IBM Spectrum Protect for AIX 8.1.12

インストール・ガイド

お願い

本書および本書で紹介する製品をご使用になる前に、199 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

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

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

本書の対象読者

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

インストール可能コンポーネント

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

これらのコンポーネントは、複数の異なるインストール・パッケージにあります。

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

IBM Spectrum Protect コンポーネント	**説明**	**追加情報**
サーバー (必須)	データベース、Global Security Kit (GSKit)、IBM® Java™ ランタイム環境 (JRE)、およびサーバーの構成と管理に役立つツールが含まれています。	70 ページの『インストール・ウィザードを使用した IBM Spectrum Protect のインストール』
言語パッケージ (オプション)	それぞれの言語パッケージ (各言語ごとに 1 つ) には、サーバーの言語に特有の情報が含まれています。	73 ページの『サーバー言語パッケージのインストール』を参照してください。
ライセンス (必須)	すべてのライセンス機能のサポートが含まれています。このパッケージをインストールした後、購入したライセンスを登録する必要があります。	**REGISTER LICENSE** コマンドを使用します。
デバイス (オプション)	メディアの管理機能を拡張します。	このドライバーでサポートされる装置のリストは、IBM サポート・ポータルから入手できます。

表 1. *IBM Spectrum Protect* インストール可能コンポーネント (続き)		
IBM Spectrum Protect コンポーネント	**説明**	**追加情報**
ストレージ・エージェント (オプション)	クライアント・システムが、ストレージ・エリア・ネットワーク (SAN) に接続されたストレージ・デバイスに直接データを書き込んだり、 そのデバイスから直接データを読み取ったりできるようにするコンポーネントをインストールします。 **要確認 :** IBM Spectrum Protect for Storage Area Networks は、個別にライセンス交付を受けた製品です。	ストレージ・エージェントについて詳しくは、Tivoli Storage Manager for Storage Area Networks (V7.1.1)を参照してください。
Operations Center (オプション)	Operations Center をインストールします。これは、ストレージ環境を管理するための Web ベースのインターフェースです。	121 ページの『第 2 部 Operations Center のインストールおよびアップグレード』を参照してください。

資料

IBM Spectrum Protect 製品ファミリーには、IBM Spectrum Protect 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。

新機能および更新内容のリストについては、新機能を参照してください。

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 サーバーのインストールおよびアップグレード

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

第 1 章 サーバーのインストール計画

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

インストールを開始する前の前提知識

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

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

制約事項 : IBM Db2® が既にインストールされているシステムに、いくつかの制限付きで、IBM Spectrum Protect サーバーをインストールして実行することができます。この場合、Db2 が単独でインストールされているか、または他のアプリケーションの一部としてインストールされているかは関係ありません。

詳細については、46 ページの『IBM Spectrum Protect サーバーとシステム上の他の IBM Db2 製品との互換性』を参照してください。

経験豊かな Db2 管理者は、拡張 SQL 照会を実行したり、Db2 ツールを使用してデータベースをモニターしたりすることができます。ただし、Db2 ツールを使用して、IBM Spectrum Protect によって事前設定されている Db2 構成設定を変更したり、別の方法で (例えば他の製品を使用して) IBM Spectrum Protect の Db2 環境を変更したりしないでください。 サーバーは、サーバーがデプロイするデータ定義言語 (DDL) およびデータベース構成を使用して構築され、幅広くテストが行われています。

重要 : IBM Spectrum Protect インストール・パッケージおよびフィックスパックと一緒にインストールされる Db2 ソフトウェアは変更しないでください。別のバージョン、リリース、またはフィックスパックの Db2 ソフトウェアをインストールしたり、それらにアップグレードしたりしないでください。データベースが損傷する可能性があります。

サーバーのインストールまたはアップグレードの前に認識する必要があるセキュリティーに関する事項

IBM Spectrum Protect サーバーの拡張セキュリティー機能に関する情報およびご使用の環境を更新するための要件を確認します。

始める前に

バージョン 8.1.2 以降、IBM Spectrum Protect には、より厳密なセキュリティー設定を適用する機能拡張が追加されました。IBM Spectrum Protect のインストールまたはアップグレードを行う前に、以下の手順を実行します。

- IBM Knowledge Center の「新機能」トピックで、『セキュリティー』セクションの情報を参照して各バージョンのセキュリティー更新について確認します。
- ご使用の環境に旧バージョンのサーバーがある場合は、技術情報 562939 の制約事項と既知の問題を参照してください。制約を回避し、最新のセキュリティー機能拡張を活用するには、ご使用の環境のすべての IBM Spectrum Protect サーバーおよびバックアップ/アーカイブ・クライアントの最新バージョンへの更新を計画してください。

セキュリティー機能拡張

V8.1.2 以降、以下のセキュリティー機能拡張が追加されました。

Transport Layer Security (TLS) を使用するセキュリティー・プロトコル

IBM Spectrum Protect V8.1.2 以降のソフトウェアでは、セキュリティー・プロトコルが強化され、サーバー、ストレージ・エージェント、およびバックアップ/アーカイブ・クライアントの間の認証に TLS バージョン 1.2 以降を使用します。

IBM Spectrum Protect V8.1.11 以降、TLS 1.3 プロトコルを有効にすることで、サーバー、クライアント、およびストレージ・エージェントの間の通信を保護することができます。TLS 1.3 を使用するには、通信セッションの双方が TLS 1.3 を使用している必要があります。いずれかが TLS 1.2 を使用している場合、デフォルトで双方が TLS 1.2 を使用します。

自動での Secure Sockets Layer (SSL) 構成と証明書の配布

V8.1.2 以降のソフトウェアを使用しているサーバー、ストレージ・エージェント、およびクライアントは、TLS を使用して相互に認証を行うように自動的に構成されます。

新規プロトコルを使用する場合、各サーバー、ストレージ・エージェント、およびクライアントには、TLS 接続で認証を行い許可するための固有の自己署名証明書が存在します。 IBM Spectrum Protect の自己署名証明書によって、エンティティー間のセキュア認証と、データ転送のための強力な暗号化が可能になり、公開鍵がクライアント・ノードに自動的に配布されます。 証明書は、V8.1.2 以降のソフトウェアを使用するすべてのクライアント、ストレージ・エージェント、およびサーバーの間で自動的に交換されます。手動で TLS を構成したり、各クライアントの証明書を手動でインストールしたりする必要はありません。この新しい TLS 機能拡張ではオプションを変更する必要はありません。また、複数のシステムにアクセスするために単一の管理者 ID を使用している場合を除いて、証明書は最初の接続時に自動的にクライアントに転送されます。

デフォルトでは自己署名証明書が配布されますが、オプションで認証局によって署名された証明書など、その他の構成を使用することもできます。証明書の使用方法については、IBM Knowledge Center の「*SSL* および *TLS* 通信」を参照してください。

セキュア通信およびパフォーマンスを実現するための TCP/IP プロトコルと TLS プロトコルの組み合わせ

IBM Spectrum Protect ソフトウェアの旧バージョンでは、すべての通信を暗号化するために TLS か TCP/IP のいずれかを選択する必要がありました。新規セキュリティー・プロトコルでは、サーバー、クライアント、およびストレージ・エージェント間の通信を保護するために、TCP/IP と TLS の組み合わせを使用できます。デフォルトでは、TLS は認証およびメタデータの暗号化にのみ使用され、一方 TCP/IP はデータ伝送に使用されます。TLS 暗号化は主に認証にのみ使用されるため、バックアップ操作やリストア操作のパフォーマンスが影響を受けることはありません。

オプションで、クライアントとサーバー間通信の場合は **SSL** クライアント・オプションを使用し、サーバー間通信の場合は **UPDATE SERVER** コマンドの **SSL** パラメーターを使用することで、TLS を使用してデータ伝送を暗号化することができます。

後方互換性による、バッチでの簡単なアップグレード計画

SESSIONSECURITY パラメーターが TRANSITIONAL に設定されている場合、IBM Spectrum Protect サーバーとクライアントのアップグレード 済みバージョンは旧バージョンに引き続き接続できます。

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後、旧バージョンのソフトウェアを使用す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、引き続き TRANSITIONAL 値を使用してサーバーに接続します。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、最初にサーバーをアップグレードする 必要はありません。 異なるバージョンを使用している場合でも、サーバーとクライアントの間の通信が中断されることはありません。 ただし、クライアントとサーバーの両方がアップグレードされるまで、セキュリティー機能拡張のメリットを享受できません。

SESSIONSECURITY パラメーターを使用した厳密なセキュリティーの適用

新しいセキュリティー・プロトコルを使用するためには、サーバー、クライアント・ノード、または管理者の各エンティティーが、**SESSIONSECURITY** パラメーターをサポートする IBM Spectrum Protect ソフトウェアを使用していることが必要です。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、およびサーバー間の通信に使用されるセキュリティーのレベルです。 このパラメーターには、次の値を指定できます。

STRICT
IBM Spectrum Protect サーバー、ノード、および管理者の間の通信に最高レベルのセキュリティー (現在は TLS 1.2) を適用します。

TRANSITIONAL
IBM Spectrum Protect ソフトウェアを V8.1.2 以降に更新するまで、既存の通信プロトコル (TCP/IP など) が使用されることを指定します。 これがデフォルトです。
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 値の要件を満たした後は、セッション・セキュリティーは自動的に STRICT 値に更新されるため、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。

SESSIONSECURITY=TRANSITIONAL が設定されており、サーバー、ノード、または管理者が STRICT 値の要件を満たしていない場合、サーバー、ノード、または管理者は引き続き TRANSITIONAL 値を使用して認証を行います。 ただし、サーバー、ノード、または管理者が STRICT 値の要件を満たすと、**SESSIONSECURITY** パラメーター値が自動的に TRANSITIONAL から STRICT に更新されます。その結果、サーバー、ノード、または管理者は、STRICT の要件を満たさないバージョンのクライアントや SSL/TLS プロトコルを使用して認証することができなくなります。

制約事項 : 管理者が IBM Spectrum Protect V8.1.2 以降のソフトウェア、または Tivoli® Storage Manager V7.1.8 以降のソフトウェアを使用してサーバーで正常に認証を行った後、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またはサーバーを 使用して、同じサーバーで認証を行うことができなくなります。この制限は、コマンド・ルーティングや、別のサーバーからの管理者として宛先 IBM Spectrum Protect サーバーで認証するサーバー間エクスポート、Operations Center を使用した管理者接続、および管理コマンド・ライン・クライアントからの接続などの機能を使用する場合の宛先サーバーにも適用されます。

クライアント・セッションおよび管理セッションの場合、管理者 ID が接続先のすべてのサーバーに対して既に証明書を取得していない限り、管理者コマンド・ルーティング・セッションは失敗する可能性があります。**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。

- 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。
- 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。

アップグレードする前に

サーバーのアップグレード前に、以下のチェックリストのガイドラインを確認します。

表 2. 計画チェックリスト

ガイドライン	説明
以下のサーバー・ファイルをバックアップします • 鍵データベース (cert.kdb および dsmkeydb.kdb) • stash ファイル (cert.sth および dsmkeydb.sth)	IBM Spectrum Protect バージョン 8.1.2 以降、サーバーの始動時に、(マスター暗号鍵が前に存在していない場合は) 自動的にマスター暗号鍵が生成されるようになりました。 マスター暗号鍵は、鍵データベース dsmkeydb.kdb に保管されます。サーバー証明書は引き続き cert.kdb 鍵データベースに保管され、 stash ファイルの cert.sth によりアクセスされます。鍵データベース (cert.kdb および dsmkeydb.kdb) そしてそれぞれの鍵データベースへのアクセスを提供する stash ファイル (cert.sth および dsmkeydb.sth) の両方を保護する必要があります。 デフォルトでは、**BACKUP DB** コマンドを指定すると、ボリューム・ヒストリー・ファイルと devconfig ファイルが保護されているのと同じ方法でマスター暗号鍵が保護されます。 データベースをリストアするときのためにデータベース・バックアップ・パスワードを覚えておいてください。旧リリースでマスター暗号鍵を保管するために使用されていた、IBM Spectrum Protect サーバーの `dsmserv.pwd` ファイルは使用されなくなりました。
管理者 ID に関するアップグレードは慎重に計画します	管理者アカウントが管理目的でログインに使用するすべてのシステムを特定します。 V8.1.2 以降のソフトウェアに対する認証に成功すると、管理者は同じサーバーで旧バージョンの IBM Spectrum Protect ソフトウェアに対する認証を行うことができません。 複数のシステムにログインする際に単一の管理者 ID を使用している場合、管理者がログインするすべてのシステムに 証明書が確実にインストールされるように、V8.1.2 以降のソフトウェアを使用するすべてのシステムのアップグレードを計画してください。 **ヒント:** すべての管理者 ID に対する **SESSIONSECURITY** パラメーターが STRICT 値に更新された場合でも、サーバーからロックアウトされることはありません。**dsmadmc** コマンドを実行しているクライアントに、サーバーのパブリック 証明書を手動でインポートできます。

