「問題分析のためのデータをエクスポート」をクリックします。

- サーバーおよびコンポーネント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、IBM サポート・ポータルにアクセスしてください。「Downloads (fixes and PTFs)」をクリックして、適用できる修正があれば適用します。
- 新規 サーバーをインストールした後、「IBM Spectrum Protect のインストール後の最初のステップの実行」を参照して、サーバーの構成方法について確認します。

コンソール・モードを使用した **IBM Spectrum Protect** のインストール

コンソール・モードでコマンド・ラインを使用して、IBM Spectrum Protect をインストールすることができます。

始める前に

インストールを始める前に、次のアクションを実行します。

- 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。オペレーティング・システムの言語が、デフォルトで、インストール・ウィザードの言語になります。

手順

以下の方法を使用して IBM Spectrum Protect をインストールします。

オプション	説明
ダウンロードしたパッケージからソフトウェアをインストールする場合:	<ol style="list-style-type: none">パッケージをダウンロードしたディレクトリーに変更します。次のコマンドを発行して、コンソール・モードでインストール・ウィザードを開始します。 <code>./install.sh -c</code> <p>オプション: コンソール・モードのインストールの一部として、応答ファイルを生成します。コンソール・モードのインストール・オプションを完了し、「要約」パネルで「G」を指定して、応答を生成します。</p>

次のタスク

- インストール・プロセス中にエラーが発生した場合、それらのエラーは、IBM Installation Manager ログ・ディレクトリーに保管されている次のようなログ・ファイルに記録されます。
`/var/ibm/InstallationManager/logs`
- サーバーおよびコンポーネント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、IBM サポート・ポータルにアクセスしてください。
「Downloads (fixes and PTFs)」をクリックして、適用できる修正があれば適用します。
- 新規 サーバーをインストールした後、「IBM Spectrum Protect のインストール後の最初のステップの実行」を参照して、サーバーの構成方法について確認します。

サイレント・モードで IBM Spectrum Protectをインストール

サーバーをサイレント・モードでインストールまたはアップグレードすることができます。サイレント・モードのインストールでは、メッセージをコンソールに送信せずに、メッセージおよびエラーをログ・ファイルに保管します。

始める前に

サイレント・インストール・メソッドの使用時にデータ入力を行うには、応答ファイルを使用できます。`input` ディレクトリーに以下のサンプル応答ファイルが含まれています。このディレクトリーは、インストール・パッケージが解凍されるディレクトリーです。

`install_response_sample.xml`

IBM Spectrum Protect コンポーネントをインストールするには、このファイルを使用します。

`update_response_sample.xml`

IBM Spectrum Protect コンポーネントをアップグレードするには、このファイルを使用します。

これらのファイルには、不要な警告を回避するのに役立つデフォルト値が含まれています。これらのファイルを使用するには、ファイルに記載されている指示に従ってください。

応答ファイルをカスタマイズしたい場合は、ファイル内のオプションを変更することができます。応答ファイルについては、応答ファイルを参照してください。

手順

1. 応答ファイルを作成します。サンプル応答ファイルを変更するか、または独自のファイルを作成することができます。
2. サイレント・モードでサーバーと Operations Center をインストールする場合、応答ファイルの Operations Center トラストストアのパスワードを作成します。

`install_response_sample.xml` ファイルを使用中の場合には、ファイルの以下の行にパスワードを追加します。ここで、`mypassword` はパスワードを表します。

```
<variable name='ssl.password' value='mypassword' />
```

このパスワードについて詳しくは、インストール・チェックリストを参照してください。

ヒント: Operations Center をアップグレードする際に、`update_response_sample.xml` ファイルを使用する場合はトラストストアのパスワードは不要です。

3. インストール・パッケージが抽出されたディレクトリーから次のコマンドを発行して、サイレント・インストールを開始します。値 `response_file` は、応答ファイル・パスとファイル名を示します。
 - `./install.sh -s -input response_file -acceptLicense`

IBM Spectrum Protect サーバーのインストール

次のタスク

- インストール・プロセス中にエラーが発生した場合、それらのエラーは、IBM Installation Manager ログ・ディレクトリーに保管されている次のようなログ・ファイルに記録されます。
`/var/ibm/InstallationManager/logs`
- サーバーおよびコンポーネント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、IBM サポート・ポータルにアクセスしてください。
「**Downloads (fixes and PTFs)**」をクリックして、適用できる修正があれば適用します。
- 新規 サーバーをインストールした後、「IBM Spectrum Protect のインストール後の最初のステップの実行」を参照して、サーバーの構成方法について確認します。

サーバー言語パッケージのインストール

サーバーの翻訳により、サーバーで米国英語以外の言語によるメッセージとヘルプを表示できます。この翻訳により、各ロケールのきまりに応じた日付、時刻、数値の形式も使用できるようになります。

始める前に

ストレージ・エージェントの言語パッケージのインストール方法については、ストレージ・エージェントの言語パックの構成を参照してください。

サーバー言語のロケール

デフォルトの言語パッケージ・オプションを使用するか、または他の言語パッケージを選択して、サーバーのメッセージおよびヘルプを表示します。

IBM Spectrum Protect サーバーのメッセージとヘルプ用に、次のデフォルト言語オプション用の言語パッケージが自動的にインストールされます:

- LANGUAGE en_US

デフォルト以外の言語またはロケールについては、インストール済み環境の要件に応じて適切な言語パッケージをインストールしてください。

以下に示す言語を使用できます。

表 10. Linux のサーバー言語

LANGUAGE	LANGUAGE のオプション値
中国語 (簡体字)	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
中国語 (繁体字)	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
米国英語	en_US
	en_US.utf8

表 10. Linux のサーバー言語 (続き)

LANGUAGE	LANGUAGE のオプション値
フランス語	fr_FR
	fr_FR.utf8
ドイツ語	de_DE
	de_DE.utf8
イタリア語	it_IT
	it_IT.utf8
日本語	ja_JP
	ja_JP.utf8
韓国語	ko_KR
	ko_KR.utf8
ブラジル・ポルトガル語	pt_BR
	pt_BR.utf8
ロシア語	ru_RU
	ru_RU.utf8
スペイン語	es_ES
	es_ES.utf8

制約事項: Operations Center のユーザーの場合、Web ブラウザーがサーバーと同じ言語を使用していないと、一部の文字が正しく表示されないことがあります。この問題が発生した場合は、サーバーと同じ言語を使用するようにブラウザーを設定してください。

言語パッケージの構成

言語パッケージを構成すると、サーバーのメッセージとヘルプが米国英語以外の言語で表示されます。インストール・パッケージは IBM Spectrum Protect で提供されています。

このタスクについて

特定のロケールのサポートを設定するには、次のいずれかのタスクを完了してください。

- サーバー・オプション・ファイル内の LANGUAGE オプションをご使用のロケール名に設定します。 例えば次のとおりです。
it_IT ロケールを使用するには、LANGUAGE オプションを it_IT に設定します。 60 ページの『サーバー言語のロケール』を参照してください。
- サーバーをフォアグラウンドで始動する場合は、LC_ALL 環境変数をサーバー・オプション・ファイルに設定されている値に一致するように設定します。 例えば、イタリア語の環境変数を設定するには、次の値を入力します。

```
export LC_ALL=it_IT
```

ロケールが正常に初期化されると、そのロケールによって、サーバーの日付、時刻、および数値がフォーマットされます。ロケールが正常に初期化されないと、サーバーは米国英語のメッセージ・ファイルと、日付、時刻、および数値形式を使用

します。

言語パッケージの更新

言語パッケージの変更または更新は、IBM Installation Manager を使用して行うことができます。

このタスクについて

同じ IBM Spectrum Protect インスタンス内では別の言語パッケージをインストールできます。

- IBM Installation Manager の「変更」機能を使用して、別の言語パッケージをインストールします。
- IBM Installation Manager の「更新」機能を使用して、新規バージョンの言語パッケージに更新します。

ヒント: IBM Installation Manager では、更新 は、インストール済みソフトウェア・パッケージに対する更新および修正を検出してインストールすることを意味します。この意味では、更新 とアップグレード は同義です。

第 3 章 IBM Spectrum Protect のインストール後の最初のステップの実行

バージョン 8.1.5 をインストールした後は、構成の準備をします。IBM Spectrum Protect インスタンスを構成する場合は、構成ウィザードを使用する方法をお勧めします。

このタスクについて

1. カーネル・パラメーター値を更新します。
64 ページの『カーネル・パラメーターのチューニング』を参照してください。
2. サーバー・インスタンス用のディレクトリーとユーザー ID を作成します。
65 ページの『サーバー・インスタンスのユーザー ID とディレクトリーの作成』を参照してください。
3. サーバー・インスタンスを構成します。以下のいずれかのオプションを選択してください。
 - 推奨されている方法である構成ウィザードを使用します。 68 ページの『構成ウィザードを使用した IBM Spectrum Protect の構成』を参照してください。
 - 手動で新規インスタンスを構成します。 69 ページの『手動でのサーバー・インスタンスの構成』を参照してください。手動構成の間に次のステップを完了します。
 - a. ディレクトリーをセットアップして IBM Spectrum Protect インスタンスを作成します。 69 ページの『サーバー・インスタンスの作成』を参照してください。
 - b. サーバーとクライアント間の通信をセットアップするために、サンプル・ファイルをコピーして新規のサーバー・オプション・ファイルを作成します。 71 ページの『サーバーとクライアントの間の通信の構成』を参照してください。
 - c. **DSMSERV FORMAT** コマンドを発行してデータベースをフォーマットします。 75 ページの『データベースとログのフォーマット』を参照してください。
 - d. データベース・バックアップのためにシステムを構成します。 76 ページの『データベース・バックアップのためのデータベース・マネージャーの準備』を参照してください。
4. データベース再編成時に制御を行うためのオプションを構成します。 78 ページの『サーバー・データベース保守のためのサーバー・オプションの構成』を参照してください。
5. サーバー・インスタンスがまだ始動していない場合は、始動します。
80 ページの『サーバー・インスタンスの開始』を参照してください。
6. ライセンスを登録します。 87 ページの『ライセンスの登録』を参照してください。

IBM Spectrum Protect サーバーのインストール

7. データベース・バックアップのためにシステムを準備します。 87 ページの『データベース・バックアップ操作のためのサーバーの準備』を参照してください。
8. サーバーをモニターします。 88 ページの『サーバーのモニター』を参照してください。

カーネル・パラメーターのチューニング

IBM Spectrum Protect および DB2 の Linux 上でのインストールおよび運用を正しく行うには、カーネル構成パラメーターを更新する必要があります。

このタスクについて

これらのパラメーターを更新しないと、DB2 および IBM Spectrum Protect のインストールが失敗する場合があります。インストールが成功した場合でも、パラメーター値を設定しないと、操作上の問題が発生する可能性があります。

カーネル・パラメーターの更新

DB2 は、プロセス間通信 (IPC) のカーネル・パラメーター値を優先設定値に自動的に増やします。

このタスクについて

Linux サーバーでカーネル・パラメーターを更新するには、以下のステップを実行します。

手順

1. `ipcs -l` コマンドを発行して、パラメーターの値をリストします。
2. 結果を分析して、現在のシステムで変更が必要かどうかを判断します。 変更が必要な場合は、`/etc/sysctl.conf` ファイル内でパラメーターを設定することができます。システムの始動時に、パラメーター値が適用されます。

次のタスク

Red Hat Enterprise Linux 6 (RHEL6) の場合は、システムの始動時に IBM Spectrum Protect サーバーを自動的に開始する前に、`kernel.shmmmax` パラメーターを `/etc/sysctl.conf` ファイル内に設定する必要があります。

Linux の DB2 データベースについて詳しくは、DB2 製品情報を参照してください。

推奨値

カーネル・パラメーターは必ず十分な値に設定にして、IBM Spectrum Protect サーバーの実行時に運用上の問題が発生しないようにしてください。

このタスクについて

以下の表に、IBM Spectrum Protect および DB2 の両方を実行する際のカーネル・パラメーターの推奨設定値を記載します。

パラメーター	説明	推奨値
kernel.randomize_va_space	kernel.randomize_va_space 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。 <code>kernel.randomize_va_space=0</code> の値を 0 に設定すると、ASLR が無効になります。 DB2 データ・サーバーは、特定の共有メモリー・オブジェクトについては固定アドレスに依存しており、アクティビティーによっては ASLR がエラーを起こすことがあります。 Linux ASLR および DB2 に関する詳細については、 http://www.ibm.com/support/docview.wss?uid=swg21365583 の技術情報を参照してください。	0
vm.swappiness	vm.swappiness 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、「DB2 製品情報」を参照してください。	0
vm.overcommit_memory	vm.overcommit_memory パラメーターは、カーネル・パラメーターが割り振ることができ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、「DB2 製品情報」を参照してください。	0

サーバー・インスタンスのユーザー ID とディレクトリーの作成

IBM Spectrum Protect サーバー・インスタンスのユーザー ID を作成し、サーバー・インスタンスがデータベースおよび回復ログ用に必要とするディレクトリーを作成します。

始める前に

このタスクを完了する前に、サーバーのスペースの計画についての情報を検討してください。 30 ページの『サーバーの詳細を計画するためのワークシート』を参照してください。

手順

1. 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。 後のステップでサーバー・インスタンスを作成するときにこのユーザー ID を使用します。

サーバー・インスタンスの所有者になるユーザー ID とグループを作成します。

- a. ユーザーおよびグループをセットアップする管理ユーザー ID から以下のコマンドを実行できます。 そのユーザーのホーム・ディレクトリー内にユーザー ID とグループを作成します。

IBM Spectrum Protect サーバーのインストール

制約事項: ユーザー ID には、小文字 (a-z)、数字 (0-9)、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 文字以内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。

例えば、グループ *tsmsrvrs* にユーザー ID *tsminst1* を作成します。次の例は、オペレーティング・システム・コマンドを使用したこのユーザー ID とグループの作成方法を示したものです。

```
groupadd tsmsrvrs -g 1111  
useradd -d /home/tsminst1 -u 2222 -g 1111 -s /bin/bash tsminst1  
passwd tsminst1
```

制約事項: DB2 は、LDAP を介した直接的なオペレーティング・システムのユーザー認証をサポートしていません。

- b. 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。

2. サーバーに必要なディレクトリーを作成します。

次の表の各項目ごとに空のディレクトリーを作成して、ディレクトリーが先ほど作成した新規ユーザー ID によって所有されていることを確認します。活動ログ・ディレクトリー、アーカイブ・ログ・ディレクトリー、およびデータベース・ディレクトリーの各ディレクトリーに、関連するストレージをマウントします。

項目	ディレクトリーを作成するためのコマンド例	ディレクトリー
サーバーのインスタンス・ディレクトリー。これは、特にこのサーバー・インスタンス用のファイル (サーバー・オプション・ファイルおよびその他のサーバー特有のファイル) を含むディレクトリーです)。	<code>mkdir /tsminst1</code>	
データベース・ディレクトリー	<code>mkdir /tsmdb001</code> <code>mkdir /tsmdb002</code> <code>mkdir /tsmdb003</code> <code>mkdir /tsmdb004</code>	
活動ログ・ディレクトリー	<code>mkdir /tsmlog</code>	
アーカイブ・ログ・ディレクトリー	<code>mkdir /tsmarchlog</code>	

次の表の各項目ごとに空のディレクトリーを作成して、ディレクトリーが先ほど作成した新規ユーザー ID によって所有されていることを確認します。活動ログ・ディレクトリー、アーカイブ・ログ・ディレクトリー、およびデータベース・ディレクトリーの各ディレクトリーに、関連するストレージをマウントします。

項目	ディレクトリーを作成するためのコマンド例	ディレクトリー
オプション: 活動ログのログ・ミラーのディレクトリー	<code>mkdir /tsmlogmirror</code>	
オプション: 2 次アーカイブ・ログ・ディレクトリー (アーカイブ・ログのフェイルオーバー・ロケーション)	<code>mkdir /tsmarchlogfailover</code>	

DSMSERV FORMAT ユーティリティーまたは構成ウィザードを使用して最初にサーバーを作成した時に、サーバー・データベースとリカバリー・ログが作成されます。そのほかに、データベース・マネージャーが使用するデータベース情報を保持するためのファイルが作成されます。

- 新規ユーザー ID をログオフします。

IBM Spectrum Protect サーバーの構成

サーバーをインストールし、構成準備をした後は、サーバー・インスタンスを構成します。

このタスクについて

次のいずれかのオプションを選択して、IBM Spectrum Protect サーバー・インスタンスを構成します。

- ローカル・システムで IBM Spectrum Protect 構成ウィザードを使用します。
68 ページの『構成ウィザードを使用した IBM Spectrum Protect の構成』を参照してください。
- 手動で新規 IBM Spectrum Protect インスタンスを構成します。 69 ページの『手動でのサーバー・インスタンスの構成』を参照してください。 手動構成の間に次のステップを完了します。
 - ディレクトリーをセットアップして IBM Spectrum Protect インスタンスを作成します。 69 ページの『サーバー・インスタンスの作成』を参照してください。
 - IBM Spectrum Protect サーバーとクライアント間の通信をセットアップするため、サンプル・ファイルをコピーして新規のサーバー・オプション・ファイルを作成します。 71 ページの『サーバーとクライアントの間の通信の構成』を参照してください。
 - DSMSERV FORMAT コマンドを発行してデータベースをフォーマットします。 75 ページの『データベースとログのフォーマット』を参照してください。

4. データベース・バックアップのためにシステムを構成します。 76 ページの『データベース・バックアップのためのデータベース・マネージャーの準備』を参照してください。

構成ウィザードを使用した **IBM Spectrum Protect** の構成

ウィザードは、ガイド付きのサーバー構成手段を提供します。 グラフィカル・ユーザー・インターフェース (GUI) を使用することにより、手動で行うと複雑ないくつかの構成ステップを避けることができます。 IBM Spectrum Protect サーバー・プログラムがインストールされているシステム上でウィザードを開始します。

始める前に

構成ウィザードを使用する前に、構成の準備をするために前述すべてのステップを実行する必要があります。これらのステップには、IBM Spectrum Protect のインストール、データベース・ディレクトリーとログ・ディレクトリーの作成、およびサーバー・インスタンス用のディレクトリーとユーザー ID の作成が含まれます。

手順

1. 次の要件を満たしているようにしてください。
 - 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) プロトコルが使用可能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/ ディレクトリー内の 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 デーモン・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 でシステム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。
 - 以下のファイルのバックアップ・コピーは、安全でセキュアな場所に保管する必要があります。
 - マスター暗号鍵ファイル (dsmkeydb.*)
 - サーバー証明書と秘密鍵のファイル (cert.*)
2. ウィザードのローカル・バージョンを開始するには、以下のようにします。
`/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 ID を使用する場合のみ実行できます。

指示に従って構成を完了します。 ウィザードは停止と再始動ができますが、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。

手動でのサーバー・インスタンスの構成

IBM Spectrum Protect バージョン 8.1.5をインストールした後、構成ウィザードを使用する代わりに IBM Spectrum Protect を手動で構成できます。

サーバー・インスタンスの作成

db2icrt コマンドを発行して、IBM Spectrum Protect インスタンスを作成します。

このタスクについて

1 つのワークステーション上に 1 つ以上のサーバー・インスタンスを持つことができます。

重要: **db2icrt** コマンドを実行する前に、以下の項目を確認してください。

- ユーザー (/home/tsminst1) のホーム・ディレクトリーが存在する。ホーム・ディレクトリーが存在しない場合は、作成する必要があります。

インスタンス・ディレクトリーには、IBM Spectrum Protect サーバーで生成される次のファイルが保管されます。

- サーバー・オプション・ファイルの `dsmerv.opt`
 - サーバーの鍵データベース・ファイル `cert.kdb`、および `.arm` ファイル（クライアントおよび他のサーバーが、サーバーの Secure Sockets Layer 証明書をインポートする際に使用します）
 - `DEVCONFIG` サーバー・オプションが完全修飾名を指定していない場合、装置構成ファイル
 - `VOLUMEHISTORY` サーバー・オプションが完全修飾名を指定していない場合、ボリューム・ヒストリー・ファイル
 - 装置クラスのディレクトリーが完全に指定されていない場合、または完全修飾でない場合、`DEVTYPE=FILE` ストレージ・プール
 - ユーザー出口
 - トレース出力 (完全修飾でない場合)
 - 以下のファイルのバックアップ・コピーは、安全でセキュアな場所に保管する必要があります。
 - マスター暗号鍵ファイル (`dsmkeydb.*`)
 - サーバー証明書と秘密鍵のファイル (`cert.*`)
 - root ユーザーおよびインスタンス・ユーザーの ID は、シェル構成ファイルに対する書き込み権限を持っている必要があります。シェル構成ファイル (`.profile` など) がホーム・ディレクトリーに存在する。詳しくは、DB2 製品情報を参照してください。Linux および UNIX の環境変数の設定を検索してください。
1. root ユーザー ID を使用してログインし、IBM Spectrum Protect インスタンスを作成します。インスタンスの名前は、そのインスタンスを所有するユーザーと同じ名前でなければなりません。**db2icrt** コマンドを使用して、次のコマンドを 1 行で入力してください。

```
/opt/tivoli/tsm/db2(instance/db2icrt -a server -u
instance_name instance_name
```

IBM Spectrum Protect サーバーのインストール

例えば、このインスタンスのユーザー ID が `tsminst1` の場合は、次のコマンドを使用してインスタンスを作成します。コマンドを 1 行で入力します。

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u  
tsminst1 tsminst1
```

要確認: この時点から先は、IBM Spectrum Protect サーバーを構成する際に、この新規ユーザー ID を使用します。`root` ユーザー ID をログアウトし、新規インスタンス・ユーザー ID でログインします。

2. データベースのデフォルト・ディレクトリーを、サーバーのインスタンス・ディレクトリーと同じになるように変更します。複数のサーバーがある場合は、それぞれのサーバーのインスタンス ID でログインします。次のコマンドを出します。

```
db2 update dbm cfg using dftdbpath instance_directory
```

例えば、`instance_directory` がインスタンス・ユーザー ID である場合は次のようにします。

```
db2 update dbm cfg using dftdbpath /tsminst1
```

3. ライブラリー・パスを変更して、サーバー操作に必要なライブラリーを組み込むようにしてください。

ヒント: 以下の例では、ディレクトリーを示します。

- `server_bin_directory` は、サーバーのインストール・ディレクトリーのサブディレクトリーです。例えば、`/opt/tivoli/tsm/server/bin` です。
- `instance_users_home_directory` は、インスタンス・ユーザーのホーム・ディレクトリーです。例えば、`/home/tsminst1` です。
- 以下のいずれかのファイルを更新して、DB2 またはサーバーの始動時のライブラリー・パスを設定します。インスタンス・ユーザーが使用するように構成されているシェルごとに更新します。

Bash または Korn シェル:

```
instance_users_home_directory/sql1ib/userprofile
```

C シェルの場合 :

```
instance_users_home_directory/sql1ib/usercshrc
```

- インスタンス・ユーザーが使用するように構成されているシェルごとに更新します。

Bash または Korn シェル:次の項目を `instance_users_home_directory/sql1ib/userprofile` ファイルに 1 行で追加します。

```
export LD_LIBRARY_PATH=server_bin_directory/  
dbbkapi:/usr/local/ibm/gsk8_64/lib64:/opt/ibm/lib:/opt/  
ibmlib64:$LD_LIBRARY_PATH
```

C シェルの場合 :次の項目を `instance_users_home_directory/sql1ib/usercshrc` ファイルに 1 行で追加します。

```
setenv LD_LIBRARY_PATH server_bin_directory/dbbkapi:/  
usr/local/ibm/gsk8_64/lib64:/  
opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
```

要確認: 以下の項目は、ライブラリー・パス内で、他の項目の前に含まれている必要があります。

- `server_bin_directory/dbbkapi`
- `/usr/local/ibm/gsk8_64/lib64`

4. 新規サーバー・オプション・ファイルを作成します。『サーバーとクライアントの間の通信の構成』を参照してください。

サーバーとクライアントの間の通信の構成

IBM Spectrum Protect のインストール中に、デフォルトのサンプル・サーバー・オプション・ファイルの `dsmserv.opt.smp` が `/opt/tivoli/tsm/server/bin` ディレクトリーに作成されます。新規サーバー・オプション・ファイルを作成して、サーバーとクライアント間の通信をセットアップする必要があります。このためには、サンプル・ファイルをサーバー・インスタンスのディレクトリーにコピーします。

このタスクについて

必ずサーバー・インスタンス・ディレクトリー (例えば、`/tsminst1`) があることを確認し、サンプル・ファイルをこのディレクトリーにコピーします。作成したファイルに `dsmserv.opt` という名前を付け、オプションを編集します。サーバー・データベースを初期化する前にこのセットアップを実行してください。サンプル・オプション・ファイル内の各例やデフォルト・エントリーはコメントの形であり、アスタリスク (*) で始まる行です。オプションに大/小文字の区別はなく、キーワードと値の間に 1 つ以上のブランク・スペースを使用できます。

オプション・ファイルを編集する場合は、以下のガイドラインに従ってください。

- オプションを活動化する場合は、その行の先頭にあるアスタリスクを取り除きます。
- 任意の列でオプションの入力を開始します。
- 1 行当たり 1 つのオプションだけを入力し、そのオプションは複数行にわたってはなりません。
- キーワードに複数のエントリーを作成すると、IBM Spectrum Protect サーバーは最後のエントリーを使用します。

サーバー・オプション・ファイルを変更した場合は、その変更を有効にするためにサーバーを再始動する必要があります。

次の通信方式を 1 つ以上指定できます。

- TCP/IP バージョン 4 またはバージョン 6
- 共有メモリー
- Secure Sockets Layer (SSL)

ヒント: パスワードは LDAP ディレクトリー・サーバーによって認証できます。または IBM Spectrum Protect サーバーによってパスワードを認証することもできます。LDAP ディレクトリー・サーバーを使用して認証されるパスワードは、より高度なシステム・セキュリティーを提供します。

IBM Spectrum Protect サーバーのインストール

TCP/IP オプションの設定:

IBM Spectrum Protect サーバーの TCP/IP オプションの範囲から選択するか、デフォルトを保存します。

このタスクについて

以下は、システムのセットアップに使用できる TCP/IP オプションのリストの例です。

```
commmethod      tcpip
tcpport        1500
tcpwindowsize   0
tcpnodelay     yes
```

ヒント: TCP/IP バージョン 4、バージョン 6、またはその両方を使用できます。

TCPPORT

TCP/IP と SSL 通信のサーバー・ポート・アドレス。 デフォルト値は 1500 です。

TCPWINDOWSIZE

データの送信時または受信時に使用される TCP/IP バッファーのサイズを指定します。セッションで使用されるウィンドウ・サイズは、サーバーおよびクライアントのウィンドウ・サイズより小さいサイズです。大きいウィンドウ・サイズを使用するとメモリー使用量は増加しますが、パフォーマンスが改善される可能性があります。

0 から 2048 の整数を指定することができます。オペレーティング・システムに対するデフォルト・ウィンドウ・サイズを使用する場合は、0 を指定します。

TCPNODELAY

サーバーが少量のメッセージを送信するかどうか、あるいは TCP/IP にメッセージをバッファーに入れさせるかを指定します。少量のメッセージを送信すると、スループットは向上しますが、ネットワークを介して送信されるパケットの数は増加します。少量のメッセージを送信する場合は YES を、TCP/IP にバッファーに入れさせる場合には NO を指定します。デフォルト値は Yes です。

TCPADMINIMPORT

サーバーの TCP/IP 通信ドライバーがクライアント・セッション以外の、TCP/IP または SSL 対応の通信要求を待つポート番号を指定します。デフォルト値は TCPPORT です。

SSLTCPPORT

(SSL のみ) サーバー TCP/IP 通信ドライバーがコマンド・ライン・バックアップ/アーカイブ・クライアントおよびコマンド・ライン管理クライアントの SSL 対応セッションの要求を待機する Secure Sockets Layer (SSL) ポート番号を指定します。

SSLTCPADMINIMPORT

(SSL のみ) サーバー TCP/IP 通信ドライバーがコマンド・ライン管理クライアントの 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。

共用メモリー・オプションの設定:

同一システム上のクライアントとサーバー間で共用メモリー通信を使用できます。共用メモリーを使用するためには、TCP/IP バージョン 4 をシステム上にインストールしておく必要があります。

このタスクについて

以下の例は、共用メモリー設定を示したものです。

```
commethod      sharedmem  
shmpport      1510
```

この例で、**SHMPORt** は、共用メモリーを使用するときのサーバーの TCP/IP ポート・アドレスを指定します。**SHMPORt** オプションを使用して、別の TCP/IP ポートを指定します。デフォルトのポート・アドレスは 1510 です。

IBM Spectrum Protect サーバー・オプション・ファイルで、毎回異なる値を使用して、**COMMETHOD** を複数回使用することができます。例えば、次の例が可能です。

```
commethod tcpip  
commethod sharedmem
```

共用メモリーを使用しているときにサーバーから次のメッセージが表示される場合があります:

```
ANR9999D shmcomm.c(1598): ThreadId<39>  
Error from msgget (2), errno = 28
```

このメッセージは、メッセージ・キューの作成が必要だが、メッセージ・キューの最大数 (**MSGMNI**) のシステムしきい値を超えることを意味します。

ご使用システムでのメッセージ・キューの最大数 (**MSGMNI**) を調べるには、次のコマンドを発行します。

