IBM Spectrum Protect
8.1.12

マルチサイト・ディスク・ソリューションのガイド

お願い

本書および本書で紹介する製品をご使用になる前に、139 ページの『特記事項』に記載されている情報をお読みください。

本書は、 IBM Spectrum® Protect (製品番号 5725-W98、5725-W99、5725-X15) のバージョン 8、リリース 1、モディフィケーション 12 、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに 適用されます。

目次

本書について

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

本書の対象読者

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

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

資料

IBM Spectrum Protect 製品ファミリーには、IBM Spectrum Protect Plus、IBM Spectrum Protect for Virtual Environments、IBM Spectrum Protect for Databases、およびその他の IBM® のストレージ管理製品が含まれています。

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

このリリースの新機能

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

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

- サーバー・コンポーネントの新機能
- クライアント・コンポーネントの新機能

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

第 1 部 マルチサイト・ディスク・データ保護ソリューションの計画

データ重複排除と複製を使用する 2 つのサイトのサーバーを使用して、マルチサイト・ディスク・データ保護ソリューションを計画します。

実装メソッド

以下の方法で、サーバーをマルチサイト・ディスク・ソリューション用に構成することができます。

Operations Center および管理コマンドを使用したサーバーの構成

ご使用のソリューション用に、一連のストレージ・システムおよびサーバー・ソフトウェアを構成することができます。 構成タスクを実行するには、Operations Center のウィザードとオプション、および IBM Spectrum Protect コマンドを使用します。概要については、1 ページの『計画ロードマップ』を参照してください。

自動化されたスクリプトを使用したサーバーの構成

特定の IBM Storwize® ストレージ・システムでの構成、および自動化されたスクリプトを使用した各サーバーの構成に関する詳細なガイダンスについては、IBM Spectrum Protect Blueprints を参照してください。

ブループリントの資料には、Operations Center のインストールと構成、Transport Security Layer (TLS) を使用したセキュア通信のセットアップのステップは記載されていません。複製は、各サーバーのセットアップ後に、コマンドを使用して構成します。IBM Spectrum Scale テクノロジーに基づく Elastic Storage Server を使用するためのオプションが含まれます。

計画ロードマップ

以下の図のアーキテクチャー・レイアウトを参照して、ダイアグラムの後に示されたロードマップ・タスクを実行することで、マルチサイト・ディスク・ソリューションを計画します。

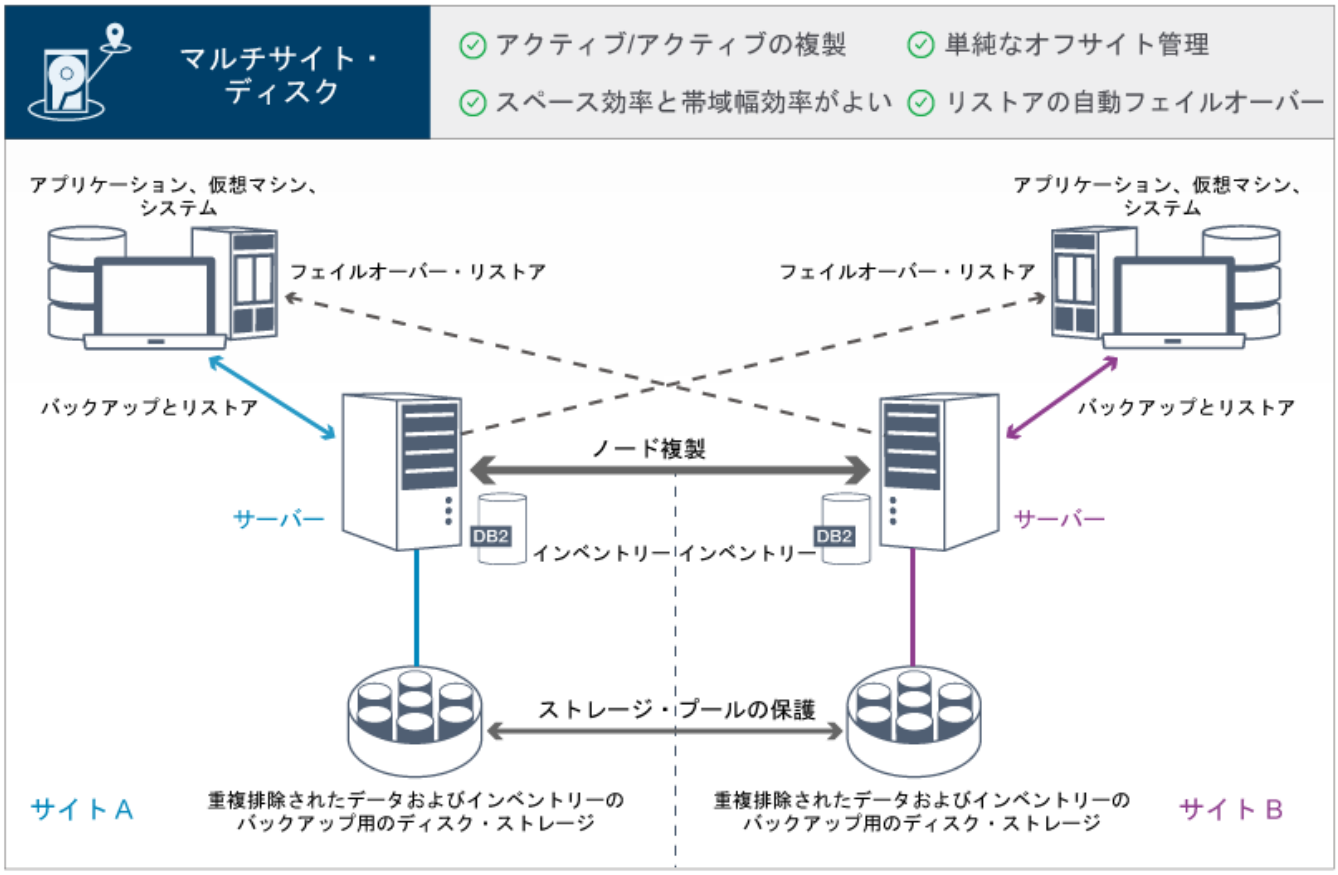


図 *1.* マルチサイト・ディスク・ソリューション

マルチサイト・ディスク環境で適切な計画を立てるには、以下のステップが必要です。

1. システム・サイズを選択します。
2. サイトを計画します。
3. ハードウェアおよびソフトウェアのシステム 要件を満たします。
4. 計画ワークシートにご使用のシステム構成の値を記録します。
5. ストレージを計画します。
6. セキュリティーを計画します。
   a. 管理者役割を計画します。
   b. セキュア通信を計画します。
   c. 暗号化データのストレージを計画します。
   d. ファイアウォール・アクセスを計画します。

システム・サイズの選択

管理するデータ量と保護するシステムに基づいて、IBM Spectrum Protect サーバーのサイズを選択します。

このタスクについて

表内の情報を使用し、管理するデータ量に基づいて、必要なサーバーのサイズを判別することができます。

次の表で、サーバーが管理するデータのボリュームについて説明します。この量には、すべてのバージョンが含まれています。データの日次量は、毎日バックアップする新規データの量です。管理対象データの合計と新規データの日次量はいずれも、データ削減前のサイズとして測定されています。

表 1. サーバーのサイズの決定

管理対象データの合計	バックアップする新規データの日次量	必要なサーバー・サイズ
60 TB - 240 TB	1 日当たり最大 10 TB	小規模
360 TB - 1440 TB	1 日当たり 10 から 30 TB	中規模
1000 TB - 4000 TB	1 日当たり 30 から 100 TB	大規模

表に示されている日次バックアップの値は、IBM Spectrum Protect for Virtual Environments で使用される 128 MB のサイズのオブジェクトを 使用して得られたテスト結果に基づいています。128 KB 未満のオブジェクトで構成されるワークロードでは、これらの日次制限を達成できない可能性があります。

サイトの計画

ユース・ケースを確認し、要因を評価することで、IBM Spectrum Protect のマルチサイト・ディスク・ソリューションに最も効率的なデータ保護を提供します。

ユース・ケース

マルチサイト・ディスク・ソリューションでは、少なくとも 1 つのバックアップ・データのコピーが作成されます。IBM Spectrum Protect サーバーが別々の場所にある場合は、バックアップ・レプリカがオフサイトに維持されます。

ヒント : ターゲット・サーバーに複製される ID とオプション・セット、およびエンタープライズ構成で管理される ID とオプション・セットを特定することで管理 ID とクライアント・オプション・セットを管理する際の競合を回避します。登録済みノードの 管理 ID が存在する場合、その同じノードに対して管理ユーザー ID を定義できません。

お客様の会社では、さまざまな理由からマルチサイト・ディスク・ソリューションの恩恵を受ける場合がありますが、マルチサイト・ディスク・ソリューションを使用する最も一般的な理由として、以下の複製シナリオがあります。

1 次サイトから災害復旧サイトへの複製

このシナリオでは、1 次サイト (サイト A) からバックアップされたデータは、2 次の災害復旧サイト (サイト B) にあるサーバーに複製されます。サイト A で災害 (サーバーの障害など) が発生した場合、サイト B のサーバーを使用して、システムをリカバリーすることができます。あるいは、サイト B でディスク・ストレージ障害が発生した後などに、サイト A のサーバーを使用して、サイト B の 1 次ストレージ・プール・データをリストアすることもできます。

2 つのアクティブ・サイトでの相互複製

このシナリオでは、各サイトのローカル・データは、サイト A とサイト B の両方のサーバーによってバックアップされます。サイト A からバックアップされたデータはサイト B に複製され、サイト B からバックアップされたデータはサイト A に複製されます。バックアップされたデータがサイト A で失われた場合、サイト B のサーバーを使用して、ストレージ・プール・データをサイト A のサーバーにリカバリーすることができます。サイト A が使用不可になった場合は、サイト A の複製データをサイト B の新規システムにリカバリーすることができます。災害復旧計画の一環として、どちらのサイトにもすべてのクライアント・ノードをバックアップおよびリストアするのに十分な容量があるように、サーバー・リソースのサイズを調整する必要があります。

1 次サイトへのリモート・サーバーの保護

このシナリオでは、比較的小規模なリモート・サーバーを構成して、1 次サイトにある大規模なサーバーにバックアップされるデータを複製します。帯域幅が制限されている場合、リモート・サイトにシステムをリストアすることは実用的ではありません。 そのような場合は、バックアップ・データをリモート・サーバーに複製する前に、1 次サイトのシステムをリカバリーすることをお 勧めします。

評価する要因

マルチサイト・ディスク・ソリューションを実装する前に、以下の要因を評価してください。

ネットワーク帯域幅

ネットワークには、ノード間で予想されるデータ転送、複製、およびクロスサイト・リストア操作 (これらは災害復旧に必要) に十分な帯域幅が必要です。 複製スループットのテストを 進める前に、ネットワークが複製トラフィックを処理できることを確認してください。 複製に必要なネットワーク帯域幅の見積もり (V7.1.1) のガイドラインを適用して、定常状態要件に必要なネットワーク帯域幅を計算します。

ネットワーク接続は、通常は共有リソースです。他のリソース・ユーザーとの競合を回避するように、ノード複製の実行をスケジュールする時刻を計画します。 また、ネットワーク制御により、アクティビティーを一部の帯域幅のみに制限することもできます。IBM Spectrum Protect には、ネットワーク使用量を制限するための制御はありません。

初期複製のリソース

2 つのサイト間でのデータ保護ソリューションをセットアップするには、最初にサイト A からサイト B のターゲット・サーバーにデータを複製する必要があります。確実に初期複製を正常に行うには、データの複製に使用可能なネットワーク帯域幅、プロセッサー・リソース、および時間があるかどうかを判別する必要があります。 初回のフルバックアップの 複製には数日間をかけるよう計画することが必要な場合もあります。初期バックアップのスケジュールを 延長できない場合は、ネットワークを使用せずにサイト A からサイト B にデータを複製することができます。 例えば、メディアを使用してバックアップ・データをエクスポートおよびインポートしたり、一時的にソース・サーバーとターゲット・サーバーを同じサイトに配置したりすることができます。

日次データ収集

マルチサイト・ディスク・ソリューションでは、日次データ収集量と合計データ保存量が、構成の容量内でなければなりません。例えば、大規模の構成には、ノード複製を含めて 1 日ごとに最大 100 TB のデータ収集容量があります。バックアップ要件が単一のサーバーの容量を超える場合、複数のサーバーを使用して必要な容量を達成するソリューションを構成することができます。

サーバー構成

サーバー構成が、マルチサイト・ディスク・ソリューションの要件を満たすか上回っている必要があります。

バックアップ・データの単一レプリカ

バックアップ・データの単一のオフサイト・コピーでデータ保護とリスク軽減の要件が満たされる場合は、マルチサイト・ディスク・ソリューションが最も効率的です。この場合、データの単一コピーは、複製サーバーが配置されている場所にオフサイトで保持されます。

関連資料

マルチサイト・ディスク・ソリューションのシステム 要件

お客様のデータ保護要件に最適な IBM Spectrum Protect ソリューションを選択した後、システム要件を確認して、データ保護ソリューションの実装を計画します。

マルチサイト・ディスク・ソリューションのシステム要件

お客様のデータ保護要件に最適な IBM Spectrum Protect ソリューションを選択した後、システム要件を確認して、データ保護ソリューションの実装を計画します。

ご使用のシステムが、使用する予定のサーバーのサイズに関するハードウェアおよびソフトウェアの前提条件を満たしていることを確認してください。

関連情報

IBM Spectrum Protect Supported Operating Systems

ハードウェア要件

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

システムのサイズの 定義については、システム・サイズの選択を参照してください。

以下の表に、構築する予定のサーバーのサイズに基づく、サーバーおよびストレージの最小ハードウェア要件を示します。ローカル区画 (LPAR) または作業区画 (WPAR) を使用している場合は、区画サイズを考慮に入れてネットワーク要件を調整してください。

以下の表の情報を開始点として使用します。 サーバーおよびストレージのハードウェア要件と仕様に関する最新の情報は、IBM Spectrum Protect Blueprints を参照してください。

ハードウェア・コンポーネント	小規模システム	中規模システム	大規模システム
サーバー・プロセッサー	AIX 6 プロセッサー・コア、3.42 GHz 以上 Linux Windows 16 プロセッサー・コア、1.7 GHz 以上	AIX 10 プロセッサー・コア、3.42 GHz 以上 Linux Windows 20 プロセッサー・コア、2.2 GHz 以上	AIX 20 プロセッサー・コア、3.42 GHz Linux Windows 44 プロセッサー・コア、2.2 GHz 以上
サーバー・メモリー	64 GB RAM	128 GB RAM	256 GB RAM
ネットワーク	• 10 GB イーサネット (1 ポート) • 8 GB ファイバー・チャネル・アダプター (2 ポート)	• 10 GB イーサネット (2 ポート) • 8 GB ファイバー・チャネル・アダプター (2 ポート)	• 10 GB イーサネット (4 ポート) • 8 GB ファイバー・チャネル・アダプター (4 ポート)
ストレージ	• データベース用に 1.45 TB SSD ディスク、加えて Operations Center レコード用のスペース • 67 TB の重複排除されたディレクトリー・コンテナー・ストレージ・プール	• データベース用に 2.53 TB SSD ディスク、加えて Operations Center レコード用のスペース • 207.9 TB の重複排除されたディレクトリー・コンテナー・ストレージ・プール	• データベース用に 6.54 TB SSD ディスク、加えて Operations Center レコード用のスペース • 1049.67 TB の重複排除されたディレクトリー・コンテナー・ストレージ・プール

正しいプロセッサー・コア・テクノロジーの実装

サーバー・プロセッサーには正しいタイプのプロセッサー・コア・テクノロジーを使用する必要があります。プロセッサー・コア・テクノロジーのタイプについて詳しくは、IBM Spectrum Protect Blueprints を参照してください。

Operations Center のデータベース・スペース所要量の見積もり

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

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

サーバーでの Operations Center の管理は、データベース用の追加スペースが必要なワークロードです。スペースの量は、サーバー上でモニターされているクライアントの数によって異なります。 ご使用のサーバーで必要なスペース量を見積もるには、以下のガイドラインを参照してください。

データベース・スペース

Operations Center では、サーバーでモニターする 1000 クライアントごとに約 1.2 GB のデータベース・スペースを使用します。例えば、2000 クライアントを持つハブ・サーバーで、それぞれ 1500 クライアントを持つ 3 つのスポーク・サーバーの管理も行うものとします。この構成では、4 つのサーバー全体で合計 6500 クライアントになり、約 8.4 GB のデータベース・スペースが必要です。この値を計算する際には、6500 クライアントを直近の 1000 の台に丸めます。つまり 7000 にします。

```
7 x 1.2 GB=8.4 GB
```

アーカイブ・ログ・スペース

Operations Center では、24 時間ごとに、1000 クライアント当たり約 8 GB のアーカイブ・ログ・スペースを使用します。ハブ・サーバーとスポーク・サーバー全体で 6500 クライアントの例では、24 時間の期間にわたって 56 GB のアーカイブ・ログ・スペースがハブ・サーバー用に使用されます。

この例の各スポーク・サーバーの場合、24 時間にわたって使用されるアーカイブ・ログ・スペースは約 16 GB です。 これらの見積もりは、デフォルトの状況収集間隔である 5 分に基づいています。収集間隔を 5 分毎から 3 分毎に減らすと、スペース要件は以下のように増加します。 以下の例は、収集間隔を 3 分ごとに 1 回に設定した場合のログ・スペース要件の増加の概算を示しています。

- ハブ・サーバー: 56 GB から約 94 GB に
- 各スポーク・サーバー: 16 GB から約 28 GB に

Operations Center をサポートするために使用可能な十分なスペースがあり、既存のサーバーの操作に影響を与えずに済むように、アーカイブ・ログ・スペースを増やしてください。

2 番目のサーバーのハードウェア要件

最初のサイトにあるすべてのものが 2 次サイトに複製されるようにサイトをセットアップする 予定の場合は、ハードウェア要件は両方のサイトで同じです。 2 次サイトにデータのサブセットのみを複製する場合は、ストレージとネットワークの要件が軽減される可能性があります。

ソフトウェア要件

IBM Spectrum Protect マルチサイト・ディスク・ソリューションの資料には、以下のオペレーティング・システムでのインストール・タスクおよび構成タスクが含まれています。リストされている最小ソフトウェア要件を満たす必要があります。

AIX システム

ソフトウェアのタイプ	最小ソフトウェア要件
オペレーティング・システム	IBM AIX® 7.1 オペレーティング・システム要件の詳細については、IBM Spectrum Protect のインストール情報を参照してください。
Gunzip ユーティリティー	IBM Spectrum Protect サーバーをインストールまたはアップグレードする場合は、事前にシステムで gunzip ユーティリティーが 使用可能になっている必要があります。gunzip ユーティリティーがインストールされ、gunzip ユーティリティーへのパスが PATH 環境変数で設定されていることを確認してください。
ファイル・システム・タイプ	JFS2 ファイル・システム AIX システムでは、大量のファイル・システム・データをキャッシュに入れることができます。これにより、サーバーおよび IBM Db2® プロセスで必要なメモリーを削減することができます。AIX サーバーでのページングを回避するには、JFS2 ファイル・システムの場合、`rbrw` マウント・オプションを使用します。ファイル・システム・キャッシュに使用されるメモリーが減り、IBM Spectrum Protect が使用できるメモリーが増えます。 IBM Spectrum Protect データベース、ログ、またはストレージ・プール・ボリュームを含むファイル・システムでは、ファイル・システム・マウント・オプション、並行入出力 (CIO)、および直接入出力 (DIO) を使用しないでください。これらのオプションを使用すると、多くのサーバー操作のパフォーマンスが低下する可能性があります。IBM Spectrum Protect および Db2 は、DIO を使用することが有益である場合には引き続き DIO を使用することができますが、IBM Spectrum Protect では、マウント・オプションを使用してこれらの技法の利点を選択的に活用する必要はありません。
その他のソフトウェア	Korn シェル (ksh)

Linux システム

ソフトウェアのタイプ	最小ソフトウェア要件
オペレーティング・システム	Red Hat® Enterprise Linux® 7 (x86_64)
ライブラリー	IBM Spectrum Protect システムに インストールされている GNU C ライブラリー バージョン 2.3.3-98.38 以降。 Red Hat Enterprise Linux Servers: • libaio • libstdc++.so.6 (32 ビットと 64 ビットのパッケージが必要です) • numactl.x86_64
ファイル・システム・タイプ	データベース関連のファイル・システムは、ext3 または ext4 を使用してフォーマット設定します。 ストレージ・プール関連のファイル・システムの場合は、XFS を使用してください。
その他のソフトウェア	Korn シェル (ksh)

Windows システム

ソフトウェアのタイプ	最小ソフトウェア要件
オペレーティング・システム	Microsoft Windows Server 2012 R2 (64 ビット) または Windows Server 2016
ファイル・システム・タイプ	NTFS
その他のソフトウェア	Windows 2012 R2 または Windows 2016 (.NET Framework 3.5 がインストールされて有効になっている) 以下のユーザー・アカウント制御ポリシーを無効にする必要があります。 • ユーザー・アカウント制御: 組み込みの Administrator アカウントに対する管理者承認モード • ユーザー・アカウント制御: 管理者承認モードですべての管理者を実行する

関連情報
AIX ネットワーク・オプションの設定

計画ワークシート

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

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

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

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

AIX

表 2. *AIX* サーバー・システムの事前構成のワークシート

項目	デフォルト値	値	最小ディレクトリー・サイズ	注
サーバーとの通信用の TCP/IP ポート・アドレス	1500		適用外	オペレーティング・システムをインストールして構成するときに、このポートを使用できることを確認してください。 ポート番号は、1024 から 32767 の範囲内の番号にすることができます。

表 2. *AIX* サーバー・システムの事前構成のワークシート *(続き)*

項目	デフォルト値	値	最小ディレクトリー・サイズ	注
サーバー・インスタンスのディレクトリー	/home/tsminst1/tsminst1		50 GB	サーバー・インスタンス・ディレクトリーの値をデフォルトから変更する場合は、11 ページの表 3 の Db2 インスタンス所有者の値も変更してください。
サーバー・インストールのディレクトリー	/		5 GB	
サーバー・インストールのディレクトリー	/usr		5 GB	
サーバー・インストールのディレクトリー	/var		5 GB	
サーバー・インストールのディレクトリー	/tmp		5 GB	
サーバー・インストールのディレクトリー	/opt		10 GB	
活動ログのディレクトリー	/tsminst1/TSMalog		• Windows 極小規模: 30 GB • 小規模および中規模: 140 GB • 大規模: 300 GB	サーバーの初期構成時に活動ログを作成する場合、サイズを 128 GB に設定します。
アーカイブ・ログのディレクトリー	/tsminst1/TSMarchlog		• Windows 極小規模: 250 GB • 小規模: 1 TB • 中規模: 2 TB • 大規模: 4 TB	

表 2. *AIX* サーバー・システムの事前構成のワークシート *(続き)*				
項目	**デフォルト値**	**値**	**最小ディレクトリー・サイズ**	**注**
データベースのディレクトリー	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		すべてのディレクトリーの最小合計スペース: • Windows 極小規模: 少なくとも 200 GB • 小規模: 少なくとも 1 TB • 中規模: 少なくとも 2 TB • 大規模: 少なくとも 4 TB	システムのサイズに応じて、データベース用に最小数のファイル・システムを作成します。 • Windows 極小規模: 少なくとも 1 個のファイル・システム • 小規模: 少なくとも 4 個のファイル・システム • 中規模: 少なくとも 4 個のファイル・システム • 大規模: 少なくとも 8 個のファイル・システム
ストレージのディレクトリー	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		すべてのディレクトリーの最小合計スペース: • Windows 極小規模: 少なくとも 10 TB • 小規模: 少なくとも 38 TB • 中規模: 少なくとも 180 TB • 大規模: 少なくとも 500 TB	システムのサイズに応じて、ストレージ用に最小数のファイル・システムを作成します。 • Windows 極小規模: 少なくとも 2 個のファイル・システム • 小規模: 少なくとも 2 個のファイル・システム • 中規模: 少なくとも 10 個のファイル・システム • 大規模: 少なくとも 30 個のファイル・システム

表 2. *AIX* サーバー・システムの事前構成のワークシート *(続き)*

項目	デフォルト値	値	最小ディレクトリー・サイズ	注
データベース・バックアップ用のディレクトリー	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		すべてのディレクトリーの最小合計スペース: • Windows 極小規模: 少なくとも 1 TB • 小規模: 少なくとも 3 TB • 中規模: 少なくとも 10 TB • 大規模: 少なくとも 16 TB	システムのサイズに応じて、データベースのバックアップ用に最小数のファイル・システムを作成します。 • Windows 極小規模: 少なくとも 1 個のファイル・システム • 小規模: 少なくとも 2 個のファイル・システム • 中規模: 少なくとも 3 個のファイル・システム • 大規模: 少なくとも 3 個のファイル・システム 最初のデータベース・バックアップ・ディレクトリーは、アーカイブ・ログのフェイルオーバー・ディレクトリーとして、およびボリューム・ヒストリー・ファイルと装置構成ファイルの 2 次コピーとしても使用されます。

表 3. *IBM Spectrum Protect* 構成のワークシート

項目	デフォルト値	値	注
Db2 インスタンス所有者	tsminst1		8 ページの表 2 でサーバー・インスタンス・ディレクトリーの値をデフォルトから変更した場合、Db2 インスタンス所有者の値も変更してください。
Db2 インスタンス所有者のパスワード	passw0rd		デフォルトとは異なるインスタンス所有者のパスワードを選択します。この値を安全な場所に必ず記録してください。
Db2 インスタンス所有者の 1 次グループ	tsmsrvrs		

表 3. *IBM Spectrum Protect* 構成のワークシート (続き)

項目	デフォルト値	値	注
サーバー名	サーバー名のデフォルト値は、システムのホスト名です。		
サーバー・パスワード	passw0rd		デフォルトとは異なるサーバー・パスワードの値を選択します。この値を安全な場所に必ず記録してください。
管理者 ID: サーバー・インスタンスのユーザー ID	admin		
管理者 ID のパスワード	passw0rd		デフォルトとは異なる管理者パスワードの値を選択します。この値を安全な場所に必ず記録してください。
スケジュールの開始時刻	22:00		デフォルトのスケジュールの開始時刻に、クライアント・ワークロード・フェーズが開始します。これは主に、クライアントのバックアップとアーカイブのアクティビティーです。クライアント・ワークロード・フェーズの間、サーバー・リソースはクライアント操作をサポートします。通常、これらの操作は、毎晩のスケジュール・ウィンドウ中に実行されます。 サーバー保守操作のスケジュールは、クライアント・バックアップ・ウィンドウの 10 時間後に開始するように定義されます。

Linux

表 4. *Linux* サーバー・システムの事前構成のワークシート

項目	デフォルト値	値	最小ディレクトリー・サイズ	注
サーバーとの通信用の TCP/IP ポート・アドレス	1500		適用外	オペレーティング・システムをインストールして構成するときに、このポートを使用できることを確認してください。 ポート番号は、1024 から 32767 の範囲内の番号にすることができます。
サーバー・インスタンスのディレクトリー	/home/tsminst1/tsminst1		25 GB	サーバー・インスタンス・ディレクトリーの値をデフォルトから変更する場合は、15 ページの表 5 の Db2 インスタンス所有者の値も変更してください。
活動ログのディレクトリー	/tsminst1/TSMalog		• Windows 極小規模: 30 GB • 小規模および中規模: 140 GB • 大規模: 300 GB	
アーカイブ・ログのディレクトリー	/tsminst1/TSMarchlog		• Windows 極小規模: 250 GB • 小規模: 1 TB • 中規模: 2 TB • 大規模: 4 TB	

表 4. *Linux* サーバー・システムの事前構成のワークシート (続き)

項目	デフォルト値	値	最小ディレクトリー・サイズ	注
データベースのディレクトリー	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		すべてのディレクトリーの最小合計スペース: • Windows 極小規模: 少なくとも 200 GB • 小規模: 少なくとも 1 TB • 中規模: 少なくとも 2 TB • 大規模: 少なくとも 4 TB	システムのサイズに応じて、データベース用に最小数のファイル・システムを作成します。 • Windows 極小規模: 少なくとも 1 個のファイル・システム • 小規模: 少なくとも 4 個のファイル・システム • 中規模: 少なくとも 4 個のファイル・システム • 大規模: 少なくとも 8 個のファイル・システム
ストレージのディレクトリー	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		すべてのディレクトリーの最小合計スペース: • Windows 極小規模: 少なくとも 10 TB • 小規模: 少なくとも 38 TB • 中規模: 少なくとも 180 TB • 大規模: 少なくとも 500 TB	システムのサイズに応じて、ストレージ用に最小数のファイル・システムを作成します。 • Windows 極小規模: 少なくとも 2 個のファイル・システム • 小規模: 少なくとも 2 個のファイル・システム • 中規模: 少なくとも 10 個のファイル・システム • 大規模: 少なくとも 30 個のファイル・システム

表 4. *Linux* サーバー・システムの事前構成のワークシート (続き)

項目	デフォルト値	値	最小ディレクトリー・サイズ	注
データベース・バックアップ用のディレクトリー	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		すべてのディレクトリーの最小合計スペース: • Windows 極小規模: 少なくとも 1 TB • 小規模: 少なくとも 3 TB • 中規模: 少なくとも 10 TB • 大規模: 少なくとも 16 TB	システムのサイズに応じて、データベースのバックアップ用に最小数のファイル・システムを作成します。 • Windows 極小規模: 少なくとも 1 個のファイル・システム • 小規模: 少なくとも 2 個のファイル・システム • 中規模: 少なくとも 3 個のファイル・システム • 大規模: 少なくとも 3 個のファイル・システム 最初のデータベース・バックアップ・ディレクトリーは、アーカイブ・ログのフェイルオーバー・ディレクトリーとして、およびボリューム・ヒストリー・ファイルと装置構成ファイルの 2 次コピーとしても使用されます。

表 5. *IBM Spectrum Protect* 構成のワークシート

項目	デフォルト値	値	注
Db2 インスタンス所有者	tsminst1		13 ページの表 4 でサーバー・インスタンス・ディレクトリーの値をデフォルトから変更した場合、Db2 インスタンス所有者の値も変更してください。
Db2 インスタンス所有者のパスワード	passw0rd		デフォルトとは異なるインスタンス所有者のパスワードを選択します。この値を安全な場所に必ず記録してください。
Db2 インスタンス所有者の 1 次グループ	tsmsrvrs		

表 5. *IBM Spectrum Protect* 構成のワークシート (続き)			
項目	**デフォルト値**	**値**	**注**
サーバー名	サーバー名のデフォルト値は、システムのホスト名です。		
サーバー・パスワード	passw0rd		デフォルトとは異なるサーバー・パスワードの値を選択します。この値を安全な場所に必ず記録してください。
管理者 ID: サーバー・インスタンスのユーザー ID	admin		
管理者 ID のパスワード	passw0rd		デフォルトとは異なる管理者パスワードの値を選択します。この値を安全な場所に必ず記録してください。
スケジュールの開始時刻	22:00		デフォルトのスケジュールの開始時刻に、クライアント・ワークロード・フェーズが開始します。これは主に、クライアントのバックアップとアーカイブのアクティビティーです。クライアント・ワークロード・フェーズの間、サーバー・リソースはクライアント操作をサポートします。通常、これらの操作は、毎晩のスケジュール・ウィンドウ中に実行されます。 サーバー保守操作のスケジュールは、クライアント・バックアップ・ウィンドウの 10 時間後に開始するように定義されます。

Windows

サーバー用に多数のボリュームが作成されるため、ドライブ名ではなく、ディレクトリーにディスク・ボリュームをマップするための Windows の機能を使用してサーバーを構成します。

例えば、C:¥tsminst1¥TSMdbpsace00 は、独自のスペースを持つボリュームへのマウント・ポイントです。ボリュームは、C: ドライブ下のディレクトリーにマップされますが、C: ドライブのスペースを占有しません。例外は、サーバー・インスタンス・ディレクトリーの C:¥tsminst1 です。これは、マウント・ポイントまたは通常のディレクトリーになります。