表 2. 計画チェックリスト (続き)

ガイドライン	説明
「TSM Server SelfSigned Key」(cert.arm) 証明書を使用する旧バージョンのクライアントで TLS を使用している場合は、クライアントを V8.1.4 以降に更新してください。	V7.1.8 より前のリリースでは、「TSM Server SelfSigned Key」というラベルのデフォルトの証明書が MD5 署名を採用していました。これは V8.1.2 以降のクライアントや Operations Center でデフォルトで必要な TLS 1.2 以降のプロトコルをサポートしていません。この問題を解決するには、次のいずれかの手順に従ってください。 • サーバーを V8.1.4 以降にアップグレードします。V8.1.4 以降、 デフォルトとして MD5 署名を採用するサーバーは、「TSM Server SelfSigned SHA Key」というラベルの SHA 署名を採用するデフォルトの証明書を使用するように自動的に更新されます。新規デフォルト証明書のコピーは、サーバー・インスタンス・ディレクトリーに位置する `cert256.arm` ファイルに保管されます。 **ヒント:** SHA 署名による新規デフォルト証明書を使用するようにサーバーを更新するには、事前に `cert256.arm` ファイルをクライアントに配布して、クライアントによるクライアント ・バックアップ障害を防いでください。各クライアントは、新規のデフォルト SHA 証明書を使用するサーバーに接続する前に、新規の証明書を取得してインポートする必要があります。以前の証明書を削除する必要がありません。 • デフォルトの証明書を手動で更新するには、技術情報 562939 の指示に従ってください。

次の作業

- 7 ページの『セキュリティー更新の適用』 の手順に従い、IBM Spectrum Protect サーバーを アップグレードまたはこれをインストールします。
- セキュリティー更新に関連する通信の問題のトラブルシューティングについては、12 ページの『セキュリティー更新のトラブルシューティング』 を参照してください。
- FAQ 情報については、FAQ - Security updates in IBM Spectrum Protect を参照してください。
- 新しいセキュリティー環境での IBM Spectrum Protect バックアップ/アーカイブ Web クライアントの使用方法については、技術情報 728037 を参照してください。

セキュリティー更新の適用

IBM Spectrum Protect の新リリースで提供されるセキュリティー更新を適用します。

始める前に

以下の情報を確認します。

- リリースで提供されるセキュリティー更新についての詳細は、IBM Knowledge Center の「新機能」トピックを参照してください。
- 適用できる更新と制約事項についての詳細は、3 ページの『サーバーのインストールまたはアップグレードの前に認識する必要があるセキュリティーに関する事項』 を参照してください。
- ご使用の環境のサーバーとクライアントをアップグレードする 順序を決定するために、以下の質問に回答してください。

表 3. アップグレード前の考慮事項に対する質問

質問	考慮事項
構成におけるサーバーの役割はどのようなものですか？	通常は、 使用環境で最初に IBM Spectrum Protect サーバーをアップグレードしてから、バックアップ/アーカイブ・クライアントをアップグレードすることができます。ただし、コマンド・ルーティング機能を使用する場合など一部の環境では、サーバーが構成内のクライアントとして機能している可能性があります。そのような場合、通信の問題を回避するために、最初にクライアントをアップグレードする方法を推奨します。さまざまなシナリオについて詳しくは、アップグレード・シナリオを参照してください。
管理者の認証には、どのシステムが使用されますか？	管理者アカウントの場合、認証の問題を防ぐために、アップグレードの順序は重要です。 – 複数のシステム上で同じ ID (ノード ID または管理 ID) を使用してログオンするクライアントは、同時にアップグレードする必要があります。サーバー証明書は、最初の接続時にクライアントに自動的に転送されます。 – サーバーをアップグレードする 前に、管理者が管理のために接続先として使用するすべてのエンドポイントについて考慮してください。単一の管理 ID を使用して複数システムにアクセスする場合、各システムにサーバーの 証明書がインストールされていることを確認します。 – 管理者 ID で IBM Spectrum Protect V8.1.2 以降のソフトウェア、または Tivoli Storage Manager V7.1.8 以降のソフトウェアを使用してサーバーで正常に認証を行った後、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またはサーバーを使用して、そのサーバーで認証を行うことができなくなります。これは、宛先 IBM Spectrum Protect サーバーを別のサーバーから管理者として認証している場合は、その宛先サーバーにも当てはまります。 これは、例えば以下の機能を使用する場合に該当します。 - コマンド・ルーティング - サーバー間のエクスポート - Operations Center での管理クライアントからの接続

表 3. アップグレード前の考慮事項に対する質問 (続き)

質問	考慮事項
システムをアップグレードする 順序を教えてください	– **サーバーをアップグレードしてからクライアント・ノードをアップグレードする 場合:** - まずハブ・サーバーをアップグレードしてから、任意のスポーク・サーバーをアップグレードします。 - サーバーを V8.1.2 以降にアップグレードした場合、旧バージョンのソフトウェアを使用するノードと管理者は、既存の通信プロトコルを使用することで新規サーバーと引き続き通信できます。**SESSIONSECURITY** が TRANSITIONAL に設定されており、サーバー、ノード、または管理者が STRICT 値の要件を満たしていない場合、サーバー、ノード、または管理者は引き続き TRANSITIONAL 値を使用して認証を行います。ただし、サーバー、ノード、または管理者が STRICT 値の要件を満たすと、 直ちに **SESSIONSECURITY** パラメーターの値が TRANSITIONAL から STRICT に自動的に更新されます。 – **クライアント・ノードをアップグレードしてからサーバーをアップグレードする 場合:** - まず管理クライアントをアップグレードしてから、次に非管理クライアントをアップグレードします。より新しいリリース・レベルのクライアントは、旧レベルのサーバーと引き続き通信します。 **重要 :** ご使用の環境内の管理クライアントのいずれか 1 つをアップグレードした場合、アップグレードしたクライアントと同じ ID を使用する他のクライアントもすべて同時にアップグレードする必要があります。 - 複数のクライアントがログオンするために 同じ ID を使用している場合を除いて、すべての非管理クライアントを同時にアップグレードする必要はありません。その後、アップグレードしたクライアントと同じ ID を使用する他のクライアントはすべて同時にアップグレードする必要があります。またサーバーの証明書を各システムにインストールする 必要があります。

このタスクについて

ご使用の環境に V7.1.8 または V8.1.2 より前のバージョンの IBM Spectrum Protect バックアップ/アーカイブ・クライアントまたは IBM Spectrum Protect サーバーが含まれている場合は、サーバーとクライアントの間の通信が中断されないように構成のカスタマイズが必要な場合があります。環境をインストールまたはアップグレードするためのこのトピックのデフォルトの 手順に従ってください。

ご使用の環境に適用される可能性があるその他のシナリオ例については、アップグレード・シナリオを参照してください。

ヒント: 最新のセキュリティー機能拡張を活用するには、ご使用の環境のすべての IBM Spectrum Protect サーバーおよびバックアップ/アーカイブ・クライアントの最新リリース・レベルへの更新を計画してください。

手順

1. ご使用の環境の IBM Spectrum Protect サーバーをインストールまたはアップグレードします。詳しくは、IBM Knowledge Center の『サーバーのインストールおよびアップグレード』トピックを参照してください。
   a) Operations Center とハブ・サーバーをアップグレードします。詳しくは、121 ページの『第 2 部 Operations Center のインストールおよびアップグレード』を参照してください。
   b) スポーク・サーバーをアップグレードします。
   c) サーバー間の通信を構成または検証します。詳細については、以下のトピックを参照してください。
      - IBM Knowledge Center の *UPDATE SERVER* コマンド。
      - IBM Knowledge Center の『ハブ・サーバーとスポーク・サーバーの間の *SSL* 通信の構成』トピック。
      - IBM Knowledge Center の『*SSL* を使用して別のサーバーと接続するためのサーバーの構成』トピック。

      ヒント:

      - IBM Spectrum Protect V8.1.2 および Tivoli Storage Manager V7.1.8 以降、**SSL** パラメーターに関して、**SSL** パラメーターを NO に設定した場合でも、指定したサーバーとの通信を SSL を使用して暗号化します。
      - V8.1.4 以降、ストレージ・エージェント、ライブラリー・クライアント、およびライブラリー・マネージャー・サーバーの間の証明書は自動的に構成されます。サーバー間接続が、セキュリティーの機能が拡張されたサーバーに対して初めて確立されたときに、証明書が交換されます。
2. 管理クライアントをインストールまたはアップグレードします。詳しくは、 IBM Knowledge Center の『クライアントのインストールおよび構成』トピックを参照してください。
3. 管理者が管理目的でログインするために使用するすべてのシステム間のセキュア通信を有効にします。
   - 管理者アカウントがログオンに使用する 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 ID 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。
4. 非管理クライアントをインストールまたはアップグレードします。詳しくは、 IBM Knowledge Center の『クライアントのインストールおよび構成』トピックを参照してください。

   要確認: 非管理クライアントを段階的にアップグレードできます。 各ノードで **UPDATE NODE** コマンドを発行し、**SESSIONSECURITY** パラメーターを TRANSITIONAL に設定することで、旧リリース・レベルのクライアントから新しいリリース・レベルのサーバーに引き続き接続できます。

```
update node nodename sessionsecurity=transitional
```

次のタスク

その他のアップグレード・シナリオがご使用の環境に適用される場合もあります。 以下の表のアップグレード・シナリオ例を参照してください。

表 4. アップグレード・シナリオ

シナリオ	考慮事項	推奨されるアップグレード方法
管理コマンド・ルーティング機能を使用して、コマンドを 1 つ以上の他のサーバーにルーティングします。V8.1.2 より前の IBM Spectrum Protect サーバーに接続したいと考えます。	• コマンド・ルーティングを使用する場合、サーバーは管理クライアントとして機能する場合があります。 • コマンド・ルーティングでは、コマンドを発行している管理者の ID とパスワードを使用します。 • 単一の管理 ID を使用して複数のシステムにアクセスする場合は、サーバーの証明書を各システムにインストールする必要があります。	• 最初に管理クライアントをアップグレードします。 **重要 :** 複数のシステム上で同じ ノード ID または管理 ID を使用してログオンするクライアントは、同時にアップグレードする必要があります。 • コマンドのルーティング先の各サーバーでは、以下の情報が構成されていることを確認してください。 – 同じ管理者 ID とパスワード – 各サーバーで必要な管理権限 – 必要な証明書がインストールされている • 管理者アカウントがログオンに使用するサーバーを V8.1.2 以降にアップグレードします。
管理クライアントは最新のリリース・バージョンにあります。**dsmadmc** コマンドを使用することによって、同じ管理者 ID をさまざまなシステムに対する認証に使用します。最新バージョンを実行している使用中の環境では、IBM Spectrum Protect サーバーに対して正常に認証されました。ここで V8.1.2 より前のバージョンのサーバーに対する認証を行うことが必要になりました。	• 管理者が V8.1.2 以降のクライアントを使用して V8.1.2 以降の IBM Spectrum Protect サーバーに対して認証を行った後は、その管理 ID は V8.1.2 以降を使用するクライアントあるいはサーバーを使用した場合のみ、そのサーバーで認証を行うことができます。 • 複数のシステムにアクセスする際に単一の管理者 ID を使用する場合、管理者がログオンするすべてのシステムにサーバーの証明書が確実にインストールされるように、V8.1.2 以降のソフトウェアを使用するすべてのシステムをアップグレードするように計画してください。	• 管理者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。 ご使用環境のすべてのサーバーを最新バージョンにアップグレードすることをお勧めします。 • 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。
IBM Spectrum Protect サーバーは、既に最新リリース・レベルにアップグレードされています。リリース・レベル V8.1.0 の管理クライアントがあり、Operations Center からこのサーバーに接続する必要があります。	• ご使用の環境内の管理クライアントのいずれか 1 つをアップグレードした場合、アップグレードしたクライアントと同じ ID を使用する他のクライアントもすべて同時にアップグレードする必要があります。 • 複数サーバー構成で 1 つの管理者 ID を使用するには、同じパスワードと権限レベル、および必要な証明書を使用してその ID をハブ・サーバーとスポーク・サーバーに登録する必要があります。	• 各サーバーで、以下の情報がセットアップされていることを確認します。 – 同じ管理者 ID とパスワード – 各サーバーで必要な管理権限 – 必要な証明書 • 非管理クライアントを段階的にアップグレードします。