```
cat /proc/sys/kernel/msgmni
```

システムの **MSGMNI** 値を増加するには、次のコマンドを発行します。

```
sysctl -w kernel.msgmni=n
```

ここで、**n** はシステムで許可するメッセージ・キューの最大数です。

Secure Sockets Layer オプションの設定:

Secure Sockets Layer (SSL) を使用することで、データとパスワードをより安全に保護することができます。

始める前に

SSL は、サーバーとクライアント間に暗号化されたセッションを作成するための標準テクノロジーです。 SSL は、公開された通信パスを介して通信する場合のセキュア・チャネルを、サーバーとクライアントに提供します。SSL では、デジタル証明書を使用してサーバーの ID が検証されます。

IBM Spectrum Protect サーバーのインストール

システム・パフォーマンスを向上できるよう、SSL はセッションで必要な場合にのみ使用するようにしてください。所要量の増大に対応できるよう、IBM Spectrum Protect サーバー上でプロセッサー・リソースを追加することを検討してください。

データベースとログのフォーマット

サーバー・インスタンスを初期化するには、**DSMSERV FORMAT** ユーティリティーを使用します。データベースおよびリカバリー・ログを初期化中は、他のサーバー活動は許可されません。

サーバー通信をセットアップしたら、データベースを初期化することができます。インスタンス・ユーザー ID を使用してログインしていることを確実にしてください。このディレクトリーは、スペース不足になる可能性のあるファイル・システム上に指定しないでください。特定のディレクトリー（例えば、アーカイブ・ログ）が使用不可または一杯になると、サーバーは停止します。詳しくは、「キャパシティ一計画」を参照してください。

出口リスト・ハンドラーの設定

各サーバー・インスタンスの **DB2NOEXITLIST** レジストリー変数を ON に設定します。サーバー・インスタンス所有者としてシステムにログオンし、次のコマンドを発行してください。

```
db2set -i server_instance_name DB2NOEXITLIST=ON
```

例えば次のとおりです。

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```

サーバー・インスタンスの初期化

サーバー・インスタンスを初期化するには、**DSMSERV FORMAT** ユーティリティーを使用します。例えば、サーバー・インスタンス・ディレクトリーが /tsminst1 である場合、以下のコマンドを発行します。

```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsize=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

ヒント: 複数のディレクトリーを指定する場合、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、必ず基礎となるファイル・システムのサイズが等しくなるようにしてください。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、並列プリフェッヂ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。

ヒント: **DSMSERV FORMAT** コマンドを発行しても DB2 が開始しない場合、ファイル・システム・マウント・オプション NOSUID を使用不可に設定する必要がある場合があります。このオプションが、DB2 インスタンスの所有者ディレクトリーが含まれているファイル・システム、あるいは DB2 データベース、活動ログ、アーカイブ・ログ、フェイルオーバー・ログ、またはミラーリングされたログが含まれているファイル・システムに設定されている場合は、システムを開始するために、このオプションを使用不可にする必要があります。

NOSUID オプションを使用不可にした後、ファイル・システムを再マウントしてから、次のコマンドを発行して DB2 を開始します。

```
db2start
```

関連情報:

➡ DSMSERV FORMAT (データベースおよびログのフォーマット)

データベース・バックアップのためのデータベース・マネージャーの準備

データベース内のデータを IBM Spectrum Protect にバックアップするには、データベース・マネージャーを使用可能にして、IBM Spectrum Protect アプリケーション・プログラミング・インターフェース (API) を構成する必要があります。

このタスクについて

IBM Spectrum Protect V7.1 から、サーバーの手動構成時に API パスワードを設定する必要がなくなりました。手動構成プロセスで API パスワードを設定した場合、データベースをバックアップしようとすると失敗することがあります。

IBM Spectrum Protect 構成ウィザードを使用してサーバー・インスタンスを作成する場合は、これらのステップを実行する必要はありません。手動でインスタンスを構成する場合は、**BACKUP DB** コマンドまたは **RESTORE DB** コマンドを発行する前に、以下の手順を実行してください。

重要: データベースを使用できない場合は、IBM Spectrum Protect サーバー全体が利用不可になります。データベースが失われてリカバリーできない場合、そのサーバーによって管理されているデータをリカバリーすることは困難か不可能な場合があります。したがって、データベースのバックアップを行うことは、非常に重要なことです。

以下のコマンドでは、例の中の値を、ご使用の実際の値に置き換えてください。例では、サーバー・インスタンス・ユーザー ID として `tsminst1` を使用し、サーバー・インスタンス・ディレクトリーとして `/tsminst1` を使用し、サーバー・インスタンス・ユーザーのホーム・ディレクトリーとして `/home/tsminst1` を使用しています。

- データベース・インスタンスの IBM Spectrum Protect API 環境変数構成を設定します。

- `tsminst1` ユーザー ID を使用してログインします。
- ユーザー `tsminst1` がログインするときには、必ず DB2 環境が正しく初期化されているようにしてください。DB2 環境は、`/home/tsminst1/sql1ib/db2profile` スクリプトの実行によって初期化されます。通常このスクリプトは、ユーザー ID のプロファイルから自動的に実行されます。`.profile` ファイルが、インスタンス・ユーザーのホーム・ディレクトリー (例えば、`/home/tsminst1/.profile`) に存在することを確認してください。`.profile` が `db2profile` スクリプトを実行しない場合は、次の行を追加してください。

```
if [ -f /home/tsminst1/sql1ib/db2profile ]; then
    . /home/tsminst1/sql1ib/db2profile
fi
```
- `instance_directory/sql1ib/userprofile` ファイルに、以下の行を追加します。

```
DSMI_CONFIG=server_instance_directory/tsmdbmgr.opt
DSMI_DIR=server_bin_directory/dbbkapi
DSMI_LOG=server_instance_directory
export DSMI_CONFIG DSMI_DIR DSMI_LOG
```

ここで、

- *instance_directory* は、サーバー・インスタンス・ユーザーのホーム・ディレクトリーです。
- *server_instance_directory* は、サーバー・インスタンス・ディレクトリーです。
- *server_bin_directory* は、サーバー bin ディレクトリーです。デフォルトのロケーションは /opt/tivoli/tsm/server/bin です。

instance_directory/sql/lib/usercshrc ファイルに、以下の行を追加します。

```
setenv DSMI_CONFIG=server_instance_directory/tsmdbmgr.opt
setenv DSMI_DIR=server_bin_directory/dbbkapi
setenv DSMI_LOG=server_instance_directory
```

2. ログオフして、tsminst1 として再度ログインするか、次のコマンドを発行します。

```
. ~/profile
```

ヒント: 最初のドット (.) 文字の後に必ずスペースを入力します。

3. *server_instance* ディレクトリー (この例では、/tsminst1 ディレクトリー) に tsmdbmgr.opt という名前のファイルを作成し、次の行を追加します。

```
SERVERNAME TSMDBMGR_TSMINST1
```

要確認: SERVERNAME の値は、tsmdbmgr.opt ファイルと dsm.sys ファイルで一貫している必要があります。

4. root ユーザーとして、以下の行を IBM Spectrum Protect API dsm.sys 構成ファイルに追加します。デフォルトで、dsm.sys 構成ファイルは、次のデフォルト・ロケーションにあります。

```
server_bin_directory/dbbkapi/dsm.sys
servername TSMDBMGR_TSMINST1
commethod tcpip
tcpserveraddr localhost
tcpport 1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

ここで、

- *servername* は、tsmdbmgr.opt ファイルの *servername* 値と一致します。
- *commethod* は、データベース・バックアップのためにサーバーへの接続に使用されるクライアント API を指定します。この値は、tcpip または sharedmem を指定できます。共有メモリーについて詳しくは、ステップ 5 を参照してください。
- *tcpserveraddr* は、クライアント API がデータベース・バックアップのためにサーバーへの接続に使用するサーバー・アドレスを指定します。データベースを確実にバックアップできるようにするために、この値を localhost にする必要があります。

IBM Spectrum Protect サーバーのインストール

- *tcpport* は、クライアント API がデータベース・バックアップのためにサーバーへの接続に使用するポート番号を指定します。*dsmerv.opt* サーバー・オプション・ファイルで指定されているのと同じ *tcpport* 値を入力してください。
- *errorlogname* は、クライアント API がデータベース・バックアップ中に発生したエラーを記録するエラー・ログを指定します。このログは通常、サーバー・インスタンス・ディレクトリー内にあります。ただし、インスタンス・ユーザー ID が書き込み許可を持っている任意の場所にこのログを配置できます。
- *nodename* は、クライアント API がデータベース・バックアップ中にサーバーに接続するために使用するノード名を指定します。データベースを確実にバックアップできるようにするために、この値を *\$\$_TSMDBMGR_\$\$* にする必要があります。

重要: *PASSWORDACCESS generate* オプションを *dsm.sys* 構成ファイルに追加しないでください。このオプションは、データベース・バックアップが失敗する原因になることがあります。

5. オプション: 共有メモリーを使用してデータベースをバックアップするようにサーバーを構成します。これにより、プロセッサーの負荷を軽減し、スループットを向上できる可能性があります。次の手順を実行してください。
 - a. *dsmerv.opt* ファイルを確認します。ファイルに以下の行がない場合は、追加してください。

```
commmethod sharedmem  
shmpport port_number
```

ここで、*port_number* は、共有メモリーに使用するポートを指定します。

- b. *dsm.sys* 構成ファイルで、以下の行を見つけます。

```
commmethod tcpip  
tcpserveraddr localhost  
tcpport port_number
```

指定された行を、以下の行で置き換えます。

```
commmethod sharedmem  
shmpport port_number
```

ここで、*port_number* は、共有メモリーに使用するポートを指定します。

サーバー・データベース保守のためのサーバー・オプションの構成

データベースの増加およびサーバーのパフォーマンスに関する問題の回避を図る目的で、サーバーは自動的にデータベース表をモニターし、必要に応じて再編成します。サーバーの実動使用を開始する前に、再編成の実行時刻を制御するサーバー・オプションを設定してください。データ重複排除を使用する予定の場合は、索引再編成を実行するオプションを必ず使用可能にしてください。

このタスクについて

表と索引の再編成には、かなりのプロセッサー・リソース、活動ログ・スペース、およびアーカイブ・ログ・スペースが必要です。データベース・バックアップは再

編成よりも優先するため、処理がオーバーラップせずに再編成が完了できるよう に、再編成の時刻と期間を選択してください。

サーバー・データベースの索引および表の再編成を最適化することができます。こ うすると、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こ とができます。方法については、技術情報 1683633 を参照してください。

これらのサーバー・オプションをサーバーの稼働中に更新した場合、更新された値 を有効にするには、サーバーを停止して再始動する必要があります。

手順

1. サーバー・オプションを変更します。

サーバー・オプション・ファイル `dsmserv.opt` を編集します。このファイル は、サーバー・インスタンス・ディレクトリーにあります。サーバー・オプショ ン・ファイルを編集する場合は、以下の指針に従ってください。

- オプションを使用可能にする場合は、その行の先頭にあるアスタリスクを削 除します。
- 任意の行でオプションを入力します。
- 1 行につき 1 つのオプションのみを入力してください。オプションとその値 の全体が 1 行になければなりません。
- ファイル内の 1 つのオプションに複数のエントリーがある場合、サーバーは 最後のエントリーを使用します。

使用可能なサーバー・オプションを表示する場合は、`/opt/tivoli/tsm/server/bin` ディレクトリーにあるサンプル・ファイル `dsmserv.opt.smp` を確認しま す。

2. データ重複排除を使用する予定の場合は、**ALLOWREORGINDEX** サーバー・オプショ ンを有効にしてください。次のオプションと値をサーバー・オプション・ファ イルに追加します。

`allowreorgindex yes`

3. 再編成の開始時刻と期間を制御する **REORGEGINETIME** および **REORGDURATION** の サーバー・オプションを設定します。サーバーが一番すいているときに再編成が 実行されるように、時刻と期間を選択してください。これらのサーバー・オプ ションは、表と索引の両方の再編成処理を制御します。

- a. **REORGEGINETIME** サーバー・オプションを使用して、再編成が開始される時 刻を設定します。24 時間制を使用して時刻を指定します。例えば、再編成 の開始時刻を 8:30 p.m. に設定するには、次のオプションと値をサーバー・ オプション・ファイルに指定します。

`reorgbegintime 20:30`

- b. サーバーが再編成を開始できる時間間隔を設定します。例えば、 **REORGEGINETIME** サーバー・オプションで設定された時刻から 4 時間の間に サーバーが再編成を開始できるように指定するには、次のオプションと値を サーバー・オプション・ファイルに指定します。

`reorgduration 4`

4. サーバーの稼働中にサーバー・オプション・ファイルを更新した場合は、サーバ ーを停止して再始動してください。

サーバー・インスタンスの開始

インスタンス・ユーザー ID (推奨される方法) または root ユーザー ID を使用して、サーバーを始動できます。

始める前に

アクセス許可とユーザー制限を正しく設定したことを確認します。手順については、81 ページの『アクセス権限およびユーザー制限の確認』を参照してください。

このタスクについて

インスタンス・ユーザー ID を使用してサーバーを始動すると、セットアップ・プロセスが簡単になり、潜在的な問題を避けることができます。ただし、場合によっては、root ユーザー ID を使用してサーバーを始動することが必要な場合があります。例えば、root ユーザー ID を使用して、サーバーが特定のデバイスにアクセスできるようにします。インスタンス・ユーザー ID または root 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セットアップすることができます。

保守タスクや再構成タスクを実行する必要がある場合は、サーバーを保守モードで始動します。

手順

サーバーを始動するには、次のいずれかをアクションを実行します。

- インスタンス・ユーザー ID を使用して、サーバーを始動します。

手順については、83 ページの『インスタンス・ユーザー ID からのサーバーの始動』を参照してください。

- root ユーザー ID を使用して、サーバーを始動します。

サーバーを始動する権限を root ユーザー ID に与える方法については、サーバーを始動する権限の root ユーザー ID への付与 (V7.1.1) を参照してください。

root ユーザー ID を使用したサーバーの始動方法については、root ユーザー ID からのサーバーの始動 (V7.1.1) を参照してください。

- サーバーを自動的に開始します。

手順については、83 ページの『Linux システムでのサーバーの自動始動』を参照してください。

- 保守モードでのサーバーの始動。

手順については、85 ページの『保守モードでのサーバーの始動』を参照してください。

アクセス権限およびユーザー制限の確認

サーバーを開始する前にアクセス権限とユーザー制限を確認してください。

このタスクについて

ulimits とも呼ばれるユーザー限度を検証しないと、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を検出する可能性があります。また、オープン・ファイルの最大数に対するシステム全体の限度も確認する必要があります。システム全体の限度は、ユーザー限度以上でなければなりません。

手順

1. サーバー・インスタンスのユーザー ID がサーバーを始動する許可を持っていることを確認します。
2. 始動する予定のサーバー・インスタンスについて、サーバー・インスタンス・ディレクトリー内のファイルの読み取りおよび書き込みの権限を持っていることを確認します。`dsmServ.opt` ファイルがサーバー・インスタンス・ディレクトリーに存在していること、およびそのファイルにサーバー・インスタンスのパラメーターが含まれていることを確認してください。
3. サーバーが磁気テープ・ドライブ、メディア・チェンジャー、または取り外し可能なメディア・デバイスに接続されており、インスタンス・ユーザー ID を使用してサーバーを始動する予定の場合、インスタンス・ユーザー ID にこれらのデバイスに対する読み取り/書き込み権限を付与します。許可を設定するには、次のいずれかをアクションを実行します。
 - システムが IBM Spectrum Protect 専用で、IBM Spectrum Protect 管理者のみがアクセス権限を持っている場合、デバイス特殊ファイルを全ユーザーによる書き込みが可能になるようにします。オペレーティング・システムのコマンド・ラインで、次のコマンドを発行します。


```
chmod +w /dev/rmtX
```
 - システムに複数のユーザーが存在する場合、IBM Spectrum Protect インスタンス・ユーザー ID を特殊装置ファイルの所有者にすることにより、アクセス権限を制限できます。オペレーティング・システムのコマンド・ラインで、次のコマンドを発行します。


```
chmod u+w /dev/rmtX
```
 - 同一システムで複数のユーザー・インスタンスが稼働中の場合、グループ名を変更 (例えば、TAPEUSERS など) し、各 IBM Spectrum Protect インスタンス・ユーザー ID をそのグループに追加します。次に、デバイス特殊ファイルの所有権をグループ TAPEUSERS に所属するように変更し、それらをグループ書き込み可能にします。オペレーティング・システムのコマンド・ラインで、次のコマンドを発行します。


```
chmod g+w /dev/rmtX
```
4. IBM Spectrum Protect デバイス・ドライバーおよび **autoconf** ユーティリティーを使用している場合、インスタンス・ユーザー ID に対して読み取り/書き込み権限を付与するには、**-a** オプションを使用します。
5. DB2 との対話中のサーバー障害を防ぐには、カーネル・パラメーターを調整します。

IBM Spectrum Protect サーバーのインストール

カーネル・パラメーターの調整についての説明は、64 ページの『カーネル・パラメーターのチューニング』を参照してください。

- 表に示された指針に基づいて、以下のユーザー制限を確認します。

表 11. ユーザー制限 (*ulimit*) 値

ユーザー制限タイプ	推奨値	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	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	無制限	<code>ulimit -Hd</code>
最大ファイル・サイズ	無制限	<code>ulimit -Hf</code>
オープン・ファイルの最大数	65536	<code>ulimit -Hn</code>
最大プロセッサー時間 (秒単位)	無制限	<code>ulimit -Ht</code>

ユーザー制限を変更するには、ご使用のオペレーティング・システムの資料の指示に従ってください。

ヒント: スクリプトを使用して自動的にサーバーを始動する予定の場合は、スクリプトでユーザー制限を設定できます。

- 最大ユーザー・プロセス数 (*nproc* 設定) のユーザー制限が最小推奨値 16384 に設定されていることを確認します。

- 現行のユーザー制限を確認するには、インスタンス・ユーザー ID を使用して `ulimit -Hu` コマンドを実行します。 例えば次のとおりです。

```
[user@Machine ~]$ ulimit -Hu  
16384
```

- 最大ユーザー・プロセス数の制限が 16384 に設定されていない場合は、値を 16384 に設定します。

以下の行を `/etc/security/limits.conf` ファイルに追加します。

```
instance_user_id      -      nproc      16384
```

ここで、*instance_user_id* は、サーバー・インスタンス・ユーザー ID を指定します。

サーバーが Red Hat Enterprise Linux 6 オペレーティング・システムにインストールされている場合は、`/etc/security/limits.d` ディレクトリー内の `/etc/security/limits.d/90-nproc.conf` ファイルを編集して、ユーザー制限を設定します。このファイルは、`/etc/security/limits.conf` ファイル内の設定値をオーバーライドします。

ヒント: 最大ユーザー・プロセス数のユーザー制限のデフォルト値は、Linux オペレーティング・システムの一部のディストリビューションおよびバージョンで変更されました。デフォルト値は 1024 です。この値を最小推奨値の 16384 に変更しないと、サーバーに障害が起きたり、停止したりする可能性があります。

インスタンス・ユーザー ID からのサーバーの始動

インスタンス・ユーザー ID からサーバーを始動するには、インスタンス・ユーザー ID を使用してログインし、サーバー・インスタンス・ディレクトリーから該当するコマンドを発行します。

始める前に

アクセス権限およびユーザー制限が正しく設定されていることを確認します。手順については、81 ページの『アクセス権限およびユーザー制限の確認』を参照してください。

手順

1. サーバーのインスタンス・ユーザー ID を使用して、IBM Spectrum Protect がインストールされているシステムにログインします。
2. db2profile スクリプトを実行するユーザー・プロファイルがない場合、以下のコマンドを発行します。

```
. /home/tsminst1/sql1lib/db2profile
```

ヒント: db2profile スクリプトを自動的に実行するためのユーザー ID ログイン・スクリプトの更新方法については、DB2 資料を参照してください。

3. サーバー・インスタンス・ディレクトリーから次のコマンドを 1 行で発行して、サーバーを始動します。

```
usr/bin/dsmserv
```

ヒント: このコマンドはフォアグラウンドで実行されるため、管理者 ID を設定して、サーバー・インスタンスに接続できます。

例えば、サーバー・インスタンスの名前が tsminst1 であり、サーバー・インスタンス・ディレクトリーが /tsminst1 である場合、以下のコマンドを発行して、インスタンスを開始できます。

```
cd /tsminst1
. ~/sql1lib/db2profile
/usr/bin/dsmserv
```

Linux システムでのサーバーの自動始動

Linux オペレーティング・システムでサーバーを自動的に始動するには、**dsmserv.rc** スクリプトを使用します。

始める前に

カーネル・パラメーターが正しく設定されていることを確認します。手順については、64 ページの『カーネル・パラメーターのチューニング』を参照してください。

サーバーは、インスタンス所有者ユーザー ID で実行するようにしてください。

アクセス権限およびユーザー制限が正しく設定されていることを確認します。手順については、81 ページの『アクセス権限およびユーザー制限の確認』を参照してください。

IBM Spectrum Protect サーバーのインストール

このタスクについて

dsmserv.rc スクリプトは、サーバーのインストール・ディレクトリー (/opt/tivoli/tsm/server/bin など) にあります。

dsmserv.rc スクリプトは、サーバーを手動で始動するためにも、/etc/rc.d/init.d ディレクトリーに項目を追加してサーバーを自動的に始動するためにも使用できます。このスクリプトは、**CHKCONFIG** や **SERVICE** などの Linux ユーティリティーと連動します。

手順

自動的に始動するようにしたいサーバー・インスタンスごとに、以下の手順を実行します。

1. **dsmserv.rc** スクリプトのコピーを /init.d ディレクトリー (例えば、/etc/rc.d/init.d) に置きます。

スクリプトのコピーのみを変更するようにしてください。元のスクリプトは変更しないでください。

2. サーバー・インスタンスの所有者名と一致するようにスクリプト・コピーを名前変更します。例えば、tsminst1 などのようにします。

スクリプトは、サーバー・インスタンス・ディレクトリーが *home_directory/tsminst1* であると仮定して作成されています。例えば /home/tsminst1/tsminst1 のようになります。

3. サーバー・インスタンス・ディレクトリーが *home_directory/tsminst1* ではない場合、次の行をスクリプト・コピー内に配置します。

```
instance_dir="${instance_home}/tsminst1"
```

この行を、ご使用のサーバー・インスタンス・ディレクトリーを指すように変更します。例えば、次のようにします。

```
instance_dir="/tsminst1"
```

4. スクリプト・コピーで、次の行を見つけます。

```
# pidfile: /var/run/dsmserv_instancename.pid
```

インスタンス名の値をサーバー・インスタンス所有者の名前に変更します。例えば、サーバー・インスタンス所有者が tsminst1 である場合、この行を次のように更新します。

```
# pidfile: /var/run/dsmserv_tsminst1.pid
```

5. サーバーを自動的に始動する実行レベルを構成します。ネットワーキングをオンにした状態で、**CHKCONFIG** ユーティリティーなどのツールを使用して、マルチユーザー・モードに対応する値を指定します。一般的に、オペレーティング・システムおよびその構成に応じて、3 または 5 の実行レベルを使用します。マルチユーザー・モードおよび実行レベルについて詳しくは、ご使用のオペレーティング・システムの資料を参照してください。

6. サーバーを始動または停止するには、以下のいずれかのコマンドを発行します。

- サーバーを開始する場合:

```
service tsminst1 start
```

- サーバーを停止する場合:

```
service tsminst1 stop
```

例

この例では以下の値を使用します。

- インスタンス所有者は `tsminst1` です。
- サーバー・インスタンス・ディレクトリーは `/home/tsminst1/tsminst1` です。
- `dsmservc.rc` スクリプトのコピーには、`tsminst1` という名前が付けられています。
- **CHKCONFIG** ユーティリティーを使用して、実行レベル 3、4、および 5 で開始するようにスクリプトを構成します。

```
cp /opt/tivoli/tsm/server/bin/dsmservc.rc /etc/rc.d/init.d/tsminst1
sed -i 's/dsmservc_instancename.pid/dsmservc_tsminst1.pid/' /etc/rc.d/init.d/tsminst1
chkconfig --list tsminst1
service tsminst1 supports chkconfig, but is not referenced in
any runlevel (run 'chkconfig --add tsminst1')
chkconfig --add tsminst1
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig --level 345 tsminst1 on
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

関連情報:

 サーバー始動スクリプト: `dsmservc.rc`

保守モードでのサーバーの始動

保守タスクや再構成タスクの実行中の中断を回避するために、保守モードでサーバーを始動することができます。

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 `dsmservc.opt` を編集する必要はありません。

IBM Spectrum Protect サーバーのインストール

- 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。

```
dsmServ 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方法を使用して、サーバーを始動します。

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。

サーバーの停止

オペレーティング・システムに制御を戻す必要が生じた場合、サーバーを停止することができます。管理およびクライアント・ノードの接続が失われるのを避けるために、サーバーを停止するのは、現行のセッションが完了またはキャンセルされたあとだけにしてください。

このタスクについて

サーバーを停止するには、IBM Spectrum Protect コマンド・ラインから次のコマンドを発行します。

```
halt
```

管理クライアントを指定してサーバーに接続できないものの、サーバーを停止したい場合は、プロセス ID 番号 (pid) を指定した **kill** コマンドを使用して、プロセスを取り消す必要があります。pid は初期設定時に表示されます。

重要: **kill** コマンドを発行する前に、必ず IBM Spectrum Protect サーバーの正しいプロセス ID を知っているようにしてください。

サーバーの稼働元ディレクトリーにある *dsmServ.v6lock* ファイルは、強制終了するプロセスのプロセス ID を識別するために使用できます。 ファイルを表示するには、次のように入力します。

```
cat /instance_dir/dsmServ.v6lock
```

サーバーを停止するには、次のコマンドを発行します。

```
kill -23 dsmServ_pid
```

ここで、*dsmServ_pid* はプロセス ID 番号です。

ライセンスの登録

データのバックアップなどのサーバー操作の開始後にデータを失うことのないよう、購入した IBM Spectrum Protect のライセンス機能は、直ちにライセンス登録を行ってください。

このタスクについて

この操作には、**REGISTER LICENSE** コマンドを使用します。

例: ライセンスの登録

基本の IBM Spectrum Protect のライセンスを登録します。

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

データベース・バックアップ操作のためのサーバーの準備

自動および手動のデータベース・バックアップ操作のためにサーバーを準備するには、テープまたはファイルの装置クラスを指定し、その他のステップを実行するようにします。

手順

1. IBM Spectrum Protect 構成が完了していることを確認します。 サーバーの構成に構成ウィザード (dsmicfgx) を使用しなかった場合は、データベース・バックアップのためにサーバーを構成するステップを手動で実行したことを確認してください。
2. データベースのバックアップに使用する装置クラスを選択し、マスター暗号鍵を保護して、パスワードを設定します。 これらすべてのアクションは、管理コマンド・ラインから **SET DBRECOVERY** コマンドを発行することで実行します。

```
set dbrecovery device_class_name protectkeys=yes password=password_name
```

ここで *device_class_name* は、データベース・バックアップに使用する装置クラスを指定し、*password_name* はパスワードを指定します。

装置クラス名を指定する必要があります。指定しないとバックアップは失敗します。 **PROTECTKEYS=YES** を指定すると、データベース・バックアップ操作中にマスター暗号鍵がバックアップされるようになります。

重要: 8 文字以上の強いパスワードを作成してください。 このパスワードは忘れないようにしてください。 データベース・バックアップにパスワードを指定した場合、データベースをリストアするために **RESTORE DB** コマンドに同じパスワードを指定する必要があります。

例

データベース・バックアップにサーバーのマスター暗号鍵のコピーを含めるかどうか指定するには、次のコマンドを実行します。