表 6. *Windows* サーバー・システムの事前構成のワークシート

項目	デフォルト値	値	最小ディレクトリー・サイズ	注
サーバーとの通信用の TCP/IP ポート・アドレス	1500		適用外	オペレーティング・システムをインストールして構成するときに、このポートを使用できることを確認してください。 ポート番号は、1024 から 32767 の範囲内の番号にすることができます。
サーバー・インスタンスのディレクトリー	C:¥tsminst1		25 GB	サーバー・インスタンス・ディレクトリーの値をデフォルトから変更する場合は、19 ページの表 7 の Db2 インスタンス所有者の値も変更してください。
活動ログのディレクトリー	C:¥tsminst1¥TSMalog		• Windows 極小規模: 30 GB • 小規模および中規模: 140 GB • 大規模: 300 GB	
アーカイブ・ログのディレクトリー	C:¥tsminst1¥TSMarchlog		• Windows 極小規模: 250 GB • 小規模: 1 TB • 中規模: 2 TB • 大規模: 4 TB	

表 6. *Windows* サーバー・システムの事前構成のワークシート (続き)

項目	デフォルト値	値	最小ディレクトリー・サイズ	注
データベースのディレクトリー	C:¥tsminst1¥TSMdbspace00 C:¥tsminst1¥TSMdbspace01 C:¥tsminst1¥TSMdbspace02 C:¥tsminst1¥TSMdbspace03 ...		すべてのディレクトリーの最小合計スペース: • Windows 極小規模: 少なくとも 200 GB • 小規模: 少なくとも 1 TB • 中規模: 少なくとも 2 TB • 大規模: 少なくとも 4 TB	システムのサイズに応じて、データベース用に最小数のファイル・システムを作成します。 • Windows 極小規模: 少なくとも 1 個のファイル・システム • 小規模: 少なくとも 4 個のファイル・システム • 中規模: 少なくとも 4 個のファイル・システム • 大規模: 少なくとも 8 個のファイル・システム
ストレージのディレクトリー	C:¥tsminst1¥TSMfile00 C:¥tsminst1¥TSMfile01 C:¥tsminst1¥TSMfile02 C:¥tsminst1¥TSMfile03 ...		すべてのディレクトリーの最小合計スペース: • Windows 極小規模: 少なくとも 10 TB • 小規模: 少なくとも 38 TB • 中規模: 少なくとも 180 TB • 大規模: 少なくとも 500 TB	システムのサイズに応じて、ストレージ用に最小数のファイル・システムを作成します。 • Windows 極小規模: 少なくとも 2 個のファイル・システム • 小規模: 少なくとも 2 個のファイル・システム • 中規模: 少なくとも 10 個のファイル・システム • 大規模: 少なくとも 30 個のファイル・システム

表 6. *Windows* サーバー・システムの事前構成のワークシート (続き)

項目	デフォルト値	値	最小ディレクトリー・サイズ	注
データベース・バックアップ用のディレクトリー	C:¥tsminst1¥TSMbkup00 C:¥tsminst1¥TSMbkup01 C:¥tsminst1¥TSMbkup02 C:¥tsminst1¥TSMbkup03		すべてのディレクトリーの最小合計スペース: • Windows 極小規模: 少なくとも 1 TB • 小規模: 少なくとも 3 TB • 中規模: 少なくとも 10 TB • 大規模: 少なくとも 16 TB	システムのサイズに応じて、データベースのバックアップ用に最小数のファイル・システムを作成します。 • Windows 極小規模: 少なくとも 1 個のファイル・システム • 小規模: 少なくとも 2 個のファイル・システム • 中規模: 少なくとも 3 個のファイル・システム • 大規模: 少なくとも 3 個のファイル・システム 最初のデータベース・バックアップ・ディレクトリーは、アーカイブ・ログのフェイルオーバー・ディレクトリーとして、およびボリューム・ヒストリー・ファイルと装置構成ファイルの 2 次コピーとしても使用されます。

表 7. *IBM Spectrum Protect* 構成のワークシート

項目	デフォルト値	値	注
Db2 インスタンス所有者	tsminst1		17 ページの表 6 でサーバー・インスタンス・ディレクトリーの値をデフォルトから変更した場合、Db2 インスタンス所有者の値も変更してください。
Db2 インスタンス所有者のパスワード	pAssW0rd		デフォルトとは異なるインスタンス所有者のパスワードを選択します。この値を安全な場所に必ず記録してください。
サーバー名	サーバー名のデフォルト値は、システムのホスト名です。		

表 7. *IBM Spectrum Protect* 構成のワークシート (続き)			
項目	**デフォルト値**	**値**	**注**
サーバー・パスワード	`passw0rd`		デフォルトとは異なるサーバー・パスワードの値を選択します。この値を安全な場所に必ず記録してください。
管理者 ID: サーバー・インスタンスのユーザー ID	`admin`		
管理者 ID のパスワード	`passw0rd`		デフォルトとは異なる管理者パスワードの値を選択します。この値を安全な場所に必ず記録してください。
スケジュールの開始時刻	`22:00`		デフォルトのスケジュールの開始時刻に、クライアント・ワークロード・フェーズが開始します。これは主に、クライアントのバックアップとアーカイブのアクティビティーです。クライアント・ワークロード・フェーズの間、サーバー・リソースはクライアント操作をサポートします。通常、これらの操作は、毎晩のスケジュール・ウィンドウ中に実行されます。 サーバー保守操作のスケジュールは、クライアント・バックアップ・ウィンドウの 10 時間後に開始するように定義されます。

ストレージの計画

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

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

データベースおよび活動ログ

- IBM Spectrum Protect データベースおよびアクティブ・ログに、次のような特性を持つ高速ディスクを使用します。
  - ファイバー・チャネルまたはシリアル接続 SCSI (SAS) インターフェースを 備えた高性能な 15k rpm ディスク
  - ソリッド・ステート・ディスク (SSD)

- SSD またはフラッシュ・ハードウェアを使用している場合を除き、活動ログをデータベースから分離してください。
- データベース用のアレイを作成する場合は、RAID レベル 5 を使用してください。

ストレージ・プール

- ストレージ・プールには、比較的低コストで低速のディスクを使用できます。
- ストレージ・プールは、アーカイブ・ログおよびデータベース・バックアップ・ストレージのディスクを共有できます。
- 大容量ディスク・タイプを使用している場合は、二重ドライブ障害に対する保護を追加するために、ストレージ・プール・アレイに RAID レベル 6 を使用してください。

関連情報

ストレージ・システムの要件とデータ破損のリスクの低減

ストレージ・アレイの計画

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

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

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

21 ページの表 8 および 22 ページの表 9 に、ストレージ・グループおよびボリューム構成のレイアウト要件を示します。

表 *8.* ストレージ・グループ構成のコンポーネント

コンポーネント	**詳細**
サーバー・ストレージ要件	サーバーによるストレージの使用法
ディスク・タイプ	ストレージ要件に合わせて使用されるディスク・タイプのサイズと速度
ディスク数	ストレージ要件に必要な各ディスク・タイプの数
ホット・スペア容量	ディスク障害の発生時に引き継ぐスペアとして予約されるディスクの数。
RAID レベル	論理ストレージに使用される RAID アレイのレベル RAID レベルは、アレイによって提供される冗長性のタイプを定義します (例えば、5 または 6)。
RAID アレイの数	作成する RAID アレイの数
RAID アレイ当たりの DDM	各 RAID アレイで使用されるディスク・ドライブ・モジュール (DDM) の数
RAID アレイ当たりの使用可能サイズ	冗長性のために失われるスペースを考慮した結果、各 RAID アレイ内でデータ・ストレージに使用できるサイズ

表 8. ストレージ・グループ構成のコンポーネント (続き)	
コンポーネント	**詳細**
合計使用可能サイズ	RAID アレイ内のデータ・ストレージに使用できる合計サイズ: 数量 x 使用可能サイズ
推奨されるストレージ・グループ名およびアレイ名	MDisk および MDisk グループに使用するのに推奨される名前
使用量	物理ディスクの一部を使用するサーバー・コンポーネント

表 9. ボリューム構成のコンポーネント	
コンポーネント	**詳細**
サーバー・ストレージ要件	物理ディスクを使用するための要件
ボリューム名	特定のボリュームに指定される固有の名前
ストレージ・グループ	ボリュームを作成するためのスペースが含まれているストレージ・グループの名前
サイズ	各ボリュームのサイズ
対象のサーバー・マウント・ポイント	ボリュームがマウントされるサーバー・システム上のディレクトリー
数量	特定の要件に対応して作成されるボリュームの数。同じ要件に対応して作成されるボリュームごとに同じ命名標準を使用してください。
使用量	物理ディスクの一部を使用するサーバー・コンポーネント

例

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

セキュリティーの計画

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

ランサムウェア攻撃からのストレージ環境の保護およびストレージ環境のリカバリーのガイドラインについては、ランサムウェアからのストレージ環境の保護を参照してください。

管理者役割の計画

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

管理者には以下のいずれかのレベルの権限を割り当てることができます。

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

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

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

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

23 ページの表 10 のシナリオでは、管理者がタスクを実行できるようにさまざまなレベルの権限を割り当てる理由を例を挙げて示します。

表 *10.* 管理者役割のシナリオ

シナリオ	セットアップする管理者 ID のタイプ
小規模な会社の管理者は、サーバーを管理し、すべてのサーバー・アクティビティーを 担当します。	• システム 権限: 1 つの管理者 ID
複数のサーバーの管理者は、システム 全体の管理も行います。その他の何人かの管理者が、それぞれのストレージ・プールを管理します。	• すべてのサーバーに対するシステム 権限: システム 全体の管理者用に 1 つの管理者 ID • 指定されたストレージ・プールに対するストレージ権限: その他の各管理者に 1 つの管理者 ID
管理者が 2 つのサーバーを管理します。他のユーザーが管理タスクを補助します。2 人のアシスタントが、重要なシステムがバックアップされていることの 確認の補助を担当します。 各アシスタントは、1 台の IBM Spectrum Protect サーバーのスケジュール済みバックアップのモニターを担当しています。	• 両方のサーバーに対するシステム 権限: 2 つの管理者 ID • オペレーター権限: 各ユーザーが担当するサーバーへのアクセス権を持つアシスタント用に 2 つの管理者 ID

セキュア通信の計画

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

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

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

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

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

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

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

関連情報
通信の保護

暗号化データのストレージの計画

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

企業で、ストレージ・プール内のデータを暗号化する必要がある場合は、IBM Spectrum Protect の暗号化を使用するオプション、または暗号化用のテープなどの外部装置を利用できます。

IBM Spectrum Protect でデータを暗号化する場合、クライアントで追加のコンピューティング・リソースが必要になります。これは、バックアップ・プロセスおよびリストア・プロセスのパフォーマンスに影響する可能性があります。

関連情報
IBM Spectrum Protect のクラウド・コンテナー・ストレージ・プールのデータ暗号化に関する考慮事項

ファイアウォール・アクセスの計画

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

24 ページの表 11 では、サーバー、クライアント、および Operations Center で使用されるポートについて説明します。

表 *11.* サーバー、クライアント、および *Operations Center* によって使用されるポート

項目	デフォルト	方向	説明
基本ポート (**TCPPORT**)	1500	アウトバウンド/インバウンド	サーバー・インスタンスには、個別に固有のポートが必要です。デフォルトを使用する代わりに、代替ポート番号を指定することができます。**TCPPORT** オプションは、クライアントからの TCP/IP セッションと SSL 対応セッションの両方を listen します。 管理可能クライアント・トラフィックの場合、**TCPADMINPORT** オプションと **ADMINONCLIENTPORT** オプションを使用して、ポート値を設定できます。
SSL 専用ポート (**SSLTCPPORT**)	デフォルトなし	アウトバウンド/インバウンド	このポートは、ポート上の通信を SSL 対応セッションのみに制限したい場合に使用します。 SSL 通信と非 SSL 通信の両方をサポートするには、**TCPPORT** オプションまたは **TCPADMINPORT** オプションを使用します。
SMB	45	インバウンド/アウトバウンド	このポートは、ネイティブ・プロトコルを使用して複数のホストと通信する構成ウィザードによって使用されます。
SSH	22	インバウンド/アウトバウンド	このポートは、ネイティブ・プロトコルを使用して複数のホストと通信する構成ウィザードによって使用されます。
SMTP	25	アウトバウンド	このポートは、サーバーから E メール・アラートを送信するために使用されます。

表 *11.* サーバー、クライアント、および *Operations Center* によって使用されるポート *(*続き*)*

項目	デフォルト	方向	説明
NDMP	デフォルトなし	インバウンド/アウトバウンド	サーバーは、NAS 装置へのアウトバウンド NDMP 制御ポート接続をオープンできる必要があります。アウトバウンド制御ポートは、NAS 装置のデータ・ムーバー定義における低位アドレスです。 ファイラーからサーバーへの NDMP リストア時に、サーバーは、NAS 装置へのアウトバウンド NDMP データ接続をオープンできる必要があります。 リストア時に使用されるデータ接続ポートは、NAS 装置上で構成することができます。 ファイラーからサーバーへの NDMP バックアップ時に、NAS 装置は、サーバーへのアウトバウンド・データ接続をオープンできる必要があり、サーバーは、インバウンド NDMP データ接続を受け入れられる必要があります。 サーバー・オプション **NDMPPORTRANGE** を使用して、NDMP データ接続として使用可能なポート・セットを制限することができます。 これらのポートとの接続用にファイアウォールを構成することができます。
複製	デフォルトなし	アウトバウンド/インバウンド	複製用のアウトバウンド・ポートのポートおよびプロトコルは、複製をセットアップするために使用される **DEFINE SERVER** コマンドによって設定されます。 複製用のインバウンド・ポートは、ソース・サーバーが **DEFINE SERVER** コマンドで指定する TCP ポートおよび SSL ポートです。
クライアント・スケジュール・ポート	クライアント・ポート: 1501	アウトバウンド	クライアントは、指定されたポートで listen し、サーバーにポート番号を伝えます。 サーバーは、サーバーが要求したスケジューリングが使用されている場合にクライアントに接続します。クライアント・オプション・ファイルで代替ポート番号を指定することができます。
長時間実行セッション	**KEEPALIVE** 設定: YES	アウトバウンド	**KEEPALIVE** オプションが有効である場合、ファイアウォール・ソフトウェアが長時間実行中の非アクティブ接続を閉じないように、クライアント/サーバー・セッション中にキープアライブ・パケットが送信されます。
Operations Center	HTTPS: 11090	インバウンド	これらのポートは、Operations Center Web ブラウザーに使用されます。代替ポート番号を指定することができます。
クライアント管理サービス・ポート	クライアント・ポート: 9028	インバウンド	クライアント管理サービス・ポートには、Operations Center からアクセス可能でなければなりません。ファイアウォールによって接続が妨げられないことを確認します。 クライアント管理サービスは、管理セッションを使用する認証に、クライアント・ノードのサーバーの TCP ポートを使用します。

第 2 部 データ保護ソリューションのマルチサイト・ディスク実装

マルチサイト・ディスク・ソリューションは、2 つのサイトで構成され、データ重複排除および複製を使用します。

実装のロードマップ

マルチサイト・ディスク環境をセットアップするには、以下のステップが必要です。

1. システムをセットアップします。
   a. ご使用の環境のサイズに合わせて、ストレージ・ハードウェアを構成し、ストレージ・アレイをセットアップします。
   b. サーバー・オペレーティング・システムをインストールします。
   c. マルチパス入出力を構成します。
   d. サーバー・インスタンスのユーザー ID を作成します。
   e. IBM Spectrum Protect 用にファイル・システムを準備します。
2. サーバーおよび Operations Center をインストールします。
3. サーバーおよび Operations Center を構成します。
   a. サーバーの初期構成を実行します。
   b. サーバー・オプションを設定します。
   c. サーバーおよびクライアントの Secure Sockets Layer を構成します。
   d. Operations Center を構成します。
   e. IBM Spectrum Protect のライセンスを登録します。
   f. データ重複排除を構成します。
   g. ビジネスに合わせたデータ保存ルールを定義します。
   h. サーバー保守スケジュールを定義します。
   i. クライアント・スケジュールを定義します。
4. クライアントをインストールし、構成します。
   a. クライアントを登録し、スケジュールに割り当てます。

      ヒント: ターゲット・サーバーに複製される ID とオプション・セット、およびエンタープライズ構成で管理される ID とオプション・セットを特定することで管理 ID とクライアント・オプション・セットを管理する際の競合を回避します。登録済みノードの 管理 ID が存在する場合、その同じノードに対して管理ユーザー ID を定義できません。
   b. クライアント管理サービスをインストールし、検証します。
   c. クライアント管理サービスを使用するように Operations Center を構成します。
5. 2 番目のサーバーを構成します。
   a. ハブとスポーク・サーバーの間の SSL 通信を構成します。
   b. 2 番目のサーバーをスポークとして追加します。
   c. 複製を有効にします。
6. 実装を完了します。

システムのセットアップ

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

ストレージ・ハードウェアの構成

ストレージ・ハードウェアを構成するには、ディスク・システムおよび IBM Spectrum Protect の全般的なガイドラインを確認します。

手順

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

   詳細については、20 ページの『ストレージの計画』を参照してください。
4. サーバー・システムが、作成されるディスク・ボリュームにアクセスできる必要があります。次の手順を実行してください。
   a) システムがファイバー・チャネル・スイッチに接続されている場合、ディスクを認識できるようにサーバーをゾーニングします。
   b) この特定のサーバーが各ディスクを認識できることをディスク・システムに通知するために、すべてのボリュームをマップします。

関連情報

ストレージの構成

サーバー・オペレーティング・システムのインストール

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

AIX システムへのインストール

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

手順

1. 製造元の指示に従い、AIX バージョン 7.1 TL4、SP6 以降をインストールします。
2. オペレーティング・システムのインストール手順に従って、TCP/IP 設定を構成します。
3. `/etc/hosts` ファイルを開き、以下のアクションを実行します。
   - ファイルを更新して、サーバーの IP アドレスとホスト名を組み込みます。例えば次のとおりです。

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

```
127.0.0.1  localhost
```

4. 次のコマンドを発行して、AIX 入出力完了ポートを有効にします。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

テストでは以下の設定が使用されました。

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

11. ユーザー処理リソースの限度 (*ulimits* とも呼ばれる) が 30 ページの表 12 のガイドラインに従って設定されていることを確認します。ulimit 値が正しく設定されていない場合、サーバーが不安定になったり、サーバーが応答できない状態になったりする可能性があります。

表 *12.* ユーザー限度 *(ulimit)* 値

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

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

Linux システムへのインストール

サーバー・システムに Linux x86_64 をインストールするには、以下の手順を実行します。

始める前に

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

手順

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

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

   a) DVD を開始した後、メニューから「**Install or upgrade an existing system**」を選択します。

   b) ようこそ画面で、「**Test this media & install Red Hat Enterprise Linux 7.8**」を選択します。

   c) 使用する言語およびキーボード設定を選択します。

   d) ロケーションを選択し、適切なタイム・ゾーンを設定します。

   e)「**ソフトウェアの選択**」を選択し、次の画面で「**サーバー (GUI を使用)**」を選択します。

   f) インストールの要約ページで、「**インストール先**」をクリックし、以下の項目を確認します。

   - インストール・ターゲットとして 300 GB のローカル・ディスクが選択されている。
   - 「その他のストレージオプション」で、「自動構成のパーティション構成」が選択されている。

   「**完了**」をクリックします。

   g)「**インストールの開始**」をクリックします。

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

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

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

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

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

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

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

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

3. /etc/hosts ファイルを開き、以下のアクションを実行します。

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

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

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

     ```
     127.0.0.1  localhost
     ```

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

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

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

   b) **mount** コマンドを発行して、DVD がマウントされていることを確認します。

   次の例のような出力が表示されるはずです。

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

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

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

   For RHEL 8:

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

   repos.d ディレクトリーが存在しない場合は、作成してください。

   d) ディレクトリーの内容をリストします。

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

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

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

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

```
vi rhel78_dvd.repo
```

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

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

For RHEL 8:

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

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

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

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

5. ソフトウェア・インストールが完了すると、以下のステップを実行して、元の YUM リポジトリーの値を復元できます。
   a) 次のコマンドを発行して、Red Hat Enterprise Linux のインストール DVD をアンマウントします。

```
unmount /mnt
```

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

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

   c) 作成したリポジトリー・ファイルを名前変更します。

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

   d) 元のファイルを元の名前に変更します。

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

6. カーネル・パラメーターの変更が必要かどうかを判別します。次の手順を実行してください。
   a) **sysctl -a** コマンドを使用して、パラメーターの値をリストします。

b) 33 ページの表 13 のガイドラインを使用して結果を分析し、何らかの変更が必要かどうかを判別します。

c) 変更が必要な場合は、/etc/sysctl.conf ファイルでパラメーターを設定します。

ファイルの変更は、システムの始動時に適用されます。

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

表 *13. Linux* カーネル・パラメーターの最適な設定

パラメーター	**説明**
kernel.shmmni	セグメントの最大数。
kernel.shmmax	共有メモリー・セグメントの最大サイズ (バイト)。 このパラメーターは、システム 起動時に IBM Spectrum Protect サーバーを自動的に始動する前に設定する必要があります。
kernel.shmall	共有メモリー・ページの最大割り振り (ページ)。
kernel.sem **kernel.sem** パラメーターには 4 つの値があります。	(SEMMSL) アレイごとの最大セマフォー数。
	(SEMMNS) システムごとの最大セマフォー数。
	(SEMOPM) セマフォー・コールごとの最大操作数。
	(SEMMNI) アレイの最大数。
kernel.msgmni	システム 全体のメッセージ・キューの最大数。
kernel.msgmax	メッセージの最大サイズ (バイト)。
kernel.msgmnb	キューのデフォルト最大サイズ (バイト)。
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。V7.1 以降のサーバー用に ASLR を使用可能にしてください。Linux ASLR および Db2 の詳細については、技術情報 1365583 を参照してください。
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。
vm.overcommit_memory	**vm.overcommit_memory** パラメーターは、カーネルが割り振りを許可する仮想メモリーの量に影響します。 カーネル・パラメーターについて詳しくは、「Db2 製品情報」を参照してください。

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

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

次のコマンドを発行します。

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

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

以下のコマンドを発行します。

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

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

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

以下のコマンドを発行します。

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

d) 変更を有効にするには、ファイアウォール定義を再ロードします。

以下のコマンドを発行します。

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

8. ユーザー処理リソースの限度 (*ulimits* とも呼ばれる) が 34 ページの表 14 のガイドラインに従って設定されていることを確認します。ulimit 値が正しく設定されていない場合、サーバーが不安定になったり、サーバーが応答できない状態になったりする可能性があります。

表 *14.* ユーザー限度 *(ulimit)* 値

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

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

Windows システムへのインストール

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

手順

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

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

6. Operations Center のハブ・サーバーで、Operations Center とのセキュア (https) 通信用にデフォルトのポートを開きます。
   ポート番号は 11090 です。
   例えば、次のコマンドを発行します。

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

マルチパス入出力の構成

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

AIX システム

手順

1. ディスク・サブシステム上のホスト定義に使用する必要があるファイバー・チャネル・ポート・アドレスを判別します。すべてのポートに対して **lscfg** コマンドを発行します。
   - 小規模および中規模のシステムでは、以下のコマンドを発行します。

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

   - 大規模のシステムでは、以下のコマンドを発行します。

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

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

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

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

```
cfgmgr
```

4. 使用可能なディスクをリストするには、次のコマンドを実行します。

```
lsdev -Ccdisk
```

出力は、以下の例のようになります。

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

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

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

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

```
lspv -u
```

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

```
hdisk4  00f8cf083fd97327  None  active
 3321360050763008101057800000000000030042145O3IBMfcp
```

この例で、*600507630081010578000000000000030* は、Storwize 管理インターフェースによって 報告されるボリュームの UID です。

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

```
bootinfo -s hdisk4
```

Linux システム

手順

1. Linux ホストに対してマルチパスを有効にするには、/etc/multipath.conf ファイルを編集します。

multipath.conf ファイルが存在しない場合は、次のコマンドを発行して作成することができます。

```
mpathconf --enable
```

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

```
defaults {
         user_friendly_names no
}

devices {
         device {
                  vendor "IBM "
                  product "2145"
                  path_grouping_policy group_by_prio
```

```
                user_friendly_names no
                path_selector "round-robin 0"
                prio "alua"
                path_checker "tur"
                failback "immediate"
                no_path_retry 5
                rr_weight uniform
                rr_min_io_rq "1"
                dev_loss_tmo 120
        }
}
```

2. システムの始動時に開始するようにマルチパス・オプションを設定します。

   以下のコマンドを発行します。

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

3. ディスクがオペレーティング・システムに認識されていてマルチパスによって管理されていることを確認するには、次のコマンドを発行します。

```
multipath -l
```

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

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

```
[root@tapsrv01 code]# multipath -l
36005076802810c509800000000000012 dm-43 IBM,2145
 size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=0 status=active
| |- 2:0:1:18 sdcw 70:64   active undef running
| `- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
  |- 1:0:1:18 sdat 66:208  active undef running
  `- 3:0:0:18 sddy 128:0   active undef running
```

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

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

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

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

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

   例えば、2 TB ディスクの装置 ID は 36005076802810c509800000000000012 です。

   次のステップで使用するために装置 ID のリストを保存します。

Windows システム

手順

1. マルチパス入出力機能がインストールされていることを確認します。必要であれば、追加のベンダー固有のマルチパス・ドライバーをインストールします。IBM FlashSystem デバイスには、Microsoft Device Specific Module (MSDSM) を使用してください。インストール手順については、IBM FlashSystem の資料 (https://www.ibm.com/support/knowledgecenter/STHGUJ_8.3.1/com.ibm.storwize.v5000.831.doc/svc_w2kmpio_21oxvp.html) を参照してください。

2. ディスクがオペレーティング・システムに認識されていてマルチパス入出力によって管理されていることを確認するには、Microsoft Windows Power Shell コマンド・プロンプトを開き、次のコマンドを発行します。

```
mpclaim -e
```

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

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

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

```
wmic diskdrive get
```

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

```
diskpart
   select Disk 1
   online disk
   attribute disk clear readonly
   select Disk 2
   online disk
   attribute disk clear readonly
   < ... >
   select Disk 49
   online disk
   attribute disk clear readonly
   exit
```

サーバーのユーザー ID の作成

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

このタスクについて

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

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

手順

1. オペレーティング・システム・コマンドを使用してユーザー ID を作成します。
   - Linux AIX サーバー・インスタンスを所有するユーザーのホーム・ディレクトリーに、グループおよびユーザー ID を作成します。

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

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

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

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

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

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

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

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

2. 新規ユーザー ID をログオフします。

サーバーのファイル・システムの準備

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

AIX システム

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

手順

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

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

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

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

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

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

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

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

   例えば次のとおりです。

   ```
   lsvg -p tsmdb
   ```

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

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

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

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

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

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

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

   ```
   crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
   crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
   crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
   ```

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

   ```
   mount -a
   ```

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

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

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

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

8. 38 ページの『サーバーのユーザー ID の作成』で作成したユーザー ID に、IBM Spectrum Protect サーバーのディレクトリーに対する読み取り/書き込み権限があることを確認します。

Linux システム

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

手順

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

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

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

   ```
   mkfs -t xfs /dev/mapper/360050763008101057800000000002c3
   ```

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

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

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

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

   ```
   mkdir /tsminst1
   ```

   各ファイル・システムに対して **mkdir** コマンドを繰り返します。

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

   例えば次のとおりです。

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

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

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

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

   ```
   [root@tapsrv04 ~]# df -h /tsminst1/*
   Filesystem                                      Size  Used Avail Use% Mounted on
   /dev/mapper/3600507630081010578000000000000003 134G  188M 132G  1%   /tsminst1/
   TSMalog
   ```

6. 38 ページの『サーバーのユーザー ID の作成』で作成したユーザー ID に、IBM Spectrum Protect のディレクトリーに対する読み取り/書き込み権限があることを確認します。

Windows システム

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

手順

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

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

   ```
   md c:¥tsminst1
   ```

   各ファイル・システムに対して **md** コマンドを繰り返します。

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

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

   a) ディスクをオンラインにします。

   b) ディスクを GPT 基本タイプ (デフォルト) に初期化します。

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

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

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

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

4. ディスク構成が完了したら、システムを再始動してください。

次のタスク

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

サーバーおよび Operations Center のインストール

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

AIX および Linux システムへのインストール

IBM Spectrum Protect サーバーと Operations Center を最初のサーバー・システムにインストールします。

始める前に

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

手順

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

詳細については、43 ページの『グラフィカル・ウィザード用の前提条件 RPM ファイルのインストール』を参照してください。

2. インストール・パッケージをダウンロードする前に、製品パッケージからインストール・ファイルを抽出したときにそれらのファイルを保管するのに十分なスペースがあることを確認してください。

スペース所要量については、ダウンロード資料 (技術情報 588093) を参照してください。

3. Passport Advantage® にアクセスし、任意の空のディレクトリーにパッケージ・ファイルをダウンロードします。
4. パッケージに対する実行権限が設定されていることを確認します。必要な場合は、次のコマンドを実行してファイル権限を変更します。

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

5. 次のコマンドを発行して、パッケージを抽出します。

```
./package_name.bin
```

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

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

```
lsuser
```

デフォルトで、このコマンドは使用可能です。

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

```
./install.sh
```

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

次のタスク

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

  Installation Manager ツールからインストール・ログ・ファイルを表示するには、「**ファイル**」 > 「**ログの表示**」をクリックします。Installation Manager ツールからこれらのログ・ファイルを収集するには、「**ヘルプ**」 > 「**問題分析のためのデータのエクスポート**」をクリックします。
- サーバーをインストールした後、使用目的に合わせてカスタマイズする前に、 サポート・サイト にアクセスしてください。「**Support and downloads**」をクリックし、適用できる修正があれば適用します。

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

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

手順

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

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

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

```
download-prerequisites.sh
```

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

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

Windows システムへのインストール

IBM Spectrum Protect サーバーと Operations Center を最初のサーバー・システムにインストールします。

始める前に

以下の前提条件が満たされていることを確認します。

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

手順

1. インストール・パッケージをダウンロードする前に、製品パッケージからインストール・ファイルを抽出したときにそれらのファイルを保管するのに十分なスペースがあることを確認してください。
   スペース所要量については、ダウンロード資料 (技術情報 588095) を参照してください。
2. パスポート・アドバンテージ にアクセスし、任意の空のディレクトリーにパッケージ・ファイルをダウンロードします。
3. 実行可能ファイルを置いたディレクトリーに変更します。
4. 実行可能ファイルをダブルクリックして、現行ディレクトリーに抽出します。
5. インストール・ファイルが抽出されたディレクトリーで、`install.bat` ファイルをダブルクリックして、インストール・ウィザードを開始します。
   インストールするパッケージを選択するときには、サーバーと Operations Center の両方を選択します。

次のタスク

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

  Installation Manager ツールからインストール・ログ・ファイルを表示するには、「**ファイル**」 > 「**ログの表示**」をクリックします。Installation Manager ツールからこれらのログ・ファイルを収集するには、「**ヘルプ**」 > 「**問題分析のためのデータのエクスポート**」をクリックします。
- サーバーをインストールした後、使用目的に合わせてカスタマイズする前に、 サポート・サイト にアクセスしてください。「**Support and downloads**」をクリックし、適用できる修正があれば適用します。