表 4. アップグレード・シナリオ (続き)

シナリオ	考慮事項	推奨されるアップグレード方法
ノード複製を使用してデータを保護します。	• サーバーのアップグレード後にサーバー間接続が初めて確立されたときに、複製のハートビートにより証明書交換が開始されます。	• サーバーをアップグレードしてからクライアントをアップグレードします。デフォルトの手順に従います。
バックアップ/アーカイブ・クライアントをアップグレードしてから、サーバーをアップグレードすることが必要です。	• サーバーを V8.1.2 以降にアップグレードした後、旧バージョンのソフトウェアを使用す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、引き続き TRANSITIONAL 値を使用してサーバーに接続します。 • サーバーとクライアント間の通信は中断されません。	• サーバーをアップグレードする前にクライアントをアップグレードする場合は、まず管理クライアントをアップグレードしてから、次に非管理クライアントをアップグレードします。より新しいリリース・レベルのクライアントは、旧レベルのサーバーと引き続き通信します。

セキュリティー更新のトラブルシューティング

IBM Spectrum Protect のアップグレード後に発生する可能性のある問題をトラブルシューティングします。

症状	解決方法
管理者アカウントが、V8.1.2 より前のソフトウェアを使用しているシステムにログインできません。	管理者が IBM Spectrum Protect V8.1.2 以降のソフトウェアを使用するサーバーで正常に認証を行った後、その管理者は V8.1.2 より前のバージョンのクライアントまたはサーバーを使用するそのサーバーでは、認証を行うことができなくなります。この制限は、コマンド・ルーティングや、別のサーバーからの管理者として宛先 IBM Spectrum Protect サーバーで認証するサーバー間エクスポート、Operations Center を使用する管理者接続、および管理コマンド・ライン・クライアントからの接続などの機能を使用する場合の宛先サーバーにも適用されます。 管理者の認証の問題を解決するには、以下の手順を実行してください。 1. 管理者のログイン元のすべてのシステムを識別し、どのシステムがその管理 ID を使用してログインしているかを識別します。 システム・ソフトウェアを IBM Spectrum Protect V8.1.2 以降にアップグレードし、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ことを確認します。 2. コマンド `update admin admin_name sessionsecurity=transitional` を発行して、管理者の **SESSIONSECURITY** パラメーター値を TRANSITIONAL に設定します。 3. 管理者接続を再試行します。 **ヒント:** 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。
ノード、管理者、またはサーバーの証明書の配布が失敗しました。	V8.1.2 以降のソフトウェアを使用しているノード、管理者、またはサーバーの **SESSIONSECURITY** 値は STRICT に設定されていますが、証明書の配布を再試行するためには、この値を TRANSITIONAL にリセットする必要があります。 新しいプロトコルを使用する場合、サーバーのパブリック証明書の自動転送が実行されるのは、セキュリティーの機能が拡張されたサーバーへの初回接続時のみです。初回接続の後、ノードの **SESSIONSECURITY** パラメーター値は TRANSITIONAL から STRICT に変更されます。 ノード、管理者、またはサーバ

症状	解決方法

	ーを一時的に TRANSITIONAL に更新することで、証明書をもう一度自動転送することができます。TRANSITIONAL に設定されている間に次の接続が行われると (必要に応じて) 証明書が自動的に転送され、**SESSIONSECURITY** パラメーターが STRICT にリセットされます。
	以下のいずれかのコマンドを発行して、**SESSIONSECURITY** パラメーターの値を TRANSITIONAL に更新します。
	• クライアント・ノードの場合、次のコマンドを発行します。
	`update node node_name sessionsecurity=transitional`
	• 管理者の場合、次のコマンドを発行します。
	`update admin admin_name sessionsecurity=transitional`
	• サーバーの場合、次のコマンドを発行します。
	`update server server_name sessionsecurity=transitional`
	あるいは、dsmcert ユーティリティーを 使用して以下のコマンドを発行することによって、パブリック証明書を手動で転送およびインポートすることができます。
	`openssl s_client -connect tapsrv04:1500 -showcerts > tapsrv04.arm`
	`dsmcert -add -server tapsrv04 -file tapsrv04.arm`
	CA 署名証明書を使用している場合は、SSL 通信を開始するクライアント、サーバー、およびストレージ・エージェントの各鍵データベースに、CA ルート証明書と任意の CA 中間証明書をインストールする必要があります。

IBM Spectrum Protect サーバー間の証明書の交換は正常に完了しませんでした。	新しいプロトコルを使用する場合、サーバーのパブリック証明書の自動転送が実行されるのは、セキュリティーの機能が拡張されたサーバーへの初回接続時のみです。初回接続の後、サーバーの **SESSIONSECURITY** パラメーター値は TRANSITIONAL から STRICT に変更されます。 2 つの IBM Spectrum Protect サーバー間の証明書交換を再試行します。詳しくは、サーバー間の証明書交換の再試行を参照してください。
IBM Spectrum Protect サーバーとクライアント・ノード間の証明書の交換が失敗しました。	新しいプロトコルを使用する場合、サーバーのパブリック証明書の自動転送が実行されるのは、セキュリティーの機能が拡張されたサーバーへの初回接続時のみです。初回接続の後、ノードの **SESSIONSECURITY** パラメーター値は TRANSITIONAL から STRICT に変更されます。 V8.1.2 より前のバージョンのクライアントとサーバー 間の証明書の交換を再度試みるには、以下のステップを実行します。 1. cert.arm 証明書を使用する SSL を使用するように構成された既存のクライアントの場合、`cert256.arm` 証明書を使用するようにクライアントを再構成します。手順については、IBM Knowledge Center の『*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。 2. サーバー・インスタンス・ディレクトリーから次のコマンドを発行して、デフォルトの証明書を更新します。 `gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed -label "TSM Server SelfSigned SHA Key"` 3. サーバーを再始動します。 V8.1.2 以降のクライアントおよびサーバーの 場合、証明書は自動的に配布されます。 クライアントまたはサーバーの 間の通信が失敗した場合、証明書の取得を再試行するには、以下のステップを実行します。

症状	解決方法

	1. ノードおよび管理者の場合、再試行するノードまたは管理者ごとに以下のコマンドを発行して、**SESSIONSECURITY** パラメーターを TRANSITIONAL に設定します。
	`update node nodename sessionsecurity=transitional`
	`update admin adminname sessionsecurity=transitional`
	ヒント : 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。
	• 管理者アカウントがログイ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、その管理者アカウントがコマンド・ルーティングに使用される前に、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 以降のクライアントを使用して V8.1.2 以降のサーバーに対して認証を行った後は、管理者は V8.1.2 以降を使用するクライアントあるいはサーバー上でしか認証できなくなります。 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。
	2. ストレージ・エージェントの場合は、STRICT 値を TRANSITIONAL に変更して、ストレージ・エージェント・オプション・ファイルの `dsmsta.opt` の **STASESSIONSECURITY** オプションを更新します。
	3. サーバーを再始動します。証明書の変更は、サーバーまたはストレージ・エージェントを再始動するまで有効になりません。
	4. ステップ 1 から 4 を完了した後も証明書を交換できない場合は、証明書をサーバーとストレージ・エージェントに手動で追加して、サーバーとストレージ・エージェントを再始動します。手順については、IBM Knowledge Center の『*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。

証明書をクライアント・システムに手動で配布します。	IBM Spectrum Protect サーバー管理者は、バックアップ/アーカイブ・クライアントを自動的にデプロイして、バックアップ/アーカイブ・クライアントが既にインストールされたワークステーションを更新することができます。詳しくは、IBM Knowledge Center の『バックアップ/アーカイブ・クライアントの自動デプロイメント』を参照してください。 証明書を手動でクライアントに追加するには、IBM Knowledge Center の『*Secure Sockets Layer* を使用した *IBM Spectrum Protect* クライアント/サーバー通信の構成』を参照してください。
クライアント・セッションに対するクライアントの証明書をリセットします。	IBM Spectrum Protect バックアップ/アーカイブ・クライアントとともにインストールされる dsmcert ユーティリティーは、サーバー証明書の証明書ストアを作成するために使用されます。dsmcert ユーティリティーを 使用してファイルを削除し、証明書を再インポートします。
非 root ユーザーが root ユーザーのファイルを管理できるように root ユーザーが許可します。	V8.1.0 および V7.1.6 以前の IBM Spectrum Protect クライアントで非 root ユーザーが前に使用していた承認コミュニケーション・エージェント (TCA) は使用できなくなりました。root ユーザーは、非 root ユーザーによるファイルの管理を許可するために以下の方法を使用できます。

症状	解決方法
	ヘルプ・デスク方式 ヘルプ・デスク方式では、root ユーザーはすべてのバックアップ操作およびリストア操作を実行することができます。非 root ユーザーは、root ユーザーに連絡して、特定のファイルをバックアップまたはリストアするように要求する必要があります。 **許可ユーザー方式** 許可ユーザー方式では、passworddir オプションを使用して、非 root ユーザーが読み取りおよび書き込み可能なパスワード・ロケーションを指定することで、非 root ユーザーにパスワード・ストアへの読み取り/書き込みアクセス権が付与されます。 この方式を使用すると、非 root ユーザーは、自分が所有するファイルのバックアップおよびリストア、暗号化の使用、および passwordaccess generate オプションによる自身のパスワードの管理を行うことができます。 詳しくは、IBM Knowledge Center の「非 *root* ユーザーによる自分のデータの管理の有効化 」を参照してください。 これらのいずれの方法でも不十分な場合は、TCA が含まれている以前のクライアントを使用する必要があります。
GSKit の互換性の問題を解決します。	GSKit を使用する複数のアプリケーションが同じシステムにインストールされている場合、非互換性の問題が発生する可能性があります。その問題を解決するには、以下の情報を参照してください。 • IBM Spectrum Protect クライアントの場合、技術情報 2011742 を参照してください。 • Db2 の場合、技術情報 7050721 を参照してください。 • IBM Spectrum Protect サーバーの場合、技術情報 2007298 を参照してください。 • 同じ Windows システム上の IBM Spectrum Protect サーバーとクライアントの場合、技術情報 7050721 を参照してください。

セキュリティー更新のトラブルシューティングについては、技術情報 2004844 を参照してください。

サーバー間の証明書交換の再試行

サーバー間の証明書交換が失敗した場合は、再度の交換を試みることができます。

手順

1. 両方のサーバーで次のコマンドを発行して、パートナー・サーバーのデータベースから証明書を削除します。

   ```
   update server servername forcesync=yes
   ```

   ヒント: このタスクのステップを完了してサーバーを再始動した後も、サーバー間セッションのたびにエラー・メッセージが引き続き表示される場合、サーバーは誤った証明書を使用している可能性があります。サーバーにより誤った証明書の使用が試みられていると判断した場合は、以下のコマンドを発行して鍵データベースから証明書を削除します。