```
set dbrecovery dbback protectkeys=yes password=protect8991
```

単一システムでの複数のサーバー・インスタンスの実行

システム上に複数のサーバー・インスタンスを作成することができます。それぞれのサーバー・インスタンスには独自のインスタンス・ディレクトリーと、データベース・ディレクトリーおよびログ・ディレクトリーがあります。

1 つのサーバーのメモリーおよびシステムのその他の所要量に、そのシステムで計画されているサーバー・インスタンス数を掛けます。

サーバーの 1 つのインスタンス用のファイル・セットは、同じシステムの別のサーバー・インスタンスで使用されるファイルとは別個に保管されます。新規インスタンス・ユーザーの作成を含めて、新規インスタンスごとに 69 ページの『サーバー・インスタンスの作成』のステップを使用します。

各サーバーによって使用されるシステム・メモリーを管理するために、**DBMEMPERCENT** サーバー・オプションを使用して、システム・メモリーのパーセンテージを制限します。すべてのサーバーが同等に重要な場合は、各サーバーに同じ値を使用します。1 つのサーバーが実動サーバーで、他のサーバーがテスト・サーバーである場合、実動サーバーの値をテスト・サーバーより高い値に設定します。

ディレクトリーは、V7.1 から V8.1 に直接アップグレードすることができます。詳しくは、アップグレードのセクション（95 ページの『第 5 章 V8.1 へのアップグレード』）を参照してください。アップグレードするときに、システム上に複数のサーバーがある場合、インストール・ウィザードを 1 回だけ実行する必要があります。インストール・ウィザードは、元のすべてのサーバー・インスタンスのデータベース情報および変数情報を収集します。

IBM Spectrum Protect V6.3 から V8.1.5 にアップグレードするときに、システム上に複数のサーバーがある場合、DB2 V9.7 に存在するすべてのインスタンスが除去され、DB2 V11.1 で再作成されます。ウィザードは、それぞれのデータベースについて `db2 upgrade db dbname` コマンドを実行します。システム上の各インスタンスのデータベース環境変数も、アップグレード・プロセス中に再構成されます。

関連タスク:

- ➡ [单一システムでの複数のサーバー・インスタンスの実行 \(V7.1.1\)](#)

サーバーのモニター

実動環境でサーバーの使用を始めるときに、サーバーによって使用されるスペースをモニターして、スペースの量が十分であることを確認します。必要な場合は、スペースを調整します。

手順

1. 活動ログ・サイズが必ずサーバー・インスタンスの処理する作業負荷に適正になるように、活動ログをモニターします。

サーバー作業負荷が通常予期されるレベルに達すると、活動ログによって使用されるスペースは、活動ログ・ディレクトリーの使用可能スペースの 80% から 90% になります。この時点で、スペースを增量する必要が生じることがあります。

す。スペースの増量が必要かどうかは、サーバー作業負荷のトランザクションのタイプによって決まります。トランザクションの特性が、活動ログのスペースがどのように使用されるかに影響します。

以下のトランザクション特性が、活動ログのスペース使用量に影響する可能性があります。

- バックアップ操作でのファイルの数とサイズ。
 - 多くの小さいファイルをバックアップするファイル・サーバーなどのクライアントでは、短時間に完了する数多くのトランザクションが発生する可能性があります。これらのトランザクションでは、大量のスペースが活動ログに使用される可能性がありますが、短時間に限られます。
 - 少数のトランザクションで大量のデータをバックアップする、メール・サーバーやデータベース・サーバーなどのクライアントでは、完了に時間がかかる少数のトランザクションが発生する可能性があります。これらのトランザクションでは、活動ログに使用されるスペースは少ないものの、長時間使用される可能性があります。
- ネットワーク接続のタイプ
 - 高速ネットワーク接続で行われるバックアップ操作の場合、トランザクションはより短時間で完了します。これらのトランザクションは、より短時間、活動ログのスペースを使用します。
 - 比較的遅い接続で行われるバックアップ操作の場合、トランザクションは完了までにより長い時間がかかります。これらのトランザクションは、より長時間、活動ログのスペースを使用します。

多様な特性をもつトランザクションをサーバーが処理している場合は、活動ログの使用するスペースは、時間とともに大幅に増加したり減少したりする可能性があります。そのようなサーバーの場合は、活動ログの通常の使用スペースのパーセンテージが通常は低くなるようにする必要がある可能性があります。この余分なスペースにより、完了までに長い時間がかかるトランザクションの場合、活動ログの増大に対応できます。

2. 常に使用可能なスペースが確保されるように、アーカイブ・ログをモニターします。

要確認: アーカイブ・ログが満杯になり、フェイルオーバー・アーカイブ・ログが満杯になると、活動ログが満杯になる可能性があり、サーバーが停止します。目標は、アーカイブ・ログが使用可能なすべてのスペースを使い切らないように、アーカイブ・ログに十分な使用可能スペースを確保することです。次のパターンに気付く可能性があります。

- a. 最初アーカイブ・ログは、通常のクライアント・バックアップ操作の実行に従って、急激に増大します。
- b. データベース・バックアップは、スケジュールに従って、または手動により定期的に行われます。
- c. 少なくともフル・データベース・バックアップが 2 回実行された後、自動的にログの整理が行われます。整理が行われると、アーカイブ・ログの使用するスペースは縮小します。
- d. 通常のクライアント操作が継続され、再びアーカイブ・ログが増大します。

IBM Spectrum Protect サーバーのインストール

- e. データベース・バックアップが定期的に行われ、フル・データベース・バックアップと同じ頻度で、ログの整理が行われます。

このパターンでは、アーカイブ・ログは最初増大しますが、その後縮小し、その後で再び増大する可能性があります。ある期間にわたって通常操作が継続されると、アーカイブ・ログの使用するスペース量は、比較的一定のレベルに達します。

アーカイブ・ログが増大し続ける場合は、次のいずれかまたは両方のアクションの実行を検討してください。

- アーカイブ・ログにスペースを追加します。別のファイル・システムにアーカイブ・ログを移動する必要が生じこともあります。
 - フル・データベース・バックアップの頻度を増加します。そうすると、ログの整理がより頻繁に実行されます。
3. フェイルオーバー・アーカイブ・ログ用のディレクトリーを定義した場合は、通常操作中にそのディレクトリーに保管されたログがあるかどうかを判別します。フェイルオーバー・ログ・スペースが使用されている場合は、アーカイブ・ログのサイズを増加することを検討してください。目標は、フェイルオーバー・アーカイブ・ログが、通常操作時ではなく、異常な状態の場合にのみ使用されることです。

第 4 章 IBM Spectrum Protect サーバー・フィックスパックのインストール

IBM Spectrum Protect 保守更新 (フィックスパックともいいます) により、サーバーを現行の保守レベルまで引き上げることができます。

始める前に

サーバーに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、実行したいレベルでサーバーをインストールします。基本リリース・レベルでサーバーのインストールを開始する必要はありません。例えば、現在 V8.1.1 がインストールされている場合、V8.1 の最新フィックスパックに直接進むことができます。保守更新が利用可能である場合、V8.1.0 のインストールから開始する必要はありません。

IBM Spectrum Protect ライセンス・パッケージがインストールされている必要があります。ライセンス・パッケージは、基本リリースの購入時に提供されます。Fix Central からフィックスパックや暫定修正をダウンロードする場合、パスポート・アドバンテージ Web サイトで入手可能なサーバー・ライセンスをインストールしてください。米国英語以外の言語でメッセージおよびヘルプを表示する場合は、選択した言語パッケージをインストールしてください。

サーバーを V8.1.5 以降にアップグレードしてから V8.1.5 より前のレベルに戻す場合は、データベースをアップグレード前の特定時点にリストアする必要があります。アップグレード・プロセス中に必要な手順を実行して、データベースをリストアできるようにしてください。必要な手順とは、データベース、ボリューム・ヒストリー・ファイル、装置構成ファイル、およびサーバー・オプション・ファイルをバックアップする操作です。詳しくは、105 ページの『第 6 章 バージョン 8.1.5 から以前のサーバーへの復帰』を参照してください。

クライアント管理サービスを使用する場合は、必ず IBM Spectrum Protect サーバーと同じバージョンにアップグレードしてください。

インストール済みサーバーの基本リリースのインストール・メディアを保持していることを確認してください。ダウンロード・パッケージから IBM Spectrum Protect をインストールした場合は、ダウンロードしたファイルが使用可能であることを確認してください。アップグレードが失敗し、サーバーのライセンス・モジュールがアンインストールされた場合は、ライセンスを再インストールするために、サーバーの基本リリースのインストール・メディアが必要になります。

以下の情報については、IBM サポート・ポータルにアクセスしてください。

- 最新の保守修正とダウンロード修正のリスト。「Downloads」をクリックし、適用可能な修正を適用します。
- 基本ライセンス・パッケージの入手方法に関する詳細。「Downloads > Passport Advantage」を検索します。

IBM Spectrum Protect フィックスパックのインストール

- サポートされているプラットフォームとシステム要件。「**IBM Spectrum Protect** サポート対象オペレーティング・システム (**supported operating systems**)」を検索します。

バックアップ/アーカイブ・クライアントをアップグレードする前に、サーバーをアップグレードする必要があります。最初にサーバーをアップグレードしないと、サーバーとクライアントの間の通信が中断される可能性があります。

重要: IBM Spectrum Protect インストール・パッケージおよびフィックスパックとともにインストールされている DB2 ソフトウェアは変更しないでください。別のバージョン、リリース、またはフィックスパックの DB2 ソフトウェアをインストールしたり、それらにアップグレードしたりしないでください。データベースが損傷する可能性があります。

手順

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、以下のステップを実行します。

- データベースのバックアップを取ります。スナップショット・バックアップを使用する方法をお勧めします。スナップショット・バックアップは、スケジュールされたデータベース・バックアップを中断しない、フル・データベース・バックアップです。例えば、以下の IBM Spectrum Protect 管理コマンドを実行します。

```
backup db type=dbsnapshot devclass=tapeclass
```

- 装置構成情報をバックアップします。次の IBM Spectrum Protect 管理コマンドを出します。

```
backup devconfig filenames=file_name
```

ここで、*file_name* は、装置構成情報を保管するファイルの名前を示します。

- ボリューム・ヒストリー・ファイルを、別のディレクトリーに保存するか、リネームします。次の IBM Spectrum Protect 管理コマンドを出します。

```
backup volhistory filenames=file_name
```

ここで、*file_name* は、ボリューム・ヒストリー情報を保管するファイルの名前を示します。

- サーバー・オプション・ファイル (通常、*dsmerv.opt* という名前) のコピーを保存します。ファイルはサーバー・インスタンス・ディレクトリーにあります。

- フィックスパックまたは暫定修正をインストールする前にサーバーを停止します。**HALT** コマンドを使用します。

- インストール・ディレクトリーに余分なスペースがあることを確認してください。このフィックスパックのインストールには、サーバーのインストール・ディレクトリーに追加の一時ディスク・スペースが必要な場合があります。追加ディスク・スペースの量は、IBM Spectrum Protect インストールの一部として新規データベースをインストールするのに必要な量と同じ量にすることができます。IBM Spectrum Protect インストール・ウィザードは、フィックスパックのインストールに必要なスペース量と使用可能な量を表示します。必要なスペース量が使用可能な量より多い場合、インストールは停止します。インス

IBM Spectrum Protect フィックスパックのインストール

トールが停止する場合、必要なディスク・スペースをファイル・システムに追加し、インストールを再開してください。

7. root ユーザーとしてログインします。
8. インストールするフィックスパックまたは暫定修正は、IBM サポート・ポータル、パスポート・アドバンテージ、または Fix Central から入手してください。
9. 実行可能ファイルを置いたディレクトリーに変更して、次のステップを実行してください。

ヒント： ファイルは現行ディレクトリーに抽出されます。 抽出するファイルを配置するディレクトリーに実行可能ファイルが存在しているようにしてください。

- a. 次のコマンドを入力してファイル許可を変更します。

```
chmod a+x 8.x.x.x-IBM-SPSRV-platform.bin
```

ここで、*platform* は、IBM Spectrum Protect がインストールされるアーキテクチャーを示します。

- b. 次のコマンドを発行してインストール・ファイルを解凍します。

```
./8.x.x.x-IBM-SPSRV-platform.bin
```

10. IBM Spectrum Protect のインストール方法を次の中から 1 つ選択します。

重要： フィックスパックがインストールされたら、構成を再度行う必要はありません。 インストールが完了したら、停止し、エラーがあれば修正し、さらにサーバーを再始動できます。

以下のいずれかの方法を使用して、IBM Spectrum Protect ソフトウェアをインストールします。

インストール・ウィザード

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。

57 ページの『インストール・ウィザードを使用した IBM Spectrum Protect のインストール』

ヒント： 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。

コンソール・モードのコマンド・ライン

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。

58 ページの『コンソール・モードを使用した IBM Spectrum Protect のインストール』

サイレント・モード

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。

59 ページの『サイレント・モードで IBM Spectrum Protectをインストール』

IBM Spectrum Protect フィックスパックのインストール

ヒント: システムに複数のサーバー・インスタンスがある場合、インストール・ウィザードを一度だけ実行します。インストール・ウィザードによってすべてのサーバー・インスタンスがアップグレードされます。

タスクの結果

インストール・プロセス中に検出されたエラーを訂正します。

インストール・ウィザードを使用してサーバーをインストールした場合は、IBM Installation Manager ツールを使用してインストール・ログを表示できます。「ファイル」 > 「ログの表示」をクリックします。ログ・ファイルを収集するには、IBM Installation Manager ツールから、「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。

コンソール・モードまたはサイレント・モードを使用してサーバーをインストールした場合は、IBM Installation Manager ログ・ディレクトリー内のエラー・ログを表示できます。例を次に示します。

```
/var.ibm/InstallationManager/logs
```

第 5 章 V8.1 へのアップグレード

新規の製品機能および更新を利用するには、IBM Spectrum Protect サーバーをバージョン 8.1.5 にアップグレードします。

このタスクについて

同じオペレーティング・システム上でサーバーをアップグレードする場合は、アップグレード手順を参照してください。サーバーを別のオペレーティング・システムにマイグレーションする手順については、IBM Spectrum Protect のアップグレードおよびマイグレーション・プロセス - よくあるご質問.

表 12. アップグレード手順

アップグレード元のバージョン	アップグレード先のバージョン	参照情報
V8.1	V8.1 フィックスパックまたは暫定修正	91 ページの『第 4 章 IBM Spectrum Protect サーバー・フィックスパックのインストール』
V7.1	V8.1	99 ページの『サーバーのインストールとアップグレードの検証』
V7.1	V8.1 フィックスパックまたは暫定修正	91 ページの『第 4 章 IBM Spectrum Protect サーバー・フィックスパックのインストール』
V5.5、V6.2、または V6.3	V8.1	IBM Spectrum Protect のアップグレードおよびマイグレーション・プロセス - よくあるご質問

V7 から V8.1 へのアップグレードには、約 20 分から 50 分程度かかります。ご使用の環境では、ラボで得られた結果と異なる結果が生じる場合があります。

クラスター環境におけるアップグレードについては、102 ページの『クラスター環境でのサーバーのアップグレード』を参照してください。

アップグレードまたはマイグレーション後に、サーバーを前のバージョンに戻すには、フル・データベース・バックアップと元のサーバーのインストール・ソフトウェアが必要になります。また、以下の主要な構成ファイルも必要になります。

- ボリューム・ヒストリー・ファイル
- 装置構成ファイル
- サーバー・オプション・ファイル

関連情報:



IBM Spectrum Protect アップグレードおよびマイグレーションのプロセス - よくある質問

V8.1 へのアップグレード

サーバーは、V7.1 から V8.1 に直接アップグレードすることができます。V7.1 をアンインストールする必要はありません。

始める前に

アップグレードするサーバーの基本リリースのインストール・メディアを保持していることを確認してください。DVD からサーバー・コンポーネントをインストールした場合は、その DVD が使用可能であることを確認してください。ダウンロード・パッケージからサーバー・コンポーネントをインストールした場合は、ダウンロードしたファイルが使用可能であることを確認してください。アップグレードが失敗し、サーバーのライセンス・モジュールがアンインストールされた場合は、ライセンスを再インストールするために、サーバーの基本リリースのインストール・メディアが必要になります。

ヒント: V8.1 以降では DVD の提供がなくなりました。

手順

サーバーを V8.1 にアップグレードするには、以下のタスクを実行します。

1. 『アップグレードの計画』
2. 97 ページの『システムの準備』
3. 99 ページの『サーバーのインストールとアップグレードの検証』

アップグレードの計画

サーバーを V7.1 から V8.1 にアップグレードする前に、関連する計画情報（システム要件やリリース情報など）を確認する必要があります。次に、実動の運用への影響を最小限に抑えることができるよう、システムをアップグレードする適切な日時を選択します。

このタスクについて

ラボのテストでは、サーバーを V7.1 から V8.1 にアップグレードするプロセスには、14 分から 45 分かかりました。ユーザーが達成できる結果は、ご使用のハードウェアおよびソフトウェア環境や、サーバー・データベースのサイズによって異なることがあります。

手順

1. 以下のハードウェア要件およびソフトウェア要件を確認します。

26 ページの『最小システム要件』

システム要件に関する最新の更新情報は、IBM Spectrum Protect サポート Web サイト (技術情報 1243309) を参照してください。

2. ご使用のオペレーティング・システムに対する特別な手順あるいは固有の情報については、サーバー・コンポーネントの関するリリース情報 (http://www.ibm.com/support/knowledgecenter/SSEQVQ_8.1.3/srv.common/r_relnotes_srv.html) および README ファイルを確認してください。
3. 実動運用への影響を最小限に抑えるために、システムのアップグレードには適切な日時を選んでください。システムの更新に要する時間は、データベースのサイズおよびその他の多くの要因によって異なります。アップグレード・プロセスを開始すると、新しいソフトウェアがインストールされて必要なライセンスがすべて再登録されるまで、クライアントはサーバーに接続できません。
4. サーバーを V6 または V7 から V8.1 にアップグレードする場合、IBM Spectrum Protect サーバーの DB2 インスタンス用のシステム ID とパスワードがあることを確認してください。システムをアップグレードするには、これらの資格情報が必要です。

システムの準備

システムを V7.1 から V8.1 にアップグレードする準備をするには、各 DB2 インスタンスに関する情報を収集する必要があります。次に、サーバー・データベースをバックアップし、主要な構成ファイルを保存し、セッションを取り消して、サーバーを停止します。

手順

1. サーバーがインストールされているコンピューターにログオンします。
インスタンス・ユーザー ID を使用してログオンしていることを確認してください。
2. DB2 インスタンスのリストを取得します。以下のシステム・コマンドを発行します。
`/opt/tivoli/tsm/db2/instance/db2ilist`

出力は、以下の例のようになります。

```
tsminst1
```

各インスタンスが、システム上で実行されているサーバーに対応していることを確認してください。

3. DB2 インスタンスごとに、そのインスタンスに対して構成されているデフォルト・データベース・パス、実際のデータベース・パス、データベース名、データベース別名、および DB2 変数を書き留めます。後で参照できるように、この記録を保持しておきます。この情報は、V7.1 データベースをリストアするために必要です。
4. 管理ユーザー ID を使用して、サーバーに接続します。
5. **BACKUP DB** のコマンドを使用してデータベースをバックアップします。推奨される方式は、スナップショット・バックアップを作成することです。これはスケジュール済みのデータベース・バックアップに割り込まないフル・データベース・バックアップです。例えば、次のコマンドを発行して、スナップショット・バックアップを作成することができます。

```
backup db type=dbsnapshot devclass=tapeclass
```

IBM Spectrum Protect サーバーのアップグレード

6. 次の管理コマンドを発行して、装置構成情報を別のディレクトリーにバックアップします。

```
backup devconfig filenames=file_name
```

ここで、*file_name* は、装置構成情報を保管するファイルの名前を示します。

ヒント: V7.1 データベースをリストアする場合、このファイルが必要です。

7. ボリューム・ヒストリー・ファイルを、別のディレクトリーにバックアップします。以下の管理コマンドを発行します。

```
backup volhistory filenames=file_name
```

ここで、*file_name* は、ボリューム・ヒストリー情報を保管するファイルの名前を示します。

ヒント: V7.1 データベースをリストアする場合、このファイルが必要です。

8. サーバー・オプション・ファイル (通常は `dsmerv.opt` という名前) のコピーを保存します。ファイルはサーバー・インスタンス・ディレクトリーにあります。
9. 新規セッションを使用不可にして、サーバー上のアクティビティーを防止します。以下の管理コマンドを発行します。

```
disable sessions client  
disable sessions server
```

10. セッションが存在するかどうか確認し、サーバーを停止することをユーザーに通知します。既存のセッションがあるか確認するには、以下の管理コマンドを発行します。

```
query session
```

11. 次の管理コマンドを発行して、セッションを取り消します。

```
cancel session all
```

このコマンドは、現行セッションを除くすべてのセッションを取り消します。

12. 次の管理コマンドを発行して、サーバーを停止します。

```
halt
```

13. サーバーがシャットダウンされ、実行中のプロセスがないことを確認します。

次のコマンドを出します。

```
ps -ef | grep dsmerv
```

14. インストール済み環境のサーバー・インスタンス・ディレクトリーで、`NODELOCK` ファイルを見つけて、それを構成ファイルを保存している別のディレクトリーに移動します。`NODELOCK` ファイルには、ご使用のシステムの以前のライセンス情報が入っています。アップグレードが完了すると、このライセンス情報は置き換えられます。

サーバーのインストールとアップグレードの検証

サーバーを V8.1 にアップグレードするプロセスを完了するには、V8.1 サーバーをインストールする必要があります。次に、サーバー・インスタンスを始動して、アップグレードが正常に行われたかどうか検証します。

始める前に

root ユーザー ID を使用してシステムにログオンする必要があります。

インストール・パッケージは、 IBM ダウンロード・サイトから入手できます。

確実にファイルを正常にダウンロードできるように、システム・ユーザーの最大ファイル・サイズの制限を無制限に設定してください。

1. 最大ファイル・サイズ値を照会するには、次のコマンドを実行します。

```
ulimit -Hf
```

2. システム・ユーザーの最大ファイル・サイズの制限が無制限に設定されていない場合は、ご使用のオペレーティング・システムの資料の手順に従って設定を無制限に変更してください。

このタスクについて

IBM Spectrum Protect インストール・ソフトウェアを使用して、以下のコンポーネントをインストールできます。

- サーバー

ヒント: サーバー・コンポーネントを選択するときに、データベース (DB2)、Global Security Kit (GSKit)、および IBM Java ランタイム環境 (JRE) が自動的にインストールされます。

- サーバー言語
- ライセンス
- 装置
- IBM Spectrum Protect for SAN
- Operations Center

手順

1. 以下のいずれかの Web サイトから該当するパッケージ・ファイルをダウンロードします。

- パスポート・アドバンテージ または Fix Central からサーバー・パッケージをダウンロードします。
- 最新情報、更新、および保守修正については、IBM サポート・ポータルにアクセスしてください。

2. 次の手順を実行してください。

- a. 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、ご使用の製品のダウンロード資料を参照してください。

IBM Spectrum Protect サーバーのアップグレード

- IBM Spectrum Protect 技術情報 4042944
 - IBM Spectrum Protect Extended Edition 技術情報 4042945
 - IBM Spectrum Protect for Data Retention 技術情報 4042946
- b. パッケージ・ファイルを、選択したディレクトリーにダウンロードします。パスに含める文字数は 128 文字以下でなければならない。必ず、インストール・ファイルを空のディレクトリーに抽出します。インストール・ファイルは、前に抽出したファイルやその他のファイルが含まれるディレクトリーには抽出しないでください。

また、このパッケージ・ファイルの実行権限を持っていることを確認してください。

- c. 必要に応じて、次のコマンドを実行してファイル許可を変更します。

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

ここで、*package_name* は、以下の例のようになります。

```
8.1.x.000-IBM-SPSRV-Linuxs390x.bin  
8.1.x.000-IBM-SPSRV-Linuxx86_64.bin  
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
```

例では、8.1.x.000 は製品リリース・レベルを表します。

- d. 次のコマンドを実行して、インストール・ファイルを抽出します。

```
./package_name.bin
```

このパッケージは大容量です。そのため、抽出にはしばらく時間がかかります。

3. 以下のいずれかの方法を使用して、IBM Spectrum Protect ソフトウェアをインストールします。インストール処理時に IBM Spectrum Protect ライセンスをインストールしてください。

ヒント: システムに複数のサーバー・インスタンスがある場合、IBM Spectrum Protect ソフトウェアを一度だけインストールして、すべてのサーバー・インスタンスをアップグレードします。

インストール・ウィザード

IBM Installation Manager のグラフィカル・ウィザードを使用してサーバーをインストールするには、57 ページの『インストール・ウィザードを使用した IBM Spectrum Protect のインストール』の指示に従ってください。

ご使用のシステムが、インストール・ウィザードを使用するための前提条件を満たしていることを確認します。それから、インストール手順を実行します。「IBM Installation Manager」ウィンドウで、「更新」または「変更」アイコンをクリックします。

コンソール・モードを使用したサーバーのインストール

コンソール・モードを使用してサーバーをインストールするには、58 ページの『コンソール・モードを使用した IBM Spectrum Protect のインストール』の指示に従ってください。

IBM Spectrum Protect サーバーのアップグレード

コンソール・モードでのサーバーのインストールに関する情報を参照して、インストール手順を完了してください。

サイレント・モード

サイレント・モードを使用してサーバーをインストールするには、 59 ページの『サイレント・モードで IBM Spectrum Protectをインストール』の指示に従ってください。

サイレント・モードでのサーバーのインストールに関する情報を参照して、インストール手順を完了してください。

ソフトウェアをインストールした後、システムを再構成する必要はありません。

4. インストール・プロセス中に検出されたエラーを訂正します。

インストール・ウィザードを使用してサーバーをインストールした場合は、IBM Installation Manager ツールを使用してインストール・ログを表示できます。

「ファイル」 > 「ログの表示」をクリックします。ログ・ファイルを収集するには、IBM Installation Manager ツールから、「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。

コンソール・モードまたはサイレント・モードを使用してサーバーをインストールした場合は、IBM Installation Manager ログ・ディレクトリー内のエラー・ログを表示できます。例を次に示します。

```
/var/ibm/InstallationManager/logs
```

5. IBM サポート・ポータル にアクセスして、修正を取得します。「**Fixes, updates, and drivers**」をクリックし、適用可能な修正を適用します。
6. アップグレードが正常に終了したかどうか確認します。
 - a. サーバー・インスタンスを開始します。
 - b. サーバーが始動時に発行するメッセージをモニターします。エラー・メッセージおよび警告メッセージがないか注意して見て、問題があれば解決します。
 - c. 管理クライアントを使用して、サーバーに接続できることを確認します。管理可能クライアント・セッションを開始するには、次の IBM Spectrum Protect 管理コマンドを実行します。
`dsmadmc`

- d. アップグレードされたシステムに関する情報を入手するには、**QUERY** コマンドを実行します。例えば、システムに関する統合情報を取得する場合は、以下の IBM Spectrum Protect 管理コマンドを実行します。

```
query system
```

データベースに関する情報を取得する場合は、以下の IBM Spectrum Protect 管理コマンドを実行します。

```
query db format=detailed
```

7. **REGISTER LICENSE** コマンドを実行して、システムにインストールされている IBM Spectrum Protect サーバー・コンポーネントのライセンスを登録します。

```
register license file=installation_directory/server/bin/component_name.lic
```

IBM Spectrum Protect サーバーのアップグレード

ここで、*installation_directory* は、コンポーネントをインストールしたディレクトリーを指定し、*component_name* はコンポーネントの省略形を指定します。

例えば、サーバーをデフォルト・ディレクトリー /opt/tivoli/tsm にインストールした場合は、次のコマンドを発行してライセンスを登録します。

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

例えば、IBM Spectrum Protect Extended Edition を /opt/tivoli/tsm ディレクトリーにインストールした場合、次のコマンドを実行します。

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

例えば、IBM Spectrum Protect for Data Retention を /opt/tivoli/tsm ディレクトリーにインストールした場合、次のコマンドを実行します。

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

制約事項:

IBM Spectrum Protect サーバーを使用して、以下の製品のライセンスを登録することはできません。

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

REGISTER LICENSE コマンドは、これらのライセンスには適用されません。これらの製品のライセンス交付は、IBM Spectrum Protect クライアントによって実行されます。

8. オプション: 追加の言語パッケージをインストールするには、IBM Installation Manager の変更機能を使用します。
9. オプション: 新規バージョンの言語パッケージにアップグレードするには、IBM Installation Manager の更新機能を使用します。

次のタスク

パスワードは LDAP ディレクトリー・サーバーによって認証できます。または IBM Spectrum Protect サーバーによってパスワードを認証することもできます。LDAP ディレクトリー・サーバーを使用して認証されるパスワードは、より高度なシステム・セキュリティーを提供します。

クラスター環境でのサーバーのアップグレード

クラスター環境でサーバーを V8.1.5 にアップグレードするには、準備作業とインストール作業を実行する必要があります。手順は、オペレーティング・システムおよびリリースによって異なります。

手順

ご使用のオペレーティング・システム、ソース・リリース、およびターゲット・リリースの手順に従ってください。

表 13. Linux オペレーティング・システム上のクラスター環境でのサーバーのアップグレード手順

ソース・リリース	ターゲット・リリース	手順
V6.3 以降	V8.1.5	System Automation for Multiplatforms で構成されたサーバーのアップグレード

クラスター環境における V8.1.5 への IBM Spectrum Protect のアップグレード

IBM Spectrum Protect の新機能を利用するため、クラスター環境の Linux オペレーティング・システムにインストールされている IBM Spectrum Protect サーバーをアップグレードできます。

手順

アップグレードするには、クラスター化のための Linux 環境の構成に関するセクションの手順に従ってください。

第 6 章 バージョン 8.1.5 から以前のサーバーへの復帰

アップグレード後にサーバーを以前のバージョンに戻す必要がある場合、元のバージョンのフル・データベース・バックアップが必要です。また、元のバージョンのサーバー・インストール・メディア、および主な構成ファイルも必要です。サーバーをアップグレードする前に、慎重に準備手順を行ってください。これにより、データ損失を最小限に抑えながら、IBM Spectrum Protect サーバーを以前のバージョンに戻すことが可能になる場合があります。

始める前に

以前のバージョンのサーバーから以下の項目を用意する必要があります。

- サーバー・データベース・バックアップ
- ボリューム・ヒストリー・ファイル
- 装置構成ファイル
- サーバー・オプション・ファイル

このタスクについて

同じリリース内で戻すか以前のリリースに戻すか（例えば、8.1.3 から 8.1.2、あるいは 8.1.3 から 7.1.2）にかかわらず、同じ手順を使用します。以前のバージョンは、V8.1 にアップグレードする前に使用していたバージョンと一致している必要があります。

重要: サーバーを以前のバージョンに戻す際にバックアップ/アーカイブ・クライアント・データを喪失しないように、**REUSEDDELAY** パラメーターを指定してください。

以前のサーバー・バージョンに戻すための手順

このタスクについて

V8.1 サーバーがあるシステムで、次のステップを実行してください。

手順

1. **HALT** コマンドを使用してサーバーを停止し、すべてのサーバー操作をシャットダウンします。
2. データベース・マネージャーからデータベースを除去して、次にデータベースおよび回復ログ・ディレクトリーを削除します。
 - a. データベースを手動で除去します。 データベースを除去する方法の 1 つとして、以下のコマンドを実行する方法があります。
`dsmser removedb tsmdb1`
 - b. データベースおよび回復ログ・ディレクトリーが占めていたスペースを再利用する必要がある場合、この時点で、これらのディレクトリーを削除できます。

以前のサーバー・バージョンへの復帰

3. アンインストール・プログラムを使用して、V8.1 サーバーをアンインストールします。アンインストールにより、サーバーおよびデータベース・マネージャーがそれらのディレクトリーと共に除去されます。 詳しくは、113 ページの『第 8 章 IBM Spectrum Protect のアンインストール』を参照してください。
4. クラスター・サービスを停止します。V8.1.5 にアップグレードする前に使用していたバージョンのサーバー・プログラムを再インストールします。このバージョンは、後の手順でリストアするデータベース・バックアップを作成したときにサーバーが実行していたバージョンと一致する必要があります。例えば、アップグレード前のサーバーが V7.1.7 であり、このサーバーで使用されていたデータベース・バックアップを使用するとします。この場合、データベース・バックアップをリストアできるようにするには、V7.1.7 フィックスパックをインストールする必要があります。
5. 構成ウィザードを使用して、新しいサーバー・データベースを構成します。 ウィザードを開始するには、以下のコマンドを発行します。