サーバーおよび Operations Center の構成

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

サーバー・インスタンスの構成

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

始める前に

次の要件を満たしているようにしてください。

Linux AIX

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

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

1. 「**スタート**」 > 「**管理ツール**」 > 「**サービス**」をクリックします。「**サービス**」ウィンドウで、「**Remote Registry**」を選択します。開始されていない場合は、「**開始**」をクリックします。
2. 次のようにして、ポート 137、139、および 445 がファイアウォールによってブロックされていないことを確認します。
   a. 「**スタート**」 > 「**コントロール パネル**」 > 「**Windows ファイアウォール**」をクリックします。
   b. 「**詳細設定**」を選択します。
   c. 「**受信の規則**」を選択します。
   d. 「**新しい規則**」を選択します。
   e. TCP ポート 137、139、および 445 のポート規則を作成して、ドメインおよびプライベート・ネットワークで接続できるようにします。
3. 「ローカル セキュリティ ポリシー」オプションにアクセスして以下のステップを実行し、ユーザー・アカウント制御を構成します。
   a. 「**スタート**」 > 「**管理ツール**」 > 「**ローカル セキュリティ ポリシー**」をクリックします。「**ローカル ポリシー**」 > 「**セキュリティのオプション**」を展開します。
   b. まだ有効になっていない場合は、「**アカウント: Administrator アカウントの状態**」 > 「**有効**」 > 「**OK**」を選択して、組み込みの管理者アカウントを有効にします。
   c. まだ無効になっていない場合は、「**ユーザー・アカウント制御: 管理者承認モードですべての管理者を実行する**」 > 「**無効**」 > 「**OK**」を選択して、すべての Windows 管理者に対してユーザー・アカウント制御を無効にします。
   d. まだ無効になっていない場合は、「**ユーザー・アカウント制御: 組み込みの Administrator アカウントに対する管理者承認モード**」 > 「**無効**」 > 「**OK**」を選択して、組み込み Administrator アカウントに対してユーザー・アカウント制御を無効にします。
4. 上記ステップでいずれかの設定を変更した場合は、構成ウィザードを先に進める前にサーバーを再始動してください。

このタスクについて

ウィザードは停止と再始動ができますが、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。

手順

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

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

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

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

バックアップ/アーカイブ・クライアントのインストール

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

手順

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

サーバーのオプションの設定

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

手順

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

サーバー・オプション	小規模システムの値	中規模システムの値	大規模システムの値
ACTIVELOGDIRECTORY	構成中に指定されたディレクトリー・パス	構成中に指定されたディレクトリー・パス	構成中に指定されたディレクトリー・パス
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Yes	No	No
ARCHLOGDIRECTORY	構成中に指定されたディレクトリー・パス	構成中に指定されたディレクトリー・パス	構成中に指定されたディレクトリー・パス
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	No	No	No
DEVCONFIG	devconf.dat	devconf.dat	devconf.dat
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500

サーバー・オプション	小規模システムの値	中規模システムの値	大規模システムの値
VOLUMEHISTORY	volhist.dat	volhist.dat	volhist.dat

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

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

```
setopt idletimeout 60
```

3. いずれかのサーバー・オプション値を更新する必要がある場合は、以下のガイドラインを使用して、dsmserv.opt ファイルを編集します。
   - オプションを有効にする場合は、その行の先頭にあるアスタリスクを削除します。
   - 各行には、1 つのオプションとそのオプションに 対して指定された値のみを入力してください。
   - ファイル内の複数の項目にオプションが出現する場合、サーバーは最後の項目を使用します。

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

関連情報

サーバー・オプションの解説

SETOPT (動的更新用サーバー・オプションの設定)

トランスポート層セキュリティーを使用したセキュア通信の構成

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

このタスクについて

IBM Spectrum Protect バージョン 8.1.2 以降では、SSL はデフォルトで有効にされており、IBM Spectrum Protect サーバーおよびバックアップ/アーカイブ・クライアントは、TLS バージョン 1.2 以降を使用して相互に通信するように自動的に構成されます。

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

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

Operations Center の構成

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

始める前に

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

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

手順

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

   48 ページの『Operations Center とハブ・サーバーの間の通信の保護』 の指示に従ってください。
2. ハブ・サーバーを指定する。

   Web ブラウザーで、以下のアドレスを入力します。

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

   ここで、

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

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

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

   初めて Operations Center にログインすると、ウィザードにより、サーバーでシステム 権限を持つ新しい管理者をセットアップするための初期構成手順が示されます。
3. オプション: システム状況を要約する日次 E メール・レポートを受け取るには、Operations Center で E メール設定を構成します。

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

Operations Center とハブ・サーバーの間の通信の保護

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

始める前に

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

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

このタスクについて

この手順では、自己署名証明書を使用してセキュア通信を実装します。

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

手順

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

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

   ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを表します。
3. 次のコマンドを発行して、「IBM 鍵管理」ウィンドウを開きます。

   ```
   ikeyman
   ```

4. 「**鍵データベース・ファイル**」 > 「**オープン**」をクリックします。
5. 「**参照**」をクリックして、以下のディレクトリーに移動します。ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを表します。
   - Linux AIX *installation_dir*/ui/Liberty/usr/servers/guiServer
   - Windows *installation_dir*¥ui¥Liberty¥usr¥servers¥guiServer
6. guiServer ディレクトリーで、gui-truststore.jks ファイルを選択します。
7. 「**オープン**」をクリックして、「**OK**」をクリックします。
8. トラストストア・ファイルのパスワードを入力して、「**OK**」をクリックします。
9. 「IBM 鍵管理」ウィンドウの「**鍵データベースの内容 (Key database content)**」域で、矢印をクリックして、リストから「**署名者証明書**」を選択します。「**追加**」をクリックします。
10. 「オープン」ウィンドウで、「**参照**」をクリックして、インスタンスを作成した管理者によって指定されたハブ・サーバー・インスタンス・ディレクトリーに移動します。例えば次のとおりです。
    - Linux AIX home/tsminst1
    - Windows c:¥Program Files¥Tivoli¥TSM¥server1

    ディレクトリーには cert256.arm 証明書が含まれています。

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

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

- Linux AIX *installation_dir*/ui/Liberty/usr/servers/guiServer
- Windows *installation_dir*¥ui¥Liberty¥usr¥servers¥guiServer

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

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

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

関連タスク

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、自動的に始動されます。例えば、構成変更を加える場合に、Web サーバーの停止と始動を行う必要がある可能性があります。

製品ライセンスの登録

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

このタスクについて

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

手順

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

1. Operations Center を開きます。
2. 設定アイコン  上にカーソルを移動して「**コマンド・ビルダー**」をクリックし、Operations Center コマンド・ビルダーを開きます。
3. **REGISTER LICENSE** コマンドを発行します。
   例えば、IBM Spectrum Protect の基本ライセンスを登録するには、次のコマンドを発行します。

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

次のタスク

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

- サーバーの別のコンピューターへの移動。
- NODELOCK ファイルの破壊。サーバーはライセンス情報を、サーバーを始動するディレクトリー内にある NODELOCK ファイルに保管します。

- Linux サーバーがインストールされているサーバーに関連付けられているプロセッサー・チップを変更する場合。

関連情報
REGISTER LICENSE (新規ライセンスの登録)

データ重複排除の構成

インライン・データ重複排除を使用するには、ディレクトリー・コンテナー・ストレージ・プールと、少なくとも 1 つのディレクトリーを作成します。

始める前に

このタスクでは、8 ページの『計画ワークシート』に記録したストレージ・プール・ディレクトリー情報を使用します。

手順

1. Operations Center を開きます。
2. Operations Center のメニュー・バーで、「**ストレージ**」の上にカーソルを移動します。
3. 表示されたリストから、「**ストレージ・プール**」をクリックします。
4. 「**+ストレージ・プール**」ボタンをクリックします。
5. 「**ストレージ・プールの追加**」ウィザードのステップを実行します。
   - インライン・データ重複排除を使用するには、コンテナー・ベースのストレージの下で「**ディレクトリー**」ストレージ・プールを選択します。
   - ディレクトリー・コンテナー・ストレージ・プールのディレクトリーを構成する場合、システムのセットアップ時にストレージ用に作成したディレクトリー・パスを指定します。
6. 新規のディレクトリー・コンテナー・ストレージ・プールを構成した後、「**クローズしてポリシーを表示**」をクリックし、管理クラスを更新してストレージ・プールの使用を開始します。

ビジネスに合わせたデータ保存ルールの定義

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

手順

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

関連タスク

クライアント・データのバックアップおよびアーカイブに関するルールの指定

クライアントを追加する前に、クライアント・データのバックアップおよびアーカイブの 操作に関する適切なルールが指定されていることを確認します。クライアント登録プロセス中に、クライアント・ノードをポリシー・ドメインに割り当てます。ポリシー・ドメインには、クライアント・データを保管する方法と時期を制御するルールがあります。

サーバー保守アクティビティーのスケジュールの 定義

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

このタスクについて

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

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

操作	スケジュール
クライアント・バックアップ	22:00 に開始します。
ノード複製	8:00 に開始するか、クライアント・バックアップの開始から 10 時間後に開始します。
データベースおよび災害復旧ファイルの処理	• データベース・バックアップは、11:00 に開始するか、クライアント・バックアップの開始から 13 時間後に開始します。このプロセスは、完了するまで実行されます。 • 装置構成情報およびボリューム・ヒストリーのバックアップは、17:00 に開始するか、データベース・バックアップの開始から 6 時間後に開始します。 • ボリューム・ヒストリーの削除は、20:00 に開始するか、データベース・バックアップの開始から 9 時間後に開始します。
インベントリーの有効期限	12:00 に開始するか、クライアント・バックアップ・ウィンドウの開始から 14 時間後に開始します。このプロセスは、完了するまで実行されます。

手順

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

1. バックアップ操作用に装置クラスを定義します。

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

   ```
   define devclass dbback_filedev devtype=file
     directory=db_backup_directories
   ```

   ここで、*db_backup_directories* は、データベース・バックアップ用に作成したディレクトリーのリストです。

Linux AIX 例えば、データベース・バックアップの対象として、/tsminst1/TSMbkup00 から始まる 4 つのディレクトリーがある場合、次のコマンドを発行します。

```
define devclass dbback_filedev devtype=file
  directory=/tsminst1/TSMbkup00,
  /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
  /tsminst1/TSMbkup03"
```

Windows 例えば、データベース・バックアップの対象として、C:¥tsminst1¥TSMbkup00 から始まる 4 つのディレクトリーがある場合、次のコマンドを発行します。

```
define devclass dbback_filedev devtype=file
  directory="c:¥tsminst1¥TSMbkup00,
  c:¥tsminst1¥TSMbkup01,c:¥tsminst1¥TSMbkup02,c:¥tsminst1¥TSMbkup03"
```

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

```
set dbrecovery dbback_filedev
```

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

   ヒント：複製のスケジュールは、後のステップで Operations Center を使用して複製を構成するときに別個に作成します。

操作	コマンド例
データベースのバックアップを取ります。	**BACKUP DB** コマンドを実行するスケジュールを作成します。小規模なシステムを構成している場合は、**COMPRESS** パラメーターを YES に設定します。 例えば、小規模なシステムで、新規の装置クラスを使用するバックアップ・スケジュールを作成するには、次のコマンドを発行します。 `define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Back up the database." startdate=today starttime=11:00:00 duration=45 durunits=minutes`
装置構成情報をバックアップします。	次のように、**BACKUP DEVCONFIG** コマンドを実行するスケジュールを作成します。 `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Backup the device configuration file." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
ボリューム・ヒストリーをバックアップします。	次のように、**BACKUP VOLHISTORY** コマンドを実行するスケジュールを作成します。 `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Back up the volume history." startdate=today starttime=17:00:00 duration=45 durunits=minutes`

操作	コマンド例
不要になった古いバージョンのデータベース・バックアップを削除します。	次のように、**DELETE VOLHISTORY** コマンドを実行するスケジュールを作成します。 `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Remove old database backups." startdate=today starttime=20:00:00 duration=45 durunits=minutes`
許可された保存期間を超えたオブジェクトを削除します。	**EXPIRE INVENTORY** コマンドを実行するスケジュールを作成します。 構成しているシステムのサイズに 基づいて、**RESOURCE** パラメーターを設定します。 • 小規模システム: 10 • 中規模システム: 30 • 大規模システム: 40 例えば、中サイズのシステムで、EXPINVENTORY という名前のスケジュールを作成するには、以下のコマンドを実行します。 `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Remove expired objects." startdate=today starttime=12:00:00 duration=45 durunits=minutes`

次のタスク

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

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

関連情報

DEFINE SCHEDULE (管理コマンドのスケジュールの定義)

クライアント・スケジュールの定義

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

手順

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

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

バックアップ/アーカイブ・クライアントのインストールおよび構成

IBM Spectrum Protect サーバー・システムのセットアップが 正常に行われた後、データのバックアップを開始するために、クライアント・ソフトウェアをインストールして構成します。

手順

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

次のタスク

クライアントを登録し、スケジュールに割り当てます。

クライアントの登録とスケジュールへの関連付け

「**クライアントの追加**」ウィザードを使用して、Operations Center 経由でクライアントの追加と登録を行います。

始める前に

クライアント・ノードでクライアント所有者権限を持つ管理ユーザー ID がクライアントに必要かどうかを判別します。クライアントに管理ユーザー ID が必要かどうかを判別するには、技術情報 7048963 を参照してください。

制約事項 : 一部のタイプのクライアントでは、クライアント・ノード名と管理ユーザー ID が一致していなければなりません。これらのクライアントは、V7.1.7 で導入された Lightweight Directory Access Protocol 認証方式を使用して認証することができません。 この認証方式 (統合モードと呼ばれる場合もある) の詳細は、Active Directory データベースを使用したユーザーの認証を参照してください。

手順

クライアントを登録するには、以下のいずれかのアクションを実行してください。

- クライアントに管理ユーザー ID が必要な場合、以下のように **REGISTER NODE** コマンドを使用し、**USERID** パラメーターを指定してクライアントを登録します。

  ```
  register node node_name password userid=node_name
  ```

  ここで *node_name* はノード名を指定し、*password* はノードのパスワードを指定します。 詳細については、ノードの登録を参照してください。
- クライアント・ノードに管理ユーザー ID が必要ない場合、Operations Center の「クライアントの追加」ウィザードを使用してクライアントを登録します。次の手順を実行してください。

  a. Operations Center メニュー・バーで、「**クライアント**」をクリックします。

  b.「クライアント」テーブルで、「**+ クライアント**」をクリックします。

  c.「**クライアントの追加**」ウィザードのステップを実行します。

  i) クライアントおよびサーバー上で冗長データを除去できるように指定します。「クライアント・サイド・データの重複排除」エリアで、「**使用可能**」チェック・ボックスを選択します。

  ii)「**構成**」ウィンドウで、**TCPSERVERADDRESS**、**TCPPORT**、**NODENAME**、および **DEDUPLICATION** の値をコピーします。

ヒント: オプション値を記録し、安全な場所に保管します。クライアント登録が完了し、クライアント・ノードにソフトウェアをインストールした後、これらの値を使用してクライアントを構成します。

iii) ウィザードの指示に従って、ポリシー・ドメイン、スケジュール、およびオプション・セットを指定します。

iv) 危険な状態の設定を指定して、クライアントに関するリスクが表示される方法を設定します。

v) 「**クライアントの追加**」をクリックします。

クライアント管理サービスのインストール

Linux および Windows オペレーティング・システム上で稼働しているバックアップ/アーカイブ・クライアント用に、クライアント管理サービスをインストールします。 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。

始める前に

- 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てください。
- クライアント管理サービスをインストールする前に、バックアップ/アーカイブ・クライアントとサーバーの間に正常な接続が確立されていることを確認してください。クライアント・システムがサーバーに接続しない限り、クライアントが使用するサーバーのトラストストア・ファイルに Secure Sockets Layer (SSL) 証明書は保存されません。

手順

以下のステップを実行して、バックアップ/アーカイブ・クライアントと同じコンピューターにクライアント管理サービスをインストールします。

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_Spectrum_Protect-CMS-*operating_system*.bin. のようなファイル名を探してください。
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。
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。
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 ウィザードの指示に従います。

   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 クライアント管理サービスの両方を選択する必要があります。

関連情報

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。

  ```
  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。 このファイルを構成する手順については、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` ファイルに正しく作成されているか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ために、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**」 > 「**プロパティー**」をクリックします。
3. 「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	`https://server.example.com`
DNS ホスト名とデフォルト以外のポートを使用	`https://server.example.com:1599`
IP アドレスとデフォルト以外のポートを使用	`https://192.0.2.0:1599`

4. 「**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。

2 番目のサーバーの構成

システム内の最初のサーバーの構成が完了したら、2 番目のサーバーを構成します。

手順

以下のセクションの手順を実行します。

1. 以下のセクションの手順を実行して、最初のサーバーと同じ構成で 2 番目のサーバーを構成します。
   a) 28 ページの『システムのセットアップ』
   b) 42 ページの『サーバーおよび Operations Center のインストール』

      マルチサイト・ディスク・ソリューションでは、ハブ・サーバーとして構成されるのは 1 つのサーバーのみであるため、2 番目のサーバーに Operations Center をインストールする必要はありません。2 番目のサーバーにインストールするインストール・パッケージを選択する際に、Operations Center を選択しないでください。
   c) 44 ページの『サーバーおよび Operations Center の構成』

      Operations Center の構成に関するタスクはスキップします。
   d) 55 ページの『バックアップ/アーカイブ・クライアントのインストールおよび構成』
2. 59 ページの『ハブ・サーバーとスポーク・サーバー間の SSL 通信の構成 』
3. 60 ページの『スポークとしての 2 番目のサーバーの追加』
4. 61 ページの『複製の有効化』

ハブ・サーバーとスポーク・サーバー間の SSL 通信の構成

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・サーバーに対するスポーク・サーバーの証明書を定義する必要があります。

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、その情報を 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. スポーク・サーバーの証明書をハブ・サーバーに定義する際は、以下の手順を実行します。
   a) スポーク・サーバー上で、スポーク・サーバー・インスタンスのディレクトリーに移動します。
   b) スポーク・サーバーの鍵データベース・ファイル内の証明書を検証します。 以下のコマンドを発行します。

      ```
      gsk8capicmd_64 -cert -list -db cert.kdb -stashed
      ```
   c) スポーク・サーバーの `cert256.arm` ファイルをハブ・サーバーに安全に転送します。
   d) 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。
   e) ハブ・サーバーに対するスポーク・サーバー証明書を定義します。 ハブ・サーバーのインスタンス・ディレクトリーから次のコマンドを発行します。ここで、*spoke_servername* はスポーク・サーバーの名前で、*spoke_cert256.arm* はスポーク・サーバー証明書のファイル名です。

      ```
      gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii -trust enable
       -label spoke_servername -file spoke_cert256.arm
      ```
2. ハブ・サーバーの証明書をスポーク・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) スポーク・サーバーの鍵データベース・ファイル内の証明書を検証します。 以下のコマンドを発行します。

      ```
      gsk8capicmd_64 -cert -list -db cert.kdb -stashed
      ```
   c) ハブ・サーバーの `cert256.arm` ファイルをスポーク・サーバーに安全に転送します。

d) スポーク・サーバー上で、スポーク・サーバー・インスタンスのディレクトリーに移動します。

e) スポーク・サーバーに対してハブ・サーバー証明書を定義します。 スポーク・サーバーのインスタンス・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* はハブ・サーバーの名前で、*hub_cert256.arm* はハブ・サーバー証明書のファイル名です。

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii -trust enable
 -label hub_servername -file hub_cert256.arm
```