   ```
   gsk8capicmd_64 -cert -delete -db cert.kdb -stashed -label certificate_labelname
   ```

2. サーバーとパートナー・サーバーの両方に対して **DELETE SERVER** コマンドを発行して、サーバー定義を削除します。サーバー定義を削除できない場合、証明書を手動で構成する必要があります。手動で証明書を構成する手順については、IBM Knowledge Center の「*SSL* を使用した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。

3. 証明書を再取得するには、各サーバーを相互に定義し、両方のサーバーで以下のコマンドを発行してサーバーが証明書を交換できるようにします。

```
set crossdefine on
set serverhladdress hladdress
set serverlladdress lladdress
set serverpassword password
```

4. 相互定義を行っているサーバーのいずれかで以下のコマンドを発行します。

```
define server servername crossdefine=yes ssl=yes
```

5. その他のバージョン 8.1.2 以降のサーバー・ペアすべてに対して、ステップ 3 を繰り返します。
6. サーバーを再始動します。
7. 証明書が交換されたことを確認するには、検証する各サーバーのサーバー・インスタンス・ディレクトリーから以下のコマンドを発行します。

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

出力例:

```
example.website.com:1542:0
```

ヒント: 複製を使用する場合は、約 5 分ごとに実行される複製ハートビートにより、サーバーのアップグレード後の初回接続時に証明書交換が開始されます。この接続により、証明書交換が実行される前に、メッセージの ANR8583E および ANR8599W がログに 1 回表示されます。複製を使用しない場合はサーバー間セッションの初回開始時に証明書が交換されます。ただし、両方のコンピューターに定義されたサーバーがないサーバー構成を除きます。

8. 仮想ボリュームとして定義されているサーバーの場合は、以下のステップを実行します。
   a) 両方のサーバーで次のコマンドを発行して、サーバーのデータベースからパートナー証明書を削除します。

   ```
   update server servername forcesync=yes
   ```

   b) ソース・サーバー上の **DEFINE SERVER** コマンドのサーバー・パスワード値、仮想ボリューム・サーバー上の **REGISTER NODE** コマンドのパスワード値、および仮想ボリューム・サーバー上の **SET SERVERPASSWORD** 値に、同じパスワードを使用するようにしてください。必要に応じて、**UPDATE SERVER**、**UPDATE NODE**、または **SET SERVERPASSWORD** の各コマンドを使用してパスワードを更新します。証明書は、仮想ボリューム・サーバーからソース・サーバーへの初回のクライアント・バックアップ操作の後に交換されます。
9. それでもサーバー間で証明書を交換できない場合は、以下のステップを実行します。
   a) 各通信サーバーのサーバー定義において、指定したサーバー名が、パートナー・サーバーで **SET SERVERNAME** コマンドを発行して設定された名前と一致することを確認します。
   b) サーバー定義に **SET SERVERPASSWORD** コマンドで指定したパスワードが設定されていることを確認します。 このパスワードは、パートナー・サーバーの **SET SERVERNAME** コマンドで指定した値と一致していることが必要です。
   c) ステップ a と b の完了後、次のコマンドを再発行します。

   ```
   update server servername forcesync=yes
   ```

   d) ステップ 1 から 3 を再試行します。

最適なパフォーマンスのための計画

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

このタスクについて

IBM Spectrum Protect Blueprints を使用することで、最適な IBM Spectrum Protect 環境がセットアップされます。

手順

1. 3 ページの『インストールを開始する前の前提知識』を確認します。
2. 以下の各サブセクションを確認します。

サーバーのハードウェアおよびオペレーティング・システムの計画

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

質問	タスク、特性、オプション、または設定	詳細情報
オペレーティング・システムおよびハードウェアが要件を満たしているか上回っていますか? • プロセッサーの数と速度 • システム・メモリー • サポートされるオペレーティング・システム・レベル	必須メモリーの最小容量を使用している場合、最小の作業負荷をサポートすることができます。 システム・メモリーを追加することでパフォーマンスが向上するかを実験することができます。 その後、そのシステム・メモリーをサーバー専用にしたままにするかを決定します。 毎日のサーバー作業負荷のサイクル全体を使用して、メモリーのバリエーションをテストします。 システム上で複数のサーバーを稼働させる場合、システムの要件を満たすように各サーバーの要件を追加します。 **制約事項 :** Active Memory Expansion (AME) を使用しないでください。AME を使用する場合、IBM Db2 ソフトウェアでは、64 KB のページではなく 4 KB のページを使用します。4 KB の各ページはアクセスすると圧縮解除され、必要ない場合には圧縮されます。 圧縮または圧縮解除が行われると、Db2 とサーバーはそのページへのアクセスを待機し、サーバーのパフォーマンスが低下します。	オペレーティング・システムの要件は、技術情報 1243309 で参照してください。 さらに、オペレーティング・システムおよびその他のアプリケーションのタスクのチューニングのガイダンスも確認します。 これらの機能を使用している場合の要件について詳しくは、以下のトピックを参照してください。 • データ重複排除のチェックリスト • ノード複製のチェックリスト サーバーとストレージのサイズ設定の要件については、IBM Spectrum Protect Blueprint を参照してください。
最適なパフォーマンスを得るようにディスクが構成されていますか?	各種ディスク・システムで実行可能なチューニングの量は、それぞれ異なります。 適切なキュー項目数とその他のディスク・システム・オプションが設定されていることを確認してください。	詳細については、以下のトピックを参照してください。 • "サーバー・データベース・ディスクの計画" • "サーバー・リカバリー・ログ・ディスクの計画" • "DISK 装置クラスまたは FILE 装置クラスのストレージ・プールの計画"

質問	タスク、特性、オプション、または設定	詳細情報
サーバーに十分なメモリーがありますか?	作業負荷が大きい場合やデータ重複排除やノード複製などの拡張機能を使用する場合、システム要件の資料で示されている最小システム・メモリーより多くのメモリーが必要になります。 データ重複排除が有効にされていないデータベースでは、以下のガイドラインを使用してメモリー要件を指定してください。 • 500 GB 未満のデータベースの場合、16 GB のメモリーが必要です。 • サイズが 500 GB から 1 TB のデータベースの場合、24 GB のメモリーが必要です。 • サイズが 1 TB から 1.5 TB のデータベースの場合、32 GB のメモリーが必要です。 • 1.5 TB より大きいデータベースの場合、40 GB のメモリーが必要です。 複製処理のための活動ログおよびアーカイブ・ログ用に追加のスペースを割り振るようにしてください。	これらの機能を使用している場合の要件について詳しくは、以下のトピックを参照してください。 • データ重複排除のチェックリスト • ノード複製のチェックリスト • メモリー所要量
システムには、IBM Spectrum Protect サーバーが同時に実行する必要があるデータ操作を処理するのに十分なホスト・バス・アダプター (HBA) がありますか?	どの操作が同時に HBA を使用する必要があるかを理解します。 例えば、サーバーは、ストレージ・プール・マイグレーションを 0.5 GB/秒の容量で完了する必要があると同時に、1 GB/秒のバックアップ・データを保管する必要があるとします。 HBA は、必要な速度ですべてのデータを処理できなければなりません。	HBA キャパシティーのチューニングを参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
ネットワーク帯域幅は、予定されているバックアップの最大スループットより大きいですか?	ネットワーク帯域幅は、システムがバックアップなどの操作を許可された時間内あるいはサービス・レベル・コミットメントを満たす時間内に完了できるものでなければなりません。 ノード複製の場合、ネットワーク帯域幅は、予定されている最大スループットより大きくなければなりません。	詳細については、以下のトピックを参照してください。 • ネットワーク・パフォーマンスのチューニング • ノード複製のチェックリスト
IBM Spectrum Protect サーバー・ファイルに推奨されるファイル・システムを使用していますか?	最適なパフォーマンスとデータ可用性を確実に得るために、ファイル・システムを使用してください。 サーバーは、その機能をサポートするファイル・システムとの直接入出力を使用します。 直接入出力を使用することで、スループットを向上させ、プロセッサーの使用を削減することができます。ご使用のオペレーティング・システムに合う推奨ファイル・システムについて詳しくは、IBM Spectrum Protect server-supported file systems を参照してください。	詳しくは、ディスク・パフォーマンスのためのオペレーティング・システムの構成を参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
十分なページング・スペースの構成を計画していますか?	ページ・スペースあるいはスワップ・スペースは、処理に使用可能なメモリーを拡張します。 システム内の RAM の空き容量が少ない場合、使用していないプログラムやデータは、メモリーからページング・スペースに移動されます。このアクションにより、メモリーがデータベース操作などの他の活動用に解放されます。 **制約事項 :** メモリーをシステムに追加する際にページング・スペースを使用しないでください。ページング・スペースは、限定された一時的なスペース拡張のみを提供するためのものです。システムでページング・スペースを使用すると、システム・メモリーが満杯になり、拡張が必要になります。 最小 32 GB のページング・スペースまたはご使用の RAM の 50% のいずれか大きいほうの値を使用します。	

サーバー・データベース・ディスクの計画

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

質問	タスク、特性、オプション、または設定	詳細情報
データベースは、高速で待ち時間が短いディスク上にありますか?	IBM Spectrum Protect データベースには、以下のドライブを使用しないでください。 • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) ほとんどのサーバー・ハードウェアにデフォルトで組み込まれている内蔵ディスクは使用しないでください。 ファイバー・チャネルまたは SAS インターフェースを 備えたエンタープライズ・レベルのソリッド・ステート・ディスク (SSD) は、最高のパフォーマンスを提供します。 IBM Spectrum Protect のデータ重複排除機能を使用する予定の場合は、1 秒あたりの入出力操作 (IOPS) の観点からディスク・パフォーマンスに焦点を置いてください。	詳しくは、データ重複排除のチェックリストを参照してください。
データベースは、活動ログ、アーカイブ・ログ、およびストレージ・プール・ボリュームに使用されているディスクあるいは LUN とは別のディスクまたは LUN に保管されていますか?	サーバー・データベースを他のサーバー・コンポーネントと分離することで、同時に実行する必要があるさまざまな操作による同じリソースの競合を減らすことができます。 **ヒント:** ソリッド・ステート・ドライブ (SSD) テクノロジーを使用する場合、データベースとアーカイブ・ログはアレイを共有できます。	
RAID を使用している場合、システムに最適な RAID レベルを選択する方法を知っていますか? すべての LUN を同じサイズとタイプの RAID を使用して定義していますか?	システムで非常に多くの書き込みを行う必要がある場合、RAID 10 は RAID 5 より優れたパフォーマンスを提供します。ただし、RAID 10 では、同じ容量の使用可能なストレージを確保するために RAID 5 より多くのディスクが必要です。 ご使用のディスク・システムが RAID の場合、すべての LUN を同じサイズとタイプの RAID を使用して定義してください。 例えば、4+1 RAID 5 と 4+2 RAID 6 を混用しないでください。	