```
. /dsmicfgx
```
6. バックグラウンドで実行されているサーバーがないことを確認します。
7. データベースを、アップグレード前の特定時点にリストアします。
8. 以下のファイルをインスタンス・ディレクトリーにコピーします。
 - 装置構成ファイル
 - ボリューム・ヒストリー・ファイル
 - サーバー・オプション・ファイル (通常は `dsserv.opt`)
9. V8.1.5 サーバーの使用中に、アップグレード前に存在していた FILE タイプのストレージ・プールに対するデータ重複排除を有効にした場合、またはアップグレード前に存在していたデータを新規ストレージ・プールに移動した場合、追加のリカバリー手順を実行する必要があります。 詳細については、107 ページの『新規ストレージ・プールを作成した場合またはデータ重複排除を使用可能にした場合の追加のリカバリー手順』を参照してください。
10. ストレージ・プールの **REUSEDDELAY** パラメーター設定値が、リストアしたデータベースの存続期間より小さい場合、そのデータベース・バックアップの後で再利用された順次アクセス・ストレージ・プール上のボリュームをリストアします。 **RESTORE VOLUME** コマンドを使用します。

ストレージ・プールのバックアップがない場合は、**FIX=YES** パラメーターを指定した **AUDIT VOLUME** コマンドを使用して、再利用されたボリュームを監査して、不整合を解決します。 例えば次のとおりです。

```
audit volume volume_name fix=yes
```

11. V8.1 サーバーを使用してクライアントのバックアップまたはアーカイブ操作が実行された場合、データが保管されていたストレージ・プール・ボリュームを監査します。

新規ストレージ・プールを作成した場合またはデータ重複排除を使用可能にした場合の追加のリカバリー手順

サーバーが V8.1.5 のサーバーとして稼働していた間に、新規ストレージ・プールを作成したか、FILE タイプのストレージ・プールに対するデータ重複排除を有効にしたか、あるいはこの両方を行った場合は、以前のサーバー・バージョンに戻すために追加の手順を実行する必要があります。

始める前に

この作業を実行するには、V8.1.5 にアップグレードする前に作成された、ストレージ・プールの完全なバックアップが必要です。

このタスクについて

サーバーが V8.1.5 サーバーとして稼働していた間に以下のいずれかまたは両方のアクションを実行した場合、この情報を使用してください。

- V8.1.5 プログラムにアップグレードする前に存在したストレージ・プールに対してデータ重複排除機能を使用可能にした。データ重複排除は、FILE 装置タイプを使用するストレージ・プールにのみ適用されます。
- アップグレード後に新規 1 次ストレージ・プールを作成して、かつ他のストレージ・プールに保管されていたデータを新規ストレージ・プールに移動した。

サーバーが再び V7 にリストアされた後、以下のステップを実行します。

手順

- データ重複排除機能を使用可能にしたストレージ・プールごとに、**RESTORE STGPOOL** コマンドを使用してストレージ・プール全体をリストアします。
- アップグレード後に作成したストレージ・プールについて、実行すべきアクションを判別します。リストアされた V8 サーバーには新規ストレージ・プールが存在しなくなっているため、既存の V8 ストレージ・プールから新規ストレージ・プールに移動されたデータは失われた可能性があります。考えられるリカバリーは、次のようにストレージ・プールのタイプによって異なります。
 - データが V8 の DISK タイプのストレージ・プールから新規ストレージ・プールに移動された場合、移動されたデータが占有していたスペースがおそらく再利用されました。そのため、V8.1.5 にアップグレードする前に作成されたストレージ・プール・バックアップを使用して、元の V7 ストレージ・プールをリストアする必要があります。

V8 の DISK タイプ・ストレージ・プールから新規ストレージ・プールに移動されたデータがない場合、これらの DISK タイプ・ストレージ・プールのストレージ・プール・ボリュームを監査します。

- データが V8 の順次アクセス・ストレージ・プールから新規ストレージ・プールに移動された場合、そのデータは依然として存在し、リストアされた V8 サーバーのストレージ・プール・ボリュームで使用できる可能性があります。サーバーが V8.1.5 サーバーとして稼働していた間に、ストレージ・プールの **REUSEDDELAY** パラメーターがレクラメーション防止の値に設定されていた場合、データが使用可能である可能性があります。サーバーが V8.1.5 サーバーとして稼働していた間にボリュームが再利用された場合、それらのボリ

以前のサーバー・バージョンへの復帰

ユームを、V8.1.5 へのアップグレード前に作成されたストレージ・プール・バックアップからリストアしてください。

第 7 章 リファレンス: IBM Spectrum Protect サーバー・データベースに使用する DB2 コマンド

このリストは、IBM サポートによって、DB2 コマンドを発行するよう指示された場合に参照として使用してください。

目的

ウィザードを使用して IBM Spectrum Protect をインストールおよび構成した後、DB2 コマンドを実行する必要がある場合はめったにありません。表 14 に、使用する、または実行するよう依頼される可能性がある一部の DB2 コマンドをリストします。このリストは、補足資料としてのみ使用することを目的としたもので、包括的なリストではありません。また、IBM Spectrum Protect 管理者が、日常的または継続的にこのリストを使用することを示唆するものではありません。一部のコマンドについては、例が示されています。詳細な出力はリストされていません。

ここに記載されているコマンドの完全な説明および構文については、DB2 製品情報を参照してください。

表 14. DB2 コマンド

コマンド	説明	例
db2icrt	インスタンス所有者のホーム・ディレクトリーに DB2 インスタンスを作成します。 ヒント: IBM Spectrum Protect 構成ウィザードは、サーバーおよびデータベースによって使用されるインスタンスを作成します。構成ウィザードを使用してサーバーをインストールして構成した後は、通常、 db2icrt コマンドは使用しません。 このユーティリティーは、DB2DIR/instance ディレクトリーにあります。ここで、DB2DIR は、DB2 データベース・システムの現行バージョンがインストールされているインストール場所を表します。	IBM Spectrum Protect インスタンスを手動で作成します。次のコマンドを 1 行で入力します。 <code>/opt/tivoli/tsm/db2(instance/db2icrt -a server -u instance_name instance_name)</code>
db2set	DB2 変数を表示します。	DB2 変数をリストします。 <code>db2set</code>
CATALOG DATABASE	システム・データベース・ディレクトリーに、データベースのロケーション情報を保管します。データベースは、ローカル・ワークステーションまたはリモート・データベース・パーティション・サーバーのいずれかにも配置できます。サーバー構成ウィザードは、サーバー・データベースを使用するために必要なすべてのカタログを扱います。サーバーを構成した後、実行しているときには、環境内で何らかの変更または損傷があった場合にのみ、このコマンドを手動で実行してください。	データベースをカタログします。 <code>db2 catalog database tsmdb1</code>

リファレンス: IBM Spectrum Protect サーバー・データベースに使用する DB2 コマンド

表 14. DB2 コマンド (続き)

コマンド	説明	例
CONNECT TO DATABASE	コマンド・ライン・インターフェース (CLI) で使用するために、指定したデータベースに接続します。	DB2 CLI から IBM Spectrum Protect データベースに接続します。 db2 connect to tsmdb1
GET DATABASE CONFIGURATION	特定のデータベース構成ファイル内にある個々の項目の値を返します。 重要: このコマンドおよびパラメーターは、DB2 によって直接設定および管理されます。これらは、単に情報提供のため、および既存の設定を表示する手段として、ここにリストされています。これらの設定の変更は、IBM サポート、または APAR や技術ガイダンス文書 (技術情報) などの業務広報によって指示される場合があります。これらの設定を手動で変更しないでください。これらの設定は、IBM による指示があった場合にのみ、IBM Spectrum Protect サーバーのコマンドまたはプロシージャーを使用して変更してください。	データベース別名についての構成情報を表示します。 db2 get db cfg for tsmdb1 データベース構成、ログ・モード、および保守などの設定を確認するために情報を取得します。 db2 get db config for tsmdb1 show detail
GET DATABASE MANAGER CONFIGURATION	特定のデータベース構成ファイル内にある個々の項目の値を返します。 重要: このコマンドおよびパラメーターは、DB2 によって直接設定および管理されます。これらは、単に情報提供のため、および既存の設定を表示する手段として、ここにリストされています。これらの設定の変更は、IBM サポート、または APAR や技術ガイダンス文書 (技術情報) などの業務広報によって指示される場合があります。これらの設定を手動で変更しないでください。これらの設定は、IBM による指示があった場合にのみ、IBM Spectrum Protect サーバーのコマンドまたはプロシージャーを使用して変更してください。	データベース・マネージャーの構成情報を取得します。 db2 get dbm cfg
GET HEALTH SNAPSHOT	データベース・マネージャーとそのデータベースのヘルス状況情報を検索します。戻された情報は、コマンドが発行された時点でのヘルス状態のスナップショットを表しています。 IBM Spectrum Protect は、ヘルス・スナップショットおよび DB2 により提供されるその他のメカニズムを使用して、データベースの状態をモニターします。 ヘルス・スナップショットまたはその他の DB2 文書で、項目またはデータベースがアラート状態である可能性があることが示される場合があります。 そのような場合は、状態を改善するためにアクションを検討する必要があることを示しています。 IBM Spectrum Protect は、状態をモニターして、適切に対応します。 DB2 データベースによって宣言されたすべてのアラートに従って対処しなければならない訳ではありません。	DB2 ヘルス・モニター・インディケーターに関するレポートを受け取ります。 db2 get health snapshot for database on tsmdb1

表 14. DB2 コマンド (続き)

コマンド	説明	例
GRANT (データベース権限)	データベース内の特定のオブジェクトに適用される特権ではなく、データベース全体に適用される権限を付与します。	ユーザー ID itmuser にアクセス権限を付与します。 db2 GRANT CONNECT ON DATABASE TO USER itmuser db2 GRANT CREATETAB ON DATABASE TO USER itmuser
RUNSTATS	表および関連する索引、または統計ビューの特性についての統計を更新します。これらの特性には、レコード数、ページ数、および平均レコード長が含まれます。 表を見る場合は、表を更新または再編成した後、このユーティリティーを実行します。 照会を最適化するためにビューの統計を使用する場合は、ビューを最適化に使用できるようにする必要があります。最適化で使用可能なビューを、統計ビューといいます。ビューを最適化に使用できるようにするには、DB2 ALTER VIEW ステートメントを使用します。基礎となる表への変更が、ビューによって返される行にかなり影響を与える場合は、 RUNSTATS ユーティリティーを実行します。 ヒント: サーバーは、必要に応じて RUNSTATS コマンドを実行するように DB2 を構成します。	单一の表で統計を更新します。 db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all
SET SCHEMA	DB2 CLI から直接 SQL コマンドを実行するための準備として、 CURRENT SCHEMA 特殊レジスターの値を変更します。 ヒント: 特殊レジスターは、データベース・マネージャーによってアプリケーション処理のために定義されるストレージ域です。これは、SQL ステートメントで参照可能な情報を保管するために使用されます。	IBM Spectrum Protect のスキーマを設定します。 db2 set schema tsmdb1
START DATABASE MANAGER	現在のデータベース・マネージャー・インスタンスのバックグラウンド・プロセスを開始します。サーバーは、サーバーを開始および停止するたびに、インスタンスとデータベースを開始および停止します。 重要: IBM サポートから特に別の指示がない限り、サーバーがインスタンスとデータベースの開始および停止を管理できるようにしてください。	データベース・マネージャーを開始します。 db2start

リファレンス: IBM Spectrum Protect サーバー・データベースに使用する DB2 コマンド

表 14. DB2 コマンド (続き)

コマンド	説明	例
STOP DATABASE MANAGER	<p>現在のデータベース・マネージャー・インスタンスを停止します。データベース・マネージャーは、明示的に停止されない限り、アクティブなままでです。このコマンドは、データベースに接続されたアプリケーションがある場合には、データベース・マネージャー・インスタンスを停止しません。データベース接続がなく、インスタンス接続はある場合、このコマンドは最初にインスタンス接続を強制的に停止します。その後に、データベース・マネージャーを停止します。また、このコマンドは、データベース・マネージャーを停止する前に、未解決のデータベースの活動を非活動化します。</p> <p>このコマンドはクライアントでは無効です。</p> <p>サーバーは、サーバーを開始および停止するたびに、インスタンスとデータベースを開始および停止します。</p> <p>重要: IBM サポートから特に別の指示がない限り、サーバーがインスタンスとデータベースの開始および停止を管理できるようにしてください。</p>	<p>データベース・マネージャーを停止します。</p> <pre>db2 stop dbm</pre>

第 8 章 IBM Spectrum Protect のアンインストール

以下の手順を使用して、IBM Spectrum Protect をアンインストールすることができます。 IBM Spectrum Protect を除去する前に、バックアップおよびアーカイブ・データが失われないようにする必要があります。

始める前に

IBM Spectrum Protect をアンインストールする前に次のステップを完了してください。

- フル・データベース・バックアップを実行します。
- ボリューム・ヒストリーと装置構成ファイルのコピーを保存します。
- 出力ボリュームを安全な場所に保管します。

このタスクについて

IBM Spectrum Protect は、グラフィック・ウィザード、コンソール・モードのコマンド・ライン、またはサイレント・モードを使用してアンインストールすることができます。

『グラフィカル・ウィザードを使用した IBM Spectrum Protect のアンインストール』

114 ページの『コンソール・モードでの IBM Spectrum Protect のアンインストール』

114 ページの『サイレント・モードでの IBM Spectrum Protect のアンインストール』

次のタスク

IBM Spectrum Protect のコンポーネントを再インストールするためのインストール・ステップについては、55 ページの『第 2 章 サーバー・コンポーネントのインストール』を参照してください。

グラフィカル・ウィザードを使用した IBM Spectrum Protect のアンインストール

IBM Installation Manager インストール・ウィザードを使用して、IBM Spectrum Protect をアンインストールできます。

手順

1. Installation Manager を開始します。

Installation Manager がインストールされているディレクトリーで、eclipse サブディレクトリー（例えば、/opt/IBM/InstallationManager/eclipse）に移動し、次のコマンドを発行します。

IBM Spectrum Protect のアンインストール

./IBMMIM

2. 「アンインストール」をクリックします。
3. 「IBM Spectrum Protect サーバー」を選択し、「次へ」をクリックします。
4. 「アンインストール」をクリックします。
5. 「終了」をクリックします。

コンソール・モードでの IBM Spectrum Protect のアンインストール

コマンド・ラインを使用して IBM Spectrum Protect をアンインストールするには、コンソール・モードのパラメーターを指定してコマンド・ラインから IBM Installation Manager のアンインストール・プログラムを実行する必要があります。

手順

1. IBM Installation Manager がインストールされているディレクトリーで、以下のサブディレクトリーに移動します。

eclipse/tools

例えば次のとおりです。

/opt/IBM/InstallationManager/eclipse/tools

2. tools ディレクトリーから以下のコマンドを発行します。
./imcl -c
3. アンインストールするには、5 を入力します。
4. IBM Spectrum Protect パッケージ・グループからアンインストールすることを選択します。
5. 「N」(次へ) を入力します。
6. IBM Spectrum Protect サーバー・パッケージをアンインストールすることを選択します。
7. 「N」(次へ) を入力します。
8. 「U」(アンインストール) を入力します。
9. 「F」(終了) を入力します。

サイレント・モードでの IBM Spectrum Protect のアンインストール

サイレント・モードで IBM Spectrum Protect をアンインストールするには、サイレント・モードのパラメーターを指定してコマンド・ラインから IBM Installation Manager のアンインストール・プログラムを実行する必要があります。

始める前に

応答ファイルを使用して、IBM Spectrum Protect サーバー・コンポーネントをサイレント・アンインストールするためのデータ入力を提供することができます。IBM Spectrum Protect には、input ディレクトリーにサンプル応答ファイル `uninstall_response_sample.xml` が含まれています。このディレクトリーは、インストール・パッケージが解凍されるディレクトリーです。このファイルには、不要な警告を回避するのに役立つデフォルト値が含まれています。

すべての IBM Spectrum Protect コンポーネントをアンインストールしたい場合は、応答ファイル内の各コンポーネントについて、`modify="false"` を設定したままにします。コンポーネントをアンインストールしたくない場合は、値を `modify="true"` に設定します。

応答ファイルをカスタマイズしたい場合は、ファイル内のオプションを変更することができます。応答ファイルについては、応答ファイルを参照してください。

手順

1. IBM Installation Manager がインストールされているディレクトリーで、以下のサブディレクトリーに移動します。

```
eclipse/tools
```

例えば次のとおりです。

```
/opt/IBM/InstallationManager/eclipse/tools
```

2. `tools` ディレクトリーから、以下のコマンドを発行します。ここで、`response_file` は、ファイル名を含めた応答ファイルのパスを示しています。

```
./imcl -input response_file -silent
```

以下にコマンド例を示します。

```
./imcl -input /tmp/input/uninstall_response.xml -silent
```

IBM Spectrum Protect のアンインストールと再インストール

IBM Spectrum Protect を、ウィザードを使用せずに手動で再インストールすることを予定している場合は、サーバー・インスタンス名とデータベース・ディレクトリーを保存するために実行する数多くのステップがあります。以前にセットアップしたサーバー・インスタンスはすべてアンインストール中に削除されますが、それらのインスタンスのデータベース・カタログはまだ存在します。

このタスクについて

IBM Spectrum Protect を手動でアンインストールおよび再インストールするには、以下のステップを完了してください。

1. アンインストールを実行する前に、現行サーバー・インスタンスのリストを作成します。以下のコマンドを実行します。

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

2. 各サーバー・インスタンスに次のコマンドを実行します。

```
db2 attach to instance_name  
db2 get dbm cfg show detail  
db2 detach
```

それぞれのインスタンスのデータベース・パスを記録します。

3. IBM Spectrum Protect をアンインストールします。 113 ページの『第 8 章 IBM Spectrum Protect のアンインストール』を参照してください。
4. サポートされるバージョンの IBM Spectrum Protect (フィックスパックを含む) をアンインストールすると、インスタンス・ファイルが作成されます。インスタンス・ファイルは、IBM Spectrum Protect の再インストールに役立つように作

IBM Spectrum Protect のアンインストール

成されます。 再インストールの際にインスタンスの資格情報の入力を求めるプロンプトが出されたときに、このファイルを確認して情報を使用します。 サイレント・インストール・モードでは、`INSTANCE_CRED` 変数を使用して、これらの資格情報を指定します。

インスタンス・ファイルは以下のロケーションにあります。

```
/etc/tivoli/tsm/instanceList.obj
```

5. IBM Spectrum Protect を再インストールします。 55 ページの『第 2 章 サーバー・コンポーネントのインストール』を参照してください。

`instanceList.obj` ファイルが存在しない場合は、以下のステップを使用して、サーバー・インスタンスを再作成する必要があります。

- a. サーバー・インスタンスを再作成します。 69 ページの『サーバー・インスタンスの作成』を参照してください。

ヒント: インストール・ウィザードはサーバー・インスタンスを構成しますが、インスタンスが存在しているかどうかはユーザーが確認する必要があります。インスタンスが存在していない場合は、手動で構成する必要があります。

- b. データベースをカタログします。一度に 1 つずつ各サーバー・インスタンスにインスタンス・ユーザーとしてログインし、次のコマンドを発行します。

```
db2 catalog database tsmdb1  
db2 attach to instance_name  
db2 update dbm cfg using dftdbpath instance_directory  
db2 detach
```

- c. サーバー・インスタンスが正常に作成されたことを確認します。次のコマンドを出します。

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

- d. ディレクトリーをリストして、IBM Spectrum Protect がサーバー・インスタンスを認識することを確認します。ホーム・ディレクトリーが表示されます (変更しなかった場合)。構成ウィザードを使用した場合は、インスタンス・ディレクトリーが表示されます。次のコマンドを出します。

```
db2 list database directory
```

`TSMDB1` がリストされているのが確認できたら、サーバーを始動できます。

IBM Installation Manager のアンインストール

IBM Installation Manager によってインストールされた製品を使用しなくなった場合、IBM Installation Manager をアンインストールできます。

始める前に

IBM Installation Manager をアンインストールする前に、IBM Installation Manager によりインストールされたすべてのパッケージを確実にアンインストールする必要があります。 アンインストール・プロセスを開始する前に、IBM Installation Manager を閉じてください。

IBM Spectrum Protect のアンインストール

インストール済みのパッケージを表示するには、コマンド・ラインから以下のコマンドを発行します。

```
cd /opt/IBM/InstallationManager/eclipse/tools  
./imcl listInstalledPackages
```

手順

IBM Installation Manager をアンインストールするには、次のステップを実行してください。

1. コマンド・ラインを開いて、ディレクトリーを `/var/ibm/InstallationManager/uninstall` に変更します。
2. 次のコマンドを出します。