3. ハブ・サーバーとスポーク・サーバーを再始動します。
4. スポーク・サーバーをハブ・サーバーに、そしてハブ・サーバーをスポーク・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・サーバーとスポーク・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_SSLTCPADMINPort SERVERPA=spoke_serverpassword
```

c) スポーク・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_SSLTCPADMINPort 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、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場合、**DEFINE SERVER** コマンドに 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。

スポーク・サーバーは「モニター対象外」状況です。 この状況は、このサーバーが **DEFINE SERVER** コマンドを使用してハブ・サーバーに対して定義されているものの、サーバーがまだスポーク・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) スポーク・サーバーをクリックして項目を強調表示し、「**スポークのモニター**」をクリックします。

関連情報

DEFINE SERVER (サーバー間の通信のためのサーバー定義)

QUERY OPTION (サーバー・オプションの照会)

スポークとしての 2 番目のサーバーの追加

環境の両方のサーバーを構成した後、2 番目のサーバーをスポークとしてハブ・サーバーに追加します。

手順

1. Operations Center を開きます。
2. Operations Center メニュー・バーで、「**サーバー**」をクリックします。
3. 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「**スポークのモニター**」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は、「**+ スポーク**」をクリックします。

4. スポーク構成ウィザードのステップを実行します。

複製の有効化

データを保護するために、ストレージ・プールの保護に加えて、ノード複製を有効にします。

手順

ソース・サーバーに登録されているすべてのクライアントに対してノード複製を有効にするには、以下の手順を実行します。

1. Operations Center を開きます。
2. Operations Center のメニュー・バーで、「**ストレージ**」の上にカーソルを移動して、「**複製**」をクリックします。
3. 「**複製**」ページで、「**+ サーバーのペア (Server Pair)**」をクリックします。
4. 「**サーバー・ペアの追加**」ウィザードのステップを実行します。
   - マルチサイト・ディスク・ソリューション用に構成した最初のサーバーとしてソース・サーバーを設定します。 ターゲット・サーバーは、2 番目のサーバーです。
   - 52 ページの『サーバー保守アクティビティーのスケジュールの 定義』でスケジュールしたサーバー保守アクティビティーに 基づいて、ノード複製のスケジュールがクライアント・バックアップ・ウィンドウの 10 時間後に開始するように設定します。
   - このウィザードは、保護するデータ量およびクライアント複製がスケジュールされている時間に基づいて、ストレージ・プール保護スケジュールをセットアップします。

次のタスク

2 つのサイト間での相互複製をセットアップする予定の場合、「**サーバー・ペアの追加**」ウィザードを再実行し、2 番目のサーバーをソースとして、最初のサーバーをターゲットとして設定します。

実装の完了

IBM Spectrum Protect ソリューションを構成して稼働した後、バックアップ操作をテストし、モニターをセットアップして、すべてがスムーズに稼働することを確認します。

手順

1. バックアップ操作をテストして、データが期待したとおりに保護されていることを確認します。
   a) Operations Center の「**クライアント**」ページで、バックアップするクライアントを 選択し、「**バックアップ**」をクリックします。
   b) Operations Center の「**サーバー**」ページで、データベースをバックアップするサーバーを 選択します。 「**バックアップ**」をクリックして、「**データベースのバックアップ**」ウィンドウの指示に従います。
   c) バックアップ操作が正常に完了し、警告メッセージおよびエラー・メッセージがないことを確認します。

   ヒント: あるいは、バックアップ/アーカイブ・クライアントの GUI を使用してクライアント・データをバックアップすることができ、管理コマンド・ラインから **BACKUP DB** コマンドを発行してサーバー・データベースをバックアップすることができます。
2. 63 ページの『第 3 部 マルチサイト・ディスク・ソリューションのモニター』の手順に従って、ご使用のソリューション用にモニタリングをセットアップします。

第 3 部 マルチサイト・ディスク・ソリューションのモニター

マルチサイト・ディスク・ソリューションを実装した後、ソリューションをモニターして正しく動作することを確認してください。

このタスクについて

IBM Spectrum Protect によるマルチサイト・ディスク・ソリューションを実装した後、既存の問題や潜在的な問題を特定するために、毎日および定期的にソリューションをモニターします。収集した情報は、問題のトラブルシューティングとシステム ・パフォーマンスの最適化に使用できます。

ソリューションをモニターするために推奨される方法は、システム状況の全体と詳細をグラフィカル・ユーザー・インターフェースで 表示する Operations Center を使用することです。さらに、システム状況を要約する日次 E メール・レポートを生成するように Operations Center を構成できます。

場合によっては、拡張モニター・ツールを使用して、特定のモニター・タスクやトラブルシューティング・タスクを実行できます。

ヒント : Linux オペレーティング・システムまたは Windows オペレーティング・システムでバックアップ/アーカイブ・クライアントの問題を診断する予定の場合は、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各コンピューターに IBM Spectrum Protect クライアント管理サービスをインストールします。こうすると、バックアップ/アーカイブ・クライアントの問題を診断するために、Operations Center で「**診断**」ボタンを使用できるようになります。クライアント管理サービスをインストールするには、56 ページの『クライアント管理サービスのインストール』の手順に従います。

手順

1. 日次モニター・タスクを実行します。手順については、63 ページの『日次モニター・チェックリスト』を参照してください。
2. 定期的なモニター・タスクを実行します。手順については、75 ページの『定期的なモニター・チェックリスト』を参照してください。
3. IBM Spectrum Protect ソリューションがライセンス 交付要件に準拠していることを確認するには、82 ページの『ライセンス準拠の検証』の手順に従います。
4. E メール状況レポートを生成するように Operations Center をセットアップするには、83 ページの『E メール・レポートを使用したシステム状況のトラッキング』を参照してください。

次のタスク

検出した問題があれば、それを解決してください。ソリューションの構成を変更することによって問題を解決するには、85 ページの『第 4 部 マルチサイト・ディスク・ソリューションの操作の管理』の指示に従ってください。以下のリソースも利用できます。

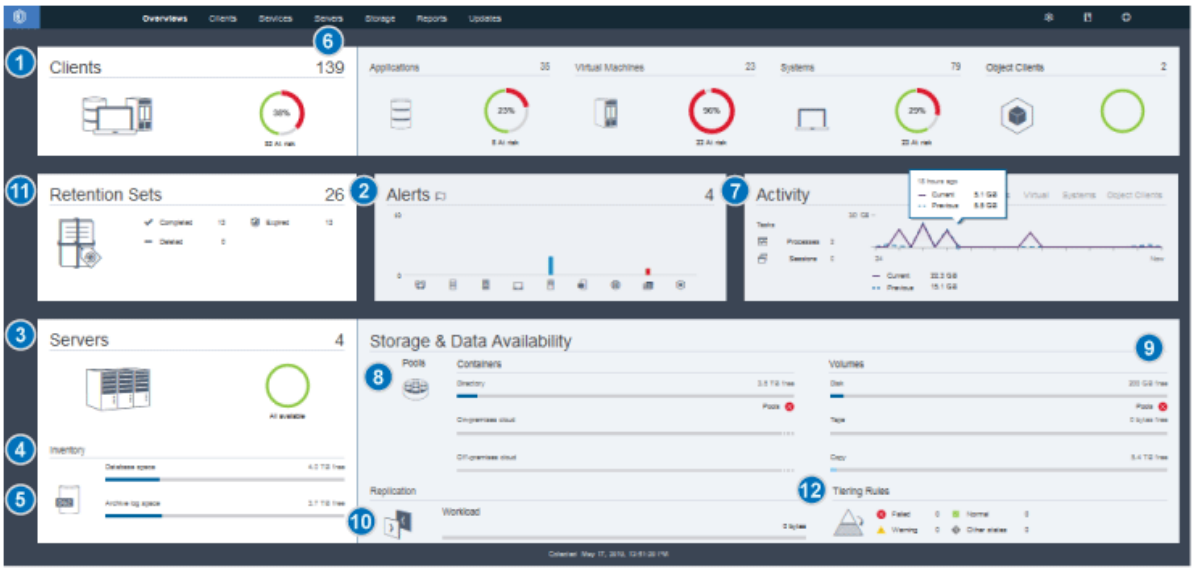
- パフォーマンスの問題を解決するには、パフォーマンスを参照してください。
- その他のタイプの問題を解決するには、トラブルシューティングを参照してください。

日次モニター・チェックリスト

IBM Spectrum Protect ソリューションの日次モニター・タスクを完了していることを確認するには、日次モニター・チェックリストを確認します。

Operations Center の「**概要**」ページから、日次モニター・タスクを実行します。「**概要**」ページにアクセスするには、Operations Center を開いて「**概要**」をクリックします。

次の図に、各タスクを実行するための場所を示します。



ヒント : 拡張モニター・タスクの管理コマンドを実行するには、Operations Center コマンド・ビルダーを使用します。コマンド・ビルダーは、コマンドを入力するときにガイドとなる先行入力機能を提供します。コマンド・ビルダーを開くには、Operations Center の「**概要**」ページに進みます。メニュー・バーで、設定アイコン にマウス・カーソルを移動し、「**コマンド・ビルダー**」をクリックします。

次の表に、日次モニター・タスクをリストして、各タスクの実行手順を示します。

表 *15.* 日次モニター・タスク

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
ランサムウェア攻撃を示す可能性があるセキュリティー通知を監視します。	ランサムウェア攻撃の可能性が IBM Spectrum Protect 環境で検出された場合、セキュリティー通知メッセージが Operations Center の前面に表示されます。 詳しくは、メッセージをクリックして「**セキュリティー通知**」ページを開いてください。	「**セキュリティー通知**」ページでは以下のアクションを実行できます。 • クライアントごとに通知詳細を表示する。 **制約事項 :** バックアップ/アーカイブ・クライアントおよび IBM Spectrum Protect for Virtual Environments クライアントの通知のみ使用可能です。 • セキュリティー通知を選択して「**確認**」をクリックすることでセキュリティー通知を確認する。 セキュリティー通知を確認すると、「**セキュリティー通知**」選択したクライアントの「確認済み」列にチェック・マークが追加されます。通知が確認済みになる基準は、所属する組織によって決まります。チェック・マークはその問題が調査済みであり、誤検出であると判明したことを意味する場合があります。あるいは、問題が存在しているものの、解決中であることを意味する場合もあります。 • 管理者にセキュリティー通知を割り当てるために、セキュリティー通知を選択し、「**割り当て**」をクリックします。 割り当てを表示するには、管理者が Operations Center にサインインして、「**概要**」 > 「**セキュリティー**」をクリックする必要があります。管理者が定期的に「**セキュリティー通知**」ページをモニターしているかどうか定かではない場合は、管理者に割り当てに関して通知してください。 • 通知が誤検出の場合、そのセキュリティー通知を選択して「**リセット**」をクリックできます。 そうすると、セキュリティー通知が削除されます。最新のバックアップ操作とのベースライン比較に使用される履歴データも削除されます。その後は新規ベースラインが計算されます。 • オプションで、**SET SECURITYNOTIF** コマンドを使用して、セキュリティー通知を無効にすることができます。

表 15. 日次モニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
1 バックアップ操作が失敗したか、未実行であるために、クライアントが保護されないリスクがあるかどうかを判別します。	クライアントが危険な状態にあるかどうかを確認するには、「クライアント」エリアで「**危険**」通知を探します。詳細を表示するには、「クライアント」エリアをクリックします。 **重要：**「**危険**」のパーセンテージが通常よりはるかに大きい場合、ランサムウェア攻撃を示している可能性があります。 ランサムウェア攻撃により、バックアップ操作が失敗し、クライアントはリスクにさらされる可能性があります。 例えば、「危険」のクライアントのパーセンテージが、通常は 5% から 10% であるにも関わらず、40% または 50% に増えた場合、その原因を調査してください。 クライアント管理サービスをバックアップ/アーカイブ・クライアントにインストールしている場合、以下のステップを実行して、クライアント・エラーおよびスケジュール・ログを表示して分析することができます。 1. 「クライアント」テーブルで、クライアントを選択して、「**詳細**」をクリックします。 2. 問題を診断するには、「**診断**」をクリックします。	クライアント管理サービスがインストールされていないクライアントの場合、クライアント・システムにアクセスして、クライアント・エラー・ログを確認します。
2 クライアント関連エラーまたはサーバー関連エラーに注意が必要であるかどうかを判別します。	報告されたアラートの重大度を判別するには、「アラート」エリアで、列の上にカーソルを移動します。	アラートに関する追加情報を表示するには、以下のステップを実行します。 1. 「アラート」エリアをクリックします。 2. 「アラート」表でアラートを選択します。 3. 「活動記録ログ」ペインでメッセージを確認します。このペインには、選択したアラートの発生前後に発行された関連メッセージが表示されます。
3 Operations Center によって管理されるサーバーがクライアントにデータ保護サービスを提供できるかどうかを判別します。	1. サーバーが危険な状態にあるかどうかを確認するには、「サーバー」エリアで「**使用不可**」通知を探します。 2. 追加情報を表示するには、「サーバー」エリアをクリックします。 3. 「サーバー」テーブルでサーバーを選択して、「**詳細**」をクリックします。	**ヒント：**サーバー・プロパティーに関連した問題を検出した場合は、次のようにして、サーバー・プロパティーを更新します。 1. 「サーバー」テーブルで、サーバーを選択して、「**詳細**」をクリックします。 2. サーバー・プロパティーを更新するには、「**プロパティー**」をクリックします。

表 15. 日次モニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
4 サーバー・データベース、活動ログ、およびアーカイブ・ログで構成されるサーバー・インベントリーに十分なスペースを使用できるかどうかを判別します。	1. 「サーバー」エリアをクリックします。 2. テーブルの「状況」列でサーバーの状況を表示して、問題があれば解決します。 • 「**正常**」 サーバー・データベース、活動ログ、およびアーカイブ・ログに十分なスペースを使用できます。 • 「**重大**」 サーバー・データベース、活動ログ、またはアーカイブ・ログに使用できるスペースが不十分です。すぐにスペースを追加する必要があります。そうしないと、サーバーによって提供されるデータ保護サービスが中断されます。 • 「**警告**」 サーバー・データベース、活動ログ、またはアーカイブ・ログがスペース不足になっています。この状態が続く場合は、スペースを追加する必要があります。 • 「**使用不可**」 状況を取得できません。サーバーが実行中であること、およびネットワークに問題がないことを確認してください。この状況は、モニター管理者 ID がロックされている場合、またはそれ以外の理由でサーバー上で使用不可になっている場合にも表示されます。この ID の名前は、IBM-OC-hub_server_name です。 • 「**モニター対象外**」 モニター対象外のサーバーがハブ・サーバーに定義されていますが、Operations Center で管理するようには構成されていません。モニター対象外サーバーを構成するには、サーバーを選択して、「**スポークのモニター**」をクリックします。	「**アラート**」ページで、関連したアラートを検索することもできます。トラブルシューティングに関する詳細な説明については、サーバーの問題の解決を参照してください。

表 15. 日次モニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
5 サーバー・データベース・バックアップ操作を確認します。	サーバーが最後にバックアップされた時期を判別するには、以下の手順を実行します。 1.「サーバー」エリアをクリックします。 2.「サーバー」テーブルで、「最終データベース・バックアップ」列を確認します。	バックアップ操作に関する詳細情報を取得するには、以下の手順を実行します。 1.「サーバー」テーブルで、行を選択して、「**詳細**」をクリックします。 2.「DB バックアップ」エリアで、チェック・マークの上にカーソルを移動し、バックアップ操作に関する情報を表示します。 データベースが最近 (例えば、過去 24 時間以内に) バックアップされていない場合、バックアップ操作を開始できます。 1. Operations Center の「**概要**」ページで、「サーバー」エリアをクリックします。 2. テーブルで、サーバーを選択して、「**バックアップ**」をクリックします。 サーバー・データベースが自動バックアップ操作用に構成されているかどうかを判別するには、以下の手順を実行します。 1. メニュー・バーで、設定アイコン にマウス・カーソルを移動し、「**コマンド・ビルダー**」をクリックします。 2. **QUERY DB** コマンドを発行します。 `query db f=d` 3. 出力で、「完全装置クラス名」フィールドを確認します。装置クラスが指定されている場合、サーバーは、自動データベース・バックアップ用に構成されています。
6 その他のサーバー保守タスクをモニターします。サーバー保守タスクには、管理コマンド・スケジュール、保守スクリプト、および関連コマンドの実行が含まれる場合があります。	サーバーの問題が原因で失敗したプロセスに関する情報を検索するには、以下の手順を実行します。 1.「**サーバー**」 > 「**保守**」をクリックします。 2. プロセスの 2 週間の履歴を取得するには、「ヒストリー」列を確認します。 3. スケジュール済みプロセスに関する詳細情報を取得するには、そのプロセスに関連したチェック・ボックスの上にカーソルを移動します。	プロセスのモニターおよび問題解決について詳しくは、Operations Center オンライン・ヘルプを参照してください。

表 15. 日次モニター・タスク (続き)		
タスク	**基本的な手順**	**詳細手順およびトラブルシューティング情報**
7 サーバーとの間で最近送受信されたデータの量が、予期した範囲内に収まっていることを確認します。	• 過去 24 時間のアクティビティーの 概要を取得するには、「アクティビティー」エリアを確認します。 • 過去 24 時間のアクティビティーを、その前の 24 時間のアクティビティーと 比較するには、「現行」エリアと「前へ」エリアの図を確認します。	• 予期したよりも多くのデータがサーバーに送信されていた場合、どのクライアントが多くのデータをバックアップしているかを判別して、原因を調べます。クライアント・サイドのデータ重複排除が正しく機能していない可能性があります。 **重要 :** バックアップ・データの量が通常より大幅に多い場合、ランサムウェア攻撃を示している可能性があります。ランサムウェアがデータを暗号化すると、システムはそのデータを変更されているものとみなし、変更されたデータがバックアップされます。 そのため、バックアップ・ボリュームが大きくなります。影響を受けるクライアントを判別するには、「**アプリケーション**」、「**仮想マシン**」、または「**システム**」タブをクリックします。 • 予期したよりも少ないデータがサーバーに送信されていた場合は、クライアント・バックアップ操作がスケジュールどおりに行われているかどうかを調べます。

表 15. 日次モニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
8 ストレージ・プールをクライアント・データのバックアップに使用できることを確認します。	1.「ストレージおよびデータの可用性 (Storage & Data Availability)」エリアに問題が示されている場合、「**プール**」をクリックして、詳細を表示します。 • 「**重大**」 状況が表示されている場合、ストレージ・プールで使用できるスペースが不十分か、アクセス状況が「使用不可」です。 **重要 :** 状況が重大な場合、その原因を次のように調査します。 – ストレージ・プールのデータ重複排除率が大幅に下がった場合、ランサムウェア攻撃を示している可能性があります。ランサムウェア攻撃中はデータが暗号化され、重複排除を行うことはできません。データ重複排除率を確認するには、「ストレージ・プール」テーブルで、「節約 (%)」列の値を参照します。 – ストレージ・プールが予期せずに 100% 利用されるようになった場合、ランサムウェア攻撃を示している可能性があります。使用率を確認するには、「使用容量」列の値を参照してください。値の上にマウスを移動し、使用スペースとフリー・スペースのパーセンテージを確認してください。 • 「**警告**」 状況が表示されている場合、ストレージ・プールがスペース不足になっているか、そのアクセス状況が「読み取り専用」です。 2. 選択したストレージ・プールの使用済みスペース、フリー・スペース、および合計スペースを表示するには、「使用済み容量」列の項目の上にカーソルを移動します。	過去 2 週間に使用されたストレージ・プールの容量を表示するには、「ストレージ・プール」テーブルの行を選択して、「**詳細**」をクリックします。

表 15. 日次モニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
9 ストレージ装置がバックアップ操作に使用可能であることを確認します。	「ストレージおよびデータ可用性」エリアで、「ボリューム」セクションの容量バーの下で、「**装置**」の横に報告されている状況を確認します。「**重大**」 ⊗ または「**警告**」 ⚠ 状況がいずれかの装置について表示されている場合は、問題を調べてください。詳細を表示するには、「**装置**」をクリックします。	以下の理由から、DISK 装置が「重大」状況または「警告」状況になっている可能性があります。 • DISK 装置クラスの場合は、ボリュームがオフラインであるか、読み取り専用アクセス状況になっている可能性があります。DISK 装置表の「ディスク・ストレージ」列に、ボリュームの状態が示されます。 • 共有されない FILE 装置クラスの場合、ディレクトリーがオフラインである可能性があります。また、スクラッチ・ボリュームを割り振るために十分なフリー・スペースがない可能性があります。DISK 装置表の「ディスク・ストレージ」列に、ディレクトリーの状態が示されます。 • 共有される FILE 装置クラスの場合、ドライブが使用不可である可能性があります。ドライブがオフラインの場合、ドライブがサーバーに対する応答を停止した場合、またはそのドライブのパスがオフラインの場合に、ドライブは使用不可になります。DISK 装置表のその他の列には、ドライブとパスの状態が示されます。

表 15. 日次モニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
10 ノード複製プロセスをモニターします。	1. ノード複製プロセスの全体的な状況を取得するには、Operations Center の「**概要**」ページで「複製」エリアを確認します。 2. 複製対象の各サーバー・ペアに関する情報を表示するには、「複製」エリアをクリックします。 **重要 :** 複製の失敗数が予期せず増加したことが確認された場合、ランサムウェア攻撃を示している可能性があります。失敗の原因を調査してください。 3. 過去 2 週間で複製されたデータ量と複製の速度を表示するには、サーバー・ペアを選択して「**詳細**」をクリックします。 4. クライアントの複製情報を表示するには、Operations Center の「**概要**」ページで、「**クライアント**」をクリックします。「複製ワークロード (Replication Workload)」列の情報を確認します。 **重要 :** 複製のワークロードの予期しない大幅な増加が確認された場合、ランサムウェア攻撃を示している可能性があります。 増加したワークロードの原因を調査してください。	拡張モニターの場合、コマンドを使用して、実行中および終了済みのノード複製プロセスに関する情報を表示します。 1. Operations Center の「**概要**」ページで、設定アイコン の上にカーソルを移動し、「**コマンド・ビルダー**」をクリックします。 2. **QUERY REPLICATION** コマンドを発行します。手順については、QUERY REPLICATION (ノード複製プロセスの照会) を参照してください。複製操作が正常に完了した場合は、「複製するファイルの合計」の値と「複製されたファイルの合計」の値が一致します。 ソース複製サーバーまたはターゲット複製サーバー上でのノード複製プロセスに関連するメッセージを表示するには、以下のステップを実行します。 1. Operations Center の「**概要**」ページで、「**サーバー**」をクリックします。 2. ソース複製サーバーまたはターゲット複製サーバーを選択し、「**詳細**」をクリックします。 • アクティブ・タスクを表示するには、「**アクティブ・タスク**」をクリックし、タスクを選択して、「**実行中**」状況が表示されることを確認します。詳細については、関連するアクティビティー・ログを参照してください。 • 完了したタスクを表示するには、「**完了タスク**」をクリックし、タスクを選択肢、「**完了**」状況が表示されることを確認します。詳細については、関連するアクティビティー・ログを参照してください。

表 15. 日次モニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
11 保存セットをモニターします。	保存セットの全体的な状況を取得するには、Operations Center の「**概要**」ページで「**保存セット**」エリアを確認します。 • 「**完了**」フィールドは、サーバー・データベースで作成され、サーバー・インベントリー内で追跡される保存セットの数を指定します。 • 「**有効期限切れ**」フィールドは、データの有効期限が切れる保存セットの数を指定します。 • 「**削除済み**」フィールドは、削除された保存セットの数を指定します。 保存ルールを表示または変更するには、「**サービス**」 > 「**保存ルール**」をクリックします。	保存セットについて詳しくは、「**保存セット**」エリアをクリックし、「**保存セット**」ページを開きます。保存セット・プロパティーを表示または変更するには、保存セットをダブルクリックします。 詳細情報については以下の関連コマンドを実行します。 1. Operations Center の「**概要**」ページで、設定アイコン の上にカーソルを移動し、「**コマンド・ビルダー**」をクリックします。 2. 実行中、中断、または完了済みの保存セット作成ジョブを判別するには、**QUERY JOB** コマンドを実行します。手順については、QUERY JOB (ジョブの照会)を参照してください。 3. 保存ルールを照会するには、**QUERY RETRULE** コマンドを実行します。手順については、QUERY RETRULE (保存ルールの照会)を参照してください。 4. 保存セットを照会するには、**QUERY RETSET** コマンドを実行します。手順については、QUERY RETSET (保存セットの照会)を参照してください。 5. 保存セットの内容を照会するには、**QUERY RETSETCONTENTS** コマンドを実行します。手順については、QUERY RETSETCONTENTS (保存セットの内容の照会)を参照してください。

表 15. 日次モニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング情報
12 ストレージ・ルールをモニターします。	ストレージ・ルール操作の全体的な状況を取得するには、Operations Center の「**概要**」ページで「**ストレージ・ルール**」エリアを確認します。	状況要約には、ストレージ・ルールの最新の処理結果が表示されます。以下の各状態にあるストレージ・ルールの数が示されます。 **正常** エラーなしで実行されたストレージ・ルールの数。 **警告** 処理を完了したが、適格データを一部のみ移動またはコピーしたストレージ・ルールの数。一部のファイルがスキップされたか、ルールの制限時間に達したか、または処理が取り消されました。 **失敗** 処理を完了しなかったストレージ・ルールの数。例えば、ターゲット・ストレージ・プールに十分なスペースがないため、あるいはサーバーがストレージ・プールにアクセスできないために、サーバーがデータの処理に失敗する場合があります。 **その他の状態** その他の状態のストレージ・ルールの数。ストレージ・ルールが定義されているサーバーが、データの提供に使用できないか、または状況をサポートしていない以前のバージョンの IBM Spectrum Protect を実行している可能性があります。ストレージ・ルールがアクティブ化されていないか、実行されなかったために、状況が適用されない場合があります。 **ヒント:** • アイコンが表示されるのは、1 つ以上のストレージ・ルールが対応する状態にある場合のみです。各ストレージ・ルールの詳細情報を表示するには、「**ストレージ・ルール**」をクリックして、「**ストレージ・ルール**」ページを表示します。 • 実行中または完了済みのストレージ・ルール・ジョブを判別するには、**QUERY JOB** コマンドを実行します。手順については、QUERY JOB (ジョブの照会)を参照してください。

定期的なモニター・チェックリスト

ソリューションが正しく動作するように、定期的なモニター・チェックリストのタスクを実行します。大きな問題となる前に潜在的な問題点を検出できるように、十分な頻度で定期的なタスクをスケジュールしてください。

ヒント: 拡張モニター・タスクの管理コマンドを実行するには、Operations Center コマンド・ビルダーを使用します。コマンド・ビルダーは、コマンドを入力するときにガイドとなる先行入力機能を提供します。コマンド・ビルダーを開くには、Operations Center の「**概要**」ページに進みます。メニュー・バーで、設定アイコン  にマウス・カーソルを移動し、「**コマンド・ビルダー**」をクリックします。

表 16. 定期的なモニター・タスク

タスク	基本的な手順	詳細手順およびトラブルシューティング
システム・パフォーマンスをモニターします。	クライアント・バックアップ操作に必要な時間の長さを判別します。 1. Operations Center の「**概要**」ページで、「**クライアント**」をクリックします。クライアントに関連付けられているサーバーを見つけます。 2.「**サーバー**」をクリックします。サーバーを選択し、「**詳細**」をクリックします。 3. 過去 24 時間の完了タスクの所要時間を表示するには、「**完了タスク**」をクリックします。 4. 24 時間より前に完了したタスクの期間を表示するには、**QUERY ACTLOG** コマンドを使用します。QUERY ACTLOG (活動記録ログの照会) の指示に従ってください。 5. クライアント・バックアップ操作の所要時間が長くなっていて、理由が不明である場合は、原因を調べてください。 バックアップ/アーカイブ・クライアントにクライアント管理サービスをインストールしている場合、以下のステップを実行して、バックアップ/アーカイブ・クライアントのパフォーマンスの問題を診断することができます。 1. Operations Center の「**概要**」ページで、「**クライアント**」をクリックします。 2. バックアップ/アーカイブ・クライアントを選択して、「**詳細**」をクリックします。 3. クライアント・ログを取得するには、「**診断**」をクリックします。	クライアントがサーバーにデータをバックアップするのに要する時間の短縮に関する説明については、一般的なクライアントのパフォーマンス問題の解決を参照してください。 パフォーマンスのボトルネックを探してください。手順については、パフォーマンス・ボトルネックの識別を参照してください。 その他のパフォーマンスの問題の特定および解決については、パフォーマンスを参照してください。

表 16. 定期的なモニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング
データ重複排除によって提供されるディスクの節約を判別します。	1. Operations Center の「**概要**」ページで、「**プール**」をクリックします。 2. プールを選択して、「**クイック検索**」をクリックします。 3. 「データ重複排除」域で、「節約されたスペース」行を確認します。	拡張モニターの場合、特定のディレクトリー・コンテナー・ストレージ・プールまたはクラウド・コンテナー・ストレージ・プールのデータ重複排除プロセスに関する詳細な統計を取得するには、以下の手順を実行します。 1. Operations Center の「**概要**」ページで、設定アイコン にマウス・カーソルを移動し、「**コマンド・ビルダー**」をクリックします。 2. **GENERATE DEDUPSTATS** コマンドを発行して、統計レポートを取得します。GENERATE DEDUPSTATS (ディレクトリー・コンテナー・ストレージ・プールのデータ重複排除統計の生成) の指示に従ってください。 3. **QUERY DEDUPSTATS** コマンドを発行して、統計レポートを表示します。QUERY DEDUPSTATS (データ重複排除統計の照会) の指示に従ってください。

装置構成およびボリューム・ヒストリー情報の現行のバックアップ・ファイルが保存されていることを確認します。	保管場所にアクセスして、ファイルを使用できることを確認します。推奨される方法は、バックアップ・ファイルを 2 つの場所に保存することです。
	ボリューム・ヒストリーおよび装置構成ファイルを見つけるには、以下の手順を実行します。
	1. Operations Center の「**概要**」ページで、設定アイコン にマウス・カーソルを移動し、「**コマンド・ビルダー**」をクリックします。
	2. ボリューム・ヒストリーおよび装置構成ファイルを見つけるには、次のコマンドを発行します。
	`query option volhistory`
	`query option devconfig`
	3. 出力で「オプション設定」列を確認して、ファイルの場所を見つけます。
	災害が発生した場合、サーバー・データベースをリストアするために、ボリューム・ヒストリー・ファイルと装置構成ファイルの両方が必要です。	

表 16. 定期的なモニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング

インスタンス・ディレクトリー・ファイル・システム用に十分なスペースが使用可能であるかどうかを判別します。	インスタンス・ディレクトリー・ファイル・システムで少なくとも 20% のフリー・スペースが使用可能であることを確認します。ご使用のオペレーティング・システムに適した処置を実行します。
	• AIX ファイル・システム内で使用可能なスペースを表示するには、オペレーティング・システムのコマンド・ラインで以下のコマンドを発行します。
	`df -g instance_directory`
	ここで、*instance_directory* は、インスタンス・ディレクトリーを指定します。
	• Linux ファイル・システム内で使用可能なスペースを表示するには、オペレーティング・システムのコマンド・ラインで以下のコマンドを発行します。
	`df -h instance_directory`
	ここで、*instance_directory* は、インスタンス・ディレクトリーを指定します。
	• Windows Windows エクスプローラー・プログラムで、ファイル・システムを右クリックして、「**プロパティ**」をクリックします。容量情報を表示します。
	インスタンス・ディレクトリーの推奨される場所は、サーバーがインストールされているオペレーティング・システムによって異なります。
	• AIX Linux `/home/tsminst1/tsminst1`
	• Windows `C:¥tsminst1`
	ヒント: 計画ワークシートを完了している場合、インスタンス・ディレクトリーの場所はワークシートに記録されています。	

表 16. 定期的なモニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング
予期しないクライアント・アクティビティーを 識別します。	クライアント・アクティビティーをモニターして、データ・ボリュームが予期した容量を超えているかどうかを判別するには、以下の手順を実行します。 1. Operations Center の「**概要**」ページで、「クライアント」エリアをクリックします。 2. 過去 2 週間のアクティビティーを表示するには、任意のクライアントをダブルクリックします。 3. クライアントに送信されたバイト数を表示するには、「**プロパティー**」タブをクリックします。 4. 「最終セッション」エリアで、「クライアントに送信」行を確認します。	「クライアント」テーブルでクライアントをダブルクリックすると、「**2 週間のアクティビティー**」エリアに、クライアントが毎日サーバーに送信したデータの容量が表示されます。 クライアント・セッションの統計が入っている SQL アクティビティーの 要約テーブルを定期的に確認してください。 現在のアクティビティーと過去のアクティビティーを 比較する場合、**SQL SELECT** ステートメントを使用してください。 アクティビティーのレベルが 前のアクティビティーとは 大きく異なる場合、ランサムウェア攻撃を示している可能性があります。 アクティビティー・ログを定期的に確認してください。 バックアップされ、検査されたファイルの数を示す ANE メッセージを検索してください。 現在のデータ重複排除率を以前の率と比べてください。 バックアップされたファイル数が異常に多かった場合、またはデータ重複排除率が予期せずに 0 まで落ちた場合に、それはランサムウェア攻撃を示している可能性があります。

表 16. 定期的なモニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング
時間の経過に伴うストレージ・プールの増大をモニターします。	1. Operations Center の「**概要**」ページで、「プール」エリアをクリックします。 2. 過去 2 週間に使用された容量を表示するには、プールを選択して、「**詳細**」をクリックします。	**ヒント:** • 重複排除されたすべてのエクステントが、インベントリーによって参照されなくなってから、ディレクトリー・コンテナー・ストレージ・プールまたはクラウド・コンテナー・ストレージ・プールから除去されるまでに経過する必要がある期間を指定するには、以下の手順を実行します。 1. Operations Center の「**ストレージ・プール**」ページで、ストレージ・プールを選択します。 2.「**詳細**」>「**プロパティー**」をクリックします。 3.「コンテナー再利用の遅延期間」フィールドに期間を指定します。 • ディレクトリー・コンテナー・ストレージ・プールおよびクラウド・コンテナー・ストレージ・プールのデータ重複排除パフォーマンスを確認するには、**GENERATE DEDUPSTATS** コマンドを使用します。 • ストレージ・プールのデータ重複排除統計を表示するには、以下の手順を実行します。 1. Operations Center の「**ストレージ・プール**」ページで、ストレージ・プールを選択します。 2.「**詳細**」>「**プロパティー**」をクリックします。 または、**QUERY EXTENTUPDATES** コマンドを使用して、ディレクトリー・コンテナー・ストレージ・プールまたはクラウド・コンテナー・ストレージ・プール内のデータ・エクステントの更新に関する情報を表示します。このコマンド出力は、参照されなくなったデータ・エクステント、およびシステムから削除するのに適格なデータ・エクステントを判別するのに役立ちます。 この出力で、システムから削除するのに適格なデータ・エクステント数をモニターします。このメトリックには、コンテナー・ストレージ・プール内で使用可能なフリー・スペース量との直接的な相関関係があります。

表 16. 定期的なモニター・タスク (続き)

タスク	基本的な手順	詳細手順およびトラブルシューティング
		• データ重複排除による節約を除去した後に、ファイル・スペースによって占有されている物理スペース量を表示するには、**select * from occupancy** コマンドを使用します。このコマンド出力には、LOGICAL_MB 値が含まれています。LOGICAL_MB は、ファイル・スペースによって使用されているスペース量です。
クライアント・スケジュールのタイミングを評価します。クライアント・スケジュールの開始時刻と終了時刻がビジネス・ニーズに合っていることを確認します。	Operations Center の「**概要**」ページで、「**クライアント**」 > 「**スケジュール**」をクリックします。 「スケジュール」テーブルで、「開始」列に、スケジュール済み操作用に構成された開始時刻が表示されます。最近の操作が開始された時刻を確認するには、クロック・アイコンの上にカーソルを移動します。	**ヒント:** クライアント操作が予想以上に長く実行されている場合に警告メッセージを受け取ることができます。次の手順を実行してください。 1. Operations Center の「概要」ページで、「**クライアント**」の上にカーソルを移動して、「**スケジュール**」をクリックします。 2. スケジュールを選択して、「**詳細**」をクリックします。 3. 行の横にある青色の矢印をクリックして、スケジュールの詳細を表示します。 4. 「**ランタイム・アラート**」フィールドに、スケジュール済み操作が完了しなかった場合に警告メッセージが発行される時刻を指定します。 5. 「**保存**」をクリックします。
保守タスクのタイミングを評価します。保守タスクの開始時刻と終了時刻がビジネス・ニーズに合っていることを確認します。	Operations Center の「**概要**」ページで、「**サーバー**」 > 「**保守**」をクリックします。 「保守」テーブルで、「最終実行時刻」列の情報を確認します。最後の保守タスクが開始された時刻を確認するには、クロック・アイコンの上にカーソルを移動します。	**ヒント:** 保守タスクの実行時間が長すぎる場合、開始時刻または最大実行時間を変更します。次の手順を実行してください。 1. Operations Center の「**概要**」ページで、設定アイコン にマウス・カーソルを移動し、「**コマンド・ビルダー**」をクリックします。 2. タスクの開始時刻または最大実行時間を変更するには、**UPDATE SCHEDULE** コマンドを発行します。手順については、UPDATE SCHEDULE (クライアント・スケジュールの更新)を参照してください。

関連情報

QUERY ACTLOG (活動記録ログの照会)
UPDATE STGPOOL (ストレージ・プールの更新)
QUERY EXTENTUPDATES (更新されたデータ・エクステントの照会)

ライセンス準拠の検証

IBM Spectrum Protect ソリューションがご使用条件の条項に準拠していることを確認します。準拠を定期的に確認することで、データの増加またはプロセッサー・バリュー・ユニット (PVU) 使用量の傾向を追跡できます。この情報を使用して、将来のライセンスの購入について計画します。

このタスクについて

ご使用のソリューションがライセンス条件に準拠しているかを確認するために使用する方法は、IBM Spectrum Protect のご使用条件の条項によって異なります。

フロントエンド・キャパシティー・ライセンス
フロントエンド・モデルでは、クライアントによってバックアップされていることが報告された 1 次データの量に基づいてライセンス要件が決定されます。クライアントには、アプリケーション、仮想マシン、およびシステムが含まれます。

バックエンド・キャパシティー・ライセンス
バックエンド・モデルでは、1 次ストレージ・プールおよびリポジトリーに保管されているデータのテラバイト単位に基づいてライセンス要件が決定されます。

ヒント:

- フロントエンドおよびバックエンドの容量見積もりの正確性を確保するには、各クライアント・ノードに最新バージョンのクライアント・ソフトウェアをインストールします。
- Operations Center のフロントエンドおよびバックエンドの容量情報は、計画と見積もりを目的として使用されます。

PVU ライセンス
PVU モデルは、サーバー装置による PVU の使用量に基づいています。

重要: IBM Spectrum Protect によって提供される PVU の計算は見積もりと見なされ、法的拘束力はありません。IBM Spectrum Protect によって報告される PVU ライセンス情報は、IBM License Metric Tool の受け入れ可能な代替とは見なされません。IBM License Metric Tool は実際の使用状況を反映するように設計されています。例えば、IBM Spectrum Protect バックアップ/アーカイブ・クライアントのインストール後、ツールでは初回の使用の後にのみ、クライアントをカウントします。IBM License Metric Tool について詳しくは、IBM ライセンス・メトリック・ツールを参照してください。

ライセンス要件について質問または懸念がある場合は、IBM Spectrum Protect ソフトウェア・プロバイダーにお問い合わせください。

手順

ライセンス準拠をモニターするには、ご使用条件の条項に対応しているステップを実行します。

ヒント: Operations Center は、フロントエンドおよびバックエンドの容量使用量の概要を示す E メール・レポートを提供します。レポートは、定期的に 1 人以上の受信者に自動的に送信することができます。 E メール・レポートを構成して管理するには、Operations Center メニュー・バーの「**レポート**」をクリックします。

オプション	説明
フロントエンド・モデル	a. Operations Center メニュー・バーで、設定アイコン の上にカーソルを移動して、「**ライセンス交付**」をクリックします。 フロントエンド・キャパシティーの見積もりが「フロントエンド使用量 (Front-end Usage)」ページに表示されます。 b.「報告なし (Not Reporting)」列に値が表示される場合は、番号をクリックして、容量使用量を報告しなかったクライアントを特定します。

オプション	説明
	c. 容量使用量を報告しなかったクライアントの容量を見積もるには、測定ツールと説明を提供する次のダウンロード・サイトにアクセスします。 https://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools スクリプトによってフロントエンド容量を測定するには、入手可能な最新のライセンス交付ガイドの手順を実行します。 d. Operations Center の見積もりと、スクリプトを使用して得られた見積もりを加算します。 e. 見積もられた容量がご使用条件に準拠していることを確認します。
バックエンド・モデル	**制約事項 :** ソース複製サーバーとターゲット複製サーバーが同じポリシー設定を使用していない場合、Operations Center を使用して、複製されたクライアントのバックエンド容量の使用量をモニターすることはできません。これらのクライアントの容量使用量を見積もる方法については、技術情報 1656476 を参照してください。 a. Operations Center メニュー・バーで、設定アイコン の上にカーソルを移動して、「**ライセンス交付**」をクリックします。 b.「**バックエンド (Back-end)**」タブをクリックします。 c. データの見積もり容量がご使用条件に準拠していることを確認します。
PVU モデル	PVU ライセンス交付条件の準拠性を評価する方法については、PVU ライセンス・モデルの準拠性の評価を参照してください。

E メール・レポートを使用したシステム状況のトラッキング

システム状況を要約する E メール・レポートを生成するように Operations Center をセットアップします。メール・サーバー接続の構成、レポート設定の変更、オプションのカスタム・レポートの作成を実行できます。

始める前に

E メール・レポートをセットアップする前に、以下の要件が満たされていることを確認します。

- レポートを E メールで送受信するために Simple Mail Transfer Protocol (SMTP) ホスト・サーバーを使用できます。SMTP サーバーは、オープン・メール・リレーとして構成されている必要があります。また、E メール・メッセージを送信する IBM Spectrum Protect サーバーに、SMTP サーバーへのアクセス権限があることを確認する必要があります。Operations Center が別のコンピューターにインストールされている場合、そのコンピューターには、SMTP サーバーへのアクセス権限は必要ありません。
- E メール・レポートをセットアップするには、サーバーのシステム 特権が必要です。
- 受信者を指定するために、1 つ以上の E メール・アドレスまたは管理者 ID を入力できます。管理者 ID を入力する予定の場合は、ID がハブ・サーバーに登録されていて、その ID に E メール・アドレスが関連付けられている必要があります。管理者の E メール・アドレスを指定するには、**UPDATE ADMIN** コマンドの **EMAILADDRESS** パラメーターを使用します。

このタスクについて

一般的な運用レポート、ライセンス準拠レポート、1 つ以上のカスタム・レポートを送信するように Operations Center を構成できます。カスタム・レポートを作成する際は、よく使われるレポート・テンプ

レートのセットからテンプレートを選択するか、管理対象サーバーを照会するために SQL SELECT ステートメントを入力します。

手順

E メール・レポートをセットアップして管理するには、以下の手順を実行します。

1. Operations Center メニュー・バーで、「**レポート**」をクリックします。
2. E メール・サーバー接続がまだ構成されていない場合は、「**メール・サーバーの構成**」をクリックして、フィールドに入力します。

   メール・サーバーを構成すると、一般的な運用レポートとライセンス準拠レポートが有効になります。
3. レポート設定を変更するには、レポートを選択し、「**詳細**」をクリックして、フォームを更新します。
4. オプション: カスタム・レポートを追加するには、「**+ レポート**」をクリックし、フィールドに入力します。

   ヒント: レポートを即時に実行して送信するには、レポートを選択して「**送信**」をクリックします。

タスクの結果

指定された設定に基づいて、有効になったレポートが送信されます。

関連情報

UPDATE ADMIN (管理者の更新)

第 4 部 マルチサイト・ディスク・ソリューションの操作の管理

この情報を使用して、サーバーを含む IBM Spectrum Protect で複数のロケーションを対象としてデータ重複排除を使用する、マルチサイト・ディスク・ソリューションの操作を管理します。

Operations Center の管理

Operations Center では、IBM Spectrum Protect 環境に関する情報状況への Web およびモバイル・アクセスが提供されています。Operations Center を使用して、複数のサーバーをモニターし、いくつかの管理タスクを実行することができます。 また、Operations Center では、IBM Spectrum Protect コマンド・ラインへの Web アクセスも可能です。

スポーク・サーバーの追加および削除

複数サーバー環境では、その他のサーバー (スポーク・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。

このタスクについて

これらのスポーク・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ポーク・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。

スポーク・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 つ以上のスポーク・サーバーを追加することができます。

始める前に

スポーク・サーバーとハブ・サーバーの間の通信は、Transport Layer Security (TLS) プロトコルを使用して保護する必要があります。通信を保護するには、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・ファイルに追加します。

手順

1. 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、サーバーがまだスポーク・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。
2. 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「**スポークのモニター**」をクリックします。
   - 追加したいサーバーが表に表示されず、セキュア SSL/TLS 通信が必要ではない場合は、表のメニュー・バーで「**+ スポーク**」をクリックします。
3. 必要な情報を提供し、スポ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、そのサーバーをスポーク・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。

スポーク・サーバーの除去

Operations Center からスポーク・サーバーを除去することができます。

このタスクについて

例えば、以下の状況ではスポーク・サーバーの除去が必要な場合があります。

- スポーク・サーバーを別のハブ・サーバーに移動したい場合。
- スポーク・サーバーを廃止したい場合。

手順

ハブ・サーバーによって管理されているサーバー・グループからスポーク・サーバーを除去するには、以下のステップを実行します。

1. IBM Spectrum Protect コマンド・ラインから、ハブ・サーバーに対して次のコマンドを発行します。

   ```
   QUERY MONITORSETTINGS
   ```

2. コマンドの出力から、「**モニター対象グループ**」フィールドにある名前をコピーします。
3. ハブ・サーバーに対して次のコマンドを発行します。ここで、*group_name* はモニター対象グループの名前を表し、*member_name* はスポーク・サーバーの名前を表します。

   ```
   DELETE GRPMEMBER group_name member_name
   ```

4. オプション: スポーク・サーバーを別のハブ・サーバーに移動したい場合は、このステップを実行しないでください。それ以外の場合は、スポーク・サーバーに対して次のコマンドを発行して、スポーク・サーバーでのアラートおよびモニターを使用不可にすることができます。

   ```
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   ```