質問	タスク、特性、オプション、または設定	詳細情報
ストリップ・サイズまたはセグメント・サイズを設定するオプションが使用可能な場合、ディスク・システムを構成する時にそのサイズを最適化するように計画していますか?	ストリップ・サイズまたはセグメント・サイズを設定できる場合、データベース用のディスク・システムでは 64 KB または 128 KB のサイズを使用してください。	データベースに使用するブロック・サイズは、表スペースに応じて変化します。 ほとんどの表スペースでは、8 KB のブロックを使用しますが、一部では 32 KB のブロックを使用します。
データベース用に少なくとも 4 つのディレクトリー (ストレージ・パスとも呼ばれる) を 4 つの異なる LUN 上に作成するように計画していますか? サブシステム上の個別のアレイごとに、1 つのディレクトリーを作成します。 アレイの数が 3 つに満たない場合、アレイ内に個別の LUN ボリュームを作成します。	作業負荷が大きくなったり、一部のフィーチャーを使用することで、最小要件より多くのデータベース・ストレージ・パスが必要になります。 データ重複排除のようなサーバー操作は、データベースに対する 1 秒当たりの入出力操作 (IOPS) の駆動回数が高くなります。このような操作は、データベースに多くのディレクトリーがある場合、パフォーマンスが向上します。 2 TB より大きい、あるいはそのサイズまで増大することが予想されるサーバー・データベースの場合、8 つのディレクトリーを使用してください。 作成するストレージ・パス数を決定する際には、予定されているシステムの増大量を考慮してください。サーバーが最初に作成されたときにストレージ・パスが存在している場合、サーバーは、より多くのストレージ・パスをより効率的に使用します。 *DB2_PARALLEL_IO* 変数を使用すると、1 つのコンテナーが含まれる表スペース、または複数の物理ディスクにコンテナーが含まれる表スペースで、強制的に並列入出力が行われます。 *DB2_PARALLEL_IO* 変数を設定しない場合、入出力並列処理は、表スペースに使用されるコンテナー数と等しくなります。 例えば、表スペースに 4 つのコンテナーが含まれる場合、使用される入出力並列処理のレベルは 4 になります。	詳細については、以下のトピックを参照してください。 • データ重複排除のチェックリスト • ノード複製のチェックリスト サーバーがデータを重複排除する場合の増大量を予測するには、技術情報 1596944 を参照してください。 IBM Spectrum Protect サーバーのデータベース・サイズ、データベース再編成、およびパフォーマンスの考慮事項に関する最新情報については、技術情報 1683633 を参照してください。 *DB2_PARALLEL_IO* 変数の設定については、IBM Db2 レジストリー変数の推奨設定を参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
データベース用のディレクトリーはすべて同じサイズですか?	すべてのディレクトリーのサイズを同一にすることで、データベース操作の並列処理の度合いが確実に一貫性のあるものになります。 データベース用のディレクトリーの中に他のディレクトリーより小さいものが 1 つ以上ある場合、並列プリフェッチが最適化される可能性が低下します。 この指針は、サーバーの初期構成の後にストレージ・パスを追加する必要がある場合にも適用されます。	
AIX® システム上のデータベース LUN のキュー項目数を増やすように計画していますか?	多くの場合、デフォルトのキュー項目数は少なすぎます。	ディスク・パフォーマンスのための AIX システムの構成を参照してください。

サーバーの回復ログ・ディスクの計画

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

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

質問	タスク、特性、オプション、または設定	詳細情報
ログは、作業負荷に十分に対応するサイズに設定するよう計画していますか?	作業負荷が不明な場合は、できるだけ大きなサイズを使用してください。 **活動ログ** 最大サイズは 512 GB です。 **ACTIVELOGSIZE** サーバー・オプションを使用して設定します。 固定サイズの活動ログが作成された後に、活動ログ・ファイル・システム上に少なくとも 8 GB のフリー・スペースがあることを確認します。 **アーカイブ・ログ** アーカイブ・ログのサイズは、サーバー・オプションではなく、ログが配置されているファイル・システムのサイズによって制限されます。 アーカイブ・ログは、少なくとも活動ログと同じ容量にします。	• ログのサイズ設定について詳しくは、技術情報 400357 のリカバリー・ログ情報を参照してください。 • データ重複排除を使用する場合のサイズ設定について詳しくは、データ重複排除のチェックリストを参照してください。
アーカイブ・フェイルオーバー・ログを定義していますか? そのログは、アーカイブ・ログとは別のディスク上に配置するよう計画していますか?	アーカイブ・フェイルオーバー・ログは、アーカイブ・ログが満杯になったときに、サーバーが緊急で使用するためのものです。 アーカイブ・フェイルオーバー・ログには、低速なディスクを使用しても構いません。	**ARCHFAILOVERLOGDIRECTORY** サーバー・オプションを使用して、アーカイブ・フェイルオーバー・ログの配置場所を指定します。 アーカイブ・フェイルオーバー・ログのディレクトリーの使用量をモニターしてください。 サーバーがアーカイブ・フェイルオーバー・ログを使用する必要がある場合、アーカイブ・ログのスペースが不足しています。
活動ログをミラーリングしている場合、1 つのタイプのミラーリングのみを使用していますか?	以下のいずれかの方法を使用して、ログをミラーリングすることができます。 ログのミラーリングには、1 つのタイプのみを使用してください。 • IBM Spectrum Protect サーバーで使用可能な **MIRRORLOGDIRECTORY** オプションを使用して、ミラーリングする場所を指定する。 • ソフトウェア・ミラーリング (Logical Volume Manager (LVM) on AIX など) を使用する。 • ディスク・システム・ハードウェア内のミラーリングを使用する。	活動ログをミラーリングする場合、活動ログとミラー・コピーに使用するディスクの両方が同じ速度と信頼性を備えている必要があります。 詳しくは、回復ログの構成およびチューニングを参照してください。

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

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

質問	タスク、特性、オプション、または設定	詳細情報
1 秒当たりの入出力操作 (IOPS) を単位として測定する際、IBM Spectrum Protect データベースに高速ディスク・ストレージを使用していますか？	データベースには、高パフォーマンス・ディスクを使用します。データ重複排除処理のために、ソリッド・ステート・ドライブ・テクノロジーを使用します。 データベースには最小で 3000 IOPS の処理能力があることを確認してください。日次バックアップのデータ量 (データ重複排除前) 1 TB につき 1000 IOPS をこの最小値に追加してください。 例えば、毎日 3 TB のデータを取り込む IBM Spectrum Protect サーバーでは、データベース・ディスクに 6000 IOPS の処理能力が必要です。 `3000 IOPS minimum + 3000 (3 TB x 1000 IOPS) = 6000 IOPS`	ディスク選択の際の推奨事項は、「サーバー・データベース・ディスクの計画」を参照してください。 IOPS の詳細については、「IBM Spectrum Protect Blueprints」を参照してください。
データベースのサイズに対して十分なメモリーがありますか?	データベース・サイズが 100 GB でデータの重複排除を行う IBM Spectrum Protect サーバーでは、最小で 40 GB のシステム・メモリーを使用してください。 バックアップ・データの保存容量が増える場合、メモリー所要量を増やすことが必要な場合があります。 定期的にメモリー使用量をモニターし、追加のメモリーが必要かどうかを判別してください。 データベース・ページのキャッシュ機能を向上させるために、追加システム・メモリーを使用してください。以下のメモリー・サイズのガイドラインは、バックアップする新規データの日次量に基づいています。 • データの日次バックアップ用に 128 GB システム・メモリー (ここでデータベース・サイズは 1 TB から 2 TB) • データの日次バックアップ用に 192 GB システム・メモリー (ここでデータベース・サイズは 2 TB から 4 TB)	メモリー所要量

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

質問	タスク、特性、オプション、または設定	詳細情報
データ重複排除で使用する予定の IBM Spectrum Protect サーバーごとに、最小で 8 個 (2.2 GHz またはそれと同等) のプロセッサー・コアを使用していますか?	クライアント・サイド・データ重複排除を使用する計画の場合は、データ重複排除処理の実行に使用できる十分なリソースがバックアップ操作時にクライアント・システムにあることを確認してください。クライアント・サイド・データ重複排除では、バックアップ・プロセス当たり少なくとも 1 つの 2.2 GHz プロセッサー・コアに相当するプロセッサーを使用してください。	• データ重複排除 FAQ • IBM Spectrum Protect Blueprints
データベース用に十分なストレージ・スペースを割り振りましたか?	大まかな見積もりとして、重複排除ストレージ・プールで保護される 25 TB のデータごとに、100 GB のデータベース・ストレージを計画してください。「保護データ」とは、データ重複排除を行う前のデータ量で、保管されているすべてのバージョンのオブジェクトが含まれます。 ファイルの平均サイズが 512 KB 未満の小さなファイルを多数使用するデータベース・バックアップ操作では、より多くのデータベース・スペースが必要です。より小さなオブジェクト・サイズに対しては、10 TB 保管ごとに 100 GB のデータベース・スペースを計画してください。 ベスト・プラクティスとしては、データ重複排除に専用の新規コンテナー・ストレージ・プールを定義してください。 データ重複排除はストレージ・プール・レベルで行われ、暗号化データを除くストレージ・プール内のすべてのデータが重複排除されます。	IBM Spectrum Protect Blueprints を使用することで、最適な IBM Spectrum Protect 環境がセットアップされます。

質問	タスク、特性、オプション、または設定	詳細情報
ご使用の環境のサイズに十分なスペースを構成するために、ストレージ・プール容量を見積もりましたか?	以下の方法を使用して、重複排除に必要なストレージ・プール容量を見積もることができます。 1. ソース・データのベース・サイズを見積もる。 2. 見積もられた変更率および成長率を使用して、毎日のバックアップ・サイズを見積もる。 3. 保存要件を決定する。 4. ベース・サイズ、毎日のバックアップ・サイズ、および保存要件を因数処理することで、ソース・データの総量を見積もる。 5. 重複排除の比率因数を適用する。 6. 圧縮の比率因数を適用する。 7. 一時的なストレージ・プールの使用を考慮するために、見積もり値を切り上げる。	この手法の使用例については、データ重複排除 FAQ を参照してください。
ディスク入出力を多くのディスク装置およびコントローラーに分散させていますか?	できるだけ多くのディスクから構成されたアレイを使用してください (ワイド・ストライピングと呼ばれることもあります)。 サブシステム上の個別のアレイごとに、1 つのデータベース・ディレクトリーを使用するようにしてください。 表スペース内のコンテナーが複数の物理ディスクにまたがる場合に、使用される表スペースごとの並列入出力を可能にするため、*DB2_PARALLEL_IO* レジストリー変数を設定してください。 入出力帯域幅が使用可能で、かつファイルのサイズが大きい (例えば、1 MB) 場合は、プロセッサー全体のリソースが、重複の検出処理に占有される可能性があります。 ファイルのサイズが小さい場合は、その他のボトルネックが発生する可能性があります。 重複排除ストレージ・プール・デバイス・クラスに 8 個以上のファイル・システムを指定し、入出力ができるだけ多くの LUN および物理装置に分散されるようにします。	ストレージ・プールをセットアップするためのガイドラインとしては、「DISK 装置クラスまたは FILE 装置クラスのストレージ・プールの計画」を参照してください。 *DB2_PARALLEL_IO* 変数の設定については、IBM Db2 レジストリー変数の推奨設定を参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
バックアップ・ストラテジーに基づいて日次操作をスケジュールしていますか?	操作の最適な順序は、以下の順番です。 1. クライアント・バックアップ 2. ストレージ・プールの保護 3. ノード複製 4. データベース・バックアップ 5. インベントリーの期限切れ	• データ重複排除およびノード複製プロセスのスケジューリング • ディレクトリー・コンテナー・ストレージ・プールの日次操作
ストレージ・プールの破損ファイルを特定するために監査操作をスケジュールしていますか?	監査操作をスケジュールするには、**DEFINE STGRULE** コマンドを使用して、**ACTIONTYPE=AUDIT** パラメーターを指定します。 ベスト・プラクティスとして、監査操作が継続的に実行されるように、**DELAY** パラメーターを指定しないでください。	
IBM Db2 ロック・リストを管理するために十分なストレージがありますか?	ラージ・ファイルまたは多数のファイルを同時に含むデータを重複排除する場合、プロセスによってストレージ・スペースの容量が不十分になる可能性があります。 ロック・リスト・ストレージの容量が不十分な場合、バックアップの失敗、データ管理プロセスの失敗、またはサーバーの停止が発生する可能性があります。 データ重複排除で処理されるファイルのサイズが 500 GB を超えている場合は、ストレージ・スペースを使い切る可能性が高くなります。ただし、クライアント・サイド・データ重複排除を使用しているバックアップ操作の数が多い場合は、それより小さいサイズのファイルでもこの問題が発生する可能性があります。	Db2 **LOCKLIST** パラメーターのチューニングについて詳しくは、サーバー・サイドのデータ重複排除のチューニングを参照してください。
IBM Spectrum Protect サーバーにデータを転送できる十分な帯域幅が使用可能ですか?	データを IBM Spectrum Protect サーバーに転送する場合、必要な帯域幅を減らすために、クライアント・サイドまたはサーバー・サイドのデータ重複排除と圧縮を使用します。 インライン圧縮を使用するには V7.1.5 以上のサーバーを使用して、拡張圧縮処理を有効にするには V7.1.6 以降のクライアントを使用します。	詳細については、**enablededup** クライアント・オプションを参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
各ストレージ・プールに割り当てるストレージ・プール・ディレクトリーの数を決定しましたか?	**DEFINE STGPOOLDIRECTORY** コマンドを使用して、ディレクトリーをストレージ・プールに割り当てます。 複数のストレージ・プール・ディレクトリーを作成し、各ディレクトリーが個別のディスク・ボリューム (LUN) にバックアップされるようにします。	
クラウド・コンテナー・ストレージ・プールで十分なディスク・スペースを割り振りましたか?	バックアップの失敗を回避するには、ローカル・ディレクトリーに十分なスペースが必要です。以下のリストを最適なディスク・スペースのガイドとして使用してください。 • シリアル接続 SCSI (SAS) および回転ディスクの場合、毎日のデータ削減 (圧縮およびデータ重複排除) の後に予想される新規データ量を計算します。 その量の最大 100 パーセント (テラバイト単位) をディスク・スペース用に割り振ります。 • オンプレミスのハイパフォーマンス・クラウド・システムに高速ネットワーク接続されているフラッシュ・ベース・ストレージ・システムの場合は、3 TB を提供します。 • ハイパフォーマンス・クラウド・システムに高速ネットワーク接続されているソリッド・ステート・ドライブ (SSD) システムの場合は、5 TB を提供します。	