```
./uninstall
```

制約事項: `root` ユーザー ID としてシステムにログインしていることが必要です。

IBM Spectrum Protect のアンインストール

第 2 部 Operations Center のインストールおよびアップグレード

IBM Spectrum Protect Operations Center は、ストレージ環境を管理するための Web ベースのインターフェースです。

始める前に

Operations Center をインストールして構成する前に、以下の情報を確認してください。

- 121 ページの『Operations Center のシステム要件』
 - 122 ページの『Operations Center のコンピューターの要件』
 - 122 ページの『ハブ・サーバーおよびスプーク・サーバーの要件』
 - 126 ページの『オペレーティング・システム要件』
 - 127 ページの『Web ブラウザーの要件』
 - 127 ページの『言語要件』
 - 128 ページの『IBM Spectrum Protect クライアント管理サービスの要件と制限』
- 130 ページの『Operations Center に必要な管理者 ID』
- 131 ページの『IBM Installation Manager』
- 132 ページの『インストール・チェックリスト』
- 135 ページの『Operations Center インストール・パッケージの入手』

このタスクについて

表 15 は、Operations Center のインストールまたはアンインストールの方法をリストし、関連の説明を検索する場所を示しています。

Operations Center のアップグレードについては、139 ページの『第 11 章 Operations Center のアップグレード』を参照してください。

表 15. Operations Center をインストールまたはアンインストールするための方法

Method	説明
グラフィカル・ウィザード	<ul style="list-style-type: none">• 136 ページの『グラフィカル・ウィザードを使用した Operations Center のインストール』• 181 ページの『グラフィカル・ウィザードを使用した Operations Center のアンインストール』
コンソール・モード	<ul style="list-style-type: none">• 136 ページの『コンソール・モードでの Operations Center のインストール』• 181 ページの『コンソール・モードでの Operations Center のアンインストール』

表 15. *Operations Center* をインストールまたはアンインストールするための方法 (続き)

Method	説明
サイレント・モード	<ul style="list-style-type: none">136 ページの『サイレント・モードでの Operations Center のインストール』182 ページの『サイレント・モードでの Operations Center のアンインストール』

第 9 章 Operations Center のインストール計画

Operations Center をインストールする前に、システム要件、Operations Center に必要な管理者 ID、およびインストール・プログラムに提供する必要がある情報を理解しておく必要があります。

このタスクについて

Operations Center から、ストレージ環境の以下の主要な局面を管理することができます。

- IBM Spectrum Protect サーバーとクライアント
- バックアップとリストア、アーカイブとリトリーブ、およびマイグレーションと再呼び出しなどのサービス
- ストレージ・プールとストレージ・デバイス

Operations Center には、以下の機能があります。

複数のサーバー用のユーザー・インターフェース

Operations Center を使用して、1 つ以上の IBM Spectrum Protect サーバーを管理できます。

複数のサーバーを含む環境では、1 つのサーバーをハブ・サーバーとして指定し、その他をスポーク・サーバーとして指定できます。ハブ・サーバーは、スポーク・サーバーからアラートおよび状況情報を受け取り、その情報は Operations Center 内の統合ビューに表示することができます。

アラートのモニター

アラートは、サーバーに関連する問題の通知であり、サーバー・メッセージによって起動されます。どのサーバー・メッセージがアラートを起動するかを定義することができ、定義されたメッセージのみがアラートとして Operations Center に表示されたり、E メールで報告されたりします。

このアラートをモニターすると、サーバーに関連する問題を特定および追跡するのに役立ちます。

便利なコマンド・ライン・インターフェース

Operations Center には、拡張機能および構成用のコマンド・ライン・インターフェースが組み込まれています。

Operations Center のシステム要件

Operations Center をインストールする前に、システムが最小要件を満たしていることを確認してください。

Operations Center System Requirements Calculator を使用すると、Operations Center および Operations Center によってモニターされるハブ・サーバーとスポーク・サーバーを実行するためのシステム要件を見積もることができます。

Operations Center のインストール計画

インストール中に検証される要件

表 16 は、インストール中に検証される前提条件をリストし、これらの要件に関する詳しい情報の検索場所を示しています。

表 16. インストール中に検証される要件

要件	詳細
最小メモリー所要量	『Operations Center のコンピューターの要件』
オペレーティング・システム要件	126 ページの『オペレーティング・システム要件』
Operations Center がインストールされるコンピューターのホスト名	132 ページの『インストール・チェックリスト』
Operations Center インストール・ディレクトリーの要件	132 ページの『インストール・チェックリスト』

Operations Center のコンピューターの要件

Operations Center は、IBM Spectrum Protect サーバーも稼働しているコンピューターにインストールするか、別のコンピューターにインストールすることができます。Operations Center をサーバーと同じコンピューターにインストールする場合、そのコンピューターは、Operations Center とサーバーの両方のシステム要件を満たしていなければなりません。

リソース要件

Operations Center を実行するには、以下のリソースが必要です。

- 1 つのプロセッサー・コア
- 4 GB のメモリー
- 1 GB のディスク・スペース

Operations Center でモニターされるハブ・サーバーおよびスパーク・サーバーは、『ハブ・サーバーおよびスパーク・サーバーの要件』で説明しているように、追加のリソースが必要です。

ハブ・サーバーおよびスパーク・サーバーの要件

初めて Operations Center を開いたときに、Operations Center を、ハブ・サーバーとして指定された 1 つの IBM Spectrum Protect サーバーと関連付ける必要があります。複数サーバー環境では、その他のサーバー (スパーク・サーバーと呼ばれる) をハブ・サーバーに接続することができます。

これらのスパーク・サーバーは、ハブ・サーバーにアラートと状況情報を送信します。Operations Center では、ハブ・サーバーおよびすべてのスパーク・サーバーのアラートと状況情報の統合ビューが表示されます。

1 つのサーバーのみが Operations Center によってモニターされている場合は、それにスパーク・サーバーが接続されていない場合でも、そのサーバーはやはりハブ・サーバーと呼ばれます。

表 17 は、Operations Center によって管理されるハブ・サーバーおよび各スパーク・サーバーにインストールする必要がある、IBM Spectrum Protect サーバーのバージョンを示しています。

表 17. ハブ・サーバーおよびスパーク・サーバー上の IBM Spectrum Protect サーバーのバージョン要件

Operations Center	ハブ・サーバー上のバージョン	各スパーク・サーバー上のバージョン
V8.1.5	V8.1.5	V6.3.4 以降 制約事項: V8.1.5 より前のバージョンを使用するサーバーでは、一部の Operations Center 機能が使用できません。

ハブ・サーバーがサポートできるスパーク・サーバーの数

ハブ・サーバーがサポートできるスパーク・サーバーの数は、構成と各スパーク・サーバーの IBM Spectrum Protect のバージョンによって異なります。ただし、一般ガイドラインとして、ハブ・サーバーは 10 台から 20 台の V6.3.4 スパーク・サーバーをサポートできますが、7.1 以降のスパーク・サーバーの場合はより多くサポートできます。

ハブ・サーバーおよびスパーク・サーバー構成の設計上のヒント

ハブおよびスパーク構成の設計では、特に状況モニターのリソース要件について検討してください。また、ハブ・サーバーとスパーク・サーバーのグループ化の方法、および複数のハブ・サーバーを使用するかどうかも検討してください。

Operations Center System Requirements Calculator を使用すると、Operations Center および Operations Center によってモニターされるハブ・サーバーとスパーク・サーバーを実行するためのシステム要件を見積もることができます。

パフォーマンスに影響を与える主な要因

Operations Center のパフォーマンスに最も重大な影響を与える要因は以下のとおりです。

- Operations Center がインストールされているコンピューターのプロセッサーとメモリー
- ハブ・サーバーとスパーク・サーバーのシステム・リソース（ハブ・サーバー・データベースのために使用されているディスク・システムも含む）
- ハブ・サーバーおよびスパーク・サーバーによって管理されているクライアント・ノードまたは仮想マシンのファイル・スペースの数
- Operations Center でのデータ最新表示の頻度

ハブ・サーバーとスパーク・サーバーのグループ化の方法

ハブ・サーバーとスパーク・サーバーは、地理的位置によってグループ化することを検討してください。例えば、同じデータ・センター内でサーバーを管理すると、ファイアウォールや、異なるロケーション間での不十分なネットワーク帯域幅が原

Operations Center のインストール計画

因で発生する問題を回避するのに役立ちます。必要な場合は、以下の 1 つ以上の特性に従って、さらにサーバーを分割することができます。

- サーバーを管理する管理者
- サーバーの資金を提供する組織団体
- サーバー・オペレーティング・システム
- サーバーを実行する言語

ヒント: ハブ・サーバーとスポーク・サーバーが同じ言語で実行されていない場合、Operations Center で破損したテキストが表示されることがあります。

エンタープライズ構成でハブ・サーバーとスポーク・サーバーをグループ化する方法

エンタープライズ構成では、IBM Spectrum Protect サーバーのネットワークはグループとして管理されます。構成マネージャー で行われた変更は、ネットワーク内の 1 つ以上の管理対象サーバー に自動的に配布されます。

Operations Center は通常、ハブ・サーバーとスポーク・サーバー上に専用の管理者 ID を登録して維持します。このモニター管理者は、常にすべてのサーバー上で同じパスワードを持っている必要があります。

エンタープライズ構成を使用する場合、スポーク・サーバーで管理者資格情報が同期化されるプロセスを改善できます。モニター管理者 ID の維持のパフォーマンスと効率を改善するには、以下の手順を実行します。

1. 構成マネージャー・サーバーを Operations Center ハブ・サーバーとして指定します。ハブ・サーバーの構成時に、`IBM-OC-hub_server_name` というモニター管理者 ID が登録されます。
2. ハブ・サーバー上で、モニター管理者 ID を新規または既存のエンタープライズ構成プロファイルに追加します。 NOTIFY SUBSCRIBERS コマンドを発行し、プロファイルを管理対象サーバーに配布します。
3. 1 つ以上の管理対象サーバーを Operations Center スpoke サーバーとして追加します。

Operations Center は、この構成を検出し、構成マネージャーがスポーク・サーバー上でモニター管理者 ID を配布および更新することを許可します。

どのような場合に複数のハブ・サーバーを使用するか

10 から 20 を超える V6.3.4 スpoke サーバーがある場合、またはリソースの制限により環境の分割が必要な場合は、複数のハブ・サーバーを構成し、それぞれのハブ・サーバーに spoke サーバーのサブセットを接続することができます。

制限:

- 単一のサーバーが、ハブ・サーバーと spoke サーバーの両方になることはできません。
- 各 spoke サーバーは、1 つのハブ・サーバーにのみ割り当てることができます。

- 各ハブ・サーバーには、別個の Web アドレスを持つ、Operations Center の別個のインスタンスが必要です。

ハブ・サーバーを選択するためのヒント

ハブ・サーバーには、十分なリソースを持ち、ネットワーク往復待ち時間が最短になるように配置されているサーバーを選択する必要があります。

重要: 同じサーバーを、複数の Operations Center のハブ・サーバーとして使用しないでください。

ハブ・サーバーとして指定するサーバーを決定する際には以下の指針を使用してください。

負荷が軽いサーバーを選択する

クライアント・バックアップやアーカイブなどの操作のために負荷が軽いサーバーを検討してください。負荷が軽いサーバーは、Operations Center のホスト・システムにも適した選択です。

このサーバーには、標準的なサーバーのワークロードと、ハブ・サーバーとして機能するための推定ワークロードの両方を処理するためのリソースがあることを確認してください。

ネットワーク往復待ち時間が最短になるようにサーバーを配置する

ハブ・サーバーとスポーク・サーバー間のネットワーク接続で、往復待ち時間が 5 ミリ秒未満になるように、ハブ・サーバーを配置します。この待ち時間は、通常、これらのサーバーを同じローカル・エリア・ネットワーク (LAN) 上に配置すると達成できます。

適切に調整されていない、他のアプリケーションによって頻繁に使用されている、または往復待ち時間が 5 ミリ秒を超えるネットワークでは、ハブ・サーバーとスポーク・サーバー間の通信状況が低下する可能性があります。例えば、往復待ち時間が 50 ミリ秒以上の場合は、通信タイムアウトが発生し、それによってスポーク・サーバーが切断されたり、Operations Center に再接続されたりする可能性があります。このような長い待ち時間は、長距離の広域ネットワーク (WAN) 通信などで発生する可能性があります。

スポーク・サーバーの距離がハブ・サーバーから離れており、Operations Center で頻繁に切断が起こる場合は、この問題を減らすために、各サーバー上の **ADMINCOMMITTIMEOUT** サーバー・オプションの値を増加することができます。

ハブ・サーバーが状況モニターのリソース要件を満たしていることを確認する

状況モニターは、各サーバー (状況モニターが有効な) 上で追加のリソースを必要とします。必要なリソースは、主にハブ・サーバーとスポーク・サーバーによって管理されるクライアントの数によって決まります。V7.1 以降のスポーク・サーバーを持つハブ・サーバーで使用するリソースは、V6.3.4 スポーク・サーバーを持つハブ・サーバーより少なくなります。

ハブ・サーバーが、プロセッサー使用量、データベース・スペース、アーカイブ・ログ・スペース、および 1 秒当たりの入出力操作 (IOPS) 処理能力のリソース要件を満たしていることを確認してください。

Operations Center のインストール計画

高 IOPS 処理能力を持つハブ・サーバーは、スポーク・サーバーからの大量の着信状況データを処理することができます。ハブ・サーバー・データベース用に以下のストレージ装置を使用すると、この容量を満たすことができます。

- エンタープライズ・レベルのソリッド・ステート・ドライブ (SSD)
- 複数のボリュームや各ボリュームに複数のスピンドルを持つ外部の SAN ディスク・ストレージ装置

クライアントが 1000 に満たない環境では、ハブ・サーバーがいくつかのスポーク・サーバーを管理している場合、ハブ・サーバー・データベースに対してベースライン処理能力の 1000 IOPS を設定することを検討してください。

ご使用の環境で複数のハブ・サーバーが必要かどうかを判別する

10,000 から 20,000 を超えるクライアント・ノードおよび仮想マシン・ファイル・スペースが 1 セットのハブ・サーバーとスポーク・サーバーによって管理されている場合、(特にスポーク・サーバーが 6.3.4 サーバーの場合) リソース要件がハブ・サーバーで使用可能な量を超えてしまう可能性があります。2 番目のサーバーをハブ・サーバーに指定し、スポーク・サーバーを新規ハブ・サーバーに移動して、負荷のバランスを取ることを検討してください。

オペレーティング・システム要件

Operations Center は、AIX システム、Linux システム、および Windows システムで使用可能です。

以下のシステム上で Operations Center を実行できます。

- Linux x86_64 システム:
 - Red Hat Enterprise Linux 6.7
 - Red Hat Enterprise Linux 7.1
 - SUSE Linux Enterprise Server 11、Service Pack 4 以降
 - SUSE Linux Enterprise Server 12
- Linux on System z (s390x 64 ビット・アーキテクチャー) システム:
 - Red Hat Enterprise Linux 7.1
 - SUSE Linux Enterprise Server 12
- Linux on Power Systems (リトル・エンディアン) システム:
 - Red Hat Enterprise Linux 7.3 (PPC64LE アーキテクチャー)

要件に関する最新情報については、Software and Hardware Requirements を参照してください。

Web ブラウザーの要件

Operations Center では、Apple、Google、Microsoft、および Mozilla の各 Web ブラウザーを実行することができます。

Web ブラウザーで Operations Center の最適な表示ができるように、必ずシステムの画面解像度を最小で 1024 X 768 ピクセルに設定してください。

最適なパフォーマンスのためには、JavaScript パフォーマンスが優れた Web ブラウザーを使用し、ブラウザーのキャッシュを有効にしてください。

Operations Center では、以下の Web ブラウザーを実行できます。

- iPad の Apple Safari

制約事項: iOS 8.x または iOS 9.x 上で Apple Safari を実行している場合、Operations Center とのセキュア通信に自己署名証明書を（証明書の追加構成なしで）使用することはできません。認証局（CA）認証を使用するか、必要に応じて自己署名証明書を構成してください。手順については、技術情報 <http://www.ibm.com/support/docview.wss?uid=swg21963153> を参照してください。

- Google Chrome 54 以降
- Microsoft Internet Explorer 11 以降
- Mozilla Firefox ESR 45 またはバージョン 48 以降

Transport Layer Security (TLS) 1.2 プロトコルを使用して Operations Center と Web ブラウザーの間の通信を保護する必要があります。Web ブラウザーは TLS 1.2 をサポートしている必要があります。TLS 1.2 が有効に設定されている必要があります。Web ブラウザーはこれらの要件を満たしていない場合、SSL エラーを表示します。

言語要件

デフォルトにより、Operations Center では、Web ブラウザーで使用されている言語が使用されます。ただし、インストール処理では、オペレーティング・システムで使用されている言語が使用されます。Web ブラウザーとオペレーティング・システムが、ユーザーが必要とする言語に設定されていることを確認してください。

表 18. Linux システムで使用できる Operations Center の言語の値

言語	言語オプションの値
中国語 (簡体字)	zh_CN
中国語、簡体字 (GBK)	zh_CN.gb18030
中国語 (簡体字) (UTF-8)	zh_CN.utf8
中国語 (繁体字) (Big5)	Zh_TW
中国語 (繁体字) (euc_tw)	zh_TW
中国語 (繁体字) (UTF-8)	zh_TW.utf8
米国英語	en_US
英語 (UTF-8)	en_US.utf8
フランス語	fr_FR

Operations Center のインストール計画

表 18. Linux システムで使用できる Operations Center の言語の値 (続き)

言語	言語オプションの値
フランス語 (UTF-8)	fr_FR.utf8
ドイツ語	de_DE
ドイツ語 (UTF-8)	de_DE.utf8
イタリア語	it_IT
イタリア語 (UTF-8)	it_IT.utf8
日本語 (EUC)	ja_JP
日本語 (UTF-8)	ja_JP.utf8
韓国語	ko_KR
韓国語 (UTF-8)	ko_KR.utf8
ポルトガル語、 ブラジル	pt_BR
ブラジル・ポルトガル語 (UTF-8)	pt_BR.utf8
ロシア語	ru_RU
ロシア語 (UTF-8)	ru_RU.utf8
スペイン語	es_ES
スペイン語 (UTF-8)	es_ES.utf8

IBM Spectrum Protect クライアント管理サービスの要件と制限

IBM Spectrum Protect クライアント管理サービスは、クライアント・ログ・ファイルなどの診断情報を収集するためにバックアップ/アーカイブ・クライアントにインストールされるコンポーネントです。ご使用のシステムでクライアント管理サービスをインストールする前に、要件と制限について理解しておく必要があります。

クライアント管理サービスの資料では、クライアント・システム はバックアップ/アーカイブ・クライアントがインストールされているシステムです。

診断情報は、Linux クライアントおよび Windows クライアントからのみ収集可能ですが、管理者は AIX、Linux、または Windows オペレーティング・システムの Operations Center で診断情報を参照できます。

クライアント管理サービスの要件

クライアント管理サービスをインストールする前に、次の要件を確認してください。

- クライアントにリモート側からアクセスするには、Operations Center 管理者にシステム権限または次のいずれかのクライアント権限レベルが必要です。
 - ポリシー権限
 - クライアント所有者権限
 - クライアント・ノード・アクセス権限
- クライアント・システムが次の要件を満たしていることを確認します。
 - クライアント管理サービスは、Linux または Windows オペレーティング・システム上で実行されるクライアント・システムにのみインストールできます。

- バックアップ/アーカイブ・クライアントでサポートされる Linux x86 64 ビット・オペレーティング・システム
- バックアップ/アーカイブ・クライアントでサポートされる Windows 32 ビットおよび 64 ビット・オペレーティング・システム
- クライアント管理サービスと Operations Center の間のデータ転送には、トランスポート層セキュリティー (TLS) 1.2 をインストールする必要があります。基本認証が提供され、データと認証情報は SSL チャネルを経由して暗号化されます。クライアント管理サービスをインストールすると、TLS 1.2 は必要な SSL 証明書とともに自動的にインストールされます。
- Linux クライアント・システムでは、クライアント管理サービスをインストールするために root ユーザー権限が必要です。
- Linux クライアント・システムなど、複数のクライアント・ノードを持つことができるクライアント・システムの場合は、それぞれのノード名がクライアント・システム上で固有であることを確認してください。

ヒント: クライアント管理サービスをインストールした後は、再度インストールする必要はありません。このサービスでは、複数のクライアント・オプション・ファイルを検出できるからです。

クライアント管理サービスの制限

クライアント管理サービスは、バックアップ/アーカイブ・クライアントから診断情報を収集するための基本サービスを提供します。クライアント管理サービスには、以下の制限があります。

- クライアント管理サービスは、バックアップ/アーカイブ・クライアント (IBM Spectrum Protect for Virtual Environments: Data Protection for VMware のデータ・ムーバー・ノードにインストールされているバックアップ/アーカイブ・クライアントを含む) を使用するシステムにのみインストールできます。
- クライアント管理サービスは、その他の IBM Spectrum Protect クライアント・コンポーネントやバックアップ/アーカイブ・クライアントが含まれない製品にインストールすることはできません。
- バックアップ/アーカイブ・クライアントがファイアウォールに保護されている場合、Operations Center は、クライアント管理サービス用に構成されているポートを使用して、ファイアウォールを通過してバックアップ/アーカイブ・クライアントに接続できるようにしてください。デフォルト・ポートは 9028 ですが、これは変更できます。
- クライアント管理サービスは、すべてのクライアント・ログ・ファイルをスキャンして、過去 72 時間の期間にわたる項目を検出します。
- Operations Center の「診断 (Diagnosis)」ページには、バックアップ/アーカイブ・クライアントの基本トラブルシューティング情報が表示されます。ただし、一部のバックアップ問題では、管理者がクライアント・システムにアクセスして詳細な診断情報を入手することが必要になる場合があります。
- クライアント・システム上のクライアント・エラー・ログ・ファイルとスケジュール・ログ・ファイルの合計サイズが 500 MB を超えると、Operations Center へのログ・レコードの送信に遅れが生じことがあります。ログ・ファイルのサイズを制御するには、**errorlogretention** または **errorlogmax** クライアント・オプションを指定して、ログ・ファイルの整理または折り返しを有効にします。

Operations Center のインストール計画

- 同じサーバーにインストールされている複数の IBM Spectrum Protect サーバーへの接続に同じクライアント・ノード名を使用すると、1 つのクライアント・ノードのログ・ファイルしか表示できません。

クライアント管理サービスの更新 (要件、制限、および資料の更新を含む) については、技術情報 1963610 を参照してください。

関連タスク:

156 ページの『IBM Spectrum Protect クライアント管理サービスでの診断情報の収集』

Operations Center に必要な管理者 ID

管理者は、Operations Center にログインするためにハブ・サーバーに有効な ID とパスワードを持っている必要があります。Operations Center がサーバーをモニターできるように、管理者 ID は Operations Center にも割り当てられます。

Operations Center では、以下の IBM Spectrum Protect 管理者 ID が必要です。

ハブ・サーバーに登録されている管理者 ID

ハブ・サーバーに登録されている管理者 ID はすべて、Operations Center へのログインに使用できます。ID の権限レベルにより、どのタスクを実行できるかが決定されます。**REGISTER ADMIN** コマンドを使用して、新規の管理者 ID を作成することができます。

制約事項: 複数サーバー環境で管理者 ID を使用するには、同じパスワードと権限レベルを使用してこの ID をハブ・サーバーとスポーク・サーバーに登録する必要があります。

これらのサーバーの認証を管理するには、以下のいずれかの方法を使用することを検討してください。

- Lightweight Directory Access Protocol (LDAP) サーバー
- 管理者定義に対する変更を自動的に配布するためのエンタープライズ構成機能。

モニター管理者 ID

最初にハブ・サーバーを構成すると、*IBM-OC-server_name* という名前の管理者 ID が、システム権限付きでハブ・サーバーに登録され、指定された初期パスワードに関連付けられます。この ID (モニター管理者と呼ばれることがある) は、Operations Center のみによって使用されるように意図されています。

この ID を削除、ロック、または変更しないでください。同じパスワードを持つ同じ管理者 ID が、追加されるスポーク・サーバーに登録されます。このパスワードは、90 日ごとにハブ・サーバーとスポーク・サーバーで自動的に変更されます。このパスワードを使用または管理する必要はありません。

制約事項: Operations Center は、モニター管理者 ID とパスワードをスポーク・サーバー上で維持します。ただし、これらの資格情報を管理するためにエンタープライズ構成を使用する場合は除きます。資格情報を管理する

ためのエンタープライズ構成の使用について詳しくは、123 ページの『ハブ・サーバーおよびスプーク・サーバー構成の設計上のヒント』を参照してください。

IBM Installation Manager

Operations Center は、IBM Installation Manager を使用します。これは、リモートまたはローカルのソフトウェア・リポジトリを使用して多くの IBM 製品をインストールまたは更新することができるインストール・プログラムです。

IBM Installation Manager の必須バージョンがまだインストールされていない場合は、Operations Center をインストールした時に自動的にインストールまたはアップグレードされます。これは、Operations Center を後で必要に応じて更新またはアンインストールできるように、システムにインストールしたままにしておく必要があります。

IBM Installation Manager で使用される一部の用語の説明を以下にリストします。

オファリング

ソフトウェア製品のインストール可能単位。

Operations Center オファリングには、IBM Installation Manager が Operations Center をインストールするために必要なメディアのすべてが含まれます。

パッケージ

オファリングをインストールするために必要なソフトウェア・コンポーネントのグループ。

Operations Center パッケージには、以下のコンポーネントが含まれています。

- IBM Installation Manager インストール・プログラム
- Operations Center オファリング

パッケージ・グループ

共通親ディレクトリーを共有するパッケージのセット。

リポジトリ

データおよびその他のアプリケーション・リソース用のリモート・ストレージまたはローカル・ストレージのエリア。

Operations Center パッケージは、IBM Fix Central 上のリポジトリに保管されています。

共有リソース・ディレクトリー

パッケージで共有されるソフトウェア・ファイルまたはプラグインが含まれるディレクトリー。

IBM Installation Manager は、インストール関連のファイルを共有リソース・ディレクトリーに保管します。これには、Operations Center の前のバージョンにロールバックするために使用されるファイルが含まれます。

インストール・チェックリスト

Operations Center をインストールする前に、インストールの資格情報などの特定の情報を確認し、インストールのために IBM Installation Manager に指定する入力を判別する必要があります。

以下のチェックリストは、Operations Center をインストールする前に確認または決定する必要がある情報をハイライトで示し、表 19 は、この情報の詳細を説明しています。

- Operations Center がインストールされるコンピューターのホスト名を確認する。
- インストールの資格情報を確認する。
- Operations Center のインストール・ディレクトリーを決定する (デフォルト・パスを受け入れない場合)。
- IBM Installation Manager のインストール・ディレクトリーを決定する (デフォルト・パスを受け入れない場合)。
- Operations Center Web サーバーが使用するポート番号を決定する (デフォルトのポート番号を受け入れない場合)。
- セキュア通信のためのパスワードを決定する。

表 19. Operations Center をインストールする前に確認または決定する情報

通知	詳細
Operations Center がインストールされるコンピューターのホスト名。	<p>ホスト名は、以下の基準を満たしていかなければなりません。</p> <ul style="list-style-type: none">• 2 バイト文字セット (DBCS) 文字および下線文字 (_) を含めてはなりません。• ホスト名にはハイフン文字 (-) を含めることができますが、名前の最終文字としてハイフンを使用することはできません。
インストールの資格情報	<p>Operations Center をインストールするには、以下のユーザー・アカウントを使用する必要があります。</p> <ul style="list-style-type: none">• root ユーザー

表 19. Operations Center をインストールする前に確認または決定する情報 (続き)

通知	詳細
Operations Center のインストール・ディレクトリー	<p>Operations Center は、インストール・ディレクトリーの <code>ui</code> サブディレクトリーにインストールされます。</p> <p>以下のパスは、Operations Center のインストール・ディレクトリーのデフォルト・パスです。</p> <ul style="list-style-type: none"> • <code>/opt/tivoli/tsm</code> <p>例えば、このデフォルト・パスを使用すると、Operations Center は以下のディレクトリーにインストールされます。</p> <pre>/opt/tivoli/tsm/ui</pre> <p>インストール・ディレクトリーのパスは、以下の基準を満たしている必要があります。</p> <ul style="list-style-type: none"> • パスに含める文字数は 128 文字以下でなければならない。 • パスには、ASCII 文字のみを含める必要がある。 • パスに、表示できない制御文字を含めることはできない。 • パスには、次のいずれの文字も使用できない。 <pre>% < > ' " \$ & ; *</pre>
IBM Installation Manager のインストール・ディレクトリー	<p>以下のパスは、IBM Installation Manager のインストール・ディレクトリーのデフォルト・パスです。</p> <ul style="list-style-type: none"> • <code>/opt/IBM/InstallationManager</code>
Operations Center Web サーバーが使用するポート番号。	<p>セキュア (<code>https</code>) ポート番号の値は、以下の基準を満たしていかなければなりません。</p> <ul style="list-style-type: none"> • 番号は、1024 から 65535 の範囲の整数でなければなりません。 • 番号は、既に使用中であったり、別のプログラムに割り振られていてはなりません。 <p>ポート番号を指定しない場合、デフォルト値は 11090 になります。</p> <p>ヒント: 後に、指定したポート番号を覚えていない場合は、以下のファイルを参照してください。ここで、<code>installation_dir</code> 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。</p> <ul style="list-style-type: none"> • <code>installation_dir/ui/Liberty/usr/servers/guiServer/bootstrap.properties</code> <p><code>bootstrap.properties</code> ファイルには、IBM Spectrum Protect サーバーの接続情報が入っています。</p>

Operations Center のインストール計画

表 19. *Operations Center* をインストールする前に確認または決定する情報 (続き)

通知	詳細
セキュア通信のためのパスワード	<p>Operations Center は、Hypertext Transfer Protocol Secure (HTTPS) を使用して Web ブラウザーと通信します。</p> <p>Operations Center では、サーバーと Operations Center 間のセキュア通信が必要です。通信を保護するには、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・ファイルを追加する必要があります。</p> <p>Operations Center のトラストストア・ファイルには、Operations Center が Web ブラウザーとの HTTPS 通信に使用する証明書が入っています。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・サーバーの間にセキュア通信をセットアップする場合、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。</p> <p>トラストストア・ファイルのパスワードは、以下の基準を満たしていなければなりません。</p> <ul style="list-style-type: none">パスワードには、最小 6 文字、最大 64 文字を含める必要があります。パスワードには、少なくとも以下の文字を含める必要があります。<ul style="list-style-type: none">1 つの大文字 (A – Z)1 つの小文字 (a – z)1 つの数字 (0 – 9)以下に示す非英数字文字のうち 2 つ: ~ @ # \$ % ^ & * _ - + = ` () { } [] : ; < > , . ? /

関連タスク:

[148 ページの『セキュア通信の構成』](#)

[153 ページの『Operations Center のトラストストア・ファイルのパスワードのリセット』](#)

第 10 章 Operations Center のインストール

Operations Center は、グラフィック・ウィザード、コンソール・モードのコマンド・ライン、またはサイレント・モードを使用してインストールすることができます。

始める前に

IBM Spectrum Protect サーバーをインストール、構成、および開始するまでは、Operations Center を構成することはできません。そのため、Operations Center をインストールする前に、122 ページの『ハブ・サーバーおよびスパーク・サーバーの要件』に記載されたサーバー・バージョンの要件に従って、該当するサーバー・パッケージをインストールしてください。

Operations Center は、IBM Spectrum Protect サーバーとともにコンピューターにインストールするか、別のコンピューターにインストールすることができます。

Operations Center インストール・パッケージの入手

インストール・パッケージは、IBM ダウンロード・サイト (IBM パスポート・アドバンテージまたは IBM Fix Central など) から入手できます。

このタスクについて

IBM ダウンロード・サイトからパッケージを入手した後、インストール・ファイルを抽出する必要があります。

手順

以下の手順を実行して、Operations Center インストール・ファイルを抽出します。以下の手順では、*version_number* を、インストールしている Operations Center のバージョンに置き換えます。

Linux システム:

- 以下のいずれかのパッケージ・ファイルを、選択したディレクトリーにダウンロードします。
 - version_number.000-IBM-SPOC-LinuxS390.bin*
 - version_number.000-IBM-SPOC-Linuxx86_64.bin*
- このパッケージ・ファイルの実行権限を持っていることを確認します。

必要な場合、次のコマンドを発行してファイル許可を変更します。

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

- 次のコマンドを発行してインストール・ファイルを解凍します。

```
./package_name.bin
```

自己解凍型のパッケージ・ファイルが、このディレクトリーに抽出されます。

Operations Center のインストール

グラフィカル・ウィザードを使用したOperations Centerのインストール

IBM Installation Manager のグラフィカル・ウィザードを使用して、Operations Center をインストールまたは更新することができます。

手順

1. Operations Center インストール・パッケージ・ファイルが抽出されたディレクトリーから、以下のコマンドを発行します。
`./install.sh`
2. ウィザードの指示に従って、IBM Installation Manager および Operations Center のパッケージをインストールします。

次のタスク

141 ページの『Operations Center の構成』を参照してください。

コンソール・モードでのOperations Centerのインストール

コンソール・モードでコマンド・ラインを使用して、Operations Center をインストールまたは更新することができます。

手順

1. インストール・パッケージ・ファイルを抽出したディレクトリーから、以下のプログラムを実行します。
`./install.sh -c`
2. コンソールの指示に従って、Installation Manager および Operations Center のパッケージをインストールします。

次のタスク

141 ページの『Operations Center の構成』を参照してください。

サイレント・モードでの Operations Center のインストール

Operations Center をサイレント・モードでインストールまたはアップグレードすることができます。サイレント・モードのインストールでは、メッセージをコンソールに送信せずに、メッセージおよびエラーをログ・ファイルに保管します。

始める前に

サイレント・インストール・メソッドの使用時にデータ入力を行うには、応答ファイルを使用できます。 `input` ディレクトリーに以下のサンプル応答ファイルが含まれています。このディレクトリーは、インストール・パッケージが解凍されるディレクトリーです。

`install_response_sample.xml`

Operations Center をインストールするには、このファイルを使用します。

`update_response_sample.xml`

Operations Center をアップグレードするには、このファイルを使用します。

これらのファイルには、不要な警告を回避するのに役立つデフォルト値が含まれています。これらのファイルを使用するには、ファイルに記載されている指示に従ってください。

応答ファイルをカスタマイズしたい場合は、ファイル内のオプションを変更することができます。応答ファイルについては、応答ファイルを参照してください。

手順

1. 応答ファイルを作成します。サンプル応答ファイルを変更するか、または独自のファイルを作成することができます。

ヒント: コンソール・モード・インストールの一部として応答ファイルを生成するには、コンソール・モード・インストールのオプションの選択を完了してください。次に、前に選択されたオプションに従って応答ファイルを生成するには、「要約」 パネルで「G」を入力します。

2. 応答ファイルの Operations Center トラストストアのパスワードを作成します。

`install_response_sample.xml` ファイルを使用中の場合には、ファイルの以下の行にパスワードを追加します。ここで、`mypassword` はパスワードを表します。

```
<variable name='ssl.password' value='mypassword' />
```

このパスワードについて詳しくは、132 ページの『インストール・チェックリスト』を参照してください。

ヒント: Operations Center をアップグレードする際に、`update_response_sample.xml` ファイルを使用する場合はトラストストアのパスワードは不要です。

3. インストール・パッケージが抽出されたディレクトリーから次のコマンドを発行して、サイレント・インストールを開始します。値 `response_file` は、応答ファイル・パスとファイル名を示します。
 -