5. オプション: スポーク・サーバー定義が別の目的 (エンタープライズ構成、コマンド・ルーティング、仮想マシンのほか、あるいはライブラリー管理など)　で使用されている場合は、このステップを実行しないでください。それ以外の場合は、ハブ・サーバーに対して次のコマンドを発行して、ハブ・サーバー上のスポーク・サーバー定義を削除することができます。

   ```
   DELETE SERVER spoke_server_name
   ```

   ヒント: モニター対象グループからサーバーが削除された直後にサーバー定義が削除された場合、Operations Center にそのサーバーの状況情報が無期限に残る可能性があります。

   この問題を回避するため、状況収集間隔の設定時間が経過するまで待機してから、サーバー定義を削除してください。状況収集間隔は、Operations Center の「設定」ページに表示されています。

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、自動的に始動されます。例えば、構成変更を加える場合に、Web サーバーの停止と始動を行う必要がある可能性があります。

手順

1. Web サーバーを停止します。
   - AIX /*installation_dir*/ui/utils ディレクトリー (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) から、次のコマンドを実行します。

     ```
     ./stopserver.sh
     ```

   - Linux 次のコマンドを発行します。

```
service opscenter.rc stop
```

- Windows 「**サービス**」ウィンドウから、「**IBM Spectrum Protect Operations Center**」サービスを停止します。

2. Web サーバーを始動します。
   - AIX */installation_dir*/ui/utils ディレクトリー (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) から、次のコマンドを実行します。

     ```
     ./startserver.sh
     ```

   - Linux 以下のコマンドを発行します。

     サーバーを始動します。

     ```
     service opscenter.rc start
     ```

     サーバーを再始動します。

     ```
     service opscenter.rc restart
     ```

     サーバーが実行中かどうかを以下のように判別します。

     ```
     service opscenter.rc status
     ```

   - Windows 「**サービス**」ウィンドウから、「**IBM Spectrum Protect Operations Center**」サービスを始動します。

初期構成ウィザードの再始動

例えば、構成変更を加える場合に、Operations Center の初期構成ウィザードの再始動を行う必要がある可能性があります。

始める前に

以下の設定を変更するには、初期構成ウィザードを再始動するのではなく、Operations Center の「**設定**」ページを使用します。

- 状況データが最新表示される頻度
- アラートがアクティブ、非アクティブ、またはクローズされている期間
- クライアントが危険な状態にあることを示す状態

Operations Center のヘルプには、これらの設定の変更方法に関する詳細情報が記載されています。

このタスクについて

初期構成ウィザードを再始動するには、ハブ・サーバー接続に関する情報を記載するプロパティー・ファイルを削除する必要があります。ただし、ハブ・サーバーに対して構成されたアラート、モニター、リスク状態、またはマルチサーバーの設定は削除されません。これらの設定は、構成ウィザードを再始動した時にウィザードのデフォルト設定として使用されます。

手順

1. Operations Center Web サーバーを停止します。
2. Operations Center がインストールされているコンピューターで、以下のディレクトリーに進みます。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。
   - AIX Linux *installation_dir*/ui/Liberty/usr/servers/guiServer

- Windows *installation_dir*¥ui¥Liberty¥usr¥servers¥guiServer

例えば次のとおりです。

- AIX Linux /opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
- Windows c:¥Program Files¥Tivoli¥TSM¥ui¥Liberty¥usr¥servers¥guiServer

3. guiServer ディレクトリーで、serverConnection.properties ファイルを削除します。
4. Operations Center Web サーバーを開始します。
5. Operations Center を開きます。
6. 構成ウィザードを使用して、Operations Center を再構成します。
   モニター管理者 ID の新規パスワードを指定します。
7. 以前にハブ・サーバーに接続された任意のスポーク・サーバーで、IBM Spectrum Protect コマンド・ライン・インターフェースから 次のコマンドを発行して、モニター管理者 ID のパスワードを更新します。

```
UPDATE ADMIN IBM-OC-hub_server_name new_password
```

制約事項 : この管理者 ID のその他の設定は変更しないでください。初期パスワードを設定した後、このパスワードは、Operations Center によって自動的に管理されます。

ハブ・サーバーの変更

Operations Center を使用して、IBM Spectrum Protect のハブ・サーバーを除去したり、別のハブ・サーバーを構成したりすることができます。

手順

1. Operations Center の初期構成ウィザードを再始動します。
   この手順の一部として、既存のハブ・サーバー接続を削除します。
2. ウィザードを使用して Operations Center を構成し、新しいハブ・サーバーに接続します。

関連タスク

初期構成ウィザードの再始動
例えば、構成変更を加える場合に、Operations Center の初期構成ウィザードの再始動を行う必要がある可能性があります。

事前構成された状態への構成のリストア

特定の問題が生じる場合、Operations Center 構成を、IBM Spectrum Protect サーバーがハブ・サーバーまたはスポーク・サーバーとして定義されていない事前構成された状態にリストアすることができます。

手順

構成をリストアするには、以下の手順を実行します。

1. Operations Center Web サーバーを停止します。
2. 以下のステップを実行して、ハブ・サーバーを構成解除します。
   a) ハブ・サーバーで、以下のコマンドを実行します。

```
SET MONITORINGADMIN ""
SET MONITOREDSERVERGROUP ""
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
REMOVE ADMIN IBM-OC-hub_server_name
```

   ヒント : IBM-OC-*hub_server_name* は、ハブ・サーバーを最初に構成した時点で自動的に作成されたモニター管理者 ID を表します。

   b) ハブ・サーバーで次のコマンドを実行して、ハブ・サーバーのパスワードをリセットします。

```
SET SERVERPASSWORD ""
```

重要: ハブ・サーバーが別の目的 (ライブラリー共有、データのエクスポートとインポート、またはノード複製など) のために他のサーバーで構成されている場合は、このステップを実行しないでください。

3. 以下のステップを実行して、スポーク・サーバーを構成解除します。
   a) ハブ・サーバーで、スポーク・サーバーのいずれかがサーバー・グループのメンバーとして 残されているかどうかを確認するために、次のコマンドを発行します。

```
QUERY SERVERGROUP IBM-OC-hub_server_name
```

   ヒント: IBM-OC-*hub_server_name* は、最初のスポーク・サーバーを構成した時点で自動的に作成されたモニター対象サーバー・グループの名前を表します。また、このサーバー・グループ名は、ハブ・サーバーを最初に構成した時点で自動的に作成されたモニター管理者 ID と同じです。

   b) ハブ・サーバー上で、サーバー・グループからスポーク・サーバーを削除するために、各スポーク・サーバーに対して以下のコマンドを実行します。

```
DELETE GRPMEMBER IBM-OC-hub_server_name spoke_server_name
```

   c) すべてのスポーク・サーバーがサーバー・グループから削除された後、ハブ・サーバーで以下のコマンドを実行します。

```
DELETE SERVERGROUP IBM-OC-hub_server_name
SET MONITOREDSERVERGROUP ""
```

   d) 各スポーク・サーバー上で、以下のコマンドを実行します。

```
REMOVE ADMIN IBM-OC-hub_server_name
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

   e) 各スポーク・サーバーで、以下のコマンドを実行して、ハブ・サーバーの定義を削除します。

```
DELETE SERVER hub_server_name
```

重要: この定義が別の目的 (ライブラリー共有、データのエクスポートとインポート、またはノード複製など) のために使用されている場合は、このステップを実行しないでください。

   f) ハブ・サーバーで、以下のコマンドを実行して、各スポーク・サーバーの定義を削除します。

```
DELETE SERVER spoke_server_name
```

重要: このサーバー定義が別の目的 (ライブラリー共有、データのエクスポートとインポート、またはノード複製など) のために使用されている場合は、このステップを実行しないでください。

4. 以下のコマンドを実行して、各サーバーでデフォルトの設定をリストアします。

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Operations Center の初期構成ウィザードを再始動します。

関連タスク

初期構成ウィザードの再始動

例えば、構成変更を加える場合に、Operations Center の初期構成ウィザードの再始動を行う必要がある可能性があります。

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、自動的に始動されます。例えば、構成変更を加える場合に、Web サーバーの停止と始動を行う必要がある可能性があります。

アプリケーション、仮想マシン、およびシステムの保護

サーバーは、アプリケーション、仮想マシン、およびシステムなどを含むクライアントのデータを保護します。クライアント・データの保護を開始するには、クライアント・ノードをサーバーに登録して、クライアント・データを保護するためのバックアップ・スケジュールを選択します。

クライアントの追加

IBM Spectrum Protect を使用するデータ保護ソリューションを実装した後、クライアントを追加することでソリューションを拡張することができます。

このタスクについて

この手順では、クライアントを追加するための基本的な手順について説明します。クライアントの構成に関する具体的な手順については、クライアント・ノードにインストールする製品の資料を参照してください。以下のタイプのクライアント・ノードを使用することができます。

アプリケーション・クライアント・ノード
アプリケーション・クライアント・ノードには、E メール・サーバー、データベース、およびその他のアプリケーションなどがあります。例えば、以下のすべてのアプリケーションがアプリケーション・クライアント・ノードです。

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

システム・クライアント・ノード
システム・クライアント・ノードには、ワークステーション、Network Attached Storage (NAS) ファイル・サーバー、および API クライアントなどがあります。

仮想マシン・クライアント・ノード
仮想マシン・クライアント・ノードは、ハイパーバイザー内の個々のゲスト・ホストで構成されます。各仮想マシンは、ファイル・スペースとして表示されます。

手順

クライアントを追加するには、以下の手順を実行します。

1. クライアント・ノードにインストールするソフトウェアを選択して、インストールを計画します。91 ページの『クライアント・ソフトウェアの選択およびインストールの計画』 の指示に従ってください。
2. クライアント・データをバックアップおよびアーカイブする 方法を指定します。93 ページの『クライアント・データのバックアップおよびアーカイブに 関するルールの指定』 の指示に従ってください。
3. クライアント・データをバックアップおよびアーカイブする 時期を指定します。95 ページの『バックアップおよびアーカイブの 操作のスケジュール』 の指示に従ってください。
4. クライアントがサーバーに 接続できるようにするには、クライアントを登録します。96 ページの『クライアントの登録』 の指示に従ってください。

5. クライアント・ノードの保護を開始するには、選択したソフトウェアをクライアント・ノードにインストールして構成します。97 ページの『クライアントのインストールおよび構成』 の指示に従ってください。

クライアント・ソフトウェアの選択およびインストールの計画

異なるタイプのデータには異なるタイプの保護が必要です。保護する必要があるデータのタイプを確認して、適切なソフトウェアを選択してください。

このタスクについて

すべてのクライアント・ノードにバックアップ/アーカイブ・クライアントをインストールし、クライアント・ノード上でクライアント・アクセプターを構成して開始できるようにする方法をお勧めします。クライアント・アクセプターは、スケジュールされた操作を効率的に実行するように設計されています。

クライアント・アクセプターは、バックアップ/アーカイブ・クライアント、IBM Spectrum Protect for Databases、IBM Spectrum Protect for Enterprise Resource Planning、IBM Spectrum Protect for Mail、および IBM Spectrum Protect for Virtual Environments の各製品のスケジュールを実行します。クライアント・アクセプターによってスケジュールが実行されない製品をインストールする場合、製品資料の構成手順に従い、スケジュールされた操作が行われることを確認する必要があります。

手順

目標に基づいて、インストールする製品を選択し、インストール手順を確認します。

ヒント: ここでクライアント・ソフトウェアをインストールする場合、クライアントを使用する前に、97 ページの『クライアントのインストールおよび構成』示されているクライアント構成タスクも完了する必要があります。

目標	製品および説明	インストール手順
ファイル・サーバーまたはワークステーションの保護	バックアップ/アーカイブ・クライアントは、ファイル・サーバーおよびワークステーションからストレージにファイルおよびディレクトリーをバックアップおよびアーカイブします。ファイルのバックアップ・バージョンおよびアーカイブ・コピーのリストアおよびリトリーブも可能です。	• クライアント環境の要件 • UNIX および Linux バックアップ/アーカイブ・クライアントのインストール • Windows クライアントの初回インストール
スナップショット・バックアップおよびリストアの機能を使用したアプリケーションの保護	IBM Spectrum Protect Snapshot は、統合されたアプリケーション認識スナップショットのバックアップおよびリストア機能を使用してデータを保護します。IBM Db2 データベース・ソフトウェア および SAP、Oracle、Microsoft Exchange、および Microsoft SQL Server のアプリケーションによって保管されたデータを保護できます。	• for UNIX and Linux のインストールおよびアップグレード • for VMware のインストールおよびアップグレード • for Windows のインストールおよび更新
IBM Domino サーバー上の E メール・アプリケーションの保護	IBM Spectrum Protect for Mail: Data Protection for IBM Domino は、データ保護を自動化して、IBM Domino サーバーをシャットダウンすることなくバックアップが実行されるようにします。	• UNIX、AIX、または Linux システムへの Data Protection for IBM Domino のインストール (V7.1.0) • Windows システムへの Data Protection for IBM Domino のインストール (V7.1.0)

目標	製品および説明	インストール手順
Microsoft Exchange サーバー上の E メール・アプリケーションの保護	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server は、データ保護を自動化して、Microsoft Exchange サーバーをシャットダウンすることなくバックアップが実行されるようにします。	のインストール、アップグレード、およびマイグレーション
Db2 データベースの保護	バックアップ/アーカイブ・クライアントのアプリケーション・プログラミング・インターフェース (API) を使用して、Db2 データを IBM Spectrum Protect サーバーにバックアップすることができます。	バックアップ/アーカイブ・クライアントのインストール (UNIX、Linux、および Windows)
IBM Informix® データベースの保護	バックアップ/アーカイブ・クライアントの API を使用して、Informix データを IBM Spectrum Protect サーバーにバックアップすることができます。	バックアップ/アーカイブ・クライアントのインストール (UNIX、Linux、および Windows)
Microsoft SQL データベースの保護	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server は、Microsoft SQL データを保護します。	Data Protection for SQL Server on Windows Server Core のインストール
Oracle データベースの保護	IBM Spectrum Protect for Databases: Data Protection for Oracle は、Oracle データを保護します。	Data Protection for Oracle のインストール
SAP 環境の保護	IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP は、SAP 環境向けにカスタマイズされた保護を提供します。この製品は、SAP データベース・サーバーの可用性の向上と管理ワークロードの軽減のために設計されています。	• Data Protection for SAP for Db2 のインストール • Data Protection for SAP for Oracle のインストール
仮想マシンの保護	IBM Spectrum Protect for Virtual Environments は、Microsoft Hyper-V および VMware の仮想環境向けに調整された保護を提供します。IBM Spectrum Protect for Virtual Environments を使用して、中央のサーバーに保管される永久差分バックアップを作成し、バックアップ・ポリシーを作成して、仮想マシンまたは個々のファイルをリストアすることができます。 あるいは、バックアップ/アーカイブ・クライアントを使用して、完全な VMware または Microsoft Hyper-V の仮想マシンをバックアップおよびリストアします。VMware 仮想マシンからファイルまたはディレクトリーをバックアップおよびリストアすることもできます。	• Data Protection for Microsoft Hyper-V のインストールとアップグレード • のインストールおよびアップグレード • バックアップ/アーカイブ・クライアントのインストール (UNIX、Linux、および Windows)

ヒント: スペース管理用のクライアントを使用するために、IBM Spectrum Protect for Space Management または IBM Spectrum Protect HSM for Windows をインストールすることができます。

クライアント・データのバックアップおよびアーカイブに関するルールの指定

クライアントを追加する前に、クライアント・データのバックアップおよびアーカイブの 操作に関する適切なルールが指定されていることを確認します。クライアント登録プロセス中に、クライアント・ノードをポリシー・ドメインに割り当てます。ポリシー・ドメインには、クライアント・データを保管する方法と時期を制御するルールがあります。

始める前に

続行方法を以下から決定してください。

- ソリューション用に構成されたポリシーについて十分な知識を持っており、変更の必要がないことが分かっている場合は、95 ページの『バックアップおよびアーカイブの 操作のスケジュール』に進みます。
- ポリシーについて十分な知識を持っていない場合は、この手順のステップに従ってください。

このタスクについて

ポリシーは、ある期間にわたって保管するデータの量、データを保存する期間、およびクライアントのリストアにデータを使用できる期間に影響を与えます。データ保護の目標に合わせてデフォルトのポリシーを更新して、お客様独自のポリシーを作成することができます。ポリシーには、以下のルールが含まれます。

- ファイルをサーバー・ストレージにバックアップしてアーカイブする 方法と時期。
- サーバー・ストレージに保持するファイルのコピー数と期間。

クライアント登録プロセス中に、クライアントをポリシー・ドメインに割り当てます。特定のクライアントのポリシーは、クライアントが割り当てられているポリシー・ドメインのルールによって決定されます。ポリシー・ドメインでは、有効なルールはアクティブ・ポリシー・セット内にあります。

クライアントがファイルをバックアップまたはアーカイブすると 、ファイルはポリシー・ドメインのアクティブ・ポリシー・セット内の管理クラスにバインドされます。管理クラスは、クライアント・データを管理するためのルールのキー・セットです。 ポリシーをさらに詳細にカスタマイズしない限り、クライアントでのバックアップおよびアーカイブ 操作では、ポリシー・ドメインのデフォルト管理クラスの設定が使用されます。ポリシーをカスタマイズするには、追加の管理クラスを定義し、その使用法をクライアント・オプションにより割り当てます。

クライアント・オプションは、クライアント・システム上の編集可能ファイルでローカルに指定することも、サーバー上のクライアント・オプション・セットで指定することもできます。 サーバー上のクライアント・オプション・セット内のオプションは、ローカルのクライアント・オプション・ファイル内のオプションをオーバーライドあるいは追加することができます。

手順

1. 93 ページの『ポリシーの表示』の手順に従って、ご使用のソリューションに対して構成されたポリシーを確認してください。
2. データ保存要件に合わせて軽微な変更が必要な場合は、94 ページの『ポリシーの編集』の手順に従ってください。
3. オプション: データ保存要件を満たすためにポリシー・ドメインを作成したり、ポリシーに大幅な変更を加える必要がある場合は、ポリシーのカスタマイズを参照してください。

ポリシーの表示

ポリシーを表示して、要件に合うように編集する必要があるかどうかを判別します。

手順

1. ポリシー・ドメインのアクティブ・ポリシー・セットを表示するには、以下の手順を実行します。
   a) Operations Center の「**サービス**」ページで、ポリシー・ドメインを選択して、「**詳細**」をクリックします。

b) ポリシー・ドメインの「**要約**」ページで、「**ポリシー・セット**」タブをクリックします。

ヒント: ランサムウェア攻撃後にデータを確実にリカバリーできるように、以下のガイドラインを適用してください。

- 「バックアップ」列の値が 2 以上であることを確認します。推奨値は 3、4 またはそれ以上です。
- 「追加バックアップの保持」列の値が 14 日以上であることを確認します。 推奨値は 30 日以上です。
- 「アーカイブの保持」列の値が 30 日以上であることを確認します。

IBM Spectrum Protect for Space Management ソフトウェアがクライアントにインストールされる場合、データがマイグレーション前にバックアップされていることを確認します。 **DEFINE MGMTCLASS** コマンドまたは **UPDATE MGMTCLASS** コマンドで、**MIGREQUIRESBKUP=YES** を指定します。次に、ヒントのガイドラインに従います。

2. ポリシー・ドメインの非アクティブなポリシー・セットを表示するには、以下の手順を実行します。
   a)「**ポリシー・セット**」ページで、「**構成**」トグルをクリックします。 これで、非アクティブなポリシー・セットを表示および編集することができます。
   b) 前後の矢印を使用して、非アクティブなポリシー・セットをスクロールします。非アクティブなポリシー・セットを表示すると、アクティブ・ポリシー・セットから非アクティブなポリシー・セットを区別する設定が強調表示されます。
   c)「**構成**」トグルをクリックします。ポリシー・セットは編集不可になります。

ポリシーの編集

ポリシー・ドメインに適用されるルールを変更するには、ポリシー・ドメインのアクティブ・ポリシー・セットを編集します。ドメインに対して別のポリシー・セットを活動化することもできます。

始める前に

ポリシーを変更すると、データ保存に影響する可能性があります。災害が発生した場合にデータを確実にリストアできるように、組織にとって重要なデータのバックアップを必ず続行してください。また、システムに、計画されたバックアップ操作に十分なストレージ・スペースがあることを確認してください。

このタスクについて

ポリシー・セット内の 1 つ以上の管理クラスを変更することにより、ポリシー・セットを編集します。アクティブ・ポリシー・セットを編集する場合、ポリシー・セットを再び活動化するまで、クライアントで変更内容を使用できません。編集したポリシー・セットをクライアントで使用できるようにするには、ポリシー・セットを活動化します。

1 つのポリシー・ドメインに対して複数のポリシー・セットを定義することはできますが、活動状態にできるのは 1 つのポリシー・セットだけです。別のポリシー・セットを活動化すると、そのポリシー・セットが現在のアクティブ・ポリシー・セットに取って代わります。

ポリシーを定義する場合の推奨方法については、ポリシーのカスタマイズ を参照してください。

手順

1. Operations Center の「**サービス**」ページで、ポリシー・ドメインを選択して、「**詳細**」をクリックします。
2. ポリシー・ドメインの「**要約**」ページで、「**ポリシー・セット**」タブをクリックします。

   「**ポリシー・セット**」ページには、アクティブ・ポリシー・セットの名前が示され、そのポリシー・セットのすべての管理クラスがリストされます。
3. 「**構成**」トグルをクリックします。ポリシー・セットは編集可能です。
4. 活動状態にないポリシー・セットを編集するには、前後の矢印を使用してポリシー・セットを見つけます。
5. 以下のいずれかのアクションを実行して、ポリシー・セットを編集します。

オプション	説明
管理クラスの追加	a.「ポリシー・セット」テーブルで、「**+ 管理クラス (Management Class)**」をクリックします。 b. データのバックアップおよびアーカイブに 関するルールを指定するには、「**管理クラスの追加**」ウィンドウのフィールドに 入力します。 c. この管理クラスをデフォルト管理クラスにするには、「**デフォルトに設定 (Make default)**」チェック・ボックスを選択します。 d.「**追加**」をクリックします。
管理クラスの削除	「管理クラス」列で、**-** をクリックします。 **ヒント :** デフォルト管理クラスを削除するには、最初に別の管理クラスをデフォルトとして割り当てる必要があります。
デフォルト管理クラスとしての管理クラスの設定	管理クラスの「デフォルト」列で、ラジオ・ボタンをクリックします。 **ヒント :** 別の管理クラスがファイルに割り当てられていないか、ファイルの管理に適切でない場合に、デフォルト管理クラスがクライアント・ファイルを管理します。クライアントが常にファイルをバックアップおよびアーカイブできるように、ファイルのバックアップとアーカイブの 両方のルールを含むデフォルト管理クラスを選択します。
管理クラスの変更	管理クラスのプロパティーを変更するには、テーブルのフィールドを 更新します。

6.「**保存**」をクリックします。

重要 : 新規ポリシー・セットを活動化すると、データが失われる可能性があります。あるポリシー・セットで保護されているデータが、別のポリシー・セットでは保護されない可能性があります。したがって、ポリシー・セットを活動化する前に、以前のポリシー・セットと新規ポリシー・セットの相違点によってデータが失われないことを確認してください。

7.「**活動化**」をクリックします。アクティブ・ポリシー・セットと新規ポリシー・セットの相違点の概要が表示されます。以下のステップを実行して、新規ポリシー・セットの変更内容がデータ保存要件と一貫していることを確認します。

a) 2 つのポリシー・セットの中の対応する管理クラスの相違点を確認して、クライアント・ファイルに対する影響を検討します。アクティブ・ポリシー・セットの管理クラスにバインドされているクライアント・ファイルは、新規ポリシー・セット内の同じ名前を持つ管理クラスにバインドされます。

b) アクティブ・ポリシー・セットの中で、新規ポリシー・セットに対応するものがない管理クラスを特定して、クライアント・ファイルに対する影響を検討します。これらの管理クラスにバインドされているクライアント・ファイルは、新規ポリシー・セット内のデフォルト管理クラスによって管理されます。

c) ポリシー・セットによって実装される変更内容を許容できる場合は、「**これらの更新がデータ損失を引き起こす可能性があることを理解している (I understand that these updates can cause data loss)**」チェック・ボックスを選択して、「**活動化**」をクリックします。

バックアップおよびアーカイブの操作のスケジュール

サーバーに新規クライアントを登録する前に、バックアップおよびアーカイブの 操作を行う際に、指定するスケジュールが使用可能であることを確認します。登録プロセス中に、スケジュールをクライアントに割り当てます。

始める前に

続行方法を以下から決定してください。

- ソリューション用に構成されたスケジュールについて十分な知識を持っており、変更の必要がないことが分かっている場合は、96 ページの『クライアントの登録』に進みます。
- スケジュールについて十分な知識を持っていない場合、またはスケジュールを変更する必要がある場合は、この手順のステップに従ってください。

このタスクについて

通常、すべてのクライアントのバックアップ操作を毎日実行する必要があります。ストレージ環境に最適なパフォーマンスを実現できるように、クライアントおよびサーバーのワークロードをスケジュールしてください。クライアントとサーバーの操作のオーバーラップを回避するために、クライアント・バックアップ/アーカイブの操作を夜間に実施するようにスケジュールすることを検討してください。クライアントおよびサーバーの操作が重なり合ったり、処理に十分な時間とリソースが与えられなかったりした場合、システム・パフォーマンスの低下、操作の失敗、その他の問題が生じる可能性があります。

手順

1. Operations Center メニュー・バーの「**クライアント**」にマウス・カーソルを移動して、使用可能なスケジュールを確認します。「**スケジュール**」をクリックします。
2. オプション: 以下のステップを実行して、スケジュールを変更または作成します。

オプション	説明
スケジュールの変更	a.「**スケジュール**」ビューで、スケジュールを選択して「**詳細**」をクリックします。 b.「**スケジュールの詳細**」ページで、行の先頭にある青色の矢印をクリックして詳細を表示します。 c. スケジュールの設定を変更し、「**保存**」をクリックします。
スケジュールの作成	「**スケジュール**」ビューで「**+スケジュール**」をクリックし、ステップを実行してスケジュールを作成します。

3. オプション: Operations Center に表示されないスケジュール設定を構成するには、サーバー・コマンドを使用します。例えば、特定のディレクトリーをバックアップし、それをデフォルト以外の管理クラスに割り当てるクライアント操作をスケジュールしたいとします。
   a) Operations Center の「**概要**」ページで、設定アイコン  上にカーソルを移動し、「**コマンド・ビルダー**」をクリックします。
   b) **DEFINE SCHEDULE** コマンドを発行してスケジュールを作成するか、**UPDATE SCHEDULE** コマンドを発行してスケジュールを変更します。コマンドについて詳しくは、DEFINE SCHEDULE (クライアント・スケジュールの定義) または UPDATE SCHEDULE (クライアント・スケジュールの更新)を参照してください。

関連情報

日次操作のスケジュールのチューニング

クライアントの登録

クライアントを登録して、クライアントがサーバーに接続できること、およびサーバーがクライアント・データを保護できることを確認します。

始める前に

クライアント・ノードでクライアント所有者権限を持つ管理ユーザー ID がクライアントに必要かどうかを判別します。クライアントに管理ユーザー ID が必要かどうかを判別するには、技術情報 7048963 を参照してください。

制約事項 : 一部のタイプのクライアントでは、クライアント・ノード名と管理ユーザー ID が一致していなければなりません。これらのクライアントは、V7.1.7 で導入された Lightweight Directory Access Protocol 認証方式を使用して認証することができません。 この認証方式 (統合モードと呼ばれる場合もある) の詳細は、Active Directory データベースを使用したユーザーの認証を参照してください。

手順

クライアントを登録するには、以下のいずれかのアクションを実行してください。

- クライアントに管理ユーザー ID が必要な場合、以下のように **REGISTER NODE** コマンドを使用し、**USERID** パラメーターを指定してクライアントを登録します。