質問	タスク、特性、オプション、または設定	詳細情報
適切なタイプのローカル・ストレージを選択しましたか?	ローカル・ストレージからクラウドへのデータ転送が、次のバックアップ・サイクルが開始される前に完了することを確認してください。 **ヒント:** データは、クラウドに移動された直後にローカル・ストレージから削除されます。 以下のガイドラインを使用します。 • ハイパフォーマンス・クラウド・システムを備えた大規模システムでは、フラッシュまたは SSD を使用します。オブジェクト・ストレージへの高速接続を備えた、専用の 10 GB 広域ネットワーク (WAN) リンクが必要です。 例えば、専用の 10 GB WAN リンクと、IBM Cloud Object Storage ロケーションまたは Amazon Simple Storage Service (Amazon S3) データ・センターへの高速接続がある場合は、フラッシュまたは SSD を使用します。 • 以下のシナリオでは、より大容量の 15000 rpm SAS ディスクを使用します。 – 中規模のシステム – 低速なクラウド接続 (例えば、1 GB) – 複数の地域にまたがるサービス・プロバイダーとして IBM Cloud Object Storage を使用する場合 • SAS または回転ディスクの場合、毎日のデータ削減 (圧縮およびデータ重複排除) の後に予想される新規データ量を計算します。 その量の最大 100 パーセント (テラバイト単位) をディスク・スペース用に割り振ります。	

質問	タスク、特性、オプション、または設定	詳細情報
クラウド・コンテナー・ストレージ・プールの場合、ストレージ・ルールとその各サブルールの並列処理の合計最大数を指定していますか?	並列処理の最大数を指定するには、**DEFINE STGRULE** コマンドを発行して、**MAXPROCESS** パラメーターを指定します。 デフォルト値は 8 です。例えば、デフォルト値の 8 が指定されており、ストレージ・ルールに 4 つのサブルールがある場合、そのストレージ・ルールが 8 つの並列処理、その各サブルールが 8 つの並列処理を実行できます。 小規模、中規模、および大規模の Blueprint システムで最適なスループットを得るために、以下の並列処理の最大数を使用してください。 • 小規模システム: 10 プロセス • 中規模システム: 25 プロセス • 大規模システム: 35 から 50 プロセス	
クラウド・コンテナー・ストレージ・プールの場合、オンプレミス IBM Cloud Object Storage システムを IBM Spectrum Protect と共に使用している場合に複数の Accesser® エンドポイントを定義していますか?	小規模、中規模、および大規模の Blueprint システムでパフォーマンスを最適化するために、データ取り込み要件に応じて、以下の数の Accesser に対して排他的アクセスを定義してください。 • 小規模システム: 1 Accesser • 中規模システム: 2 Accesser • 大規模システム: 3 から 4 の Accesser	詳しくは、IBM Spectrum Protect Cloud Blueprints を参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
クラウド・コンテナー・ストレージ・プールの場合、オンプレミス IBM Cloud Object Storage システムを IBM Spectrum Protect と共に使用している場合に複数の Accesser エンドポイントを定義していますか?	一般的に、小規模、中規模、および大規模の Blueprint システムで専用 IBM Cloud Object Storage エンドポイントに接続するには、以下のイーサネット機能が必要です。 • 小規模システム: 1 Gbit • 中規模システム: 5 Gbit • 大規模システム: 10 Gbit **ヒント:** オブジェクト・ストレージへのクライアント・データの取り込みおよび同時データ転送によっては、複数の 10 Gbit イーサネット・ネットワークが必要になる場合があります。 イーサネット接続を構成する場合、ネットワーク管理者と連携して、以下の要因について考慮してください。 • サーバーのイーサネット機能 • サーバーと IBM Cloud Object Storage エンドポイントの間のネットワークの特性 • クラウド・ストレージ・プールを介したオブジェクト・ストレージ上での最終取り込みポイント	

DISK 装置クラスまたは FILE 装置クラスのストレージ・プールの計画

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

質問	タスク、特性、オプション、または設定	詳細情報
ストレージ・プールの LUN は、時間制約内にワークロードを適切に処理するために、256 KB の順次読み取りおよび書き込み用のスループット速度を維持できますか?	ピークの負荷について計画する場合、サーバーがディスク・ストレージ・プールに対して同時に読み取りあるいは書き込みを行うすべてのデータを考慮してください。 例えば、同時に実行されるクライアント・バックアップ操作とサーバーのデータ移動操作 (マイグレーションなど) によって生じるデータの流れのピークについて考慮します。 IBM Spectrum Protect サーバーは、ストレージ・プールに対して大部分は 256 KB のブロックで読み取りおよび書き込みを行います。 ディスク・システムに処理能力がある場合は、ランダム読み取り/書き込み操作ではなく順次読み取り/書き込み操作を使用して、最適なパフォーマンスを得られるようにディスク・システムを構成します。	詳しくは、ディスク・システムの基本パフォーマンスの分析を参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
データベース用に十分なストレージ・スペースを割り振りましたか?	以下のデータベース・サイズ・ガイドラインは、大まかな見積もりとして、データベースの拡大を考慮した小規模、中規模、大規模の Blueprint システムをベースにしています。 • 小規模システム: 1 TB 以上 • 中規模システム: 2 TB 以上 • 大規模システム: 4 TB 以上 **ヒント:** 保護する必要があるデータ量、保管されるファイル数、およびデータ重複排除を使用するかどうかに基づいて、より多くのメモリーが必要になることがあります。データ重複排除を使用する場合、サーバー上の重複排除されたエクステントを判別するためにデータベースへの照会が頻繁に行われるため、データベースの負荷が大きくなります。 大まかな見積もりとして、重複排除ストレージ・プールで保護される 50 TB のデータごとに、100 GB のデータベース・ストレージを計画してください。「保護データ」とは、データ重複排除を行う前のデータ量で、保管されているすべてのバージョンのオブジェクトが含まれます。 保護データが数百 TB 存在する場合、または数 TB 単位のデータを毎日バックアップしている場合、データベースの開始サイズは 1 TB 以上でなければなりません。IBM Spectrum Protect を使用して、ご使用のシステムに合わせてデータベースをサイズ変更します。	IBM Spectrum Protect Blueprints を使用することで、最適な IBM Spectrum Protect 環境がセットアップされます。 データベース・サイズに基づいて、操作を完了するためにサーバーに割り振る必要がある最小メモリー量については、メモリー所要量を参照してください。
読み取りおよび書き込みキャッシュを使用するようにディスクが構成されていますか?	パフォーマンスを向上させるには、使用するキャッシュを増やします。	
IBM Spectrum Protect データベースをクラウド・オブジェクト・ストレージにバックアップする必要がありますか?	災害復旧目的のために、データベースのクラウド・オブジェクト・ストレージへのバックアップ、およびクラウド・オブジェクト・ストレージからのリストアが可能です。 データベース・バックアップ操作を効率的に実行するために、オブジェクト・ストレージ・エンドポイント、IBM Cloud Object Storage Accesser、ネットワーク帯域幅、およびデータ・ストリームを調整できます。	クラウド・オブジェクト・ストレージへのデータベース・バックアップの調整

質問	タスク、特性、オプション、または設定	詳細情報
FILE 装置クラスを使用するストレージ・プールの場合、ストレージ・プール・ボリュームを使用するのに適したサイズを判別しましたか?	ディスクを使用するストレージ・プールの最適なボリュームの数とサイズ に記載されている情報を確認します。FILE 装置クラス・ボリュームのサイズを推定するための情報がない場合は、50 GB のボリュームを使用して開始してください。	通常、ボリュームが小さすぎる場合、問題はより頻繁に発生します。 ボリュームのサイズが必要なサイズより大きい場合は、問題が報告されることはほとんどありません。 使用するボリューム・サイズを判別する場合、予防措置として、必要なサイズより大きいサイズを選択してください。
FILE 装置クラスを使用するストレージ・プールの場合、事前割り振りボリュームを使用していますか?	スクラッチ・ボリュームを使用すると、ファイルがフラグメント化される場合があります。 ストレージ・プールがボリュームを使い尽くしていないことを確認するには、**MAXSCRATCH** パラメーターをゼロより大きい値に設定します。	**DEFINE VOLUME** サーバー・コマンドを使用して、ストレージ・プールにボリュームを事前割り振りします。 **DEFINE STGPOOL** または **UPDATE STGPOOL** サーバー・コマンドを使用して、**MAXSCRATCH** パラメーターを設定します。
FILE 装置クラスを使用するストレージ・プールの場合、クライアント・セッションの最大数と定義済みのボリューム数を比較しましたか?	同時に実行されるクライアント・セッションの予想ピーク数を処理できるように、常にストレージ・プール内に十分な使用可能ボリュームを保持してください。 ボリュームには、スクラッチ・ボリューム、空ボリューム、または部分的に使用されたボリュームがあります。	FILE 装置クラスを使用するストレージ・プールの場合、一度にボリュームに書き込みを行えるのは 1 つのセッションまたはプロセスのみです。