```
./install.sh -s -input response_file -acceptLicense
```

次のタスク

141 ページの『Operations Center の構成』を参照してください。

第 11 章 Operations Center のアップグレード

Operations Center のアップグレードは、グラフィック・ウィザード、コンソール・モードのコマンド・ライン、またはサイレント・モードのいずれの方式を使用しても行えます。

始める前に

Operations Center をアップグレードする前に、システム要件とインストール・チェックリストを確認します。Operations Center の新しいバージョンでは、要件と考慮事項が、現在使用しているバージョンよりも多くなっているか、異なっている可能性があります。

このタスクについて

Operations Center のアップグレードの手順は、Operations Center のインストールの手順と同じですが、以下の例外があります。

- IBM Installation Manager の「インストール」機能ではなく、「更新」機能を使用します。

ヒント: IBM Installation Manager では、更新 は、インストール済みソフトウェア・パッケージに対する更新および修正を検出してインストールすることを意味します。この意味では、更新 とアップグレード は同義です。

- Operations Center をサイレント・モードでアップグレードする場合は、トラストストア・ファイルのパスワードを作成するステップをスキップすることができます。

Operations Center のアップグレード

第 12 章 Operations Center の概要

Operations Center を使用してストレージ環境を管理するには、その前に構成を行う必要があります。

このタスクについて

Operations Center をインストールした後で、次の基本的な構成手順を行います。

1. ハブ・サーバーを指定する。
2. いくつかの spoke・サーバーを追加する。
3. オプションで、ハブ・サーバーと spoke・サーバー上で E メール・アラートを構成する

図 1 には、Operations Center の構成を示します。

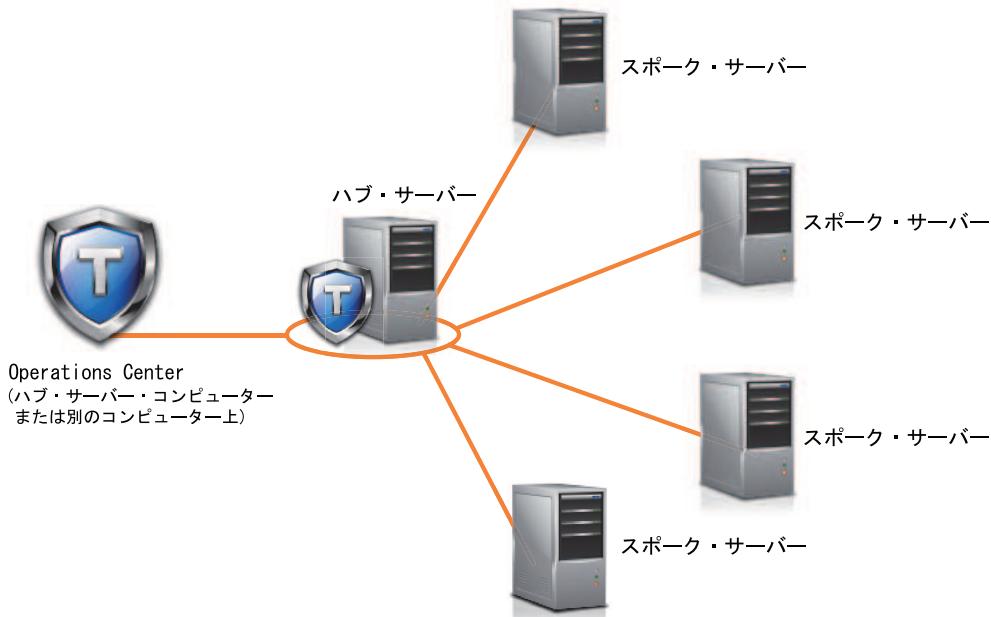


図 1. ハブ・サーバーと spoke・サーバーを持つ Operations Center の構成の例

Operations Center の構成

初めて Operations Center を開いたときに、ストレージ環境を管理するように構成する必要があります。Operations Center を、ハブ・サーバーとして指定された IBM Spectrum Protect サーバーと関連付ける必要があります。その後で、追加の IBM Spectrum Protect サーバーを spoke・サーバーとして接続できます。

Operations Center の概要

ハブ・サーバーの指定

初めて Operations Center に接続するときに、どの IBM Spectrum Protect サーバーをハブ・サーバーにするかを指定する必要があります。

始める前に

Operations Center では、ハブ・サーバーと Operations Center 間のセキュア通信が必要です。通信を保護するには、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・ファイルを追加する必要があります。詳しくは、148 ページの『Operations Center とハブ・サーバー間のセキュア通信』を参照してください。

手順

Web ブラウザーで、次のアドレスを入力します。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、*secure_port* は、そのコンピューター上で Operations Center が HTTPS 通信用に使用するポート番号を表します。

`https://hostname:secure_port/oc`

ヒント:

- URL では大文字と小文字が区別されます。例えば、示されているように、「oc」を小文字で入力してください。
- ポート番号について詳しくは、インストール・チェックリストを参照してください。
- 初めて Operations Center に接続している場合は、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
- サーバーのイベント・レコードの保存期間が 14 日より少ない場合、そのサーバーをハブ・サーバーとして構成すると、期間が自動的に 14 日にリセットされます。

次のタスク

ご使用環境に複数の IBM Spectrum Protect サーバーがある場合は、他のサーバーをスポーク・サーバーとしてハブ・サーバーに追加します。

重要: ハブ・サーバーまたはスポーク・サーバーとして構成した後は、サーバーの名前を変更しないでください。

関連概念:

122 ページの『ハブ・サーバーおよびスポーク・サーバーの要件』

130 ページの『Operations Center に必要な管理者 ID』

スプーク・サーバーの追加

Operations Center のハブ・サーバーを構成した後、そのハブ・サーバーに 1 つ以上のスプーク・サーバーを追加することができます。

始める前に

Transport Layer Security (TLS) プロトコルを使用してハブ・サーバーとスプーク・サーバーの間の通信を保護する必要があります。通信を保護するには、ハブ・サーバーのトラストストア・ファイルにスプーク・サーバーの証明書を追加する必要があります。

手順

- Operations Center メニュー・バーで、「サーバー」をクリックします。「サーバー」ページが開きます。

「サーバー」ページの表では、サーバーの状況が「モニター対象外」になっている可能性があります。この状況は、管理者が **DEFINE SERVER** コマンドを使用してこのサーバーをハブ・サーバーに対して定義したが、サーバーがまだスプーク・サーバーとして構成されていないことを意味しています。

- 次の手順のいずれかを実行してください。
 - サーバーをクリックして強調表示し、表メニュー・バーで「スプークのモニター」をクリックします。
 - 追加したいサーバーがテーブルに表示されていない場合、および、セキュアな SSL/TLS 通信を必要としている場合は、テーブルのメニュー・バーで「+ スプーク」をクリックします。
- 必要な情報を提供し、スプーク構成ウィザードの手順を完了します。

ヒント: サーバーのイベント・レコードの保存期間が 14 日より少ない場合、そのサーバーをスプーク・サーバーとして構成すると、期間が自動的に 14 日にリセットされます。

メール・アラートの管理者への送信

アラートは、IBM Spectrum Protect サーバーに関する問題の通知であり、サーバー・メッセージによって起動されます。アラートは、Operations Center に表示され、サーバーから管理者に E メールで送信することができます。

始める前に

アラートに関する管理者への E メール通知を構成する前に、以下の要件を満たしていることを確認してください。

- E メールでアラートを送受信するには、SMTP サーバーが必要です。また、E メールでアラートを送信するサーバーは、SMTP サーバーへのアクセス権限が必要です。

ヒント: 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は SMTP サーバーへのアクセス権限は必要ありません。

Operations Center の概要

- 管理者は、E メール通知を構成するためのシステム特権を持っていなければなりません。

このタスクについて

E メール通知は、アラートの最初の発生時のみ送信されます。また、E メール通知を構成する前にアラートが生成された場合、そのアラートの E メール通知は送信されません。

以下の方法で、E メール通知を構成できます。

- 個々のアラートの通知の送信
- アラート要約の送信

アラート要約には、現在のアラートに関する情報が含まれます。要約には、アラートの合計数、アクティブおよび非アクティブ・アラートの合計数、最も古いアラート、最も新しいアラート、および最も頻繁に発生しているアラートが含まれています。

E メールによるアラート要約を受信する最大 3 人の管理者を指定できます。アラート要約は、ほぼ毎時に送信されます。

手順

アラートに関する管理者への E メール通知を構成するには、E メール通知の発信元の各ハブ・サーバーおよびスパーク・サーバーに対して、以下の手順を実行します。

- アラート・モニターがオンになっていることを確認するために、次のコマンドを発行します。

QUERY MONITORSETTINGS

- コマンド出力で、アラート・モニターがオフであることが示された場合は、次のコマンドを発行します。そうでなり場合は、次の手順に進みます。

SET ALERTMONITOR ON

- E メール通知の送信を有効にするために、次のコマンドを発行します。

SET ALERTEMAIL ON

- E メール通知の送信に使用する SMTP サーバーを定義するために、次のコマンドを発行します。

SET ALERTEMAILSMTPHOST *host_name*

- SMTP サーバーのポート番号を指定するために、次のコマンドを発行します。

SET ALERTEMAILSMTPPORT *port_number*

デフォルトのポート番号は 25 です。

- アラートの送信者の E メール・アドレスを指定するために、次のコマンドを発行します。

SET ALERTEMAILFROMADDR *email_address*

- E メール通知を受信する必要がある管理者 ID ごとに、E メール通知をアクティブにして、E メール・アドレスを指定するために、次のコマンドのいずれかを発行します。

```
REGISTER ADMIN admin_name ALERT=YES EMAILADDRESS=email_address
UPDATE ADMIN admin_name ALERT=YES EMAILADDRESS=email_address
```

8. 以下のオプションの一方または両方を選択して、E メール通知を受信する管理者 ID を指定します。

- 個々のアラートの通知の送信

個々のアラートの E メール通知を受信する管理者 ID を指定または更新するには、次のコマンドのいずれかを発行します。

```
DEFINE ALERTTRIGGER message_number ADMIN=admin_name1,admin_name2
UPDATE ALERTTRIGGER message_number ADDADMIN=admin_name3 DELADMIN=admin_name1
```

ヒント: Operations Center の「アラートの構成」ページで、E メール通知を受け取る管理者を選択することができます。

- アラート要約の送信

E メールでアラート要約を受信する管理者 ID を指定または更新するには、次のコマンドを発行します。

```
SET ALERTSUMMARYTOADMINS admin_name1,admin_name2,admin_name3
```

アラート要約は受信するが、個々のアラートに関する通知は受信しない場合は、以下の手順を実行します。

- 『メール・アラートの一時的な中断』の説明に従って、個々のアラートに関する通知を一時停止します。
- 個別の管理者 ID が次のコマンドにリストされていることを確認します。

```
SET ALERTSUMMARYTOADMINS admin_name1,admin_name2,admin_name3
```

E メール・アラートの複数の管理者への送信

以下の例は、管理者 myadmin、djasmin、および csadmin にメッセージ ANR1075E に関するアラートが E メールで送信される原因となるコマンドを示しています。

```
SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
UPDATE ADMIN djasmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djasmin,csadmin
```

メール・アラートの一時的な中断

特定の状況では、E メール・アラートを一時的に中断したい場合があります。例えば、アラート要約は受け取りたいが、個々のアラートに関する通知は中断したい場合、あるいは管理者が休暇を取っているときは E メール・アラートを中断したい場合があります。

始める前に

143 ページの『メール・アラートの管理者への送信』の説明に従って、管理者への E メール通知を構成します。

Operations Center の概要

手順

個々のアラートまたはアラート要約の E メール通知を中断します。

- 個々のアラートに関する通知の中断

次のいずれかの方法を使用します。

UPDATE ADMIN コマンド

管理者への E メール通知をオフにするには、次のコマンドを発行します。

```
UPDATE ADMIN admin_name ALERT=NO
```

後に再び E メール通知をオンにするには、次のコマンドを発行します。

```
UPDATE ADMIN admin_name ALERT=YES
```

UPDATE ALERTTRIGGER コマンド

特定のアラートが管理者に送信されないようにするには、次のコマンドを発行します。

```
UPDATE ALERTTRIGGER message_number DELADMIN=admin_name
```

管理者へのそのアラートの送信を再び開始するには、以下のコマンドを出します。

```
UPDATE ALERTTRIGGER message_number ADDADMIN=admin_name
```

- アラート要約に関する通知の中断

アラート要約が管理者に送信されないようにするには、次のコマンドのリストからその管理者 ID を除去します。

```
SET ALERTSUMMARYTOADMINS admin_name1,admin_name2,admin_name3
```

管理者 ID が上記のコマンドにリストされている場合、個別の管理者 ID への個々のアラートに関する通知が中断されても、その管理者は E メールによるアラート要約を受け取ります。

ログイン画面へのカスタマイズ・テキストの追加

組織のソフトウェアの利用条件などのカスタマイズ・テキストを Operations Center のログイン画面に追加して、Operations Center のユーザーがユーザー名とパスワードを入力する前にそれらのテキストを確認できるようにすることができます。

手順

ログイン画面にカスタマイズ・テキストを追加するには、以下のステップを実行します。

1. Operations Center がインストールされているコンピューター上で、次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。

```
installation_dir/ui/Liberty/usr/servers/guiServer
```

2. ディレクトリー内で、ログイン画面に追加するテキストが入った `loginText.html` というファイルを作成します。 特殊な非 ASCII テキストは、UTF-8 でエンコードされている必要があります。

ヒント: HTML タグを追加してテキストをフォーマット設定できます。

3. Operations Center のログイン画面で、追加したテキストを確認します。

Operations Center を開くには、Web ブラウザーで次のアドレスを入力します。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、*secure_port* は、そのコンピューター上で Operations Center が HTTPS 通信用に使用するポート番号を表します。

`https://hostname:secure_port/oc`

REST サービスの有効化

Representational State Transfer (REST) を使用するアプリケーションは、Operations Center に接続することで、ストレージ環境を照会および管理することができます。

このタスクについて

この機能を有効にすると、REST サービスは、以下のアドレスに呼び出しを送信することで、ハブ・サーバーおよびスポーク・サーバーと対話できるようになります。

`https://oc_host_name:port/oc/api`

ここで、*oc_host_name* は Operations Center ホスト・システムのネットワーク名または IP アドレス、*port* は Operations Center のポート番号です。デフォルトのポート番号は 11090 です。

Operations Center で使用可能な REST サービスについては、技術情報 <http://www-01.ibm.com/support/docview.wss?uid=swg21997347> を参照するか、以下の REST 呼び出しを発行します。

`https://oc_host_name:port/oc/api/help`

手順

1. Operations Center メニュー・バーで、設定アイコン  上にカーソルを移動し、「設定」をクリックします。
2. 「一般」ページで、「管理 REST API の使用可能化」チェック・ボックスを選択します。
3. 「保存」をクリックします。

セキュア通信の構成

Operations Center は、Hypertext Transfer Protocol Secure (HTTPS) を使用して Web ブラウザーと通信します。Transport Layer Security (TLS) により、Operations Center とハブ・サーバー間および、ハブ・サーバーと関連のスパーク・サーバー間の通信を保護します。

このタスクについて

IBM Spectrum Protect サーバーと Operations Center 間、およびハブ・サーバーとスパーク・サーバー間のセキュア通信のために TLS 1.2 が必要です。

Operations Center とハブ・サーバー間のセキュア通信

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・ファイルに追加する必要があります。

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ーです。トラストストア・ファイルには、Operations Center が Web ブラウザーとの HTTPS 通信に使用する証明書が入っています。

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します。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、パスワードをリセットすることができます。 153 ページの『Operations Center のトラストストア・ファイルのパスワードのリセット』を参照してください。

手順

- cert256.arm 証明書を、ハブ・サーバーの鍵データベース・ファイル内のデフォルト証明書として指定します。

cert256.arm をデフォルト証明書として指定するには、以下の手順を実行します。

- a. ハブ・サーバー・インスタンス・ディレクトリーから、次のコマンドを発行します。

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed  
-label "TSM Server SelfSigned SHA Key"
```
- b. 鍵データベース・ファイルに対する変更を受け取れるように、ハブ・サーバーを再始動します。
2. cert256.arm 証明書がハブ・サーバーの鍵データベース・ファイル内のデフォルト証明書として設定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。

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```
3. Operations Center Web サーバーを停止します。
4. Operations Center がインストールされているオペレーティング・システムのコマンド・ラインに進みます。

5. **iKeycmd** ユーティリティーまたは **iKeyman** ユーティリティーを使用して、Operations Center のトラストストア・ファイルに証明書を追加します。

iKeycmd ユーティリティーは、コマンド・ライン・インターフェースであり、**iKeyman** ユーティリティーは IBM Key Management グラフィカル・ユーザー・インターフェースを開きます。

iKeycmd ユーティリティーと **iKeyman** ユーティリティーは root ユーザーとして実行する必要があります。

コマンド・ライン・インターフェースを使用して、TLS 証明書を追加するには、以下の手順を実行します。

- 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。
 - *installation_dir/ui/jre/bin*
- iKeycmd** コマンドを発行し、ハブ・サーバーの鍵データベース・ファイル内のデフォルト証明書として *cert256.arm* 証明書を追加します。

```
ikeycmd -cert -add
-db /installation_dir/Liberty/usr/servers/guiServer/gui-truststore.jks
-file /fvt/comfrey/srv/cert256.arm
-label 'label description'
-pw 'password' -type jks -format ascii -trust enable
```

ここで、

installation_dir

Operations Center がインストールされるディレクトリー。

ラベルの説明

ラベルに割り当てる説明。

パスワード

Operations Center のインストール時に作成したパスワード。パスワードをリセットするには、Operations Center をアンインストールし、.jks ファイルを削除してから Operations Center を再インストールします。

「IBM 鍵管理」ウィンドウを使用して証明書を追加するには、以下の手順を実行します。

- 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。
 - *installation_dir/ui/jre/bin*
- 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**
- 「鍵データベース・ファイル」 > 「オープン」をクリックします。
- 「オープン」ウィンドウで、「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。
 - *installation_dir/ui/Liberty/usr/servers/guiServer*

Operations Center の概要

- e. guiServer ディレクトリーで、gui-truststore.jks ファイルを選択します。
- f. 「オープン」をクリックして、「OK」をクリックします。
- g. 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。
- h. 「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。
- i. 「追加」をクリックします。
- j. 「オープン」ウィンドウで、「参照」をクリックして、次の例に示すように、ハブ・サーバー・インスタンス・ディレクトリーに進みます。
 - /opt/tivoli/tsm/server/bin

この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。

- 1) 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。
 - *installation_dir/ui/Liberty/usr/servers/guiServer*
- 2) 「オープン」ウィンドウで、guiServer ディレクトリーに進みます。
- k. 証明書として cert256.arm 証明書を選択します。

ヒント: 選択した証明書を、ハブ・サーバーの鍵データベース・ファイル内のデフォルト証明書として設定する必要があります。詳しくは、ステップ 1 (148 ページ) とステップ 2 (148 ページ) を参照してください。

- l. 「オープン」をクリックして、「OK」をクリックします。
- m. 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。
- n. 「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。
- o. 「IBM 鍵管理」ウィンドウを閉じます。
6. Operations Center Web サーバーを始動します。
7. Operations Center への初回接続時に、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・サーバーと通信するためのポート番号を特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。

Operations Center が以前に構成されていた場合は、`serverConnection.properties` ファイルの内容を表示して、接続情報を確認する

ことができます。`serverConnection.properties` ファイルは、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あります。

- `installation_dir/ui/Liberty/usr/servers/guiServer`

次のタスク

ハブ・サーバーとスポーク・サーバー間の TLS 通信のセットアップについては、『ハブ・サーバーとスポーク・サーバー間の通信の保護』を参照してください。

ハブ・サーバーとスポーク・サーバー間の通信の保護

Transport Layer Security (TLS) プロトコルを使用してハブ・サーバーとスポーク・サーバーの間の通信を保護するには、ハブ・サーバーに対してスポーク・サーバーの証明書、そしてスポーク・サーバーに対してハブ・サーバーの証明書を定義する必要があります。また、スポーク・サーバーをモニターするように Operations Center を構成することも必要です。

このタスクについて

ハブ・サーバーは、スポーク・サーバーから状況およびアラートの情報を受信して、この情報を Operations Center で表示します。スポーク・サーバーから状況とアラートの情報を受信するには、スポーク・サーバーの証明書をハブ・サーバーのトラストストア・ファイルに追加する必要があります。また、スポーク・サーバーをモニターするように Operations Center を構成することも必要です。

クライアント更新の自動デプロイメントなど、Operations Center の他の機能を有効にするには、ハブ・サーバーの証明書をスポーク・サーバーのトラストストア・ファイルに追加する必要があります。

手順

1. スpoke サーバーの証明書を hub サーバーに定義する際は、以下の手順を実行します。
 - a. スpoke サーバー上で、spoke サーバー・インスタンスのディレクトリーに移動します。
 - b. 必要な `cert256.arm` 証明書を、spoke サーバーの鍵データベース・ファイル内のデフォルト証明書として指定します。次のコマンドを出します。

```
gsk8capicmd_64 -cert -setDefault -db cert.kdb -stashed  
-label "TSM Server SelfSigned SHA Key"
```
 - c. スpoke サーバーの鍵データベース・ファイル内の証明書を確認します。次のコマンドを出します。

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```
 - d. スpoke サーバーの `cert256.arm` ファイルを hub サーバーに安全に転送します。
 - e. hub サーバー上で、hub サーバー・インスタンス・ディレクトリーに移動します。
 - f. hub サーバーに対して spoke サーバーの証明書を定義します。hub サーバー・インスタンス・ディレクトリーから次のコマンドを発行します。

Operations Center の概要

ここで、*spoke_servername* はスプーク・サーバーの名前であり、*spoke_cert256.arm* はスプーク・サーバーの証明書のファイル名です。

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii  
-label spoke_servername -file spoke_cert256.arm
```

2. ハブ・サーバーの証明書をスプーク・サーバーに定義する際は、以下の手順を実行します。

- a. ハブ・サーバー上で、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。

- b. 必須の *cert256.arm* 証明書を、ハブ・サーバーの鍵データベース・ファイル内のデフォルト証明書として指定します。次のコマンドを出します。

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed  
-label "TSM Server SelfSigned SHA Key"
```

- c. スプーク・サーバーの鍵データベース・ファイル内の証明書を確認します。次のコマンドを出します。

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

- d. ハブ・サーバーの *cert256.arm* ファイルをスプーク・サーバーに安全に転送します。

- e. スプーク・サーバー上で、スプーク・サーバー・インスタンスのディレクトリーに移動します。

- f. スプーク・サーバーに対してハブ・サーバーの証明書を定義します。スプーク・サーバー・インスタンス・ディレクトリーから次のコマンドを発行します。ここで、*hub_servername* はスプーク・サーバーの名前であり、*hub_cert256.arm* はハブ・サーバーの証明書のファイル名です。

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii  
-label hub_servername -file hub_cert256.arm
```

3. ハブ・サーバーとスプーク・サーバーを再始動します。

4. スプーク・サーバーをハブ・サーバーに、そしてハブ・サーバーをスプーク・サーバーに定義する際は、以下の手順を実行します。

- a. ハブ・サーバーとスプーク・サーバーの両方で以下のコマンドを実行します。

```
SET SERVERPASSWORD server_password  
SET SERVERHLADDRESS ip_address  
SET SERVERLLADDRESS tcp_port
```

- b. ハブ・サーバーでは、次の例に従って、**DEFINE SERVER** コマンドを発行します。

```
DEFINE SERVER spoke_servername HLA=spoke_address  
LLA=spoke_SSLLTCPADMINPort SERVERPA=spoke_serverpassword
```

- c. スプーク・サーバーでは、次の例に従って、**DEFINE SERVER** コマンドを発行します。

```
DEFINE SERVER hub_servername HLA=hub_address  
LLA=hub_SSLLTCPADMINPort SERVERPA=hub_serverpassword
```

ヒント: デフォルトでは、サーバーがオブジェクト・データを送受信する場合を除いて、サーバー通信は暗号化されます。オブジェクト・データは TCP/IP を使用して送受信します。オブジェクト・データを暗号化しないように選択することで、サーバー・パフォーマンスは TCP/IP セッションを経由した通信と同様になり、セッションは保護されます。サーバーがオブ

ジェクト・データを送受信する場合でも、指定されたサーバーとのすべての通信を暗号化するには、**DEFINE SERVER** コマンドで SSL=YES パラメーターを指定します。

5. スポーク・サーバーをモニターするように Operations Center を構成するには、以下の手順を実行します。
 - a. Operations Center メニュー・バーで、「サーバー」をクリックします。スパーク・サーバーは「モニター対象外」状況です。この状況は、**DEFINE SERVER** コマンドを使用してこのサーバーがハブ・サーバーに対して定義されているものの、サーバーがまだスパーク・サーバーとして構成されていないことを意味しています。
 - b. スパーク・サーバーをクリックして項目を強調表示し、「スパークのモニター」をクリックします。

Operations Center のトラストストア・ファイルのパスワードのリセット

Operations Center とハブ・サーバー間のセキュア通信をセットアップするには、Operations Center のトラストストア・ファイルのパスワードを知っている必要があります。このパスワードは、Operations Center のインストール時に作成します。パスワードが不明な場合は、リセットすることができます。

このタスクについて

パスワードをリセットするには、新規パスワードを作成し、Operations Center のトラストストア・ファイルを削除して、Operations Center Web サーバーを再始動する必要があります。

重要: トラストストアのパスワードが不明な場合のみ、以下のステップを実行してください。トラストストアのパスワードを知っており、パスワードを変更するだけの場合には、以下のステップを実行しないでください。パスワードをリセットするには、トラストストア・ファイルを削除する必要があります。これにより、トラストストア・ファイルに保管済みの証明書はすべて削除されます。トラストストアのパスワードを知っている場合、iKeycmd または iKeyman のユーティリティーを使用してパスワードを変更できます。

手順

1. Operations Center Web サーバーを停止します。
2. 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。
`installation_dir/ui/Liberty/usr/servers/guiServer`
3. `bootstrap.properties` ファイルを開きます。このファイルには、トラストストア・ファイルのパスワードが入っています。パスワードが暗号化されていない場合、そのパスワードを使用してトラストストア・ファイルを開くことができます。パスワードをリセットする必要はありません。

以下の例は、暗号化されたパスワードと暗号化されていないパスワード間の相違を示しています。

Operations Center の概要

暗号化されたパスワードの例

暗号化されたパスワードには、先頭にテキスト・ストリング {xor} が付いています。

次の例は、**tsm.truststore.pswd** パラメーターの値として、暗号化されたパスワードを示しています。

```
tsm.truststore.pswd={xor}MiYPPiwsKDAAt0w==
```

暗号化されていないパスワードの例

次の例は、**tsm.truststore.pswd** パラメーターの値として、暗号化されていないパスワードを示しています。

```
tsm.truststore.pswd=J8b%^B
```

4. パスワードをリセットするには、**bootstrap.properties** ファイル内のパスワードを新規パスワードに置き換えます。パスワードは、暗号化パスワードで置き換えることも、非暗号化パスワードで置き換えることもできます。後で使用するために、暗号化されていないパスワードを覚えておいてください。

暗号化されたパスワードを作成する場合、以下の手順を実行します。

- a. 暗号化されていないパスワードを作成します。

トラストストア・ファイルのパスワードは、以下の基準を満たしていかなければなりません。

- パスワードには、最小 6 文字、最大 64 文字を含める必要があります。
- パスワードには、少なくとも以下の文字を含める必要があります。
 - 1 つの大文字 (A – Z)
 - 1 つの小文字 (a – z)
 - 1 つの数字 (0 – 9)
 - 以下に示す非英数字文字のうち 2 つ:
~ @ # \$ % ^ & * _ - + = ` |
() { } [] : ; < > , . ? /

- b. オペレーティング・システムのコマンド・ラインから、以下のディレクトリーに移動します。

```
installation_dir/ui/Liberty/bin
```

- c. パスワードを暗号化するには、次のコマンドを発行します。ここで、*myPassword* は、暗号化されていないパスワードを表します。

```
securityUtility encode myPassword --encoding=aes
```

5. **bootstrap.properties** ファイルをクローズします。

6. 次のディレクトリーに移動します。

```
installation_dir/ui/Liberty/usr/servers/guiServer
```

7. *gui-truststore.jks* ファイルを削除します。これは Operations Center のトラストストア・ファイルです。

8. Operations Center Web サーバーを開始します。

タスクの結果

Operations Center の新しいトラストストア・ファイルが自動的に作成され、Operations Center の TLS 証明書がそのトラストストア・ファイルに自動的に入れられます。

Web サーバーの開始と停止

Operations Center の Web サーバーは、サービスとして実行され、自動的に開始します。例えば、構成変更を行う場合などに、Web サーバーを停止および開始する必要がある場合があります。

手順

Web サーバーを停止および開始します。

- 以下のコマンドを発行します。
 - サーバーを停止する場合:
`service opscenter.rc stop`
 - サーバーを開始する場合:
`service opscenter.rc start`
 - サーバーを再始動するには、次のコマンドを実行します。
`service opscenter.rc restart`

サーバーが稼働しているかどうかを判別するには、次のコマンドを発行します。

```
service opscenter.rc status
```

Operations Center の開始

Operations Center を開始すると、デフォルトで「概要」ページが表示されます。ただし、Web ブラウザーで、Operations Center にログインしたときに開くページをブックマークすることができます。

手順

1. Web ブラウザーで、次のアドレスを入力します。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、*secure_port* は、そのコンピューター上で Operations Center が HTTPS 通信用に使用するポート番号を表します。

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

ヒント:

- URL では大文字と小文字が区別されます。例えば、示されているように、「oc」を小文字で入力してください。
 - HTTPS 通信用のデフォルト・ポート番号は 11090 ですが、別のポート番号を Operations Center のインストール時に指定することができます。
2. ハブ・サーバーに登録されている管理者 ID を使用してログインします。

Operations Center の概要

「概要」ページで、クライアント、サービス、サーバー、ストレージ・プール、およびストレージ・デバイスの要約情報を表示することができます。項目をクリックするか、Operations Center メニュー・バーを使用して、詳細を表示することができます。

モバイル・デバイスからのモニター: ストレージ環境をリモートからモニターするには、モバイル・デバイスの Web ブラウザーで Operations Center の「概要」ページを表示します。Operations Center は、iPad の Apple Safari Web ブラウザーをサポートします。その他のモバイル・デバイスも使用できます。

IBM Spectrum Protect クライアント管理サービスでの診断情報の収集

クライアント管理サービス は、バックアップ/アーカイブ・クライアントに関する診断情報を収集し、その情報を基本モニター機能のために Operations Center が使用できるようにします。

このタスクについて

クライアント管理サービスをインストールした後、Operations Center の「診断 (Diagnosis)」ページを表示して、バックアップ/アーカイブ・クライアントのトラブルシューティング情報を入手できます。

診断情報は、Linux クライアントおよび Windows クライアントからのみ収集可能ですが、管理者は AIX、Linux、または Windows オペレーティング・システムの Operations Center で診断情報を参照できます。

データ・ムーバーに関する診断情報を収集するため、IBM Spectrum Protect for Virtual Environments: Data Protection for VMware のデータ・ムーバー・ノードに クライアント管理サービス をインストールすることもできます。

ヒント: クライアント管理サービスの資料では、クライアント・システム はバックアップ/アーカイブ・クライアントがインストールされているシステムです。

グラフィカル・ウィザードを使用したクライアント管理サービスのインストール

クライアント・ログ・ファイルなど、バックアップ/アーカイブ・クライアントに関する診断情報を収集するには、管理するクライアント・システムにクライアント管理サービスをインストールする必要があります。

始める前に

128 ページの『IBM Spectrum Protect クライアント管理サービスの要件と制限』を確認します。

このタスクについて

クライアント管理サービスは、バックアップ/アーカイブ・クライアントと同じコンピューターにインストールする必要があります。

手順

1. クライアント管理サービス用のインストール・パッケージを IBM ダウンロード・サイト (IBM パスポート・アドバンテージや IBM Fix Central など) からダウンロードします。<version>-IBM-SPCMS-<operating system>.bin のようなファイル名を探します。

次の表に、インストール・パッケージの名前を示します。

クライアント・オペレーティング・システム	インストール・パッケージ名
Linux x86 64 ビット	8.1.x.000-IBM-SPCMS-Linuxx64.bin
Windows 32 ビット	8.1.x.000-IBM-SPCMS-Windows32.exe
Windows 64 ビット	8.1.x.000-IBM-SPCMS-Windows64.exe

2. 管理するクライアント・システム上にディレクトリーを作成して、そこにインストール・パッケージをコピーします。
3. インストール・パッケージ・ファイルの内容を抽出します。
 - Linux クライアント・システム上で、次の手順を実行します。
 - a. 次のコマンドを発行して、ファイルを実行可能ファイルに変更します。
chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
 - b. 次のコマンドを出します。
. /8.1.x.000-IBM-SPCMS-Linuxx64.bin
 - Windows クライアント・システム上で、Windows エクスプローラーに表示されているインストール・パッケージ名をダブルクリックします。
4. インストール・ファイルと関連のファイルを抽出したディレクトリーから、インストール・バッチ・ファイルを実行します。これは、ステップ 2 で作成したディレクトリーです。
 - Linux クライアント・システムでは、次のコマンドを発行します。
. /install.sh
 - Windows クライアント・システムでは、「install.bat」をダブルクリックします。
5. クライアント管理サービスをインストールするには、IBM Installation Manager ウィザードの説明に従ってください。

IBM Installation Manager がまだクライアント・システムにインストールされていない場合は、「IBM Installation Manager」と「IBM Spectrum Protect Client Management Services」の両方を選択する必要があります。

ヒント: 共有リソース・ディレクトリーと IBM Installation Manager のインストール・ディレクトリーのデフォルトの場所を受け入れることができます。

Operations Center の概要

次のタスク

159 ページの『クライアント管理サービスが正しくインストールされていることの確認』の指示に従います。

サイレント・モードでの クライアント管理サービス のインストール

クライアント管理サービス をサイレント・モードでインストールすることができます。サイレント・モードを使用する場合は、応答ファイルにインストール値を指定してから、インストール・コマンドを実行します。

始める前に

128 ページの『IBM Spectrum Protect クライアント管理サービスの要件と制限』を確認します。

156 ページの『グラフィカル・ウィザードを使用したクライアント管理サービスのインストール』の説明に従って、インストール・パッケージを抽出します。

このタスクについて

クライアント管理サービスは、バックアップ/アーカイブ・クライアントと同じコンピューターにインストールする必要があります。

インストール・パッケージが抽出されたディレクトリー内の `input` ディレクトリーに、次のサンプル応答ファイルが入っています。

`install_response_sample.xml`

このサンプル・ファイルをデフォルト値で使用することも、カスタマイズすることもできます。

ヒント: サンプル・ファイルをカスタマイズする場合は、サンプル・ファイルのコピーを作成し、名前を変更して、そのコピーを編集してください。

手順

1. サンプル・ファイルに基づいて応答ファイルを作成するか、あるいはサンプル・ファイル `install_response_sample.xml` を使用します。

どちらの場合も、応答ファイルでクライアント管理サービスのポート番号を必ず指定します。デフォルト・ポートは 9028 です。例えば次のとおりです。

`<variable name='port' value='9028'>`

2. コマンドを実行して、クライアント管理サービスをインストールし、使用条件に同意します。インストール・パッケージ・ファイルが抽出されたディレクトリーから、以下のコマンドを発行します。ここで、`response_file` は、ファイル名を含む応答ファイル・パスを表します。

Linux クライアント・システム:

`./install.sh -s -input response_file -acceptLicense`

例えば次のとおりです。