  ```
  register node node_name password userid=node_name
  ```

  ここで *node_name* はノード名を指定し、*password* はノードのパスワードを指定します。 詳細については、ノードの登録を参照してください。
- クライアント・ノードに管理ユーザー ID が必要ない場合、Operations Center の「クライアントの追加」ウィザードを使用してクライアントを登録します。次の手順を実行してください。

  a. Operations Center メニュー・バーで、「**クライアント**」をクリックします。

  b.「クライアント」テーブルで、「**+ クライアント**」をクリックします。

  c.「**クライアントの追加**」ウィザードのステップを実行します。

  i) クライアントおよびサーバー上で冗長データを除去できるように指定します。「クライアント・サイド・データの重複排除」エリアで、「**使用可能**」チェック・ボックスを選択します。

  ii)「**構成**」ウィンドウで、**TCPSERVERADDRESS**、**TCPPORT**、**NODENAME**、および **DEDUPLICATION** の値をコピーします。

  ヒント : オプション値を記録し、安全な場所に保管します。クライアント登録が完了し、クライアント・ノードにソフトウェアをインストールした後、これらの値を使用してクライアントを構成します。

  iii) ウィザードの指示に従って、ポリシー・ドメイン、スケジュール、およびオプション・セットを指定します。

  iv) 危険な状態の設定を指定して、クライアントに関するリスクが表示される方法を設定します。

  v)「**クライアントの追加**」をクリックします。

関連情報

tcpserveraddress オプション
Tcpport オプション
nodename オプション
deduplication オプション

クライアントのインストールおよび構成

クライアント・ノードの保護を開始するには、選択したソフトウェアをインストールして構成する必要があります。

手順

ソフトウェアを既にインストール済みの場合、ステップ 98 ページの『2』を開始します。

1. 以下のいずれかのアクションを実行します。
   - アプリケーション・ノードまたはクライアント・ノードにソフトウェアをインストールするには、以下の手順に従います。

ソフトウェア	説明へのリンク
IBM Spectrum Protect バックアップ/アーカイブ・クライアント	– UNIX および Linux バックアップ/アーカイブ・クライアントのインストール – Windows クライアントの初回インストール **ヒント：**Operations Center を使用して既存のクライアントを更新することもできます。手順については、クライアント更新のスケジュールを参照してください。
IBM Spectrum Protect for Databases	– Data Protection for Oracle のインストール – Data Protection for SQL Server on Windows Server Core のインストール
IBM Spectrum Protect for Mail	– UNIX、AIX、または Linux システムへの Data Protection for IBM Domino のインストール (V7.1.0) – Windows システムへの Data Protection for IBM Domino のインストール (V7.1.0) – のインストール、アップグレード、およびマイグレーション
IBM Spectrum Protect Snapshot	– for UNIX and Linux のインストールおよびアップグレード – for VMware のインストールおよびアップグレード – for Windows のインストールおよび更新
IBM Spectrum Protect for Enterprise Resource Planning	– Data Protection for SAP for Db2 のインストール – Data Protection for SAP for Oracle のインストール

- 仮想マシン・クライアント・ノードにソフトウェアをインストールするには、選択したバックアップ・タイプの説明に従います。

バックアップ・タイプ	説明へのリンク
仮想マシンの完全 VMware バックアップを作成する予定の場合は、IBM Spectrum Protect バックアップ/アーカイブ・クライアントをインストールして構成します。	– UNIX および Linux バックアップ/アーカイブ・クライアントのインストール – Windows クライアントの初回インストール
仮想マシンの永久増分フルバックアップを作成する予定の場合は、同じクライアント・ノードまたは別のクライアント・ノードに IBM Spectrum Protect for Virtual Environments およびバックアップ/アーカイブ・クライアントをインストールして構成します。	– Data protection for VMware **ヒント：**IBM Spectrum Protect for Virtual Environments およびバックアップ/アーカイブ・クライアントのソフトウェアは、IBM Spectrum Protect for Virtual Environments インストール・パッケージで入手できます。

2. クライアントがサーバーに接続できるようにするには、クライアント・オプション・ファイルで **TCPSERVERADDRESS**、**TCPPORT**、および **NODENAME** オプションの値を追加または更新します。クライアントの登録時 (96 ページの『クライアントの登録』) に記録した値を使用します。
   - AIX、Linux、または Mac OS X のオペレーティング・システムにインストールされたクライアントの場合、クライアント・システムのオプション・ファイル `dsm.sys` に値を追加します。
   - Windows オペレーティング・システムにインストールされたクライアントの 場合は、`dsm.opt` ファイルに値を追加します。

デフォルトでは、オプション・ファイルはインストール・ディレクトリーにあります。

3. Linux オペレーティング・システムまたは Windows オペレーティング・システムにバックアップ/アーカイブ・クライアントをインストールした場合は、クライアントにクライアント管理サービスをインストールしてください。56 ページの『クライアント管理サービスのインストール』 の指示に従ってください。
4. スケジュールされた操作を実行するようにクライアントを構成します。99 ページの『スケジュール済み操作を実行するためのクライアントの構成』 の指示に従ってください。
5. オプション: ファイアウォール経由での通信を構成します。101 ページの『ファイアウォールを介したクライアント/サーバー通信の構成』 の指示に従ってください。
6. テスト・バックアップを実行し、データが計画通りに保護されていることを確認します。

   例えば、バックアップ/アーカイブ・クライアントの場合、以下のステップを実行します。

   a) Operations Center の「**クライアント**」ページで、バックアップするクライアントを 選択し、「**バックアップ**」をクリックします。

   b) バックアップが正常に完了したこと、および警告メッセージやエラー・メッセージがないことを確認します。
7. Operations Center で、クライアントに対してスケジュールされた操作の結果をモニターします。

次のタスク

クライアントからバックアップする 対象を変更するには、105 ページの『クライアント・バックアップの範囲の変更』の手順を実行してください。

スケジュール済み操作を実行するためのクライアントの構成

クライアント・ノードで、クライアント・スケジューラーを構成して開始する必要があります。クライアント・スケジューラーにより、スケジュール済み操作を実行するためのクライアントとサーバーの 間の通信が可能になります。例えば、スケジュール済み操作には通常、クライアントからのファイルのバックアップが含まれます。

このタスクについて

すべてのクライアント・ノードにバックアップ/アーカイブ・クライアントをインストールし、クライアント・ノード上でクライアント・アクセプターを構成して開始できるようにする方法が推奨されます。クライアント・アクセプターは、スケジュールされた操作を効率的に実行するように設計されています。クライアント・アクセプターは、以下の必要時にのみスケジューラーが実行されるようにクライアント・スケジューラーを管理します。

- 次回のスケジュール済み操作についてサーバーを照会する時間になった場合
- 次回のスケジュール済み操作を開始する時間になった場合

クライアント・アクセプターを使用すると、クライアント上のバックグラウンド・プロセスの数を減らして、メモリー保存の問題を回避することができます。

クライアント・アクセプターは、バックアップ/アーカイブ・クライアント、IBM Spectrum Protect for Databases、IBM Spectrum Protect for Enterprise Resource Planning、IBM Spectrum Protect for Mail、および IBM Spectrum Protect for Virtual Environments の各製品のスケジュールを実行します。クライアント・アクセプターによってスケジュールが 実行されない製品をインストールした場合、製品資料の構成手順に従い、スケジュールされた操作が行われることを確認します。

お客様のビジネスで、サード・パーティー製スケジューリング・ツールを標準手法として使用している場合は、クライアント・アクセプターの代わりにそのスケジューリング・ツールを使用することができます。一般に、サード・パーティー製スケジューリング・ツールでは、オペレーティング・システムのコマンドを使用して直接にクライアント・プログラムを開始します。サード・パーティー製スケジューリング・ツールを構成するには、製品資料を参照してください。

手順

クライアント・アクセプターを使用して、クライアント・スケジューラーを構成して開始するには、クライアント・ノードにインストールされているオペレーティング・システムの手順に従ってください。

AIX および Oracle Solaris

a. バックアップ/アーカイブ・クライアント GUI から、「**編集**」 > 「**クライアント・プリファレンス**」をクリックします。
b. 「**Web クライアント**」タブをクリックします。
c. 「**管理対象サービス・オプション (Managed Services Options)**」フィールドで、「**スケジュール**」をクリックします。クライアント・アクセプターによっても Web クライアントを管理する場合は、「**両方**」オプションをクリックします。
d. スケジューラーが無人で開始できるようにするには、dsm.sys ファイルで、**passwordaccess** オプションを generate に設定します。
e. クライアント・ノードのパスワードを保管するには、次のコマンドを発行して、プロンプトが出されたときにクライアント・ノードのパスワードを入力します。

```
dsmc query sess
```

f. コマンド・ラインで次のコマンドを発行して、クライアント・アクセプターを開始します。

```
/usr/bin/dsmcad
```

g. システムの再始動後にクライアント・アクセプターが自動的に開始されるようにするには、システムのスタートアップ・ファイル (通常は /etc/inittab) に次の項目を追加します。

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Client Acceptor Daemon
```

Linux

a. バックアップ/アーカイブ・クライアント GUI から、「**編集**」 > 「**クライアント・プリファレンス**」をクリックします。
b. 「**Web クライアント**」タブをクリックします。
c. 「**管理対象サービス・オプション (Managed Services Options)**」フィールドで、「**スケジュール**」をクリックします。クライアント・アクセプターによっても Web クライアントを管理する場合は、「**両方**」オプションをクリックします。
d. スケジューラーが無人で開始できるようにするには、dsm.sys ファイルで、**passwordaccess** オプションを generate に設定します。
e. クライアント・ノードのパスワードを保管するには、次のコマンドを発行して、プロンプトが出されたときにクライアント・ノードのパスワードを入力します。

```
dsmc query sess
```

f. root ユーザー ID でログインして次のコマンドを発行し、クライアント・アクセプターを開始します。

```
service dsmcad start
```

g. システムの再始動後にクライアント・アクセプターが自動的に開始されるようにするには、シェル・プロンプトで次のコマンドを発行してサービスを追加します。

```
# chkconfig --add dsmcad
```

MAC OS X

a. バックアップ/アーカイブ・クライアント GUI で、「**編集**」 > 「**クライアント・プリファレンス**」をクリックします。

b. スケジューラーが無人で開始できるようにするには、「**権限**」をクリックし、「**パスワード生成**」を選択し、「**適用**」をクリックします。

c. サービスの管理方法を指定するには、「**Web クライアント**」をクリックし、「**スケジュール**」を選択し、「**適用**」をクリックし、「**OK**」をクリックします。

d. 生成されたパスワードが保存されたことを確認するには、バックアップ/アーカイブ・クライアントを再始動します。

e. IBM Spectrum Protect Tools for Administrators アプリケーションを使用して、クライアント・アクセプターを開始します。

Windows

a. バックアップ/アーカイブ・クライアント GUI で、「**ユーティリティー**」 > 「**セットアップ・ウィザード**」 > 「**クライアント・スケジューラーの構成**」をクリックします。「**次へ**」をクリックします。

b. 「**スケジューラー・ウィザード (Scheduler Wizard)**」ページの情報を読み、「**次へ**」をクリックします。

c. 「**スケジューラー・タスク (Scheduler Task)**」ページで、「**新規または追加のスケジューラーのインストール (Install a new or additional scheduler)**」を選択して、「**次へ**」をクリックします。

d. 「**スケジューラーの名前およびロケーション (Scheduler Name and Location)**」ページで、追加するクライアント・スケジューラーの名前を指定します。次に、スケジューラーを管理するために「**クライアント・アクセプター・デーモン (CAD) の使用 (Use the Client Acceptor daemon (CAD))**」を選択して、「**次へ**」をクリックします。

e. このクライアント・アクセプターに割り当てる名前を入力します。デフォルトの名前は、Client Acceptor です。「**次へ**」をクリックします。

f. ウィザードの各ステップを実行して、構成を完了します。

g. クライアント・オプション・ファイル `dsm.opt` を更新し、**passwordaccess** オプションを `generate` に設定します。

h. クライアント・ノード・パスワードを保管するには、コマンド・プロンプトで次のコマンドを発行します。

```
dsmc query sess
```

プロンプトが表示されたら、クライアント・ノード・パスワードを入力します。

i. 「**サービス・コントロール**」ページからクライアント・アクセプター・サービスを開始します。例えば、デフォルト名を使用した場合は、クライアント・アクセプター・サービスを開始します。「**スケジューラーの名前およびロケーション**」ページで指定したスケジューラー・サービスを開始しないでください。スケジューラー・サービスは、必要に応じてクライアント・アクセプター・サービスによって自動的に開始および停止されます。

ファイアウォールを介したクライアント/サーバー通信の構成

クライアントがファイアウォールを 介してサーバーと通信する必要がある場合は、ファイアウォール経由のクライアント/サーバー通信を有効にする必要があります。

始める前に

「クライアントの追加」ウィザードを使用してクライアントを登録した場合は、そのプロセス中に取得した、クライアント・オプション・ファイルのオプション値を検索してください。 その値を使用して、ポートを指定することができます。

このタスクについて

重要 : サーバーまたはストレージ・エージェントによって使用されているセッションが終了される可能性がある方法でファイアウォールを構成しないでください。有効なセッションが終了すると、予測不能な結果が生じる可能性があります。入出力エラーが原因で、プロセスおよびセッションが終了したように見えることがあります。除外セッションがタイムアウト制限にかからないようにす

るには、IBM Spectrum Protect コンポーネントの既知のポートを構成します。**KEEPALIVE** サーバー・オプションがデフォルト値の YES に設定されたままであることを確認します。こうすると、クライアント/サーバー通信が確実に中断されなくなります。**KEEPALIVE** サーバー・オプションの設定手順については、KEEPALIVE を参照してください。

手順

以下のポートを開いて、ファイアウォール経由のアクセスを許可します。

バックアップ/アーカイブ・クライアント、コマンド・ライン管理クライアント、およびクライアント・スケジューラー用の TCP/IP ポート
クライアント・オプション・ファイルで **tcpport** オプションを使用して、ポートを指定します。クライアント・オプション・ファイル内の **tcpport** オプションは、サーバー・オプション・ファイル内の **TCPPORT** オプションと一致している必要があります。デフォルト値は 1500 です。 デフォルト以外の値を使用する場合は、1024 から 32767 の範囲内の数値を指定します。

Web クライアントとリモート・ワークステーションの間の通信を可能にするための HTTP ポート
リモート・ワークステーションのクライアント・オプション・ファイルで **httpport** オプションを設定することにより、リモート・ワークステーション用のポートを指定します。デフォルト値は 1581 です。

リモート・ワークステーション用の TCP/IP ポート
デフォルト値 0 (ゼロ) を指定すると、2 つの空きポート番号がリモート・ワークステーションにランダムに割り当てられます。ポート番号がランダムに割り当てられないようにするには、リモート・ワークステーションのクライアント・オプション・ファイルで **webports** オプションを設定して値を指定します。

管理セッション用の TCP/IP ポート
サーバーが管理クライアント・セッションの要求を待機するポートを指定します。クライアントの **tcpadminport** オプションの値は、**TCPADMINPORT** サーバー・オプションの値と一致している必要があります。こうすると、プライベート・ネットワーク内の管理セッションを保護できます。

クライアントの操作の管理

Operations Center ではエラーを解決するための提案を提供しているので、それを使用してバックアップ/アーカイブ・クライアントに関連したエラーを評価して解決することができます。その他のタイプのクライアントでのエラーについては、クライアント上のエラー・ログを調べて、製品資料を確認する必要があります。

このタスクについて

場合によっては、クライアント・アクセプターを停止してから開始することで、クライアント・エラーを解決できることがあります。クライアント・ノードまたは管理者 ID がロックされている場合は、クライアント・ノードまたは管理者 ID をアンロックすることで問題を解決してから、パスワードをリセットすることができます。

クライアント・エラーの特定および解決に関する詳細な手順については、クライアントの問題の解決を参照してください。

クライアント・エラー・ログのエラーの評価

Operations Center からの提案を取得するか、クライアント上のエラー・ログを調べると、クライアント・エラーを解決することができます。

始める前に

Linux オペレーティング・システムまたは Windows オペレーティング・システムでバックアップ/アーカイブ・クライアントのエラーを解決するには、クライアント管理サービスがインストール済みで開始されていることを確認してください。インストールの手順については、56 ページの『クライアント管理サービス

のインストール』を参照してください。インストールの検証手順については、56 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』を参照してください。

手順

クライアント・エラーを診断して解決するには、以下のいずれかの処置を行ってください。

- クライアント管理サービスがクライアント・ノードにインストールされている場合は、以下の手順を実行してください。
  a) Operations Center の「概要」ページで、「**クライアント**」をクリックして、クライアントを選択します。
  b)「**詳細**」をクリックします。
  c) クライアントの「要約」ページで、「**診断**」タブをクリックします。
  d) 取得したログ・メッセージを確認します。

  ヒント:

  –「クライアント・ログ」ペインを表示するか非表示にするには、「クライアント・ログ」バーをダブルクリックします。
  –「クライアント・ログ」ペインのサイズを変更するには、「クライアント・ログ」バーをクリックしてドラッグします。

  「診断」ページに提案が表示された場合は、提案を選択します。「クライアント・ログ」ペインで、提案に関連するクライアント・ログ・メッセージが強調表示されます。
  e) 提案を使用して、エラー・メッセージに示された問題を解決します。

  ヒント: 提案は、クライアント・メッセージのサブセットでのみ提供されます。
- クライアント管理サービスがクライアント・ノードにインストールされていない場合は、インストール済みのクライアントのエラー・ログを確認してください。

クライアント・アクセプターの停止および再始動

ソリューションの構成を変更する場合、バックアップ/アーカイブ・クライアントがインストールされているすべてのクライアント・ノードでクライアント・アクセプターを再開する必要があります。

このタスクについて

場合によっては、クライアント・アクセプターを停止してから再開することにより、クライアント・スケジューリングの問題を解決できることがあります。スケジュールされた操作を確実にクライアントで実行できるように、クライアント・アクセプターが実行されている必要があります。例えば、サーバーの IP アドレスまたはドメイン名を変更する場合、クライアント・アクセプターを再開する必要があります。

手順

クライアント・ノードにインストールされているオペレーティング・システムの手順に従ってください。

AIX および Oracle Solaris

- クライアント・アクセプターを停止するには、以下のステップを完了させます。
  a. コマンド・ラインで次のコマンドを発行して、クライアント・アクセプターのプロセス ID を判別します。

  ```
  ps -ef | grep dsmcad
  ```

  出力を確認します。次の出力例では、6764 がクライアント・アクセプターのプロセス ID です。

  ```
  root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
  ```

  b. コマンド・ラインで以下のコマンドを発行します。

```
kill -9 PID
```

ここで、*PID* は、クライアント・アクセプターのプロセス ID を指定します。

- クライアント・アクセプターを開始するには、コマンド・ラインで次のコマンドを発行します。

```
/usr/bin/dsmcad
```

Linux

- クライアント・アクセプターを (再開せずに) 停止するには、次のコマンドを発行します。

```
# service dsmcad stop
```

- クライアント・アクセプターを停止して再始動するには、次のコマンドを実行します。

```
# service dsmcad restart
```

MAC OS X

「**アプリケーション**」 > 「**ユーティリティー**」 > 「**端末 (Terminal)**」をクリックします。

- クライアント・アクセプターを停止するには、以下のコマンドを発行します。

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- クライアント・アクセプターを開始するには、以下のコマンドを発行します。

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- クライアント・アクセプター・サービスを停止するには、以下のステップを完了させます。
  a. 「**スタート**」 > 「**管理ツール**」 > 「**サービス**」をクリックします。
  b. クライアント・アクセプター・サービスをダブルクリックします。
  c. 「**停止**」をクリックしてから、「**OK**」をクリックします。
- クライアント・アクセプター・サービスを再始動するには、以下のステップを完了させます。
  a. 「**スタート**」 > 「**管理ツール**」 > 「**サービス**」をクリックします。
  b. クライアント・アクセプター・サービスをダブルクリックします。
  c. 「**開始**」をクリックしてから、「**OK**」をクリックします。

関連情報

クライアントのスケジューリング問題の解決

パスワードの再設定

クライアント・ノードまたは管理者 ID のパスワードを紛失したり忘れたりした場合は、パスワードをリセットできます。誤ったパスワードを使用してシステムへのアクセスを複数回試みると、クライアント・ノードまたは管理者 ID がロックされる場合があります。この問題を解決する手順を実行できます。

手順

パスワードの問題を解決するには、以下のいずれかの処置を行ってください。

- バックアップ/アーカイブ・クライアントがクライアント・ノードにインストールされていて、パスワードを紛失したり忘れたりした場合は、以下の手順を実行します。
  1. **UPDATE NODE** コマンドを発行して、新規パスワードを生成します。

```
update node node_name new_password forcepwreset=yes
```

ここで、*node_name* にはクライアント・ノードを指定し、*new_password* には割り当てるパスワードを指定します。

2. 変更したパスワードについて、クライアント・ノードの所有者に通知します。クライアント・ノードの所有者が指定のパスワードでログインすると、新規パスワードが自動的に生成されます。セキュリティーを強化するため、このパスワードはユーザーには表示されません。

   ヒント: 以前にクライアント・オプション・ファイルで **passwordaccess** オプションを generate に設定した場合は、パスワードが自動的に生成されます。

- パスワードの問題が原因で管理者がロックアウトされた場合は、以下の手順を実行します。

1. サーバーへのアクセス権限を管理者に付与するには、**UNLOCK ADMIN** コマンドを発行します。手順については、UNLOCK ADMIN (管理者のアンロック)を参照してください。
2. **UPDATE ADMIN** コマンドを使用して新規パスワードを設定します。

   ```
   update admin admin_name new_password forcepwreset=yes
   ```

   ここで、*admin_name* には管理者の名前を指定し、*new_password* には割り当てるパスワードを指定します。

- クライアント・ノードがロックされている場合、以下の手順を実行します。

1. クライアント・ノードがロックされている理由と、そのクライアント・ノードをアンロックする必要があるかどうかを判別します。例えば、クライアント・ノードが廃止されている場合、そのクライアント・ノードは実稼働環境から除去されています。廃止操作を元に戻すことはできないため、クライアント・ノードはロックされたままになります。また、クライアント・データが法的調査の対象である場合に、クライアント・ノードがロックされることもあります。
2. クライアント・ノードをアンロックする必要がある場合は、**UNLOCK NODE** コマンドを使用します。手順については、UNLOCK NODE (クライアント・ノードのアンロック)を参照してください。
3. **UPDATE NODE** コマンドを発行して、新規パスワードを生成します。

   ```
   update node node_name new_password forcepwreset=yes
   ```

   ここで、*node_name* にはノードの名前を指定し、*new_password* には割り当てるパスワードを指定します。

4. 変更したパスワードについて、クライアント・ノードの所有者に通知します。クライアント・ノードの所有者が指定のパスワードでログインすると、新規パスワードが自動的に生成されます。セキュリティーを強化するため、このパスワードはユーザーには表示されません。

   ヒント: 以前にクライアント・オプション・ファイルで **passwordaccess** オプションを generate に設定した場合は、パスワードが自動的に生成されます。

クライアント・バックアップの範囲の変更

クライアント・バックアップ操作をセットアップする場合、不要なオブジェクトを除外する方法をお勧めします。例えば、バックアップ操作から一時ファイルを除外したい場合が多くあります。

このタスクについて

バックアップ操作から不要なオブジェクトを除外すると、バックアップ操作に必要なストレージ・スペースの量とストレージのコストを管理しやすくなります。 ライセンス交付パッケージによっては、ライセンス交付のコストを制限できる場合もあります。

手順

バックアップの適用範囲を変更する方法は、クライアント・ノードにインストールされている製品によって異なります。

- バックアップ/アーカイブ・クライアントの場合、include-exclude リストを作成して、ファイル、ファイル・グループ、あるいはディレクトリーをバックアップ操作に組み込みこんだり、バックアップ操作

から除外したりすることができます。 include-exclude リストを作成するには、包含/除外リストの作成の手順に従います。

1 つのタイプのすべてのクライアントに対して、確実に include-exclude リストを一貫して使用するために、必要なオプションが含まれるサーバー上にクライアント・オプション・セットを作成することができます。 その後、クライアント・オプション・セットを同じタイプの各クライアントに割り当てます。 詳細については、クライアント・オプション・セットによるクライアント操作の制御を参照してください。

- バックアップ/アーカイブ・クライアントの場合、**domain** オプションを使用して、差分バックアップ操作に含めるオブジェクトを指定することができます。ドメイン・オプション の指示に従ってください。
- その他の製品の場合、バックアップ操作に含めるオブジェクトおよびバックアップ操作から除外するオブジェクトを定義するには、製品資料の手順に従ってください。

クライアント・アップグレードの管理

クライアントのフィックスパックまたは暫定修正が入手可能になると、製品の改善点を利用するためにクライアントをアップグレードすることができます。サーバーおよびクライアントは、さまざまな時点で、さまざまなレベルにアップグレードできますが、いくつかの制約事項があります。

始める前に

1. IBM Spectrum Protect のサーバーとクライアントの互換性とアップグレードの考慮事項でクライアント/サーバーの互換性要件を確認します。ソリューションに V7.1 より前のレベルのサーバーまたはクライアントが含まれている場合、ガイドラインを調べて、クライアント・バックアップおよびアーカイブの操作が中断されないようにしてください。
2. Supported Operating Systems で、クライアントのシステム 要件を確認します。
3. ソリューションにストレージ・エージェントまたはライブラリー・クライアントが含まれている場合、ライブラリー・マネージャーとして構成されているサーバーとのストレージ・エージェントおよびライブラリー・クライアントの互換性に関する情報を確認してください。 IBM Spectrum Protect サーバーとストレージ・エージェントおよびライブラリー・クライアントの互換性 を参照してください。

   ライブラリー・マネージャーおよびライブラリー・クライアントをアップグレードする 予定の場合は、最初にライブラリー・マネージャーをアップグレードする 必要があります。

手順

ソフトウェアをアップグレードするには、以下の表にリストされた手順を実行します。

ソフトウェア	説明へのリンク
IBM Spectrum Protect バックアップ/アーカイブ・クライアント	• クライアント更新のスケジュール
IBM Spectrum Protect Snapshot	• for UNIX and Linux のインストールおよびアップグレード • for VMware のインストールおよびアップグレード • for Windows のインストールおよび更新
IBM Spectrum Protect for Databases	• Data Protection for SQL Server のアップグレード • Data Protection for Oracle のインストール • のインストール、アップグレード、およびマイグレーション
IBM Spectrum Protect for Enterprise Resource Planning	• のアップグレード • のアップグレード

ソフトウェア	説明へのリンク
IBM Spectrum Protect for Mail	• UNIX、AIX、または Linux システムへの Data Protection for IBM Domino のインストール (V7.1.0) • Windows システムへの Data Protection for IBM Domino のインストール (V7.1.0) • のインストール、アップグレード、およびマイグレーション
IBM Spectrum Protect for Virtual Environments	• のインストールおよびアップグレード • Data Protection for Microsoft Hyper-V のインストールとアップグレード

クライアント・ノードの廃止

クライアント・ノードが不要になった場合、実稼働環境から削除するためのプロセスを開始できます。例えば、ワークステーションが IBM Spectrum Protect サーバーにデータをバックアップしていて、ワークステーションが使用されなくなった場合、ワークステーションを廃止できます。

このタスクについて

廃止プロセスを開始すると、サーバーは、クライアント・ノードをロックして、サーバーにアクセスできないようにします。クライアント・ノードに属するファイルは段階的に削除され、その後クライアント・ノードが削除されます。以下のタイプのクライアント・ノードを廃止できます。

アプリケーション・クライアント・ノード
アプリケーション・クライアント・ノードには、E メール・サーバー、データベース、およびその他のアプリケーションなどがあります。例えば、以下のすべてのアプリケーションがアプリケーション・クライアント・ノードです。

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

システム・クライアント・ノード
システム・クライアント・ノードには、ワークステーション、Network Attached Storage (NAS) ファイル・サーバー、および API クライアントなどがあります。

仮想マシン・クライアント・ノード
仮想マシン・クライアント・ノードは、ハイパーバイザー内の個々のゲスト・ホストで構成されます。各仮想マシンは、ファイル・スペースとして表示されます。

制約事項: オブジェクト・クライアント・ノードを廃止することはできません。

クライアント・ノードを廃止するための最も単純な方法は、Operations Center を使用することです。廃止プロセスはバックグラウンドで実行されます。クライアントがクライアント・データを複製するように構成されている場合、Operations Center は、クライアントを廃止する前に、ソース複製サーバーとターゲット複製サーバー上の複製からクライアントを自動的に削除します。

ヒント: あるいは、**DECOMMISSION NODE** コマンドまたは **DECOMMISSION VM** コマンドを発行して、クライアント・ノードを廃止できます。この方法は、以下の場合に使用できます。

- 将来の廃止プロセスをスケジュールするか、スクリプトを使用して一連のコマンドを実行するには、廃止プロセスをバックグラウンドで実行することを指定します。
- デバッグの目的で廃止プロセスをモニターするには、廃止プロセスをフォアグラウンドで実行することを指定します。フォアグラウンドでプロセスを実行する場合は、他のタスクを続行する前に処理が完了するまで待つ必要があります。

手順

以下のいずれかのアクションを実行します。

- Operations Center を使用してバックグラウンドでクライアントを廃止するには、以下の手順を実行します。
  a) Operations Center の「**概要**」ページで、「**クライアント**」をクリックして、クライアントを選択します。
  b)「**その他**」 > 「**廃止**」をクリックします。
- 管理コマンドを使用してクライアント・ノードを廃止するには、以下の手順を実行します。
  a) **QUERY NODE** コマンドを発行して、クライアント・ノードがノード複製用に構成されているかどうかを判別します。
  例えば、クライアント・ノードの名前が AUSTIN である場合、次のコマンドを実行します。

  ```
  query node austin format=detailed
  ```

  「**複製状態**」出力のフィールドを確認します。
  b) クライアント・ノードが複製用に構成されている場合、**REMOVE REPLNODE** コマンドを発行して、クライアント・ノードを複製から除去します。
  例えば、クライアント・ノードの名前が AUSTIN である場合、次のコマンドを発行します。

  ```
  remove replnode austin
  ```

  c) 以下のいずれかのアクションを実行します。
  – アプリケーションまたはシステムのクライアント・ノードをバックグラウンドで廃止するには、**DECOMMISSION NODE** コマンドを発行します。例えば、クライアント・ノードの名前が AUSTIN である場合、次のコマンドを発行します。

  ```
  decommission node austin
  ```

  – アプリケーションまたはシステムのクライアント・ノードをフォアグラウンドで廃止するには、**DECOMMISSION NODE** コマンドを発行して、wait=yes パラメーターを指定します。例えば、クライアント・ノードの名前が AUSTIN である場合、次のコマンドを発行します。

  ```
  decommission node austin wait=yes
  ```

  – 仮想マシンをバックグラウンドで廃止するには、**DECOMMISSION VM** コマンドを発行します。例えば、データ・センター・ノードが AUSTIN でファイル・スペース ID が 7 の場合、以下のコマンドを発行します。

  ```
  decommission vm austin 7 nametype=fsid
  ```

  仮想マシン名に 1 つ以上のスペースが含まれている場合、名前を二重引用符で囲みます。例えば、仮想マシン名が CODY 2 でファイル・スペース名が ¥VMFULL-CODY 2 の場合、以下のコマンドを発行します。

  ```
  decommission vm austin "\vmfull-cody 2"
  ```

  – 仮想マシンをフォアグラウンドで廃止するには、**DECOMMISSION VM** コマンドを発行して、wait=yes パラメーターを指定します。例えば、次のコマンドを発行します。

  ```
  decommission vm austin 7 nametype=fsid wait=yes
  ```

  仮想マシン名に 1 つ以上のスペースが含まれている場合、名前を二重引用符で囲みます。例えば、仮想マシン名が CODY 2 でファイル・スペース名が ¥VMFULL-CODY 2 の場合、以下のコマンドを発行します。

  ```
  decommission vm austin "\vmfull-cody 2" wait=yes
  ```

次のタスク

プロセスを実行した直後にユーザー・インターフェースやコマンド出力にエラー・メッセージが表示される場合がありますので、それを注意して確認します。

クライアント・ノードが廃止されたことを確認できます。

1. Operations Center の「**概要**」ページで、「**クライアント**」をクリックします。
2. 「クライアント」テーブルの「危険」列で、以下のような状態を確認します。
   - 「DECOMMISSIONED」状態は、ノードが廃止されていることを示します。
   - ヌル値は、ノードが廃止されていないことを示します。
   - 「PENDING」状態は、 ノードを廃止中であるか、廃止プロセスが失敗したことを示します。

   ヒント: 保留中の廃止プロセスの状況を確認したい場合は、次のコマンドを実行します。

   ```
   query process
   ```
3. コマンドの出力を確認します。
   - 廃止プロセスが進行中の場合、そのプロセスについての状況が表示されます。例えば次のとおりです。

   ```
   query process

    Process     Process Description           Process Status
     Number
   --------     --------------------     -------------------------------------------
          3          DECOMMISSION NODE        Number of backup objects deactivated
                                              for node NODE1: 8 objects deactivated.
   ```
   - 廃止プロセスについての状況が表示されなくて、エラー・メッセージも表示されない場合は、プロセスが完了していません。ノードに関連付けられたファイルがまだ非活動化されていない場合、プロセスが完了しない場合があります。 ファイルが非活動状態になったあと、廃止プロセスを再度実行してください。
   - 廃止プロセスについての状況が表示されなくて、エラー・メッセージが表示される場合は、プロセスが失敗しています。廃止プロセスを再度実行してください。

関連情報

DECOMMISSION NODE (クライアント・ノードの廃止)

DECOMMISSION VM (仮想マシンの廃止)

QUERY NODE (ノードの照会)

REMOVE REPLNODE (複製からのクライアント・ノードの除去)

ストレージ・スペースを解放するためのデータの非活動化

場合によっては、IBM Spectrum Protect サーバーに保管されているデータを非活動化することができます。非活動化プロセスを実行すると、指定された日時より前に保管されたすべてのバックアップ・データが非活動化され、有効期限が切れると削除されます。こうすると、サーバー上のスペースを解放できます。

このタスクについて

一部のアプリケーション・クライアントは常にデータを活動バックアップ・データとしてサーバーに保存します。活動バックアップ・データはインベントリー満了ポリシーによって管理されていないので、そのデータは自動的に削除されず、サーバーのストレージ・スペースを無期限に使用します。不要なデータによって使用されているストレージ・スペースを解放するために、データを非活動化することができます。