質問	タスク、特性、オプション、または設定	詳細情報
FILE 装置クラスを使用するストレージ・プールの場合、装置クラスの **MOUNTLIMIT** パラメーターを、並行してマウントされる可能性があるボリューム数を構成するのに十分な大きさの値に設定していますか?	データ重複排除を使用するストレージ・プールの場合、通常、**MOUNTLIMIT** パラメーターの範囲は 500 から 1000 の間です。 **MOUNTLIMIT** の値を、すべてのアクティブ・セッションで必要なマウント・ポイントの最大数に設定します。必要なマウント・ポイントの最大数に影響する以下のパラメーターを確認してください。 • **MAXSESSIONS** サーバー・オプション。このオプションは、並行して実行できる IBM Spectrum Protect セッションの最大数です。 • **MAXNUMMP** パラメーター。このパラメーターは、各クライアント・ノードが使用できるマウント・ポイントの最大数を設定します。 例えば、クライアント・ノードのバックアップ・セッションの最大数が一般的に 100 で、各ノードで MAXNUMMP=2 が設定されている場合、100 個のノードに対してそれぞれ 2 個のマウント・ポイントを乗算することで、**MOUNTLIMIT** パラメーターの値 200 が得られます。	**REGISTER NODE** または **UPDATE NODE** サーバー・コマンドを使用して、クライアント・ノードの **MAXNUMMP** パラメーターを設定します。
DISK 装置クラスを使用するストレージ・プールの場合、各ファイル・システムに配置するストレージ・プール・ボリュームの数を判別しましたか?	DISK 装置クラスを使用するストレージ・プール用のストレージをどのように構成するかは、ディスク・システムに RAID を使用しているかどうかによって異なります。 RAID を使用していない場合は、物理ディスクごとに 1 つのファイル・システムを構成し、各ファイル・システムに対して 1 つのストレージ・プール・ボリュームを定義します。 *n*+1 個のボリュームで RAID 5 を使用している場合は、以下のいずれかの方法でストレージを構成します。 • LUN 上に *n* 個のファイル・システムを構成し、ファイル・システムごとに 1 つのストレージ・プール・ボリュームを定義する。 • LUN に対して 1 つのファイル・システムと *n* 個のストレージ・プール・ボリュームを構成する。	この指針に従ったレイアウト例については、サーバー・ストレージ・プールのレイアウト例を参照してください。

質問	タスク、特性、オプション、または設定	詳細情報
複数のファイル・システム間で入出力が分散されるようにストレージ・プールを作成しましたか?	必ず、各ファイル・システムをディスク・システム上の異なる LUN 上に配置してください。 一般に 10 個から 30 個のファイル・システムを持つことが適切な目標ですが、それらのファイル・システムは確実に約 250 GB 以上になるようにしてください。	詳細については、以下のトピックを参照してください。 • サーバーのディスク・ストレージのチューニング • ストレージ・プールとボリュームのチューニングおよび構成
ストレージ・プールの破損ファイルを特定するために監査操作をスケジュールしていますか?	監査操作をスケジュールするには、**DEFINE STGRULE** コマンドを使用して、**ACTIONTYPE=AUDIT** パラメーターを指定します。 監査操作を最適化し、継続的に実行されるようにするために、**DELAY** パラメーターは指定しないでください。	

正しいタイプのストレージ・テクノロジーの計画

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

手順

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

表 *5. IBM Spectrum Protect* 要件を提供するためのストレージ・テクノロジー・タイプ

ストレージ・テクノロジー・タイプ	データベース	活動ログ	アーカイブ・ログとフェイルオーバー・アーカイブ・ログ	ストレージ・プール
ソリッド・ステート・ディスク (SSD)	次の状況の場合は、データベースを SSD に配置します。 – IBM Spectrum Protect データ重複排除を使用している場合。 – 毎日 8 TB を超える新規データをバックアップする場合。	IBM Spectrum Protect データベースを SSD に配置する場合、ベスト・プラクティスとしては、活動ログを SSD に配置します。使用可能なスペースがない場合は、代わりに高パフォーマンス・ディスクを使用してください。	SSD は、データベースおよび活動ログに使用するために節約してください。 アーカイブ・ログとフェイルオーバー・アーカイブ・ログは、低速なストレージ・テクノロジー・タイプに配置することができます。	SSD は、データベースおよび活動ログに使用するために節約してください。 ストレージ・プールは、低速なストレージ・テクノロジー・タイプに配置することができます。

表 5. *IBM Spectrum Protect* 要件を提供するためのストレージ・テクノロジー・タイプ (続き)

ストレージ・テクノロジー・タイプ	データベース	活動ログ	アーカイブ・ログとフェイルオーバー・アーカイブ・ログ	ストレージ・プール
高パフォーマンス・ディスクは、以下の特性を備えています。 **– 15k rpm ディスク** **– 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**	高パフォーマンス・ディスクは、以下の状況で使用します。 – サーバーがデータ重複排除を行わない場合。 – サーバーがノード複製を行わない場合。 サーバー・データベースは、そのログとストレージ・プール、および他のアプリケーションのデータから切り離してください。	高パフォーマンス・ディスクは、以下の状況で使用します。 – サーバーがデータ重複排除を行わない場合。 – サーバーがノード複製を行わない場合。 パフォーマンスと可用性を確保するために、活動ログはサーバー・データベース、アーカイブ・ログ、およびストレージ・プールから切り離してください。	アーカイブ・ログおよびフェイルオーバー・アーカイブ・ログに高パフォーマンス・ディスクを使用することができます。 可用性を確保するために、これらのログはデータベースおよび活動ログから切り離してください。	ストレージ・プール用の高パフォーマンス・ディスクは、以下の状況で使用します。 – データが頻繁に読み取られる場合。 – データが頻繁に書き込まれる場合。 パフォーマンスと可用性を確保するために、ストレージ・プール・データはサーバー・データベースとログ、および他のアプリケーションのデータから切り離してください。
中パフォーマンス・ディスクまたは高パフォーマンス・ディスクは、以下の特性を備えています。 **– 10k rpm ディスク** **– ファイバー・チャネルまたは SAS インターフェース**	ディスク・システム内で異なるディスク・テクノロジーを混用する場合は、高速なディスクをデータベースおよび活動ログに使用します。 サーバー・データベースは、そのログとストレージ・プール、および他のアプリケーションのデータから切り離してください。	ディスク・システム内で異なるディスク・テクノロジーを混用する場合は、高速なディスクをデータベースおよび活動ログに使用します。 パフォーマンスと可用性を確保するために、活動ログはサーバー・データベース、アーカイブ・ログ、およびストレージ・プールから切り離してください。	アーカイブ・ログおよびフェイルオーバー・アーカイブ・ログに中パフォーマンスまたは高パフォーマンス・ディスクを使用することができます。 可用性を確保するために、これらのログはデータベースおよび活動ログから切り離してください。	ストレージ・プール用の中パフォーマンス・ディスクまたは高パフォーマンス・ディスクは以下の状況で使用します。 – データが頻繁に読み取られる場合。 – データが頻繁に書き込まれる場合。 パフォーマンスと可用性を確保するために、ストレージ・プール・データはサーバー・データベースとログ、および他のアプリケーションのデータから切り離してください。
SATA、Network Attached Storage	データベースにはこのストレージを使用しないでください。XIV ストレージ・システムにはデータベースを配置しないでください。	活動ログにはこのストレージを使用しないでください。	これらのログは一度だけ書き込みが行われ、読み取りも頻繁に行われないため、この低速なストレージ・テクノロジーを使用することができます。	低速ストレージ・テクノロジーは、以下の状況で使用します。 – データが頻繁に書き込まれない場合 (一度だけの書き込みなど)。 – データが頻繁に読み取られない場合。

表 5. *IBM Spectrum Protect* 要件を提供するためのストレージ・テクノロジー・タイプ *(続き)*				
ストレージ・テクノロジー・タイプ	**データベース**	**活動ログ**	**アーカイブ・ログとフェイルオーバー・アーカイブ・ログ**	**ストレージ・プール**
テープおよび仮想テープ				長期間保存する場合、あるいはデータを頻繁に使用しない場合に使用します。

サーバー・インストールへのベスト・プラクティスの適用

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

手順

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

ベスト・プラクティス	詳細情報
サーバー・データベースには高速のディスクを使用します。ファイバー・チャネルまたは SAS インターフェースを 備えたエンタープライズ・レベルのソリッド・ステート・ディスク (SSD) は、最高のパフォーマンスを提供します。	データベースには高速で待ち時間が短いディスクを使用します。データ重複排除およびノード複製を使用する場合は、SSD を使用することが基本です。 Serial Advanced Technology Attachment (SATA) および Parallel Advanced Technology Attachment (PATA) ディスクは使用しないでください。詳細およびヒントについては、以下のトピックを参照してください。 – "サーバー・データベース・ディスクの計画" – "正しいタイプのストレージ・テクノロジーの計画"
サーバー・システムに十分なメモリーがあることを確認してください。	オペレーティング・システムの要件は、技術情報 1243309 で参照してください。 作業負荷が大きくなると、最小要件より多くのリソースが必要になります。 データ重複排除やノード複製などの拡張機能を使用すると、システム要件の資料で示されている最小メモリーより多くのメモリーが必要になる可能性があります。 複数のインスタンスを実行する予定の場合、各インスタンスごとに、1 つのサーバー用にリストされているメモリーが必要です。1 つのサーバーで必要なメモリーに、システムで計画しているインスタンスの数を乗算します。

ベスト・プラクティス	詳細情報
サーバー・データベース、活動ログ、アーカイブ・ログ、およびディスク・ストレージ・プールを相互に分離して配置します。	すべての IBM Spectrum Protect ストレージ・リソースを別のディスク上に保持します。 ストレージ・プール・ディスクを、サーバー・データベースおよびログのディスクから分離して保持します。 ストレージ・プールとデータベースの両方が同じディスク上にあると、ストレージ・プール操作がデータベース操作を妨害する可能性があります。 理想的には、サーバー・データベースとログも相互に分離してください。 詳細およびヒントについては、以下のトピックを参照してください。 – "サーバー・データベース・ディスクの計画" – "サーバー・リカバリー・ログ・ディスクの計画" – "DISK 装置クラスまたは FILE 装置クラスのストレージ・プールの計画"
サーバー・データベースには、少なくとも 4 つのディレクトリーを使用します。 大規模なサーバーや拡張機能を使用するサーバーの場合は、8 つのディレクトリーを使用します。	各ディレクトリーを他の LUN および他のアプリケーションから分離された LUN 上に配置します。 サーバーのデータベースが 2 TB より大きい場合、あるいはそのサイズより大きくなると予想される場合、そのサーバーは大規模なサーバーとして考慮してください。 そのようなサーバーでは、8 つのディレクトリーを使用します。 「サーバー・データベース・ディスクの計画」を参照してください。
データ重複排除、ノード複製、あるいはその両方を使用している場合は、データベース構成およびその他の項目に関する指針に従ってください。	これらの機能が使用されている場合に、サーバーがどの程度の処理能力で稼働できるかという点で非常に重要であるため、サーバー・データベースは指針に従って構成してください。 詳細およびヒントについては、以下のトピックを参照してください。 – データ重複排除のチェックリスト – ノード複製のチェックリスト
FILE タイプのデバイス・クラスを使用するストレージ・プールの場合、ストレージ・プール・ボリュームのサイズに関する指針に従ってください。 通常、50 GB のボリュームが最適です。	ボリューム・サイズを判別するには、ディスクを使用するストレージ・プールの最適なボリュームの数とサイズ の情報を参照してください。 キャパシティー要件だけではなく、スループット要件にも基づいて、ストレージ・プール装置およびファイル・システムを構成します。 IBM Spectrum Protect で使用するストレージ・デバイスは、入出力が多い他のアプリケーションから分離し、そのストレージで十分なスループットが得られるようにしてください。 詳細については、DISK または FILE のストレージ・プールのチェックリストを参照してください。
IBM Spectrum Protect クライアント操作とサーバー保守活動をスケジュールし、それらの操作のオーバーラップを回避または最小化します。	詳細については、以下のトピックを参照してください。 – 日次操作のスケジュールのチューニング – サーバー構成のチェックリスト
継続的に操作をモニターします。	モニタリングを行うことで、問題を早期に発見することができ、原因の特定も容易になります。 最大 1 年間モニタリング・レポートの記録を保持することで、増大の傾向を把握し、増大に備えて計画することができます。 パフォーマンスのための環境のモニタリングおよび保守を参照してください。

IBM Spectrum Protect サーバーの最小システム要件

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

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

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

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

ハードウェア要件

表 1 に、AIX システムのサーバーに必要な最小ハードウェア要件が記載されています。サーバーが最小要件を満たしていない場合、インストールは失敗します。ディスク・スペースの計画について詳しくは、49 ページの『キャパシティー計画』を参照してください。