```
./install.sh -s -input /cms_install/input/install_response.xml -acceptLicense
```

Windows クライアント・システム:

```
install.bat -s -input response_file -acceptLicense
```

例えば次のとおりです。

```
install.bat -s -input c:\cms_install\input\install_response.xml -acceptLicense
```

次のタスク

『クライアント管理サービスが正しくインストールされていることの確認』の指示に従います。

クライアント管理サービスが正しくインストールされていることの確認

クライアント管理サービスを使用してバックアップ/アーカイブ・クライアントに関する診断情報を収集する前に、クライアント管理サービスのインストールと構成が正しく行われていることを確認できます。

手順

クライアント・システムのコマンド・ラインで、次のコマンドを実行して、クライアント管理サービスの構成を表示します。

- Linux クライアント・システムでは、次のコマンドを発行します。

```
client_install_dir/cms/bin/CmsConfig.sh list
```

ここで、*client_install_dir* はバックアップ/アーカイブ・クライアントがインストールされているディレクトリーです。例えば、デフォルトのクライアント・インストールでは、次のコマンドを発行します。

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

出力は、以下のテキストのようになります。

```
Listing CMS configuration
```

```
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252

Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

- Windows クライアント・システムでは、次のコマンドを発行します。

```
client_install_dir\CMS\bin\CMSConfig.bat list
```

ここで、*client_install_dir* はバックアップ/アーカイブ・クライアントがインストールされているディレクトリーです。例えば、デフォルトのクライアント・インストールでは、次のコマンドを発行します。

```
C:\\"Program Files"\Tivoli\TSM\cms\bin\CMSConfig.bat list
```

出力は、以下のテキストのようになります。

Operations Center の概要

```
Listing CMS configuration

server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252

Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

クライアント管理サービスのインストールと構成が正しく行われている場合、出力にはエラー・ログ・ファイルの場所が表示されます。

出力テキストは、次の構成ファイルから抽出されます。

- Linux クライアント・システム:

client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml

- Windows クライアント・システム:

client_install_dir\cms\Liberty\usr\servers\cmsServer\client-configuration.xml

出力に項目が含まれていない場合は、*client-configuration.xml* ファイルを構成する必要があります。このファイルの構成方法については、163 ページの『カスタム・クライアント・インストールのためのクライアント管理サービスの構成』を参照してください。**CmsConfig verify** コマンドを使用して、ノード定義が *client-configuration.xml* ファイル内で正しく作成されていることを確認することができます。

クライアント管理サービスを使用するための Operations Center の構成

クライアント管理サービスのデフォルト構成を使用しなかった場合、クライアント管理サービスにアクセスするように Operations Center を構成する必要があります。

始める前に

クライアント管理サービスがクライアント・システムにインストールされ、開始されていることを確認します。

デフォルト構成が使用されているかどうかを確認します。以下のいずれかの条件に該当する場合、デフォルト構成は使用されていません。

- クライアント管理サービスがデフォルトのポート番号 (9028) を使用していない。
- バックアップ/アーカイブ・クライアントが、バックアップ/アーカイブ・クライアントのインストール先のクライアント・システムと同じ IP アドレスでアクセスされない。例えば、以下の状態では、異なる IP アドレスが使用される可能性があります。
 - コンピューター・システムに 2 つのネットワーク・カードがある。バックアップ/アーカイブ・クライアントは 1 つのネットワークで通信するように構成されており、一方、クライアント管理サービスはもう 1 つのネットワークで通信します。

- クライアント・システムが動的ホスト構成プロトコル (DHCP) を使用して構成されている。その結果、クライアント・システムに IP アドレスが動的に割り当てられ、その IP アドレスが、前のバックアップ/アーカイブ・クライアント操作中に IBM Spectrum Protect サーバーに保存されます。クライアント・システムが再始動すると、クライアント・システムには別の IP アドレスが割り当てられる可能性があります。Operations Center が常にクライアント・システムを確実に検出できるようにするには、完全修飾ドメイン・ネームを指定します。

手順

クライアント管理サービスを使用するように Operations Center を構成するには、以下の手順を実行します。

1. 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。
2. 「詳細」をクリックします。
3. 「プロパティー」タブをクリックします。
4. 「一般」セクションの「リモート診断 URL」フィールドに、クライアント・システム上のクライアント管理サービスの URL を指定します。

アドレスの先頭は `https` でなければなりません。次の表に、リモート診断 URL の例を示します。

URL のタイプ	例
DNS ホスト名とデフォルト・ポート 9028 を使用	<code>https://server.example.com</code>
DNS ホスト名とデフォルト以外のポートを使用	<code>https://server.example.com:1599</code>
IP アドレスとデフォルト以外のポートを使用	<code>https://192.0.2.0:1599</code>

5. 「保存」をクリックします。

次のタスク

Operations Center の「診断」タブから、クライアント・ログ・ファイルなどのクライアント診断情報にアクセスできます。

クライアント管理サービス の始動と停止

クライアント管理サービスは、クライアント・システムにインストールされた後に自動的に開始されます。状況によっては、サービスを停止して開始する必要が生じることがあります。

手順

- Linux クライアント・システム上でクライアント管理サービスを停止、開始、または再始動するには、次のコマンドを発行します。
 - サービスを停止する場合:
`service cms.rc stop`
 - サービスを開始する場合:

Operations Center の概要

- ```
service cms.rc start
```
- サービスを再始動する場合:

```
service cms.rc restart
```
  - Windows クライアント・システムで、「サービス」ウィンドウを開き、IBM Spectrum Protect Client Management Services サービスの停止、開始、または再始動を行います。

## クライアント管理サービス のアンインストール

クライアント診断情報の収集が不要になった場合、クライアント管理サービスをクライアント・システムからアンインストールできます。

### このタスクについて

クライアント管理サービスをアンインストールするには、IBM Installation Manager を使用する必要があります。IBM Installation Manager をもう使用する予定がない場合には、これもアンインストールできます。

### 手順

1. クライアント管理サービスをクライアント・システムからアンインストールします。
  - a. 次のようにして、IBM Installation Manager を開きます。
    - Linux クライアント・システム上の IBM Installation Manager がインストールされているディレクトリーで、eclipse サブディレクトリー (例えば、/opt/IBM/InstallationManager/eclipse) に移動し、次のコマンドを発行します。

```
./IBMMIM
```
    - Windows のクライアント・システムでは、「スタート」メニューから IBM Installation Manager を開きます。
  - b. 「アンインストール」をクリックします。
  - c. 「IBM Spectrum Protect Client Management Services」を選択し、「次へ」をクリックします。
  - d. 「アンインストール」をクリックしてから、「終了」をクリックします。
  - e. 「IBM Installation Manager」ウィンドウを閉じます。
2. IBM Installation Manager を、もはや必要でない場合は、クライアント・システムからアンインストールします。
  - a. IBM Installation Manager アンインストール・ウィザードを開きます。
    - Linux クライアント・システムでは、IBM Installation Manager のアンインストール・ディレクトリー (例えば、/var/ibm/InstallationManager/uninstall) に移動し、次のコマンドを発行します。

```
./uninstall
```
    - Windows のクライアント・システムでは、「スタート」 > 「コントロール パネル」をクリックします。次に、「プログラムのアンインストール」 > 「IBM Installation Manager」 > 「アンインストール」をクリックします。

- b. 「IBM Installation Manager」 ウィンドウで、まだ選択されていない場合は「IBM Installation Manager」を選択して、「次へ」をクリックします。
- c. 「アンインストール」をクリックしてから、「終了」をクリックします。

## カスタム・クライアント・インストールのためのクライアント管理サービスの構成

クライアント管理サービスは、クライアント構成ファイル (`client-configuration.xml`) 内の情報を使用して、診断情報を検出します。クライアント管理サービスがログ・ファイルの場所を検出できない場合は、**CmsConfig** ユーティリティーを実行して、ログ・ファイルの場所を `client-configuration.xml` ファイルに追加する必要があります。

### **CmsConfig** ユーティリティー

デフォルトのクライアント構成を使用していない場合は、クライアント・システムで **CmsConfig** ユーティリティーを実行して、クライアント・ログ・ファイルの場所を検出し、`client-configuration.xml` ファイルに追加することができます。構成の完了後、クライアント管理サービスは、クライアント・ログ・ファイルにアクセスし、それらを Operations Center での基本的な診断機能に使用できるようにすることができます。

また、**CmsConfig** ユーティリティーを使用して、クライアント管理サービスの構成を表示したり、`client-configuration.xml` ファイルからノード名を削除したりすることもできます。

`client-configuration.xml` ファイルは、次のディレクトリーにあります。

- Linux クライアント・システム:

`client_install_dir/cms/Liberty/usr/servers/cmsServer`

- Windows クライアント・システム:

`client_install_dir\cms\Liberty\usr\servers\cmsServer`

ここで、`client_install_dir` はバックアップ/アーカイブ・クライアントがインストールされているディレクトリーです。

**CmsConfig** ユーティリティーは以下の場所にあります。

| クライアント・オペレーティング・システム | ユーティリティーの場所と名前                                        |
|----------------------|-------------------------------------------------------|
| Linux                | <code>client_install_dir/cms/bin/CmsConfig.sh</code>  |
| Windows              | <code>client_install_dir\cms\bin\CmsConfig.bat</code> |

**CmsConfig** ユーティリティーを使用するには、ユーティリティーに含まれている任意のコマンドを発行します。必ず、各コマンドを 1 行に入力してください。

## Operations Center の概要

**CmsConfig discover** コマンド:

**CmsConfig discover** コマンドを使用すると、オプション・ファイルおよびログ・ファイルを自動的に検出し、それらをクライアント構成ファイル `client-configuration.xml` に追加することができます。これにより、クライアント管理サービスがクライアント・ログ・ファイルにアクセスして、それらを Operations Center での診断に確実に使用できるようにすることができます。

通常、クライアント管理サービスのインストーラーは **CmsConfig discover** コマンドを自動的に実行します。しかし、バックアップ/アーカイブ・クライアントの変更(クライアントの追加や、サーバー構成またはログ・ファイルの場所の変更など)を行った場合は、手動でこのコマンドを実行する必要があります。

クライアント管理サービスが `client-configuration.xml` 内にログ定義を作成するには、IBM Spectrum Protect のサーバー・アドレス、サーバー・ポート、およびクライアント・ノード名を入手する必要があります。クライアント・オプション・ファイル(通常は、Linux クライアント・システム上の `dsm.sys`、および Windows クライアント・システム上の `dsm.opt`)でノード名が定義されていない場合は、クライアント・システムのホスト名が使用されます。

クライアント構成ファイルを更新するには、クライアント管理サービスは 1 つ以上のログ・ファイル (`dserror.log` や `dsmsched.log` など) にアクセスする必要があります。最良の結果を得るために、**CmsConfig discover** コマンドは、バックアップ/アーカイブ・クライアントのコマンド `dsmc` の場合と同じディレクトリーで、同じ環境変数を使用して実行してください。これにより、正しいログ・ファイルが検出される可能性が高くなります。

クライアント・オプション・ファイルがカスタムの場所にあるか、標準的なオプション・ファイル名が付いていない場合には、検出の対象範囲を絞るためにクライアント・オプション・ファイルのパスを指定することもできます。

### 構文

```
►—CmsConfig discover— configPath—►
```

### パラメーター

#### *configPath*

クライアント・オプション・ファイルのパス(通常は `dsm.opt`)。クライアント・オプション・ファイルがデフォルトの場所にない場合、またはデフォルトの名前ではない場合は、構成パスを指定します。クライアント管理サービスは、クライアント・オプション・ファイルをロードし、そこからクライアント・ノードおよびログを検出します。このパラメーターはオプションです。

Linux クライアント・システムでは、クライアント管理サービスは常にクライアント・ユーザー・オプション・ファイル(`dsm.opt`)をロードし、次にクライアント・システム・オプション・ファイル(通常は `dsm.sys`)を検索します。ただし、*configPath* パラメーターの値は、常にクライアント・ユーザー・オプション・ファイルになります。

**Linux クライアント・システムの例**

- クライアント・ログ・ファイルを検出し、ログ定義を自動的に client-configuration.xml ファイルに追加します。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh discover
```

出力:

```
Discovering client configuration and logs.
```

```
server.example.com:1500 SUSAN
 /opt/tivoli/tsm/client/ba/bin/dsmerror.log
```

```
Finished discovering client configuration and logs.
```

- /opt/tivoli/tsm/client/ba/bin/daily.opt ファイルに指定されている構成ファイルとログ・ファイルを検出し、ログ定義を client-configuration.xml ファイルに自動的に追加します。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh discover /opt/tivoli/tsm/client/ba/bin/daily.opt
```

出力:

```
Discovering client configuration and logs
```

```
server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys
```

```
Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

```
Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

```
Finished discovering client configuration and logs.
```

**Windows クライアント・システムの例**

- クライアント・ログ・ファイルを検出し、ログ定義を自動的に client-configuration.xml ファイルに追加します。

C:\Program Files\Tivoli\TSM\cms\bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig discover
```

出力:

```
Discovering client configuration and logs.
```

```
server.example.com:1500 SUSAN
C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
```

```
Finished discovering client configuration and logs.
```

## Operations Center の概要

- c:\program files\tivoli\tsm\baclient\daily.opt ファイルに指定されている構成ファイルおよびログ・ファイルを検出し、ログ定義を client-configuration.xml ファイルに自動的に追加します。

C:\Program Files\Tivoli\TSM\cms\bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig discover "c:\program
files\tivoli\tsm\baclient\daily.opt"
```

出力:

```
Discovering client configuration and logs

server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252

Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252

Finished discovering client configuration and logs.
```

**CmsConfig addnode** コマンド:

**CmsConfig addnode** コマンドを使用して、client-configuration.xml 構成ファイルにクライアント・ノード定義を手動で追加します。このノード定義には、IBM Spectrum Protect サーバーと通信するために クライアント管理サービス が必要とする情報が含まれています。

このコマンドは、クライアント・オプション・ファイルまたはクライアント・ログ・ファイルがクライアント・システム上のデフォルト以外の場所に保管されている場合にのみ使用してください。

構文

```
►—CmsConfig addnode—nodeName—serverIP—serverPort—serverProtocol—optPath—►
```

パラメーター

*nodeName*

ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。ただし、Linux クライアント・システムなどの複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

*serverIP*

クライアント管理サービス の認証を行う IBM Spectrum Protect サーバーの TCP/IP アドレス。このパラメーターは必須です。

サーバーに 1 文字から 64 文字の TCP/IP アドレスを指定できます。サーバー・アドレスは、TCP/IP ドメイン・ネームまたは数値 IP アドレスにすること

ができます。数値 IP アドレスは TCP/IP v4 または TCP/IP v6 のアドレスにすることができます。IPv6 アドレスを使用できるのは、クライアント・システムに対して **commmethod V6Tcpip** オプションが指定されている場合だけです。

例:

- server.example.com
- 192.0.2.0
- 2001:0DB8:0:0:0:0:0:0

#### *serverPort*

IBM Spectrum Protect サーバーとの通信に使用される TCP/IP ポート番号。1 から 32767 の範囲の値を指定できます。このパラメーターは必須です。

例: 1500

#### *serverProtocol*

クライアント管理サービスと IBM Spectrum Protect サーバー間の通信に使用されるプロトコル。このパラメーターは必須です。

以下のいずれかの値を指定できます。

| 値      | 意味                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------|
| NO_SSL | SSL セキュリティー・プロトコルは使用されません。                                                                                    |
| SSL    | SSL セキュリティー・プロトコルが使用されます。                                                                                     |
| FIPS   | 連邦情報処理標準 (FIPS) モードで TLS 1.2 プロトコルが使用されます。<br>ヒント: あるいは、TLS_1.2 と入力して、TLS 1.2 プロトコルが FIPS モードで使用されることを指定できます。 |

#### *optPath*

クライアント・オプション・ファイルの完全修飾パス。このパラメーターは必須です。

例 (Linux クライアント): /opt/backup\_tools/tivoli/tsm/baclient/dsm.sys

例 (Windows クライアント): C:\backup\tools\Tivoli\TSM\baclient\dsm.opt

#### Linux クライアント・システムの例

クライアント・ノード SUSAN のノード定義を `client-configuration.xml` ファイルに追加します。ノードが通信する IBM Spectrum Protect サーバーは、サーバー・ポート 1500 上の `server.example.com` です。SSL セキュリティー・プロトコルは使用されません。クライアント・システム・オプション・ファイルのパスは `/opt/tivoli/tsm/client/ba/bin/custom_opt.sys` です。

`/opt/tivoli/tsm/cms/bin` ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh addnode SUSAN server.example.com 1500 NO_SSL
/opt/tivoli/tsm/client/ba/bin/custom_opt.sys
```

## Operations Center の概要

出力:

```
Adding node.
Finished adding client configuration.
```

### Windows クライアント・システムの例

クライアント・ノード SUSAN のノード定義を `client-configuration.xml` ファイルに追加します。ノードが通信する IBM Spectrum Protect サーバーは、サーバー・ポート 1500 上の `server.example.com` です。SSL セキュリティー・プロトコルは使用されません。クライアント・オプション・ファイルのパスは `c:\program files\ibm\tsm\baclient\custom.opt` です。

C:\Program Files\Tivoli\TSM\cms\bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig addnode SUSAN server.example.com 1500 NO_SSL "c:\program
files\ibm\tsm\baclient\custom.opt"
```

出力:

```
Adding node.
Finished adding client configuration.
```

### CmsConfig setopt コマンド:

**CmsConfig setopt** コマンドを使用して、最初にクライアント・オプション・ファイルの内容を読み取らずに、クライアント・オプション・ファイルのパス (通常は `dsm.opt`) を、既存のノード定義に設定します。

このコマンドは、クライアント・オプション・ファイルが標準的な名前でないか、デフォルト以外の場所にある場合に役立ちます。

要件: ノード定義が存在しない場合、最初に **CmsConfig addnode** コマンドを発行してノード定義を作成する必要があります。

**CmsConfig discover** コマンドとは異なり、**CmsConfig setopt** コマンドでは、`client-configuration.xml` ファイル内に関連付けられたログ定義が作成されません。**CmsConfig addlog** コマンドを使用して、ログ定義を作成する必要があります。

### 構文

```
►►—CmsConfig setopt—nodeName—optPath—►►
```

#### パラメーター

##### *nodeName*

ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。ただし、Linux クライアント・システムなどの複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

***optPath***

クライアント・オプション・ファイルの完全修飾パス。このパラメーターは必須です。

例 (Linux クライアント): /opt/backup\_tools/tivoli/tsm/baclient/dsm.opt

例 (Windows クライアント): C:\backup\tools\Tivoli\TSM\baclient\dsm.opt

**Linux クライアント・システムの例**

ノード SUSAN のクライアント・オプション・ファイル・パスを設定します。クライアント・オプション・ファイルのパスは /opt/tivoli/tsm/client/ba/bin/dsm.opt です。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.opt
```

出力:

```
Adding node configuration file.
```

```
Finished adding client configuration file.
```

**Windows クライアント・システムの例**

ノード SUSAN のクライアント・オプション・ファイル・パスを設定します。クライアント・オプション・ファイルのパスは c:\program  
files\tivoli\tsm\baclient\dsm.opt です。

C:\Program Files\Tivoli\TSM\cms\bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig setopt SUSAN "c:\program
files\tivoli\tsm\baclient\dsm.opt"
```

出力:

```
Adding node configuration file.
```

```
Finished adding client configuration file.
```

**CmsConfig setsys コマンド:**

Linux クライアント・システム上で、**CmsConfig setsys** コマンドを使用して、最初にクライアント・システム・オプション・ファイルの内容を読み取ることなく、クライアント・システム・オプション・ファイルのパス (通常は dsm.sys) を既存のノード定義に設定します。

このコマンドは、クライアント・システム・オプション・ファイルが標準的な名前でないか、デフォルト以外の場所にある場合に役立ちます。

要件: ノード定義が存在しない場合、最初に **CmsConfig addnode** コマンドを発行してノード定義を作成する必要があります。

## Operations Center の概要

**CmsConfig discover** コマンドとは異なり、**CmsConfig setsys** コマンドでは、client-configuration.xml ファイル内に関連ログ定義が作成されません。  
**CmsConfig addlog** コマンドを使用して、ログ定義を作成する必要があります。

### 構文

►►—CmsConfig setsys—nodeName—sysPath—————►►

#### パラメーター

##### nodeName

ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。ただし、Linux クライアント・システムなどの複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

##### sysPath

クライアント・システム・オプション・ファイルの完全修飾パス。このパラメーターは必須です。

例: /opt/backup\_tools/tivoli/tsm/baclient/dsm.sys

### 例

ノード SUSAN のクライアント・システム・オプション・ファイル・パスを設定します。クライアント・システム・オプション・ファイルのパスは /opt/tivoli/tsm/client/ba/bin/dsm.sys です。

/opt/tivoli/tsm/cms/bin ディレクトリーから、以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.sys
```

出力:

```
Adding node configuration file.
```

```
Finished adding client configuration file.
```

#### CmsConfig addlog コマンド:

**CmsConfig addlog** コマンドを使用して、クライアント・ログ・ファイルの場所を client-configuration.xml 構成ファイルの既存のノード定義に手動で追加してください。このコマンドは、クライアント・ログ・ファイルがクライアント・システム上のデフォルト以外の場所に保管されている場合にのみ使用してください。

要件: ノード定義が存在しない場合、最初に **CmsConfig addnode** コマンドを発行してノード定義を作成する必要があります。

### 構文

►►—CmsConfig addlog—nodeName—logPath—————►►

▶ [language—dateFormat—timeFormat—encoding] ◀

### パラメーター

#### *nodeName*

ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1つのノード名のみが IBM Spectrum Protect サーバーに登録されています。ただし、Linux クライアント・システムなどの複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

#### *logPath*

ログ・ファイルの完全修飾パス。このパラメーターは必須です。

例 (Linux クライアント): /opt/backup\_tools/tivoli/tsm/baclient/dsmerror.log

例 (Windows クライアント): C:\\$backup\tools\\$Tivoli\\$TSM\\$baclient\\$dsmerror.log

#### *language*

ログ・ファイルの言語ロケール。このパラメーターはオプションです。ただし、このパラメーターを指定する場合は、**dateFormat**、**timeFormat**、および **encoding** の各パラメーターも指定する必要があります。以下の言語のロケールを指定する必要があります。

| 言語          | ロケール  |
|-------------|-------|
| ブラジル・ポルトガル語 | pt_BR |
| 中国語 (簡体字)   | zh_CN |
| 中国語 (繁体字)   | zh_TW |
| チェコ語        | cs_CZ |
| 英語          | en_US |
| フランス語       | fr_FR |
| ドイツ語        | de_DE |
| ハンガリー語      | hu_HU |
| イタリア語       | it_IT |
| 日本語         | ja_JP |
| 韓国語         | ko_KR |
| ポーランド語      | pl_PL |
| ロシア語        | ru_RU |
| スペイン語       | es_ES |

#### *dateFormat*

クライアント・ログ・ファイルのタイム・スタンプ項目の日付形式。このパラメーターはオプションです。ただし、このパラメーターを指定する場合は、**language**、**timeFormat**、および **encoding** の各パラメーターも指定する必要があります。

次の表に、言語の日付形式を示します。

## Operations Center の概要

ヒント: 表にリストされているいずれかの日付形式を使用する代わりに、バックアップ/アーカイブ・クライアントの **dateformat** オプションを使用して日付形式を指定できます。

| 言語          | 日付形式       |
|-------------|------------|
| 中国語 (簡体字)   | yyyy-MM-dd |
| 中国語 (繁体字)   | yyyy/MM/dd |
| チェコ語        | dd.MM.yyyy |
| 英語          | MM/dd/yyyy |
| フランス語       | dd/MM/yyyy |
| ドイツ語        | dd.MM.yyyy |
| ハンガリー語      | yyyy.MM.dd |
| イタリア語       | dd/MM/yyyy |
| 日本語         | yyyy-MM-dd |
| 韓国語         | yyyy/MM/dd |
| ポーランド語      | yyyy-MM-dd |
| ブラジル・ポルトガル語 | dd/MM/yyyy |
| ロシア語        | dd.MM.yyyy |
| スペイン語       | dd.MM.yyyy |

### *timeFormat*

クライアント・ログ・ファイルのタイム・スタンプ項目の時刻形式。このパラメーターはオプションです。ただし、このパラメーターを指定する場合は、**language**、**dateFormat**、および **encoding** の各パラメーターも指定する必要があります。

次の表に、ユーザーが指定できるデフォルトの時刻形式とクライアント・オペレーティング・システムの例を示します。

ヒント: 表にリストされているいずれかの時刻形式を使用する代わりに、バックアップ/アーカイブ・クライアントの **timeformat** オプションを使用して時刻形式を指定できます。

| 言語        | Linux クライアント・システムの時刻形式 | Windows クライアント・システムの時刻形式 |
|-----------|------------------------|--------------------------|
| 中国語 (簡体字) | HH:mm:ss               | HH:mm:ss                 |
| 中国語 (繁体字) | HH:mm:ss               | ahh:mm:ss                |
| チェコ語      | HH:mm:ss               | HH:mm:ss                 |
| 英語        | HH:mm:ss               | HH:mm:ss                 |
| フランス語     | HH:mm:ss               | HH:mm:ss                 |
| ドイツ語      | HH:mm:ss               | HH:mm:ss                 |
| ハンガリー語    | HH.mm.ss               | HH:mm:ss                 |
| イタリア語     | HH:mm:ss               | HH:mm:ss                 |
| 日本語       | HH:mm:ss               | HH:mm:ss                 |
| 韓国語       | HH:mm:ss               | HH:mm:ss                 |
| ポーランド語    | HH:mm:ss               | HH:mm:ss                 |

| 言語          | Linux クライアント・システムの時刻形式 | Windows クライアント・システムの時刻形式 |
|-------------|------------------------|--------------------------|
| ブラジル・ポルトガル語 | HH:mm:ss               | HH:mm:ss                 |
| ロシア語        | HH:mm:ss               | HH:mm:ss                 |
| スペイン語       | HH:mm:ss               | HH:mm:ss                 |

*encoding*

クライアント・ログ・ファイルの項目の文字エンコード。このパラメーターはオプションです。ただし、このパラメーターを指定する場合は、**language**、**dateFormat**、および **timeFormat** の各パラメーターも指定する必要があります。

Linux クライアント・システムの場合は、標準の文字エンコードは UTF-8 です。Windows クライアント・システムの場合は、デフォルトのエンコード値が次の表に示されています。クライアント・システムが異なる形式にカスタマイズされている場合は、**encoding** パラメーターを使用して、デフォルト以外の値を指定します。

| 言語          | エンコード        |
|-------------|--------------|
| 中国語 (簡体字)   | CP936        |
| 中国語 (繁体字)   | CP950        |
| チェコ語        | Windows-1250 |
| 英語          | Windows-1252 |
| フランス語       | Windows-1252 |
| ドイツ語        | Windows-1252 |
| ハンガリー語      | Windows-1250 |
| イタリア語       | Windows-1252 |
| 日本語         | CP932        |
| 韓国語         | CP949        |
| ポーランド語      | Windows-1250 |
| ブラジル・ポルトガル語 | Windows-1252 |
| ロシア語        | Windows-1251 |
| スペイン語       | Windows-1252 |

**Linux クライアント・システムの例**

クライアント・ログ・ファイルの場所を `client-configuration.xml` ファイル内のクライアント・ノード SUSAN の既存の定義に追加します。クライアント・ログ・ファイルのパスは `/usr/work/logs/dsmerror.log` です。言語の指定、時刻形式、およびフランス語地域の日付形式を追加します。

`/opt/tivoli/tsm/cms/bin` ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh addlog SUSAN /usr/work/logs/dsmerror.log fr_FR
yyyy/MM/dd HH:MM:ss UTF-8
```

## Operations Center の概要

出力:

```
Adding log.
Finished adding log.
```

### Windows クライアント・システムの例

クライアント・ログ・ファイルの場所を `client-configuration.xml` 内のクライアント・ノード SUSAN の既存の定義に追加します。クライアント・ログ・ファイルのパスは `c:\work\logs\dserror.log` です。言語の指定、時刻形式、およびフランス語地域の日付形式を追加します。

`C:\Program Files\Tivoli\TSM\cms\bin` ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig addlog SUSAN c:\work\logs\dserror.log fr_FR yyyy/MM/dd
HH:MM:ss UTF-8
```

出力:

```
Adding log.
Finished adding log.
```

### CmsConfig remove コマンド:

**CmsConfig remove** コマンドは、クライアント構成ファイル (`client-configuration.xml`) からクライアント・ノード定義を削除するために使用します。クライアント・ノード名に関連付けられているすべてのログ・ファイル項目も削除されます。