非活動化プロセスを実行すると、指定された日付より前に保管されたすべての活動バックアップ・データが非活動状態になります。データは、有効期限が切れると削除され、リストアできません。非活動化機能は、Oracle データベースを保護するアプリケーション・クライアントにのみ適用されます。

手順

1. Operations Center の「概要」ページで、「**クライアント**」をクリックします。
2. 「クライアント」テーブルで、1 つ以上のクライアントを選択して、「**その他**」>「**クリーンアップ (Clean Up)**」をクリックします。

   コマンド・ライン方式 : DEACTIVATE DATA コマンドを使用して、データを非活動化します。

関連情報

DEACTIVATE DATA (クライアント・ノードのデータの非活動化)

データ・ストレージの管理

効率性を高めるためにデータを管理し、クライアント・データを保管するためのサポート対象装置およびメディアをサーバーに追加します。

関連情報

ストレージ・プール・タイプ

ストレージ・プール・コンテナーの監査

データベース情報とストレージ・プール内のコンテナーとの間に不整合がないかを検査するために、ストレージ・プール・コンテナーを監査します。

このタスクについて

以下の状況で、ストレージ・プール・コンテナーを監査します。

- **QUERY DAMAGED** コマンドを発行したときに、問題が検出された場合
- サーバーが損傷データ・エクステントに関するメッセージを表示した場合
- ハードウェアが問題を報告して、ストレージ・プール・コンテナーに関連するエラー・メッセージが表示された場合

手順

1. ストレージ・プール・コンテナーを監査するには、**AUDIT CONTAINER** コマンドを発行します。
   例えば、`000000000000076c.dcf` というコンテナーを監査するには、次のコマンドを発行します。

   ```
   audit container c:¥tsm-storage¥07¥000000000000076c.dcf
   ```

2. ANR4891I メッセージの出力を参照し、損傷データ・エクステントに関する情報を確認します。

次のタスク

ストレージ・プール・コンテナーの問題を検出した場合、構成に基づいてデータをリストアすることができます。**REPAIR STGPOOL** コマンドを使用して、ストレージ・プール内のコンテンツを修復できます。

制約事項 : ストレージ・プールのコンテンツを修復できるのは、**PROTECT STGPOOL** コマンドを使用してストレージ・プールを保護している場合だけです。

関連情報

AUDIT CONTAINER (ディレクトリー・コンテナー・ストレージ・プールのデータベース情報の整合性の検査)

QUERY DAMAGED (ディレクトリー・コンテナー・ストレージ・プールまたはクラウド・コンテナー・ストレージ・プールの損傷データの照会)

インベントリー容量の管理

データベース、活動ログ、およびアーカイブ・ログの容量を管理して、ログの状況に基づいてタスク用にインベントリーがサイジングされていることを確認します。

始める前に

活動ログとアーカイブ・ログには以下の特性があります。

- 活動ログは最大サイズ 512 GB にすることができます。ご使用のシステム用の活動ログのサイジングについて詳しくは、ストレージ・アレイの計画を参照してください。
- アーカイブ・ログ・サイズは、それがインストールされているファイル・システムのサイズに 制限されます。 アーカイブ・ログのサイズは、活動ログのように定義済みサイズで維持されません。アーカイブ・ログ・ファイルは、必要がなくなったときに自動的に削除されます。

ベスト・プラクティスとして、アーカイブ・ログ・ディレクトリーがフルになった場合にアーカイブ・ログ・ファイルを保管するために、オプションでアーカイブ・フェイルオーバー・ログを作成することができます。

フルになっているインベントリーのコンポーネントを判別するには、Operations Center を確認します。いずれかのインベントリー・コンポーネントのサイズを増やす前に、必ずサーバーを停止してください。

手順

- データベースのサイズを 増やすには、以下の手順を実行します。
  - 別々のドライブまたはファイル・システムで、データベースのディレクトリーを 1 つ以上作成します。
  - **EXTEND DBSPACE** コマンドを実行して、データベースに 1 つ以上のディレクトリーを追加します。このディレクトリーは、データベース・マネージャーのインスタンス・ユーザー ID からアクセス可能でなければなりません。デフォルトで、データはすべてのデータベース・ディレクトリー全体に再配布され、スペースはレクラメーション処理されます。

    ヒント :

    - データの再配布とスペースのレクラメーション処理を実行するのに必要な時間は、ご使用のデータベースのサイズに応じて変化します。適切な計画を立てていることを確認してください。
    - データベース操作での並列処理の整合度を確保するために、必ず既存のディレクトリーと同じサイズのディレクトリーを指定してください。 データベース用のディレクトリーの中に他のディレクトリーより小さいものが 1 つ以上ある場合、並列プリフェッチおよびデータベース 分散が最適化される可能性が低下します。
  - サーバーを一時停止してから再始動して、新規ディレクトリーを完全に使用します。
  - 必要な場合は、データベースを再編成してください。サーバー・データベースの索引および表の再編成を行うと、予期しないデータベースの増加やパフォーマンスの問題を回避するために役立ちます。データベースの再編成について詳しくは、Tivoli Storage Manager V7.1.1.200 以降のサーバーのデータベースの拡大とパフォーマンス低下問題の解決と防止 を参照してください。
- V7.1 以降のサーバーでデータベースのサイズを 減らすには、サーバー・インスタンス・ディレクトリーから以下の IBM Db2 コマンドを発行します。

  制約事項 : これらのコマンドは入出力アクティビティーを 増やすので、サーバーのパフォーマンスに影響を与える可能性があります。パフォーマンス上の問題を最小限に抑えるために、1 つのコマンドが完了するまで待ってから、次のコマンドを発行してください。Db2 コマンドは、サーバーの実行中に発行することができます。

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
```

```
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
```

- 活動ログのサイズを増やすか減らすには、以下の手順を実行します。

  a) 活動ログの場所に、増加したログ・サイズに必要なスペースがあることを確認します。 ログ・ミラーがある場合は、この場所にも増加したログ・サイズに十分なスペースが必要です。

  b) サーバーを停止します。

  c) dsmserv.opt ファイルで、**ACTIVELOGSIZE** オプションを活動ログの新規サイズ (メガバイト単位) に更新します。

  活動ログ・ファイルのサイズは、ACTIVELOGSIZE オプションの値に基づきます。スペース所要量についてのガイドラインを以下の表に示します。

表 *17.* ボリュームおよびファイルのスペース 要件の見積もり方法	
ACTIVELOGSize オプションの値	**ACTIVELOGSize スペースに加えて、活動ログ・ディレクトリー内に予約するフリー・スペース容量**
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

  活動ログのサイズを最大サイズ 512 GB に変更するには、次のサーバー・オプションを入力します。

```
activelogsize 524288
```

  d) 新しい活動ログ・ディレクトリーを使用する計画の場合は、**ACTIVELOGDIRECTORY** サーバー・オプションに指定したディレクトリー名を更新します。新しいディレクトリーは空であり、データベース・マネージャーのユーザー ID からアクセス可能でなければなりません。

  e) サーバーを再始動します。

- ストレージに必要なスペースの量を減らすには、アーカイブ・ログを圧縮します。
次のコマンドを発行して、アーカイブ・ログの動的圧縮を有効にします。

```
setopt archlogcompress yes
```

制約事項 : ボリュームの使用率が高く、過重な作業負荷が続くシステムで **ARCHLOGCOMPRESS** サーバー・オプションを使用可能にする場合には、注意が必要です。このようなシステム環境でこのオプションを使用可能にすると、活動ログ・ファイル・システムからアーカイブ・ログ・ファイル・システムへのログ・ファイルのアーカイブが遅延する可能性があります。この遅延によって、活動ログ・ファイル・システムがスペース 不足になる場合があります。アーカイブ・ログ圧縮が使用可能になった後で、必ず、活動ログ・ファイル・システム内の使用可能なスペースをモニターしてください。活動ログ・ディレクトリー・ファイル・システムの 使用量がスペース不足状態に近づいてきたら **ARCHLOGCOMPRESS** サーバー・オプシ ョンを使用不可にする必要があります。 **SETOPT** コマンドを使用すると、サーバーを一時停止せずに、アーカイブ・ログの圧縮を即座に使用不可にできます。

関連情報

ACTIVELOGSIZE サーバー・オプション
EXTEND DBSPACE (データベースのスペースの拡張)
SETOPT (動的更新用サーバー・オプションの設定)

メモリーおよびプロセッサーの使用量の管理

サーバーがバックアップやデータ重複排除などのデータ・プロセスを実行できるように、必ず、メモリー要件およびプロセッサー使用量を管理してください。特定のプロセスを実行するときのパフォーマンスへの影響を検討してください。

始める前に

- ご使用の構成が、必要なハードウェアおよびソフトウェアを使用していることを確認します。詳細については、 Supported Operating Systems を参照してください。
- データベース・ログおよびリカバリー・ログなどのリソースの管理について詳しくは、ストレージ・アレイの計画を参照してください。
- システム・メモリーをさらに追加して、パフォーマンスが向上するかどうかを判別します。メモリー使用量を定期的にモニターし、追加メモリーが必要かどうかを判別してください。

手順

1. 可能な場合は、ファイル・システム・キャッシュからメモリーを解放します。
2. システム上の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ます。各サーバーのデータベース・マネージャーが使用できるシステム・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、その他のサーバーがテスト・サーバーの場合は、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てください。
3. 専用メモリーが使い尽くされないようにするために、データベースのユーザー・データ制限および専用メモリーを設定します。専用メモリーを使い尽くすと、エラーが発生したり、パフォーマンスが最適にならなかったり、システムが不安定になったりする可能性があります。

スケジュール済み活動のチューニング

保守タスクを毎日スケジュールし、ソリューションが正しく動作するようにしてください。 ソリューションのチューニングにより、サーバー・リソースを最大限に活用して、ソリューションで利用可能な各種の機能を効果的に使用します。

手順

1. 定期的にシステム・パフォーマンスをモニターし、クライアント・バックアップ・タスクおよびサーバー保守タスクが正常に完了していることを確認します。 63 ページの『第 3 部 マルチサイト・ディスク・ソリューションのモニター』 の指示に従ってください。
2. オプション: モニター情報でサーバー・ワークロードが増加していることが示された場合は、計画情報を再検討してください。 以下のケースでシステムの 容量が適切であるかを確認します。
   - クライアント数が増加した場合
   - バックアップするデータ量が増加した場合
   - バックアップに使用可能な時間が変更された場合
3. ソリューションが、期待するレベルで実行されているかを確認します。
   クライアント・スケジュールを参照し、タスクがスケジュールされた時間フレーム内に完了しているかを確認します。
   a. Operations Center の「**クライアント**」ページで、クライアントを選択します。
   b.「**詳細**」をクリックします。

c. クライアントの「**要約**」ページから、「**バックアップ済み**」および「**複製済み**」アクティビティーを確認し、リスクがないかを識別します。

必要に応じて、クライアント・バックアップ操作の時間および頻度を調整します。

4. 以下の保守タスクについて、24 時間以内に正常に完了するように、十分な時間をスケジュールします。
   a. ストレージ・プールを保護します。
   b. ノード・データを複製します。
   c. データベースのバックアップを取ります。
   d. 満了処理を実行し、サーバー・ストレージからクライアント・バックアップおよびアーカイブ・ファイルのコピーを削除します。

ヒント: 適切な時間に正しい順序で開始されるように、保守タスクをスケジュールします。 例えば、クライアント・バックアップが正常に完了した後に複製タスクをスケジュールします。

関連タスク

サーバー保守アクティビティーのスケジュールの 定義

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

関連情報

データの重複排除 (V7.1.1)

パフォーマンス

サーバーから別のサーバーへのクライアントの移動

サーバー上のスペースが不足することを回避するため、あるいはワークロードの問題を解決するために、クライアント・ノードをサーバー間で移動する必要がある場合があります。

始める前に

ソリューションに必要な容量を計画し、クライアント・ノード用に十分なスペース (将来の成長に備えたスペースも含む) をサーバー上に確保してください。

このタスクについて

クライアント・ノードを移動する場合、既存のバックアップを元のサーバー上に残し、満了ポリシーに従って有効期限切れにすることも、既存のバックアップを新規サーバーにエクスポートすることもできます。

手順

クライアント・ノードを別のサーバーに移動するには、以下の手順を実行します。

1. **EXPORT NODE** コマンドを使用して、クライアント・ノードを新規サーバーに直接エクスポートします。
2. 新規サーバー名を使用して、クライアント・オプション・ファイルを更新します。
3. 新規サーバー上で、クライアント・ノードがデータをバックアップするためのスケジュールを 割り当てます。
   a. Operations Center の「**クライアント**」ページで、クライアント・ノードを選択します。
   b.「**その他**」>「**スケジュールのアソシエーション**」をクリックします。
   c. 選択したクライアント・ノードを割り当てるスケジュールの行のチェック・ボックスを選択します。
   d.「**保存**」をクリックします。
4. **EXPORT NODE** コマンドを再発行し、元のサーバーから新規サーバーにデータを増分エクスポートします。 データを増分エクスポートすることで、最初にエクスポート処理してからクライアント・ノードにスケジュールを割り当てるまでの間にバックアップされたデータがエクスポートされます。
5. クライアント・ノードをモニターし、設定したスケジュールに従ってデータがバックアップされていることを確認し、クライアント・ノードにリスクがないかをモニターします。「**クライアント**」の上にカーソルを移動し、「**スケジュール**」をクリックします。

6. 以下のステップを実行して、元のサーバーからクライアント・ノードを廃止します。
   a. Operations Center の「**概要**」ページで、「**クライアント**」をクリックします。
   b.「**クライアント**」テーブルで、クライアント・ノードを選択します。
   c.「**その他**」>「**廃止**」をクリックします。

   元のサーバーからクライアント・ノードが除去されます。ポリシー設定の指定に従ってデータの有効期限が切れると、クライアント・ノード・データが削除されます。クライアント・ノード・データが削除された後、クライアントがサーバーから除去されます。

関連情報

EXPORT NODE (クライアント・ノード情報のエクスポート)

IMPORT NODE (クライアント・ノード情報のインポート)

複製の管理

複製は、災害復旧サイトでデータをリカバリーするため、およびソース・サーバーとターゲット・サーバーで同じレベルのファイルを維持するために使用します。ノード・レベルで複製を管理することができます。また、ストレージ・プール・レベルでデータを保護することもできます。

複製の互換性

IBM Spectrum Protect での複製操作をセットアップする前に、ソース複製サーバーとターゲット複製サーバーが複製について互換性があることを確認する必要があります。

表 *18.* サーバー・バージョンの複製の互換性

ソース複製サーバーのバージョン	**ターゲット複製サーバーとして互換性のあるバージョン**
V7.1	V7.1 以降
V7.1.1	V7.1 以降
V7.1.3	V7.1.3 以降
V7.1.4	V7.1.3 以降
V7.1.5	V7.1.3 以降
V7.1.6	V7.1.3 以降
V7.1.7	V7.1.3 以降
V7.1.8	V7.1.3 以降
V8.1	V7.1.3 以降
V8.1.1	V7.1.3 以降
V8.1.2	V7.1.3 以降
V8.1.3	V7.1.3 以降
V8.1.4	V7.1.3 以降
V8.1.5	V7.1.3 以降
V8.1.6	V7.1.3 以降
V8.1.7	V7.1.3 以降

表 18. サーバー・バージョンの複製の互換性 (続き)	
ソース複製サーバーのバージョン	**ターゲット複製サーバーとして互換性のあるバージョン**
V8.1.8	V8.1.8、V8.1.7、V8.1.6、V8.1.1、V7.1.9、V7.1.8、および V7.1.7
V8.1.9	V8.1.9、V8.1.8、V8.1.7、V8.1.6、V8.1.1、V7.1.9、V7.1.8、および V7.1.7
V8.1.10	V8.1.10、V8.1.9、V8.1.8、V8.1.7、V8.1.6、V8.1.1、V7.1.9、V7.1.8、および V7.1.7
V8.1.11	V8.1.11、V8.1.10、V8.1.9、V8.1.8、V8.1.7、V8.1.6、V8.1.1、V7.1.9、V7.1.8、および V7.1.7
V8.1.12	V8.1.12、V8.1.11、V8.1.10、V8.1.9、V8.1.8、V8.1.7、V8.1.6、V8.1.1、V7.1.13、V7.1.12、V7.1.11、V7.1.10、V7.1.9、V7.1.8、および V7.1.7

ノード複製の使用可能化

データを保護するためにノード複製を使用可能にすることができます。

始める前に

ソース・サーバーとターゲット・サーバーが複製について互換性がある必要があります。

このタスクについて

メタデータを含むすべてのクライアント・データを複製するには、クライアント・ノードを複製します。デフォルトでは、サーバーを最初に始動したときにノード複製は使用不可になっています。

ヒント:

- 複製処理時間を短縮するには、クライアント・ノードを複製する前に、ストレージ・プールを保護します。 ノード複製が開始されると、ストレージ・プール保護によって既に複製されているデータ・エクステントはスキップされます。
- 複製の処理を完了するには、メモリー量の増加と十分な帯域幅が必要です。 トランザクションを確実に完了できるように、データベースとそのログのサイズを調整します。

手順

ノード複製を使用可能にするには、Operations Center で以下の手順を実行します。

a)「**サーバー**」ページで、「**詳細**」をクリックします。

b)「**詳細**」ページで、「**プロパティー**」をクリックします。

c)「**複製**」セクションで、「**アウトバウンド複製**」フィールドの「**使用可能**」を選択します。

d)「**保存**」をクリックします。

次のタスク

オプションで、次のうちの 1 つまたは両方のアクションを実行します。

- 複製が正常に行われたことを確認するには、63 ページの『日次モニター・チェックリスト』を参照してください。
- Linux IBM Spectrum Protect サーバーがノードをリモート・サーバーに複製する場合、Aspera® Fast Adaptive Secure Protocol (FASP®) テクノロジーがリモート・サーバーへのデータ・スループットを改善できるかどうかを判別します。 Aspera FASP テクノロジーがシステム 環境内のデータ転送を最適化できるかどうかの確認 の指示に従ってください。

関連資料

複製の互換性

IBM Spectrum Protect での複製操作をセットアップする前に、ソース複製サーバーとターゲット複製サーバーが複製について互換性があることを確認する必要があります。

ディレクトリー・コンテナー・ストレージ・プール内のデータの保護

ディレクトリー・コンテナー・ストレージ・プール内のデータを保護することで、ノード複製の時間が短縮され、ディレクトリー・コンテナー・ストレージ・プール内のデータの修復が可能になります。

始める前に

少なくとも 1 つのディレクトリー・コンテナー・ストレージ・プールがターゲット複製サーバー上に存在していることを確認してください。 Operations Center で複製を有効にする際に、ストレージ・プール保護をスケジュールすることができます。複製を構成し、ストレージ・プール保護を有効にするには、以下のステップを実行します。

1. Operations Center のメニュー・バーで、「**ストレージ**」の上にカーソルを移動して、「**複製**」をクリックします。
2. 「複製」ページで、「**サーバー・ペア**」をクリックします。
3. 「サーバー・ペアの追加」ウィザードのステップをすべて実行します。

このタスクについて

ディレクトリー・コンテナー・ストレージ・プールの保護では、データ・エクステントを別のストレージ・プールにバックアップするため、ノード複製のパフォーマンスを向上させることができます。 ノード複製が開始されると、ストレージ・プール保護によって既にバックアップされたデータ・エクステントはスキップされます。そのため、複製の処理時間が短縮されます。 ストレージ・プールの保護を 1 日に複数回スケジュールして、データの変更に対応することができます。

ストレージ・プールを保護することにより、既存のデータおよびメタデータを複製するリソースを使用しないため、サーバーのパフォーマンスが向上します。ストレージ・プールを保護してバックアップする場合にのみ、ディレクトリー・コンテナー・ストレージ・プールを使用する必要があります。

代替の保護戦略 : 複製を使用する代わりに、データをコンテナー・コピー・ストレージ・プールにコピーすることで、ディレクトリー・コンテナー・ストレージ・プール内のデータを保護することができます。 コンテナー・コピー・ストレージ・プール内のデータは、テープ・ボリュームに保管されます。 オフサイトに保管されたテープ・コピーは、複製環境における追加の災害復旧保護を提供します。

手順

1. あるいは、ストレージ・プール保護を有効にするには、ソース・サーバーから **PROTECT STGPOOL** コマンドを使用して、ディレクトリー・コンテナー・ストレージ・プール内のデータ・エクステントをバックアップすることができます。
   例えば、POOL1 という名前のディレクトリー・コンテナー・ストレージ・プールを保護するには、次のコマンドを発行します。

   ```
   protect stgpool pool1
   ```

   PROTECT STGPOOL コマンドの操作の一部として、ターゲット・ストレージ・プール内の損傷エクステントが修復されます。エクステントは、修復されるためには、ターゲット・サーバー上で既に損傷ありとしてマークされている必要があります。例えば、**AUDIT CONTAINER** コマンドは、**PROTECT STGPOOL** コマンドが発行される前に、ターゲット・ストレージ・プール内の損傷を識別する可能性があります。
2. オプション: 損傷エクステントがターゲット・ストレージ・プールで修復されていて、1 つのターゲット・ストレージ・プール内で複数のソース・ストレージ・プールを保護している場合は、以下のステップを実行して、完全に修復されたことを確認します。

a) 可能な限り多くの損傷を修復するために、すべてのソース・ストレージ・プールに対して **PROTECT STGPOOL** コマンドを発行します。

b) すべてのソース・ストレージ・プールに対して再び **PROTECT STGPOOL** コマンドを発行します。この 2 回目の操作では、**FORCERECONCILE=YES** パラメーターを使用します。

このステップにより、他のソース・プールからの修復がすべてのソース・ストレージ・プールによって適切に認識されるようになります。

タスクの結果

ディレクトリー・コンテナー・ストレージ・プールが保護されている場合、損傷が発生したら、**REPAIR STGPOOL** コマンドを使用してストレージ・プールを修復することができます。

制約事項 : クライアント・ノードを複製しても、ディレクトリー・コンテナー・ストレージ・プールを保護していなければ、ストレージ・プールを修復することはできません。

次のタスク

オプションで、次のうちの 1 つまたは両方のアクションを実行します。

- 複製のワークロードの状況を確認するには、63 ページの『日次モニター・チェックリスト』の指示に従ってください。
- Linux IBM Spectrum Protect サーバーがノードをリモート・サーバーに複製する場合、Aspera Fast Adaptive Secure Protocol (FASP) テクノロジーがリモート・サーバーへのデータ・スループットを改善できるかどうかを判別します。 Aspera FASP テクノロジーがシステム 環境内のデータ転送を最適化できるかどうかの確認 の指示に従ってください。

関連情報

ディレクトリー・コンテナー・ストレージ・プール内のデータの修復およびリカバリー

AUDIT CONTAINER (ディレクトリー・コンテナー・ストレージ・プールのデータベース情報の整合性の検査)

PROTECT STGPOOL (ストレージ・プール・データの保護)

複製設定の変更

Operations Center で複製設定を変更します。複製セッションの数、複製ルール、複製するデータ、複製のスケジュール、および複製ワークロードなどの設定を変更します。

このタスクについて

以下のシナリオで、複製設定のカスタマイズが必要になる場合があります。

- データの優先順位の変更
- 複製ルールの変更
- ターゲット・サーバーとなる別のサーバーに関する要件
- サーバーのパフォーマンスに悪影響を与えるスケジュール済みプロセス

手順

Operations Center を使用して、複製設定を変更します。

タスク	手順
複製ルールを変更します。	a.「**サーバー**」ページで、「**詳細**」をクリックします。 b.「**詳細**」ページで、「**プロパティー**」をクリックします。 c.「**複製**」セクションで、「**デフォルト・アーカイブ・ルール**」、「**デフォルト・バックアップ・ルール**」、または「**デフォルト・スペース管理ルール**」から適用する複製ルールを選択します。 d.「**保存**」をクリックします。
複製レコードを保存する期間を指定します。	a.「**サーバー**」ページで、「**詳細**」をクリックします。 b.「**詳細**」ページで、「**プロパティー**」をクリックします。 c.「**複製**」セクションで、「**複製履歴の保持**」フィールドに複製レコードを保存する必要がある日数を入力します。 あるいは、複製レコードが不要な場合は、「**保存しない**」チェック・ボックスを選択します。 d.「**保存**」をクリックします。
ターゲット複製サーバーを指定します。	a.「**サーバー**」ページで、「**詳細**」をクリックします。 b.「**詳細**」ページで、「**プロパティー**」をクリックします。 c.「**複製**」セクションで、ターゲット・サーバーを指定します。 d.「**保存**」をクリックします。
複製プロセスを取り消します。	a.「**サーバー**」ページで、「**アクティブ・タスク**」をクリックします。 b. 取り消すプロセスまたはセッションを選択します。 c.「**キャンセル**」をクリックします。

ソース・サーバーとターゲット・サーバーで別々の保存ポリシーの設定

ターゲット複製サーバーで、複製されたクライアント・ノード・データをソース・サーバーとは異なる方法で管理するポリシーを設定できます。例えば、ソース・サーバーとターゲット・サーバーで異なる数のファイルのバージョンを維持できます。

手順

1. ソース複製サーバーから、**VALIDATE REPLICATION** コマンドを発行して、複製構成を検証し、ソース複製サーバーがターゲット複製サーバーと通信できることを検証します。
   例えば、複製されている 1 つのクライアント・ノードの名前を使用して、構成を検証します。

   ```
   validate replication node1 verifyconnection=yes
   ```

2. ソース複製サーバーから、**VALIDATE REPLPOLICY** コマンドを発行して、ソース複製サーバーとターゲット複製サーバーのポリシー間の差異を確認します。
   例えば、ソース・サーバーとターゲット・サーバー CVT_SRV2 のポリシーの間の差異を表示するには、ソース・サーバーから次のコマンドを発行します。

   ```
   validate replpolicy cvt_srv2
   ```

3. 必要に応じて、ターゲット・サーバーのポリシーを更新します。

   ヒント : Operations Center を使用して、ターゲット・サーバーのポリシーを変更することができます。94 ページの『ポリシーの編集』 の指示に従ってください。

例えば、ターゲット・サーバーでソース・サーバーよりも短い期間にわたってファイルの非活動バージョンを維持するには、複製されたクライアント・データに適用される管理クラスの「**バックアップ**」設定を低くします。

4. ソース・サーバーで **SET DISSIMILARPOLICIES** コマンドを発行して、ターゲット複製サーバーが、複製されたクライアント・ノード・データの管理にポリシーを使用できるようにします。
例えば、ターゲット複製サーバー CVT_SRV2 のポリシーを使用可能にするには、ソース・サーバーで次のコマンドを発行します。

```
set dissimilarpolicies cvt_srv2 on
```

複製プロセスが次回実行されるときに、複製されたクライアント・ノード・データを管理するためにターゲット複製サーバーのポリシーが使用されます。

ヒント: Operations Center を使用して複製を構成し、ソース複製サーバーとターゲット複製サーバーが一致しない場合、ソース複製サーバーに指定されたポリシーが使用されます。 **SET DISSIMILARPOLICIES** コマンドを使用してターゲット複製サーバー上のポリシーを有効にした場合、ターゲット複製サーバーに指定されたポリシーが使用されます。 ターゲット複製サーバーにソース複製サーバー上のノードが使用するポリシーがない場合、STANDARD ポリシーが使用されます。

関連情報

EXPORT POLICY (ポリシー情報のエクスポート)

SET DISSIMILARPOLICIES (複製データを管理するためのポリシーをターゲット複製サーバー上で有効にする)

VALIDATE REPLICATION (クライアント・ノードの複製の妥当性検査)

VALIDATE REPLPOLICY (ターゲット複製サーバー上のポリシーの妥当性検査)

サーバーの保護

サーバーおよびクライアント・ノードへのアクセスの制御、データの暗号化、およびセキュアなアクセス・レベルとパスワードの維持により、IBM Spectrum Protect サーバーおよびデータを保護します。

セキュリティーの概念

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

トランスポート層セキュリティー

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

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

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

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

SSL を使用可能にする各サーバー、クライアント、またはストレージ・エージェントは、信頼された自己署名証明書を使用するか、認証局 (CA) が署名する固有の証明書を取得する必要があります。独自の証明書を使用するか、CA から証明書を購入することができます。どちらかの証明書をインストールして、IBM Spectrum Protect サーバー、クライアント、またはストレージ・エージェントの鍵データベースに追加す

る必要があります。証明書は、SSL 通信の要求や開始を行う SSL クライアントやサーバーによって 検証されます。一部の CA 証明書は、デフォルトで鍵データベースにプリインストールされています。

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

権限レベル

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

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

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

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

パスワード

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

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

表 *19.* パスワード認証の特性

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

セッション・セキュリティー

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

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

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

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

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

表 *20. SESSIONSECURITY* パラメーターの設定に使用されるコマンド

エンティティー	**コマンド**
クライアント・ノード	• REGISTER NODE • UPDATE NODE
管理者	• REGISTER ADMIN • UPDATE ADMIN
サーバー	• DEFINE SERVER • UPDATE SERVER

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

ヒント :

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

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

関連情報

通信の保護

管理者の管理

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

手順

管理者の設定を変更するには、以下のタスクを実行します。

タスク	手順

管理者の追加	システム権限を持つ管理者 (ADMIN1) を追加してパスワードを指定するには、以下の手順を実行します。
	a. 以下のコマンドを発行して、管理者を登録し、パスワードとして **Pa$#$twO** を指定します。
	`register admin admin1 Pa$#$twO`
	b. 以下のコマンドを発行して、管理者にシステム権限を付与します。
	`grant authority admin1 classes=system`

管理権限の変更	管理者 ADMIN1 の権限レベルを変更します。
	• 以下のコマンドを発行して、管理者にシステム権限を付与します。
	`grant authority admin1 classes=system`
	• 次のコマンドを発行して、管理者のシステム権限を取り消します。
	`revoke authority admin1 classes=system`

管理者の削除	以下のコマンドを発行して、管理者 ADMIN1 を削除して IBM Spectrum Protect サーバーにアクセスできないようにします。 `remove admin admin1`
サーバーへのアクセスの一時停止	**LOCK ADMIN** コマンドまたは **UNLOCK ADMIN** コマンドを使用して、管理者をロックまたはアンロックします。

パスワード要件の変更

最小パスワード限界、パスワード長、パスワードの有効期限を変更したり、IBM Spectrum Protect の認証を使用可能または使用不可にしたりすることができます。

このタスクについて

パスワード認証を適用してパスワード制限を管理することにより、潜在的なセキュリティー・リスクからデータとサーバーを保護します。

手順

IBM Spectrum Protect サーバーのパスワード要件を変更するには、以下のタスクを実行します。

表 21. *IBM Spectrum Protect* サーバーの認証タスク

タスク	手順
無効なパスワード試行の制限の設定。	a. Operations Center の「**サーバー**」ページで、サーバーを選択します。 b.「**詳細**」をクリックして、「**プロパティー**」タブをクリックします。 c.「**無効なサインオン試行数の限度**」フィールドで、無効な試行回数を設定します。 インストール時のデフォルト値は 0 です。
パスワードの最小長の設定。	a. Operations Center の「**サーバー**」ページで、サーバーを選択します。 b.「**詳細**」をクリックして、「**プロパティー**」タブをクリックします。 c.「**最小パスワード長**」フィールドで、文字数を設定します。
パスワードの満了期間の設定。	a. Operations Center の「**サーバー**」ページで、サーバーを選択します。 b.「**詳細**」をクリックして、「**プロパティー**」タブをクリックします。 c.「**パスワード共通の有効期限**」フィールドで、日数を設定します。

デフォルトの認証方式の設定。	**SET DEFAULTAUTHENTICATION** コマンドを発行します。例えば、サーバーをデフォルトの認証方式として使用する場合、以下のコマンドを発行します。
	`set defaultauthentication local`
	サーバーを使用して認証を行うように 1 つのクライアント・ノードを更新するには、**UPDATE NODE** コマンドに AUTHENTICATION=LOCAL を組み込みます。
	`update node authentication=local`

関連情報

LDAP サーバーを使用した IBM Spectrum Protect ユーザーの認証

パスワードおよびログオン手順の管理 (V7.1.1)

システムでの IBM Spectrum Protect の保護

不正アクセスを防止するために、IBM Spectrum Protect サーバーが稼働しているシステムを保護します。

手順

無許可のユーザーが、サーバー・データベースおよびサーバー・インスタンスのディレクトリーにアクセスできないようにします。実装時に構成したこれらのディレクトリーに対するアクセス設定を保持してください。

サーバーへのユーザー・アクセスの制限

権限レベルによって、管理者が IBM Spectrum Protect サーバーで実行できる内容が決まります。システム権限を持つ管理者は、サーバーに対してすべてのタスクを実行できます。ポリシー権限、ストレージ権限、またはオペレーター権限を持つ管理者は、タスクのサブセットを実行できます。

手順

1. **REGISTER ADMIN** コマンドを使用して管理者を登録した後、**GRANT AUTHORITY** コマンドを使用して、管理者の権限レベルを設定します。

   権限の設定および変更について詳しくは、123 ページの『管理者の管理』を参照してください。
2. 一部のタスクを実行するための管理者の権限を制御するには、以下の 2 つのサーバー・オプションを使用します。
   a) **QUERYAUTH** サーバー・オプションを使用して、**QUERY** コマンドと **SELECT** コマンドを発行するために管理者に必要な権限レベルを選択できます。デフォルトでは、権限レベルは不要です。この要件を、権限レベル (システムを含む) の 1 つに変更できます。
   b) **REQSYSAUTHOUTFILE** サーバー・オプションを使用して、サーバーによる外部ファイルへの書き込みが行われるコマンドにはシステム権限が必要であることを指定できます。デフォルト解釈では、このようなコマンドにはシステム権限が必要です。
3. クライアント・ノードでのデータ・バックアップを、root ユーザー ID または許可ユーザーのみに制限できます。
   例えば、バックアップを root ユーザー ID に制限するには、**REGISTER NODE** コマンドまたは **UPDATE NODE** コマンドを発行して、**BACKUPINITIATION=root** パラメーターを指定します。

```
update node backupinitiation=root
```

ポートの制約事項によるアクセスの制限

ポートの制約事項を適用して、サーバーへのアクセスを制限します。

このタスクについて

セキュリティー要件に基づいて、特定のサーバーへのアクセスの制限が必要になることがあります。IBM Spectrum Protect サーバーは、4 つの TCP/IP ポート (通常の TCP/IP プロトコルまたは Secure Sockets Layer (SSL)/Transport Layer Security (TLS) プロトコルのどちらにも使用できる 2 つ、SSL/TLS プロトコルのみに使用できる 2 つ) で listen するように構成することができます。

手順

サーバー・オプションを設定して、125 ページの表 22 にリストされているように、必要なポートを指定することができます。

表 *22.* サーバー・オプションおよびポート・アクセス

サーバー・オプション	**ポート・アクセス**
TCPPORT	サーバーの TCP/IP 通信ドライバーがクライアント・セッションの要求を待つポート番号を指定します。 このポートは、TCP/IP セッションおよび SSL 対応セッションの両方を listen します。デフォルト値は 1500 です。

表 22. サーバー・オプションおよびポート・アクセス (続き)	
サーバー・オプション	**ポート・アクセス**
TCPADMINPORT	サーバーの TCP/IP 通信ドライバーがクライアント・セッション以外のセッションの要求を待機するポート番号を指定します。このポートは、TCP/IP セッションおよび SSL 対応セッションの両方を listen します。デフォルトは、**TCPPORT** の値です。 **TCPPORT** オプションおよび **SSLTCPPORT** オプションを使用する通常のクライアント・トラフィックから管理クライアント・トラフィックを分離するには、このオプションを使用します。
SSLTCPPORT	サーバーの SSL TCP/IP ポート・アドレスを指定します。このポートは、SSL 対応セッションのみを listen します。デフォルトのポート値は使用できません。
SSLTCPADMINPORT	サーバーの TCP/IP 通信ドライバーが 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。デフォルトのポート値は使用できません。 **TCPPORT** オプションおよび **SSLTCPPORT** オプションを使用する通常のクライアント・トラフィックから管理クライアント・トラフィックを分離するには、このオプションを使用します。

制約事項:

以下の制約事項は、SSL 専用サーバー・ポート (**SSLTCPPORT** および **SSLTCPADMINPORT**) を指定した場合に適用されます。

- **DEFINE SERVER** または **UPDATE SERVER** のコマンドの **LLADDRESS** でサーバーの SSL 専用ポートを指定する際には、**SSL=YES** パラメーターも指定する必要があります。
- クライアントの **TCPPORT** オプションでサーバーの SSL 専用ポートを指定する際には、SSL クライアント・オプションで **YES** も指定する必要があります。

関連資料

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

サーバーの停止および始動

保守タスクまたは再構成タスクを実行する前に、サーバーを停止します。次に、サーバーを保守モードで始動します。保守タスクまたは再構成タスクを終了したら、サーバーを実動モードで再始動します。

始める前に

IBM Spectrum Protect サーバーを停止および始動するには、システム特権またはオペレーター特権が必要です。

サーバーの停止

サーバーを停止する前に、すべてのデータベース・バックアップ操作が完了していること、およびその他すべてのプロセスとセッションが終了していることを確認して、システムを準備します。こうすることで、サーバーを安全にシャットダウンして、データが保護されていることを確認できます。

このタスクについて

HALT コマンドを発行してサーバーを停止すると、以下のアクションが行われます。

- すべてのプロセスおよびクライアント・ノード・セッションが取り消されます。
- すべての現行トランザクションが停止されます。(トランザクションは、サーバーの再始動時にロールバックされます。)

手順

システムを準備してサーバーを停止するには、以下の手順を実行します。

1. **DISABLE SESSIONS** コマンドを発行して、新規クライアント・ノード・セッションが開始しないようにします。

   ```
   disable sessions all
   ```

2. 以下のステップを実行して、進行中のクライアント・ノード・セッションまたはプロセスがないかを判別します。

   a. Operations Center の「**概要**」ページで「**アクティビティー**」領域を参照して、現在アクティブであるプロセスおよびセッションの総数を確認します。 その数が毎日のストレージ管理の日常業務時に表示される通常の数と大幅に異なる場合は、Operations Center の他の状況標識を表示して、問題がないかを確認します。

   b.「**アクティビティー**」領域のグラフを参照して、以下の期間中のネットワーク・トラフィックの量を比較します。

   - 現在の期間 (直近 24 時間の間)
   - 直前の期間 (現在の期間の前の 24 時間)

   直前の期間のグラフが予想されるトラフィック量を表している場合、現在の期間のグラフで示される大幅な差異は、問題を示している可能性があります。

   c.「**サーバー**」ページで、プロセスおよびセッションを表示したいサーバーを選択して、「**詳細**」をクリックします。 サーバーがハブ・サーバーまたはスポーク・サーバーとして Operations Center で登録されていない場合は、管理コマンドを使用して、プロセスに関する情報を取得します。 **QUERY PROCESS** コマンドを発行してプロセスを照会し、**QUERY SESSION** コマンドを発行してセッションに関する情報を取得します。

3. クライアント・ノード・セッションが完了するまで待つか、それらを取り消します。プロセスおよびセッションを取り消すには、以下のステップを実行します。

   - 「**サーバー**」ページで、プロセスおよびセッションを表示したいサーバーを選択して、「**詳細**」をクリックします。
   - 「**アクティブ・タスク**」タブをクリックして、キャンセルする 1 つ以上のプロセス、セッション、またはその両方の組み合わせを選択します。
   - 「**キャンセル**」をクリックします。
   - サーバーがハブ・サーバーまたはスポーク・サーバーとして Operations Center で登録されていない場合は、管理コマンドを使用してセッションを取り消します。 **CANCEL SESSION** コマンドを発行してセッションを取り消し、**CANCEL PROCESS** コマンドを使用してプロセスを取り消します。

     ヒント: 取り消すプロセスがテープ・ボリュームがマウントされるのを待機している場合、そのマウント要求は取り消されます。例えば、**EXPORT**、**IMPORT**、または **MOVE DATA** コマンドを発行すると、コマンドにより、テープ・ボリュームのマウントを必要とするプロセスが開始される場合があります。ただし、自動化ライブラリーによってテープ・ボリュームがマウントされている場合は、マウント・プロセスが完了するまで、取り消し操作は有効になりません。システム環境によっては、数分かかる場合があります。

4. **HALT** コマンドを発行して、サーバーを停止します。

   ```
   halt
   ```

保守または再構成のタスクのためのサーバーの始動

サーバーの保守タスクや再構成タスクを開始する前に、サーバーを保守モードで始動します。保守モードでサーバーを始動するときは、保守タスクや再構成タスクを中断する可能性がある操作を使用不可にします。

このタスクについて

MAINTENANCE パラメーターを指定して **DSMSERV** ユーティリティーを 実行し、サーバーを保守モードで始動します。

保守モードでは、以下の操作が使用不可になります。

- 管理コマンド・スケジュール
- クライアント・スケジュール
- サーバー上のストレージ・スペースのレクラメーション
- インベントリーの有効期限
- ストレージ・プールのマイグレーション

さらに、クライアントがサーバーとのセッションを 開始できなくなります。

ヒント:

- サーバーを保守モードで始動するために、サーバー・オプション・ファイル dsmserv.opt を編集する必要はありません。
- サーバーが保守モードで稼働している間、ストレージ・スペースのレクラメーション、インベントリー満了処理、およびストレージ・プールのマイグレーションのプロセスを 手動で開始できます。

手順

- サーバーを保守モードで始動するには、次のコマンドを発行します。

  ```
  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。使用するオペレーティング・システムの指示に従って、以下を実行します。
   - AIX
   - Linux
   - Windows

保守モード中に使用不可になっていた操作が再び使用可能になります。

サーバーのアップグレード計画

フィックスパックまたは暫定修正が入手可能になると、製品の改善点を利用するために IBM Spectrum Protect サーバーをアップグレードすることができます。サーバーおよびクライアントは、さまざまな時点でアップグレードできます。サーバーをアップグレードする 前に、必ず計画ステップを完了してください。

このタスクについて

次のガイドラインに従ってください。

- サーバーをアップグレードするために、インストール・ウィザードを使用する方法をお勧めします。ウィザードを開始した後、「**IBM Installation Manager**」ウィンドウで、「**更新**」アイコンをクリックします。「**インストール**」または「**変更**」アイコンをクリックしないでください。
- サーバー・コンポーネントと Operations Center コンポーネントの両方のアップグレードが入手可能な場合、両方のコンポーネントをアップグレードするためのチェック ・ボックスを選択します。

手順

1. フィックスパックおよび暫定修正のリストを確認します。IBM Spectrum Protect のダウンロード - 最新のフィックスパックと暫定修正を参照してください。
2. README ファイルに記載されている製品の改善点を確認します。

   ヒント: サポート・サイトからインストール・パッケージ・ファイルを入手すると、README ファイルにもアクセスできます。
3. サーバーのアップグレード先のバージョンが、他のコンポーネント (ストレージ・エージェントやライブラリー・クライアントなど) と互換性があることを確認します。IBM Spectrum Protect サーバーとストレージ・エージェントおよびライブラリー・クライアントの互換性 を参照してください。
4. ソリューションに V7.1 より前のレベルのサーバーまたはクライアントが含まれている場合、ガイドラインを調べて、クライアント・バックアップおよびアーカイブの 操作が中断されないようにしてください。IBM Spectrum Protect のサーバーとクライアントの 互換性とアップグレードの考慮事項を参照してください。
5. アップグレード手順を確認します。サーバー・データベース、装置構成情報、およびボリューム・ヒストリー・ファイルをバックアップしたことを確認します。

次のタスク

フィックスパックまたは暫定修正をインストールするには、ご使用のオペレーティング・システム用の指示に従います。

- AIX サーバー・フィックスパックのインストール
- Linux サーバー・フィックスパックのインストール
- Windows

障害やシステム更新に対する準備

計画された停電やシステム 更新の間にシステムが整合した状態を保持できるように、IBM Spectrum Protect を準備します。

このタスクについて

サーバーを管理、保護、および保守するためのアクティビティーを 必ず定期的にスケジュールしてください。

手順

1. 以下のステップを実行して、進行中のプロセスおよびセッションをキャンセルします。
   a. Operations Center の「**サーバー**」ページで、プロセスおよびセッションを確認したサーバーを選択し、「**詳細**」をクリックします。
   b.「**アクティブ・タスク**」タブをクリックして、キャンセルする 1 つ以上のプロセス、セッション、またはその両方の組み合わせを選択します。
   c.「**キャンセル**」をクリックします。

2. **HALT** コマンドを発行して、サーバーを停止します。

```
halt
```

ヒント : halt コマンドを Operations Center から発行するには、「**設定**」アイコンの上にカーソルを移動し、「**コマンド・ビルダー**」をクリックします。次に、サーバーを選択し、`halt` を入力して **Enter** キーを押します。

災害復旧計画の実装

災害が発生した場合にアプリケーションをリカバリーするため、およびサーバーの高可用性を確保するために、災害復旧戦略を実装します。

このタスクについて

クライアント・ノード・リカバリーのビジネス優先度、データのリカバリーに使用するシステム、クライアント・ノードがリカバリー・サーバーに接続されているかを識別することで、災害復旧要件を判別します。データを保護するために、複製およびストレージ・プールの保護を使用してください。また、ディレクトリー・コンテナー・ストレージ・プールを保護する頻度も判別する必要があります。

リカバリー・ドリルの実行

災害復旧ドリルをスケジュールして、IBM Spectrum Protect サーバーのリカバリー可能度を認定する監査を準備し、障害発生後にデータをリストアして操作を再開できることを確認します。ドリルは、重大な状況が発生する前にすべてのデータが復元されて操作が再開可能であることを確認する場合にも役立ちます。

このタスクについて

マルチサイト・ディスク・ソリューションでは、回復サイトのターゲット・サーバーでデータを確実に使用でき、リカバリー時間が高速になるように、ノード複製を使用します。障害がある場合、ソース・サーバーは、データ・リカバリーのためにターゲット・サーバーに自動的にフェイルオーバーできます。災害が発生してソース・サーバーが使用不可になった場合、クライアント・ノードは、ターゲット複製サーバーに関する情報を自動的にクライアント・オプション・ファイルに記録します。 古いクライアントの場合は、クライアント・オプション・ファイルを手動で更新する必要がある場合があります。

手順

1. ターゲット複製サーバーからデータを手動でリストアするには、ターゲット複製サーバーを指すようにクライアント・オプション・ファイルを更新します。 ノード複製の設定への変更は必要ありません。
2. ターゲット複製サーバーにデータを保管するように、クライアント・ノードを構成します。

   制約事項 : 通常はソース複製サーバーにデータをバックアップするクライアント・ノードは、ターゲット複製サーバー上で複製されたクライアント・ノードにデータをバックアップすることができません。
3. 以下のステップを実行して、クライアント・データ・リカバリーをテストしてください。
   a. クライアント・システムを類似のオペレーティング・システムにリストアします。ファイル・スペース内で同じファイル・スペース量を持つ同じファイル・システム名を使用します。
   b. データ用に十分なスペースがあるシステムに、データをリストアします。
   c. クライアントが正常にリストアされたことを確認します。例えば、仮想マシンをリストアする場合、仮想マシンの電源がオンであること、およびファイルが使用可能であることを確認します。

関連タスク

複製の管理

複製は、災害復旧サイトでデータをリカバリーするため、およびソース・サーバーとターゲット・サーバーで同じレベルのファイルを維持するために使用します。ノード・レベルで複製を管理することができます。また、ストレージ・プール・レベルでデータを保護することもできます。

関連情報

データベースのリストア後のクライアント・ノード・データの複製 (V7.1.1)

データ損失またはシステム障害からのリカバリー

IBM Spectrum Protect を使用して、災害時あるいはシステム障害の発生時に失われたデータをリカバリーすることができます。 ディレクトリー・コンテナー・ストレージ・プール、クライアント・データ、およびデータベースをリカバリーすることができます。

始める前に

ストレージ環境に最適なパフォーマンスを実現できるように、クライアントおよびサーバーのワークロードをスケジュールしてください。スケジュールの一部として、**PROTECT STGPOOL** コマンドおよび **REPLICATE NODE** コマンドを発行します。クライアント・ノードを複製する前に、ストレージ・プールを保護してください。ノード複製が開始されると、ストレージ・プール保護によって既に複製されているデータ・エクステントはスキップされます。そのため、複製の処理時間が短縮されます。

手順

リカバリーする必要があるコンポーネントに基づいて、以下のリカバリー方式を使用します。

リカバリーするコンポーネント	手順	詳細情報
ディレクトリー・コンテナー・ストレージ・プール	ディレクトリー・コンテナー・ストレージ・プールをリカバリーするには、以下の手順を実行します。 a. **AUDIT CONTAINER** コマンドを使用して **ACTION=SCANALL** パラメーターを指定し、ディレクトリー・コンテナー・ストレージ・プールに損傷データ・エクステントがあるかどうかスキャンします。 b. **REPAIR STGPOOL** コマンドを使用して、ディレクトリー・コンテナー・ストレージ・プール内の損傷データ・エクステントを修復します。 **制約事項 :** ストレージ・プールが保護されている場合にのみ、ストレージ・プールを修復できます。 c. **AUDIT CONTAINER** コマンドを使用して **ACTION=REMOVEDAMAGED** パラメーターを指定し、損傷データ・エクステントを削除します。	135 ページの『ストレージ・プールの修復』

リカバリーするコンポーネント	手順	詳細情報
クライアント・データ	**前提条件:** • ソース複製サーバー、ターゲット複製サーバー、およびクライアントのレベルが V7.1 以降でなければなりません。いずれかのサーバーがこれより前のレベルである場合、自動フェイルオーバーは無効になり、手動フェイルオーバーを使用しなければなりません。 データ・リカバリーのために自動的にターゲット・サーバーにフェイルオーバーするようにクライアントを手動で構成します。 自動フェイルオーバー用にクライアントを有効にした場合は、自動フェイルオーバー機能を使用してデータをリカバリーすることができます。`usereplicationfailover` オプションがクライアント・オプション・ファイル内にないか、または `yes` に設定されているかを確認できます。障害のためにソース・サーバーを使用できない場合、自動フェイルオーバーを使用してターゲット・サーバーからデータをリカバリーします。 **ヒント:** • **SET FAILOVERHLADDRESS** コマンドは、フェイルオーバー中の複製サーバーの IP アドレスが、複製プロセスに指定されている IP アドレスと異なる場合に、そのアドレスを指定するために使用します。	• 134 ページの『複製コピーからの損傷データのリカバリー』 • SET FAILOVERHLADDRESS (フェイルオーバー高位アドレスの設定)
データベース	**前提条件:** • 災害の後で データベースをリストアするには、現行の装置構成ファイルのコピーを持っている必要があります。装置構成ファイルは再作成できません。 • データベースのバックアップ・バージョンがあることを確認してください。 **DSMSERV RESTORE DB** サーバー・ユーティリティーを 使用して、IBM Spectrum Protect データベースを最新状態または特定の時点にリストアします。	DSMSERV RESTORE DB (データベースのリストア)

関連情報

AUDIT CONTAINER (ディレクトリー・コンテナー・ストレージ・プールのデータベース情報の整合性の検査)

DSMSERV RESTORE DB (データベースのリストア)

データベースのリストア

災害発生後に IBM Spectrum Protect データベースのリストアが必要になることがあります。データベースは、最新の状態、あるいは指定した特定時点にリストアすることができます。 データベースをリストアするには、完全、差分、またはスナップショットのデータベース・バックアップ・ボリュームが必要です。

始める前に

データベースおよび回復ログ・ディレクトリーが消失している場合は、それらをまず再作成してから、**DSMSERV RESTORE DB** サーバー・ユーティリティーを 実行してください。例えば、次のコマンドを使用します。

Linux AIX

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activelog
mkdir /archlog
mkdir /archfaillog
```

Windows

```
mkdir e:¥tsm¥db001
mkdir f:¥tsm¥db001
mkdir g:¥tsm¥db001
mkdir h:¥tsm¥activelog
mkdir i:¥tsm¥archlog
mkdir j:¥tsm¥archfaillog
```

制約事項:

- データベースを最新バージョンにリストアするには、アーカイブ・ログ・ディレクトリーを見つける必要があります。ディレクトリーが見つからない場合は、特定時点にのみデータベースをリストアできます。
- データベース・リストア操作に Secure Sockets Layer (SSL) を使用することはできません。
- データベース・バックアップのリリース・レベルがリストア対象のサーバーのリリース・レベルと異なっている場合、サーバー・データベースをリストアすることはできません。例えば、バージョン 8.1 のサーバーを使用している場合にバージョン 7.1 データベースをリストアすると、エラーが発生します。

このタスクについて

特定時点リストア操作は、通常、災害復旧などのシチュエーションに使用されるか、またはデータベース内に不整合を引き起こす可能性のあるエラーの影響を取り除くために使用されます。データベースが消失した時点にデータベースをリカバリーするには、データベースを最新バージョンにリカバリーします。

手順

DSMSERV RESTORE DB サーバー・ユーティリティーを 使用して、データベースをリストアします。リストアするデータベースのバージョンに応じて、以下のいずれかの方法を選択します。

- データベースを最新バージョンにリストアします。例えば、次のコマンドを使用します。

  ```
  dsmserv restore db
  ```

- データベースを特定時点にリストアします。例えば、2015 年 4 月 19 日に作成したバックアップの集合までデータベースをリストアするには、次のコマンドを使用します。

  ```
  dsmserv restore db todate=04/19/2015
  ```

次のタスク

データベースをリストアしていて、ディレクトリー・コンテナー・ストレージ・プールがサーバーに存在している場合は、データベースとファイル・システムの間の不整合を特定する必要があります。

1. データベースを特定時点にリストアしていて、ディレクトリー・コンテナー・ストレージ・プールの再使用を遅らせなかった場合は、すべてのコンテナーを監査する必要があります。すべてのコンテナーを監査するには、次のコマンドを発行します。

   ```
   audit container stgpool
   ```

2. サーバーがシステム 上のコンテナーを識別できない場合、以下の手順を実行して、コンテナーのリストを表示します。

   a. 管理クライアントから、以下のコマンドを発行します。

   ```
   select container_name from containers
   ```

   b. ファイル・システムから、ソース・サーバー上のストレージ・プール・ディレクトリーに対して次のコマンドを発行します。

   ヒント：ストレージ・プール・ディレクトリーがコマンド出力に表示されます。

   Linux AIX
   ```
   [root@source]$ ls -lR
   ```

   Windows
   ```
   c:\source_stgpooldir>dir /s
   ```

   c. ファイル・システムとサーバーでリストされたコンテナーを比較します。

   d. **AUDIT CONTAINER** コマンドを発行して、サーバーの出力で欠落しているコンテナーを指定します。**ACTION=REMOVEDAMAGED** パラメーターを指定して、コンテナーを削除します。

   e. ファイル・システムでコンテナーが削除されたことを確認するには、表示されたメッセージを確認します。

   ヒント：データベースのリストア操作後、サーバー・データベースで参照されていない、ファイル・システム内のコンテナーが存在している場合、**QUERY STGPOOL** コマンドはストレージ・プールの使用率を誤って表示します。データベースを特定時点にリストアした場合、コンテナーはファイル・システムに残りますが、サーバー・データベースでは参照されません。ストレージ・プールの使用率に関する正確な統計を得るには、ファイル・システムで使用可能であるものの、サーバー・データベースでは参照されないコンテナーを手動で削除する必要があります。

関連情報

データベースのリストア後のクライアント・ノード・データの複製 (V7.1.1)

AUDIT CONTAINER (ディレクトリー・コンテナー・ストレージ・プールのデータベース情報の整合性の検査)

DSMSERV RESTORE DB (データベースのリストア)

複製コピーからの損傷データのリカバリー

ソース複製サーバーが使用できない場合、ターゲット複製サーバーに保管されている複製コピーから損傷データをリカバリーすることができます。

始める前に

SET REPLSERVER コマンドで指定するサーバー名は、既存のサーバー定義の名前と一致している必要があります。 また、ターゲット複製サーバーとして使用されるサーバーの名前でなければなりません。 このコマンドで指定されたサーバー名が、既存のサーバー定義のサーバー名に一致していない場合、コマンドは失敗します。

ヒント：

- ターゲット複製サーバーを変更あるいは削除する場合は、注意してください。ターゲット複製サーバーを変更すると、複製されたクライアント・ノード・データは別のターゲット複製サーバーに送信されます。ターゲット複製サーバーを除去すると、クライアント・ノード・データは複製されません。

手順

1. ターゲット・サーバー上のデータの複製状況を確認します。複製状況は、最新のバックアップが 2 次サーバーに複製されているかどうかを示します。
2. ソース複製サーバーをターゲット複製サーバーとして設定することにより、ターゲット複製サーバーからデータをリストアします。
   例えば、ソース複製サーバーをターゲット複製サーバーの server1 として設定するには、次のコマンドを発行します。

```
set replserver server1
```

次のタスク

ソース複製サーバー上の IBM Spectrum Protect データベースをリストアすると、複製が自動的に無効になります。 複製を再度有効にする前に、ターゲット複製サーバーにあるデータのコピーが必要かどうかを判別してください。

関連情報

データベースのリストア後のクライアント・ノード・データの複製 (V7.1.1)

ストレージ・プールの修復

災害またはシステム障害が発生した場合は、ディレクトリー・コンテナー・ストレージ・プールで重複排除されたデータ・エクステントを修復することができます。

始める前に

AUDIT CONTAINER コマンドを使用して、データベースとディレクトリー・コンテナー・ストレージ・プールの間の不整合を特定します。ディレクトリー・コンテナー・ストレージ・プール内の損傷データ・エクステントを識別することで、修復すべきデータ・エクステントを判別できます。

ストレージ・プールを修復する前に、ストレージ・プールが **PROTECT STGPOOL** コマンドを使用して保護されていることを確認します。

手順

1. ディレクトリー・コンテナー・ストレージ・プールを修復するには、**REPAIR STGPOOL** コマンドを使用します。
   例えば、ストレージ・プール STGPOOL1 を修復するには、次のコマンドを発行します。

```
repair stgpool stgpool1
```

2. 1 つ以上のソース・ストレージ・プールに対する **PROTECT STGPOOL** コマンドで、損傷したストレージ・プールがターゲット・ストレージ・プールとして指定されている場合、すべてのソース・ストレージ・プールに対して **PROTECT STGPOOL** コマンドを発行してください。
3. すべての損傷データが特定され、他のソース・ストレージ・プールから修復されるように、すべてのソース・ストレージ・プールから **PROTECT STGPOOL** コマンドを再発行し、**FORCERECONCILE=YES** パラメーターを指定します。
4. 損傷データを参照するオブジェクトを除去するには、**AUDIT CONTAINER** コマンドを発行し、**ACTION=REMOVEDAMAGED** パラメーターを指定します。
5. 損傷ストレージ・プールが、1 つ以上のソース・サーバーからノード複製を行う際のターゲット・ストレージ・プールとなっている場合、すべてのソース・ストレージ・サーバーから **REPLICATE NODE** コマンドを実行します。

6. 損傷が修復されたら、**PROTECT STGPOOL** コマンドを発行して、ストレージ・プールが他のディレクトリー・コンテナー・ストレージ・プールに保護されるようにします。

次のタスク

QUERY DAMAGED コマンドを使用して、出力に損傷データ・エクステントが表示されないことを確認します。

関連情報

ディレクトリー・コンテナー・ストレージ・プール内のデータの修復およびリカバリー

AUDIT CONTAINER (ディレクトリー・コンテナー・ストレージ・プールのデータベース情報の整合性の検査)

QUERY DAMAGED (ディレクトリー・コンテナー・ストレージ・プールまたはクラウド・コンテナー・ストレージ・プールの損傷データの照会)

REPAIR STGPOOL (ディレクトリー・コンテナー・ストレージ・プールの修復)

付録 A 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身体に障害を持つユーザーが情報技術コンテンツを快適に使用できるように支援します。

概要

IBM Spectrum Protect ファミリーの製品は、以下の主なアクセシビリティ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) を使用する操作

IBM Spectrum Protect ファミリー製品は、最新の W3C 標準 WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/) が、US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) および Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/) に準拠するように使用されています。 アクセシビリティー機能を利用するには、最新リリースのスクリーン・リーダーと、この製品によってサポートされる最新の Web ブラウザーを使用してください。

IBM Knowledge Center の製品資料は、アクセシビリティーに対応しています。IBM Knowledge Center のアクセシビリティー機能については、Accessibility section of the IBM Knowledge Center help (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に、また使いやすさを実現するために、カスケーディング・スタイル・シートが使用されています。 このアプリケーションには、視覚に障害のあるユーザーがシステム表示設定を使用するための、同等の方式 (ハイコントラスト・モードなど) が用意されています。 フォント・サイズの制御は、デバイスまたは Web ブラウザーの設定を使用して行うことができます。

Web ユーザー・インターフェースには、アプリケーションの機能領域に素早くナビゲートできる WAI-ARIA ナビゲーション・ランドマークが含まれています。

ベンダー・ソフトウェア

IBM Spectrum Protect 製品ファミリーには、IBM の使用許諾契約書の対象とならないベンダー・ソフトウェアが含まれます。IBM は、それらの製品のアクセシビリティー機能を保証するものではありません。ベンダーの製品のアクセシビリティー機能については、ベンダーにお問い合わせください。

関連アクセシビリティー情報

IBM では、標準の IBM ヘルプ・デスクとサポート Web サイトに加えて、聴覚に障害のあるお客様が営業担当者やサポート・サービスに連絡が取れるように TTY 電話サービスを開設しています。

TTY サービス
800-IBM-3383 (800-426-3383)
(北アメリカ内)

IBM のアクセシビリティーに対する取り組みについて詳しくは、IBM Accessibility (www.ibm.com/able) を参照してください。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。 この資料は、IBM から他の言語でも提供されている可能性があります。ただし、これを入手するには、本製品または当該言語版製品を所有している必要がある場合があります。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。 日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。 本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。 これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。 ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について 実施権を許諾することを意味するものではありません。 実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒 *103-8510*
東京都中央区日本橋箱崎町 *19* 番 *21* 号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

IBM およびその直接または間接の子会社は、本書を特定物として現存するま まの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕 疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとし ます。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部では ありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、 自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

本書に含まれるパフォーマンス・データは、特定の動作および環境条件下で得られたものです。 実際の結果は、異なる可能性があります。

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 をご覧ください。

Adobe は、Adobe Systems Incorporated の米国およびその他の国における登録商標です。

Linear Tape-Open、LTO、および Ultrium は、HP、IBM Corp. および Quantum の米国およびその他の国における商標です。

Intel および Itanium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

登録商標 Linux は、世界中で商標の所有者である Linux Torvalds の独占的ライセンシーである Linux Foundation のサブライセンスに従って使用されています。

Microsoft、Windows、および Windows NT は、Microsoft Corporation の米国およびその他の国における商標です。

Java™ およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

VMware、VMware vCenter Server、および VMware vSphere は VMware, Inc. または子会社の米国およびその他の国における登録商標または商標です。

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用条件

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。 ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権利

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも 含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。 ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項をご確認ください。

この「ソフトウェア・オファリング」は、Cookie もしくはその他のテクノロジーを使用して個人情報を収集することはありません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie などの各種テクノロジーの使用について詳しくは、「IBM プライバシー・ステートメント」(http://www.ibm.com/privacy/jp/ja/)、「IBM オンライン・プライバシー・ステートメント」(http://www.ibm.com/privacy/details/jp/ja) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』というタイトルのセクション、および「IBM Software Products and Software-as-a-Service Privacy Statement」(http://www.ibm.com/software/info/product-privacy) を参照してください。

用語集

IBM Spectrum Protect 製品ファミリーの用語と定義が記載されている用語集を使用できます。

IBM Spectrum Protect 用語集 を参照してください。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

[マ行]

[ヤ行]

[ラ行]

[数字]

A

D

E

I

K

L

O

R

S

T

W

[特殊文字]

プログラム番号: 5725-W98
5725-W99
5725-X15