#### 構文

```
►—CmsConfig remove—nodeName—————►
```

#### パラメーター

##### *nodeName*

ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。ただし、Linux クライアント・システムなどの複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

### Linux クライアント・システムの例

`client-configuration.xml` ファイルから SUSAN のノード定義を削除します。

`/opt/tivoli/tsm/cms/bin` ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh remove SUSAN
```

出力:

Removing node.

Finished removing node.

### Windows クライアント・システムの例

`client-configuration.xml` ファイルから SUSAN のノード定義を削除します。

C:\Program Files\Tivoli\TSM\cms\bin ディレクトリーから、次のコマンドを発行します。

コマンド:

`cmsconfig remove SUSAN`

出力:

Removing node.

Finished removing node.

### CmsConfig verify コマンド:

**CmsConfig verify** コマンドを使用して、ノード定義が `client-configuration.xml` ファイル内で正しく作成されていることを確認します。ノード定義にエラーがある場合、あるいはノードが正しく定義されていない場合は、適切な **CmsConfig** コマンドを使用してノード定義を修正する必要があります。

#### 構文

```
►—CmsConfig verify—nodeName—►
 |cmsPort—►
```

#### パラメーター

##### *nodeName*

ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。ただし、Linux クライアント・システムなどの複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

##### *cmsPort*

クライアント管理サービスとの通信に使用される TCP/IP ポート番号。クライアント管理サービスのインストール時にデフォルトのポート番号を使用しなかった場合は、ポート番号を指定します。デフォルトのポート番号は 9028 です。このパラメーターはオプションです。

### Linux クライアント・システムの例

ノード SUSAN のノード定義が `client-configuration.xml` ファイル内に正しく作成されていることを確認します。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

## Operations Center の概要

コマンド:

```
./CmsConfig.sh verify SUSAN
```

検査プロセス中に、クライアント・ノード名または管理ユーザー ID とパスワードの入力を求められます。

出力:

```
Verifying node.
```

```
Verifying the CMS service configuration for node SUSAN.
The CMS configuration looks correct.
```

```
Verifying the CMS service works correctly on port 9028.
```

```
Enter your user id: admin
Enter your password:
```

```
Connecting to CMS service and verifying resources.
The CMS service is working correctly.
Finished verifying node.
```

### Windows クライアント・システムの例

ノード SUSAN のノード定義が `client-configuration.xml` ファイル内に正しく作成されていることを確認します。

C:\Program Files\Tivoli\TSM\cms\bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig verify SUSAN
```

検査プロセス中に、クライアント・ノード名または管理ユーザー ID とパスワードの入力を求められます。

出力:

```
Verifying node.
```

```
Verifying the CMS service configuration for node SUSAN.
The CMS configuration looks correct.
```

```
Verifying the CMS service works correctly on port 9028.
```

```
Enter your user id: admin
Enter your password:
```

```
Connecting to CMS service and verifying resources.
The CMS service is working correctly.
Finished verifying node.
```

**CmsConfig list** コマンド:

**CmsConfig list** コマンドは、クライアント管理サービス構成を表示するために使用します。

構文

►►—CmsConfig list————►►

**Linux** クライアント・システムの例

クライアント管理サービスの構成の表示。次に、出力を表示して、コマンドを正しく入力したことを確認します。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

コマンド:

./CmsConfig.sh list

出力:

```
Listing CMS configuration

server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252

Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

**Windows** クライアント・システムの例

クライアント管理サービスの構成の表示。次に、出力を表示して、コマンドを正しく入力したことを確認します。

C:\Program Files\Tivoli\TSM\cms\bin ディレクトリーから、次のコマンドを発行します。

コマンド:

cmsconfig list

出力:

```
Listing CMS configuration

server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252

Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

## Operations Center の概要

**CmsConfig help** コマンド:

**CmsConfig** ユーティリティー・コマンドの構文を表示するには、**CmsConfig help** コマンドを使用します。

構文

►►—CmsConfig help————►►

### Linux クライアント・システムの例

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

./CmsConfig help

### Windows クライアント・システムの例

C:\Program Files\Tivoli\TSM\cms\bin ディレクトリーから、次のコマンドを発行します。

CmsConfig help

クライアント管理サービスの拡張機能:

デフォルトでは、IBM Spectrum Protect クライアント管理サービスは、クライアント・ログ・ファイルからのみ情報を収集します。その他のクライアント・アクションを開始するには、クライアント管理サービスに組み込まれている Representational State Transfer (REST) API にアクセスします。

API 開発者は、REST アプリケーションを作成して、以下のクライアント・アクションを開始することができます。

- クライアント・オプション・ファイル (例えば、Linux クライアントの `dsm.sys` ファイルや、Linux および Windows クライアントの `dsm.opt` ファイルなど) の照会および更新。
- IBM Spectrum Protect クライアント・アクセプターおよびスケジューラーの状況の照会。
- クライアント・ノードのファイルのバックアップおよびリストア。
- スクリプトを使用したクライアント管理サービスの機能の拡張。

クライアント管理サービス REST API について詳しくは、Client Management Services REST API Guide を参照してください。

---

## 第 13 章 Operations Center のインストールのトラブルシューティング

Operations Center のインストールで問題が発生し、それを解決できない場合は、既知の問題の説明を参照して可能な解決策を探すことができます。

---

### 日本語、中国語、または韓国語のフォントが正しく表示されない

Red Hat Enterprise Linux 5 上の Operations Center で、中国語、日本語、または韓国語のフォントが正しく表示されません。

#### 解決策

Red Hat から入手可能な以下のフォント・パッケージをインストールしてください。

- fonts-chinese
- fonts-japanese
- fonts-korean

## **Operations Center のトラブルシューティング**

---

## 第 14 章 Operations Center のアンインストール

Operations Center は、グラフィック・ウィザード、コンソール・モードのコマンド・ライン、またはサイレント・モードを使用してアンインストールすることができます。

---

### グラフィカル・ウィザードを使用したOperations Centerのアンインストール

IBM Installation Manager のグラフィカル・ウィザードを使用して、Operations Center をアンインストールすることができます。

#### 手順

1. IBM Installation Manager を開きます。

IBM Installation Manager がインストールされているディレクトリーで、eclipse サブディレクトリー (例えば、/opt/IBM/InstallationManager/eclipse) に移動し、次のコマンドを発行します。

```
./IBMMIM
```

2. 「アンインストール」をクリックします。
3. Operations Centerのオプションを選択して、「次へ」をクリックします。
4. 「アンインストール」をクリックします。
5. 「終了」をクリックします。

---

### コンソール・モードでのOperations Centerのアンインストール

コマンド・ラインを使用して Operations Center をアンインストールするには、コンソール・モードのパラメーターを指定してコマンド・ラインから IBM Installation Manager のアンインストール・プログラムを実行する必要があります。

#### 手順

1. IBM Installation Manager がインストールされているディレクトリーで、以下のサブディレクトリーに移動します。

```
eclipse/tools
```

例えば次のとおりです。

```
/opt/IBM/InstallationManager/eclipse/tools
```

2. tools ディレクトリーから以下のコマンドを発行します。

```
./imcl -c
```

3. アンインストールするには、5 を入力します。

4. IBM Spectrum Protect パッケージ・グループからアンインストールすることを選択します。

5. 「N」(次へ) を入力します。

## Operations Center のアンインストール

6. Operations Center パッケージをアンインストールすることを選択します。
7. 「N」(次へ) を入力します。
8. 「U」(アンインストール) を入力します。
9. 「F」(終了) を入力します。

---

## サイレント・モードでの Operations Center のアンインストール

サイレント・モードで Operations Center をアンインストールするには、サイレント・モードのパラメーターを指定してコマンド・ラインから IBM Installation Manager のアンインストール・プログラムを実行する必要があります。

### 始める前に

応答ファイルを使用して、Operations Center サーバーをサイレント・アンインストールするためのデータ入力を提供することができます。IBM Spectrum Protect には、`input` ディレクトリーにサンプル応答ファイル `uninstall_response_sample.xml` が含まれています。このディレクトリーは、インストール・パッケージが解凍されるディレクトリーです。このファイルには、不要な警告を回避するのに役立つデフォルト値が含まれています。

Operations Center をアンインストールするには、応答ファイル内の Operations Center 項目について、`modify="false"` を設定したままにします。

応答ファイルをカスタマイズしたい場合は、ファイル内のオプションを変更することができます。応答ファイルについては、応答ファイルを参照してください。

### 手順

1. IBM Installation Manager がインストールされているディレクトリーで、以下のサブディレクトリーに移動します。

`eclipse/tools`

例えば次のとおりです。

`/opt/IBM/InstallationManager/eclipse/tools`

2. `tools` ディレクトリーから、以下のコマンドを発行します。ここで、`response_file` は、ファイル名を含めた応答ファイルのパスを示しています。

`./imcl -input response_file -silent`

以下にコマンド例を示します。

`./imcl -input /tmp/input/uninstall_response.xml -silent`

---

## 第 15 章 Operations Center の前のバージョンへのロールバック

デフォルトでは、IBM Installation Manager は、更新、フィックス、またはパッケージの以降のバージョンで問題が発生した場合にロールバックするために、パッケージの前のバージョンを保存します。

### 始める前に

ロールバック機能は、Operations Center が更新された後にのみ使用可能です。

### このタスクについて

IBM Installation Manager がパッケージを前のバージョンにロールバックすると、現行バージョンのパッケージ・ファイルがアンインストールされ、前のバージョンが再インストールされます。

前のバージョンにロールバックするには、IBM Installation Manager は、そのバージョンのファイルにアクセスする必要があります。デフォルトでは、それぞれの連続するインストール中に、これらのファイルが保存されます。保存されるファイルの数は、各バージョンのインストールに伴い増加するため、定期的なスケジュールでファイルをシステムから削除することが必要になる場合があります。しかし、ファイルを削除すると、前のバージョンにロールバックできなくなります。

保存されたファイルを削除するか、今後のインストール時にこれらのファイルを保存するためにプリファレンスを更新するには、以下の手順を実行します。

1. IBM Installation Manager で、「ファイル」 > 「プリファレンス」をクリックします。
2. 「プリファレンス」ページで、「ロールバックのファイル」をクリックして、プリファレンスを指定します。

### 手順

Operations Center の前のバージョンにロールバックするには、IBM Installation Manager の「ロールバック」機能を使用します。



---

### 第 3 部 付録



---

## 付録 A. インストール・ログ・ファイル

インストール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。

インストール・ログ・ファイルは、Installation Manager ツールから「ファイル」>「ログの表示」をクリックすると表示できます。これらのログ・ファイルを収集するには、Installation Manager ツールから「ヘルプ」>「問題分析のためのデータをエクスポート」をクリックします。



---

## 付録 B. IBM Spectrum Protect 製品ファミリーのアクセシビリティー機能

アクセシビリティー機能は、運動障害または視覚障害などの障害を持つユーザーが情報技術コンテンツを快適に使用できるように支援します。

### 概要

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ー機能を提供します。

- キーボードのみによる操作
- スクリーン・リーダー(読み上げソフトウェア)に使用する操作

IBM Spectrum Protect ファミリー製品は、最新の W3C 標準 WAI-ARIA 1.0 ([www.w3.org/TR/wai-aria/](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。アクセシビリティー機能を利用するには、最新リリースのスクリーン・リーダーと、この製品によってサポートされる最新の Web ブラウザーを使用してください。

IBM Knowledge Center の製品資料は、アクセシビリティーに対応しています。IBM Knowledge Center のアクセシビリティー機能については、Accessibility section of the IBM Knowledge Center help ([www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility](http://www.ibm.com/support/knowledgecenter/about/releasenotes.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、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、同等の方法(ハイコントラスト・モードなど)が用意されています。フォント・サイズの制御は、デバイスまたは Web ブラウザーの設定を使用して行うことができます。

Web ユーザー・インターフェースには、アプリケーションの機能領域に素早くナビゲートできる WAI-ARIA ナビゲーション・ランドマークが含まれています。

## ベンダー・ソフトウェア

IBM Spectrum Protect 製品ファミリーには、IBM の使用許諾契約書の対象とならないベンダー・ソフトウェアが含まれます。IBM は、それらの製品のアクセシビリティー機能を保証するものではありません。ベンダーの製品のアクセシビリティー機能については、ベンダーにお問い合わせください。

## 関連アクセシビリティ情報

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専門

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、隨時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む)との間での情報交換、および(ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

本書に含まれるパフォーマンス・データは、特定の動作および環境条件下で得られたものです。実際の結果は、異なる可能性があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

#### 著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。 IBM は、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® 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。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、Windows、および Windows NT は、Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

## 製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

### 適用条件

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

### 個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布（頒布、送信を含む）または表示（上映を含む）することはできません。

### 商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権利 ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、

データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは默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、以下の具体的な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 およびさまざまテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie などの各種テクノロジーの使用について詳しくは、「IBM オンラインでのプライバシー・ステートメントのハイライト」(<http://www.ibm.com/privacy/jp/ja/>)、「IBM オンラインでのプライバシー・ステートメント」(<http://www.ibm.com/privacy/details/jp/ja>) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』というタイトルのセクション、および「IBM Software Products and Software-as-a-Service Privacy Statement」(<http://www.ibm.com/software/info/product-privacy>) を参照してください。

---

## 用語集

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。

他の IBM 製品の用語集を確認するには、IBM 用語 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・フェイルオーバー・ログ・スペース  
  description 49  
アーカイブ・ログ  
  ストレージ・テクノロジーの選択 22  
  スペース要件 35  
アーカイブ・ログ・ディレクトリー 65  
アクセシビリティ機能 189  
アクセス権限  
  設定  
    サーバーの始動前 81  
アップグレード  
  サーバー<sup>†</sup>  
    推定時間 96  
    8.1 への 95  
    V7.1 から V8.1 96  
アラート  
  E メールによる送信 143  
アンインストール 115  
  クライアント管理サービス 162  
  IBM Installation Manager 116  
アンインストールと再インストール 115  
以前のサーバー・バージョンへの復帰 105  
一時スペース 34  
一時ディスク・スペース 34  
インスタンス・ディレクトリー 65  
インスタンス・ユーザー ID 52  
インストール  
  回復ログ 75  
  クライアント管理サービス 156  
  グラフィカル・ユーザー・インターフェース  
    使用 57  
  コンソール・モードでコマンド・ラインを使用した  
    使用 58  
  サーバー 3, 55  
  最小必要要件 27  
  前提知識 3  
  装置サポート 55  
  データベース 75  
  フィックスパック 91  
  Operations Center 135  
  インストール、サーバーの  
    サイレント 59  
  インストール、IBM Spectrum Protect サーバーの 59  
  インストール可能コンポーネント vii

インストールの検査  
  クライアント管理サービス 159  
インストール・ウィザード 57  
インストール・ディレクトリー  
  Operations Center  
    Installation Manager 132  
  インストール・パッケージ 55  
    Operations Center 135  
  インストール・ログ 57, 58  
  ウィザード 63  
  オファリング 29, 131  
  オプション  
    サーバーの始動 80  
  オプション、クライアント  
    SSLTCPADMINPORT 72  
    SSLTCPPORT 72  
    TCPADMINPORT 72  
    TCPPORT 72  
    TCPWINDOWSIZE 72  
  オプション・ファイル (options file)  
    編集 71  
  オペレーティング・システム要件  
    Operations Center 126

## [カ行]

カーネル・パラメーター、チューニング  
  概要 64  
  更新 64  
  最小推奨値 64  
開始  
  クライアント管理サービス 161  
  サーバー 80  
    スタンダロン・モード 85  
    保守モード 85  
改訂の要約  
  バージョン 8.1 ix  
回復ログ  
  アーカイブ・フェイルオーバー・ログ・スペース 49  
  インストール 75  
概要  
  Operations Center 119, 121  
カスタム構成  
  クライアント管理サービス 163  
活動化  
  サーバー 80  
活動ログ  
  ストレージ・テクノロジーの選択 22  
  スペース要件 35  
管理コマンド  
  HALT 86

管理コマンド (続き)

- REGISTER LICENSE 87
- 管理者 ID 130
- 管理者パスワード 130
- キーボード 189
- 期限切れ
  - サーバー・オプション 80
- 技術的な変更 ix
- キャパシティー計画
  - 回復ログのスペース要件
    - 活動ログ・ミラー 48
    - 活動ログとアーカイブ・ログ 35
  - データベースのスペース要件
    - 開始サイズ 31
    - ストレージ・プールのキャパシティーに基づく見積もり 34
    - ファイル数に基づく見積もり 31
- 共有リソース・ディレクトリー 29, 131
- 共用メモリー通信方式 73
- 共用メモリー・クライアント・オプション 73
- クライアント管理サービス
  - インストール 162
  - インストール 156
    - サイレント・モードで 158
  - インストールの検査 159
  - 開始および停止 161
  - 拡張機能 178
  - カスタム・クライアント・インストールのための構成 163
  - クライアント・オプション・ファイル・パスの設定 168
  - クライアント・システム・ファイル・パスの設定 169
  - 構成の表示 177
  - 診断情報の収集 156
  - ノード定義の追加 166
  - ノード名の削除 174, 175
  - 要件と制限 128
  - ログ・ファイルの場所の追加 170
- CmsConfig addlog 170
- CmsConfig addnode 166
- CmsConfig discover 164
- CmsConfig help 178
- CmsConfig list 177
- CmsConfig remove 174, 175
- CmsConfig setopt 168
- CmsConfig setsys 169
- CmsConfig ユーティリティー 163
- Operations Center
  - クライアント・ログ・ファイルの表示 156
- Operations Center の構成 160
- REST API 178
- クライアント・オプション
  - 共用メモリー通信用 73
- クライアント・ノード
  - 以前のサーバー・バージョンへの復帰
    - 影響を受けるデータ 105

- クラスター環境
- Linux でのサーバーのアップグレード
  - V6 から V8.1.5 103
  - V8.1.5 へのサーバーのアップグレード 102
- グループ 65
- 計画、キャパシティー
  - 回復ログのスペース要件 35
  - 活動ログ・ミラー 48
  - データベースのスペース要件
    - 開始サイズ 31
    - ストレージ・プールのキャパシティーに基づく見積もり 34
    - ファイル数に基づく見積もり 31
- 言語
  - セット 61
  - 言語サポート 61
  - 言語パッケージ 60, 62
  - 更新 62, 139
  - 構成 63, 67, 69
    - スパーク・サーバー 143
    - ハブ・サーバー 142
    - Operations Center 122, 141
  - 構成、ウィザード 67, 68
  - 構成、サーバー・インスタンス 67
  - 構成、手動 67, 69
  - 構成ウィザード 68
  - 互換性、サーバー、他の DB2 製品との 27
- コマンド
  - 管理、SET DBRECOVERY 87
  - DSMSERV FORMAT 75
- コマンド、管理
  - HALT 86
  - REGISTER LICENSE 87
  - コンソールの言語サポート 60
  - コンソール・モード 58
  - コンポーネント
    - インストール可能 vii

## [サ行]

サーバー
 

- アップグレード
  - 8.1 への 95
  - V7.1 から V8.1 96
- アップグレード後
  - 以前のサーバー・バージョンへの復帰 105
- アップグレードの前に
  - 準備手順の重要性 105

開始
 

- 自動 83
- スタンドアロン・モード 85
- 保守モード 85

互換性
 

- DB2 製品 27
- 停止 86
- パフォーマンスの最適化 3

サーバー (続き)  
  命名のベスト・プラクティス 52

サーバー AIX  
  アップグレード  
    V8.1 96

サーバー、  
  開始 80  
  活動化 80  
  セットアップ 80

サーバー、IBM Spectrum Protect  
  オプション 71, 72  
  停止 86

サーバーのアーカイブ・ログ  
  ディスクのチェックリスト 10

サーバーの回復ログ  
  ディスクのチェックリスト 10

サーバーの活動ログ  
  ディスクのチェックリスト 10

サーバーの始動  
  ユーザー ID から 83

サーバーの自動始動 83

サーバーの停止 86

サーバー・インスタンス 67, 69  
  命名 52  
  命名のベスト・プラクティス 52

サーバー・インスタンス、作成 69

サーバー・インスタンスの作成 63, 67

サーバー・オプション  
  調整 71  
  dsmserv.opt.smp 71

サーバー・オプション・ファイル (server options file)  
  設定 71

サーバー・データベース  
  再編成オプション 78  
  ストレージ・パス 8  
  ディスクのチェックリスト 8  
  ディレクトリー 8

サーバー・ハードウェア  
  サーバー・システムのチェックリスト 4  
  ストレージ・テクノロジーの選択 22  
  ディスク上のストレージ・プールに関するチェックリスト  
    20

サーバー・ライセンス 87

最初のステップ 63

サイレント・インストール  
  IBM Spectrum Protect 59

暫定修正 91

時間  
  サーバーのアップグレード 96

システム要件 26  
  Operations Center 121, 122, 126, 127  
  自動始動、サーバー 83  
  修正 55  
  状況モニター 122  
  資料 viii  
  新機能 ix

身体障害 189

スクリプト  
  サーバーの自動始動 83  
  dsmserv.rc 83

スタンドアロン・モード 85

ストレージ・テクノロジーの選択 22

ストレージ・プール 20  
  以前のサーバー・バージョンへの復帰 105  
  ストレージ・テクノロジーの選択 22

スポーク・サーバー 122  
  追加 143

制限  
  クライアント管理サービス 128

セキュア通信 148, 151

セキュア通信のためのパスワード 132

前提条件の検査  
  Operations Center 121

ソフトウェア要件  
  IBM Spectrum Protect 27

## [夕行]

チューニング  
  Operations Center 122

通信の使用可能化 71

通信方式  
  共有メモリー 73  
  TCP/IP 72

データ重複排除  
  以前のサーバー・バージョンに 戻したときの影響 105

データベース  
  インストール 75  
  ストレージ・テクノロジーの選択 22  
  名前 52  
  バックアップ 87

データベース・ディレクトリー 65

データベース・マネージャー 34, 76

停止  
  クライアント管理サービス 161  
  サーバー 86

ディスク・システム  
  活動ログのチェックリスト 10  
  サーバーの回復ログのチェックリスト 10  
  サーバー・データベースのチェックリスト 8  
  選択 22  
  ディスク上のストレージ・プール 20  
  分類 22

ディスク・スペース 27

ディスク・パフォーマンス  
  活動ログのチェックリスト 10  
  サーバーの回復ログのチェックリスト 10  
  サーバー・データベースのチェックリスト 8  
  ディスク上のストレージ・プールに関するチェックリスト  
    20

ディレクトリー  
  言語 54

ディレクトリー (続き)  
装置 54  
デフォルト・インストール 54  
命名、サーバーの 52  
DB2 54  
ディレクトリー、インスタンス 65  
デバイス・ドライバー、IBM Spectrum Protect vii  
デフォルト・インストール・ディレクトリー 54  
トラストストア・ファイル 148, 151  
  パスワードのリセット 153  
Operations Center 132  
トラブルシューティング  
  Operations Center のインストール 179  
    RHEL 5 上の韓国語フォント 179  
    RHEL 5 上の中国語フォント 179  
    RHEL 5 上の日本語フォント 179  
トランスポート層セキュリティー (TLS) 73  
トランスポート層セキュリティー・プロトコル 148, 151

## [ナ行]

名前、ベスト・プラクティス  
  インスタンス・ユーザー ID 52  
  サーバー名 52  
  サーバー・インスタンス 52  
  データベース名 52  
  ディレクトリー、サーバーの 52

## [ハ行]

ハードウェア要件  
  IBM Spectrum Protect 27  
  パスポート・アドバンテージ 55  
  パスワード  
    Operations Center ト拉斯ストア・ファイル 132, 153  
  バックアップ  
    データベース 87  
  パッケージ 29, 131  
  パッケージ・グループ 29, 131  
  パフォーマンス  
    構成のベスト・プラクティス 24  
    ユーザー制限、最適なパフォーマンスのための設定 80  
  Operations Center 122  
  ハブ・サーバー 122  
    構成 142  
  ファイル  
    dsmserv.opt.smp 71  
  フィックスパック 91  
  複数の DB2 コピー 27  
  複数のサーバー  
    アップグレード  
      複数のサーバー 88  
  米国英語 61  
  ポート番号  
    Operations Center 132, 155

ホーム・ディレクトリー 69  
保守更新 91  
保守モード 85  
翻訳 60  
翻訳機能 60  
  
[マ行]  
メモリー所要量 27  
モニター  
  ログ 88  
モニター管理者 130  
モバイル・デバイス  
  ストレージ環境のモニター 155

## [ヤ行]

ユーザー ID 65  
ユーザー制限 80  
  設定  
    サーバーの始動前 81  
要件  
  クライアント管理サービス 128

## [ラ行]

ライセンス  
  インストール可能パッケージ vii  
ライセンス、IBM Spectrum Protect 87  
リソース要件  
  Operations Center 122  
リファレンス、DB2 コマンド 109  
リポジトリ 29, 131  
ロールバック 50, 51  
  Operations Center 183  
ログイン画面のテキスト  
  Operations Center 146  
ログ・ファイル  
  インストール 187

## [ワ行]

ワークシート  
  サーバー・スペースの計画 30

**A**  
AIX 上の IBM Spectrum Protect  
  アップグレード  
    V8.1 96  
AIX のアップグレード  
  サーバー  
    V8.1 96  
API 76

API 構成 76

## B

BACKUP DB コマンド 76

## C

client-configuration.xml ファイル 159, 163  
CmsConfig ユーティリティー  
  クライアント管理サービス 163  
  検出 164  
  ヘルプ 178  
  addlog 170  
  addnode 166  
  list 177  
  remove 174, 175  
  setopt 168  
  setsys 169

## D

DB2 コマンド 109  
DB2 製品、互換性、サーバー 27  
DB2 ディレクトリー 54  
db2icrt コマンド 69  
db2profile 83  
DEFINE DEVCLASS 87  
DISK デバイス・クラス  
  ストレージ・テクノロジーの選択 22  
  ディスク・システムのチェックリスト 20  
DSMSERV FORMAT コマンド 75  
dsmserv.v6lock 86

## E

E メール・アラート 143  
  一時的な中断 145

## F

FILE デバイス・クラス  
  ストレージ・テクノロジーの選択 22  
  ディスク・システムのチェックリスト 20

## H

HALT コマンド 86  
HTTPS 148, 151  
  トラストストア・ファイルのパスワード 132, 153

## I

IBM Installation Manager 29, 131, 132  
  アンインストール 116  
IBM Knowledge Center viii  
IBM Spectrum Protect  
  アップグレード  
    8.1 95  
    V7.1 から V8.1 96  
  アンインストール 113  
    グラフィカル・インストール・ウィザードの使用 113  
    コンソール・モードでコマンド・ラインを使用した 114  
    サイレント・モードで 114  
  インストール 57, 58  
  インストール・パッケージ 55  
  サーバーの変更  
    バージョン 8.1 ix  
IBM Spectrum Protect サポート・サイト 55  
IBM Spectrum Protect デバイス・ドライバー、インストール  
  可能パッケージ vii  
IBM Spectrum Protect フィックスパック 91  
IBM Spectrum Protect、セットアップ 80  
Installation Manager 29, 131, 132  
  ログ・ディレクトリー 187  
iPad  
  ストレージ環境のモニター 155

## K

KILL コマンド 86  
Knowledge Center viii

## L

LANGUAGE オプション 60, 61  
Linux on Power Systems (リトル・エンディアン)  
  システム要件 27  
Linux on System z  
  システム要件 27  
Linux x86\_64  
  システム要件 27

## O

Operations Center vii  
  アップグレード 119, 139  
  アンインストール 181  
    グラフィカル・ウィザードの使用 181  
    コンソール・モードでコマンド・ラインを使用した 181  
    サイレント・モードで 182  
  インストール 119, 135  
    グラフィカル・ウィザードの使用 136  
    コンソール・モードでコマンド・ラインを使用した 136  
    サイレント・モードで 136  
  インストールのための資格情報 132

## Operations Center (続き)

インストールのトラブルシューティング 179  
インストール・ディレクトリー 132  
インストール・パッケージ 135  
オープン 142, 155  
オペレーティング・システム要件 126  
概要 121  
管理者 ID 130  
言語要件 127  
構成 141  
コンピューターの要件 122  
システム要件 121  
spoak・サーバー 122, 143  
セキュア通信のためのパスワード 132, 153  
前提条件の検査 121  
ハブ・サーバー 122  
ポート番号 132, 155  
前のバージョンへのロールバック 183  
ログイン画面のテキスト 146  
Chrome 127  
Firefox 127  
IE 127  
Internet Explorer 127  
Safari 127  
SSL 148, 151  
URL 155  
Web サーバー 155  
Web ブラウザーの要件 127  
Operations Center のアップグレード 119  
Operations Center のインストール 119  
Operations Center の構成  
  クライアント管理サービスの場合 160

## R

REGISTER LICENSE コマンド 87

## S

Secure Sockets Layer 148, 151  
Secure Sockets Layer (SSL) 71  
  使用による通信 73  
  トランスポート層セキュリティー (TLS) 73  
SET DBRECOVERY 87  
SSL 148, 151  
  トラストストア・ファイルのパスワード 132, 153  
SSL (Secure Sockets Layer)  
  使用による通信 73  
  トランスポート層セキュリティー 73  
SSLTCPADMINPORT オプション 72  
SSLTCPPORT オプション 72

## T

TCPNODELAY オプション 72  
TCPPORT オプション 72  
TCPWINDOWSIZE オプション 72  
TCP/IP  
  設定オプション 72  
  バージョン 4 71, 72  
  バージョン 6 71, 72  
TLS 148, 151

## U

Ubuntu Server LTS 27  
ulimits  
  設定  
    サーバーの始動前 81  
URL  
  Operations Center 155

## W

Web サーバー  
  開始 155  
  停止 155



**IBM**<sup>®</sup>

プログラム番号: 5725-W99

5725-W98

5725-X15

Printed in Japan

**日本アイ・ビー・エム株式会社**  
〒103-8510 東京都中央区日本橋箱崎町19-21