表 6. ハードウェア要件

ハードウェアのタイプ	ハードウェア要件
一般	ディスクのみの環境の場合、この製品とリリースでサポートされているオペレーティング・システムを実行できる、適切にプロビジョンされ、構成されたハードウェアを使用してください。 他のタイプのストレージ (テープなど) を使用する環境の場合、ご使用の装置のベンダーにサポート要件を問い合わせてください。
プロセッサー	IBM Spectrum Protect は POWER6® 以降のプロセッサーが必要です。

表 6. ハードウェア要件 (続き)

ハードウェアのタイプ	ハードウェア要件
ディスク・スペース	以下の最小値のディスク・スペース • インストール・ディレクトリー用に 7.5 GB • /tmp ディレクトリー用に 4 GB • /var ディレクトリー用に 2.5 GB • root ユーザーのホーム・ディレクトリー用に 128 MB • 共有リソース域用に 2 GB 問題が発生して診断が必要な場合、初期障害データ・キャプチャー機能 (FFDC) ログやその他の一時使用 (トレース・ログの収集など) に使用するために、システム上に使用可能な一時スペースあるいはその他のスペースを持つことが最適です。 データベースとログ・ファイル用にかなりの量の追加ディスク・スペースが必要です。データベースのサイズは、保管されるクライアント・ファイルの数、およびサーバーがそれらを 管理する方法によって異なります。デフォルトの活動ログ・スペースは 16 GB で、これはほとんどのワークロードおよび構成で必要な最小スペースです。 活動ログを作成する場合、複製を実行するために少なくとも 64 GB が必要です。 複製とデータ重複排除の両方を使用する場合は、128 GB の活動ログを作成してください。 アーカイブ・ログには、デフォルトの活動ログ・スペースの少なくとも 3 倍 (48 GB) のスペースを割り振ります。データ重複排除を使用する場合、あるいはクライアントから大量のワークロードが発生することが想定される場合は、十分なリソースを確保するようにしてください。 パフォーマンスを最適化し、入出力を容易にするには、データベースに対して少なくとも 2 つの等しいサイズのコンテナーまたは論理装置番号 (LUN) を指定します。さらに、各活動ログおよびアーカイブ・ログには、それぞれ独自のコンテナーまたは LUN が必要です。 ディスク・スペースについて詳しくは、49 ページの『キャパシティー計画』を参照してください。
メモリー	1 日当たりの日次取り込み量が 200 GB 以下の、最高 500 GB のデータベースを使用するサーバーの最小システム・メモリー要件を以下に示します。 • データ重複排除とノード複製なしの標準サーバー操作の場合 16 GB • データ重複排除またはノード複製を行う場合 24 GB • データ重複排除と同時にノード複製を行う場合 32 GB より大きなサイズのデータベースと、より高い取り込み能力に対応するための特定のメモリー所要量については、IBM Spectrum Protect サーバー・メモリーの調整表を参照してください。 データ重複排除を使用する場合のさらに具体的なメモリー要件については、オペレーティング・システムに応じた IBM Spectrum Protect Blueprint を参照してください。

ソフトウェア要件

45 ページの表 7 に、AIX システムのサーバーに必要な最小ソフトウェア要件が記載されています。

表 7. ソフトウェア要件

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	AIX 7.1 • AIX 7.1 TL5 および SP5 以降。 • xlC.rte 13.1 以降のファイル・セットを持つ、最小 C++ ランタイム・レベル。レベルが 13.1 未満である場合、ファイル・セットは自動的にアップグレードされます。このファイル・セットは、IBM C++ Runtime Environment Components for AIX の March 2016 フィックスパック・パッケージに含まれています。 AIX 7.2 • AIX 7.2 TL3 および SP3 以降。 • xlC.rte 13.1.3.1 以降のファイル・セットを持つ、最小 C++ ランタイム・レベル。レベルが 13.1.3.1 未満である場合、ファイル・セットは自動的にアップグレードされます。 • 技術情報 6430303 を参照してください。 AIX 保守レベルに関する 最新の推奨事項については、技術情報 21165448 を参照してください。
通信プロトコル	構成済みの通信方式
処理	非同期入出力を使用可能にする必要があります。
デバイス・ドライバー	IBM Spectrum Protect デバイス・ドライバーは、IBM 以外のドライブおよびテープ・ライブラリーに必要です。IBM Spectrum Protect デバイス・ドライバーのパッケージには、デバイス・ドライバー・ツールと ACSLS デーモンが入っています。 IBM 3590、3592、または Ultrium テープ・ライブラリーまたはドライブの 場合、IBM デバイス・ドライバーが必要です。 最新のデバイス・ドライバーをインストールしてください。IBM ドライバー・パッケージは、Fix Central で入手できます。 IBM Spectrum Protect サーバーで磁気テープ装置を使用する前に、デバイス・ドライバーを構成してください。
Gunzip ユーティリティー	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。
その他のソフトウェア	• Korn シェル (ksh) • Lightweight Directory Access Protocol (LDAP) サーバーを使用して IBM Spectrum Protect ユーザーを認証するには、以下のいずれかのディレクトリー・サーバーを使用する必要があります。 – Microsoft Active Directory (Windows Server 2012、Windows Server 2012 R2、Windows Server 2016) – IBM Security Directory Server V6.3 – IBM Security Directory Server V6.4

IBM Spectrum Protect サーバーとシステム上の他の IBM Db2 製品との互換性

Db2 サーバーと同じシステムに IBM Spectrum Protect 製品をデプロイして使用する他の製品を、いくつかの制限付きでインストールすることができます。

Db2 サーバーと同じシステムに IBM Spectrum Protect 製品を使用する他の製品をインストールして使用するためには、必ず次の基準が満たされていることを確認してください。

表 *8. IBM Spectrum Protect* サーバーとシステム上の他の *DB2®* 製品との互換性

基準	説明
バージョン・レベル	Db2 製品を使用する他の製品は、Db2 バージョン 9 以降を使用する必要があります。 Db2 製品では、バージョン 9 から製品のカプセル化と分離がサポートされます。このバージョンから、コード・レベルが異なる複数の Db2 製品のコピーを同一システム上で実行することができます。 詳細については、複数のコピーに関する情報 (Db2 製品情報) を参照してください。
ユーザー ID とディレクトリー	ユーザー ID、フェンス・ユーザー ID、インストールの場所、その他のディレクトリー、および関連情報が複数の Db2 のインストールにおいて共有されていないことを確認してください。ご使用の指定は、IBM Spectrum Protect サーバーのインストールと構成に使用した ID と場所とは異なっていなければなりません。**dsmicfgx** ウィザードを使用してサーバーを構成した場合、これらはウィザードの実行時に入力した値です。手動での構成方法を使用した場合、使用した手順を必要に応じて見直し、そのサーバーに使用した値を思い出してください。

表 8. *IBM Spectrum Protect* サーバーとシステム上の他の *DB2®* 製品との互換性 (続き)	
基準	**説明**
リソース割り振り	IBM Spectrum Protect サーバーと、Db2 製品を使用する他のアプリケーション両方の要件と比較して、システムのリソースと 機能を検討してください。 他の Db2 アプリケーションに十分なリソースを提供するためには、IBM Spectrum Protect サーバーの設定を変更して、サーバーが使用するシステム・メモリーおよびリソースを削減する必要がある場合があります。 同様に、プロセッサーまたはメモリーのリソースの獲得において、他の Db2 アプリケーション作業負荷が IBM Spectrum Protect サーバーと競合している場合は、予期されるクライアント作業負荷または他のサーバー操作の処理で、サーバーのパフォーマンスに悪影響がある場合があります。 リソースを分離して、複数のアプリケーションでのプロセッサー、メモリー、および他のシステム・リソースの調整と割り振りにより多くの能力を提供するには、ロジカル・パーティション (LPAR)、ワークロード・パーティション (WPAR)、または他の仮想ワークステーション・サポートを使用することを検討してください。例えば、Db2 アプリケーションを独自の仮想システムで実行します。

IBM Installation Manager

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

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

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

オファリング
ソフトウェア製品のインストール可能単位。

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

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

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

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

パッケージ・グループ
共通親ディレクトリーを共有するパッケージのセット。

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

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

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

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

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

サーバーの詳細を計画するためのワークシート

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

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

項目	名前とユーザー ID	ロケーション
IBM Spectrum Protect サーバーの始動と実行に使用する ID である、サーバーのインスタンス・ユーザー *ID*		
インスタンス・ユーザー ID を含むディレクトリーである、サーバーのホーム・ディレクトリー		
データベース・インスタンス名		

項目	名前とユーザー ID	ロケーション
サーバーのインスタンス・ディレクトリー。これは、特にこのサーバー・インスタンス用のファイル (サーバー・オプション・ファイルおよびその他のサーバー特有のファイル) を含むディレクトリーです。		
サーバー名。サーバーごとに固有の名前を使用してください。		

キャパシティー計画

IBM Spectrum Protect のキャパシティー計画には、データベース、リカバリー・ログ、および共有リソース域などのリソースの管理が含まれます。

始める前に

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

データベースのスペース 所要量の見積もり

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

このタスクについて

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

IBM Spectrum Protect データベースの最大サイズは 8 TB です。

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

ファイル数に基づくデータベース・スペース所要量の見積もり

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

このタスクについて

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

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

  制約事項 : このガイドラインには、データ重複排除中に使用されるスペースは含まれていません。
- キャッシュ・ファイル、コピー・ストレージ・プール・ファイル、活動データ・プール・ファイル、および重複排除されたファイルごとに、100 から 200 バイト。

- さまざまなデータ・アクセス・パターンや、データのサーバー・バックエンド・プロセスをサポートするには、データベースの最適化のために追加のスペースが必要です。余分なスペース量は、ファイル・オブジェクトの合計バイト数の見積もりの 50% に相当します。

以下の単一クライアントの例では、上記のガイドラインの最大値に基づいて計算が行われます。これらの例では、ファイル集約が使用される可能性については考慮されていません。一般に、小さいファイルを集約すると、必要なデータベース・スペースの量が削減されます。ファイルの集合は、スペース管理ファイルに影響を与えません。

手順

1. ファイル・バージョン数を計算します。ファイル・バージョン数を求めるために、以下の各値を加算してください。
   a) バックアップ・ファイルの数を計算します。
   例えば、500,000 個ものクライアント・ファイルが同時にバックアップされる可能性があります。この例では、ストレージ・ポリシーは、最大 3 個のバックアップ・ファイル・コピーを保持するように設定されています。

   ```
   500,000 files * 3 copies = 1,500,000 files
   ```

   b) アーカイブ・ファイル数を計算します。
   例えば、100,000 個ものクライアント・ファイルが、アーカイブ・コピーである場合があります。
   c) スペース管理対象ファイルの数を計算します。
   例えば、200,000 個ものクライアント・ファイルが、クライアント・ワークステーションからマイグレーションされる場合があります。

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

   ```
   (1,500,000 + 100,000 + 200,000) * 1000 = 1.8 GB
   ```

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

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

   ```
   100,000 files * 200 bytes = 19 MB
   ```

   b) コピー・ストレージ・プール・ファイルの数を計算します。
   すべての 1 次ストレージ・プールは、コピー・ストレージ・プールにバックアップされます。

   ```
   (1,500,000 + 100,000 + 200,000) * 200 bytes = 343 MB
   ```

   c) 活動ストレージ・プール・ファイルの数を計算します。
   1 次ストレージ・プールにあるすべての活動クライアント・バックアップ・データは、活動データ・ストレージ・プールにコピーされます。1 次ストレージ・プールで 1,500,000 個のバックアップ・ファイルの 500,000 個のバージョンが活動状態であると想定します。

   ```
   500,000 * 200 bytes = 95 MB
   ```

   d) 重複排除されたファイルの数を計算します。
   重複排除されたストレージ・プールに、50,000 個のファイルが含まれていると想定します。

   ```
   50,000 * 200 bytes = 10 MB
   ```

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

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

```
(1.8 + 0.5) * 50% = 1.2 GB
```

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

```
1.8 + 0.5 + 1.2 = 3.5 GB
```

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

```
500 * 3.5 = 1.7 TB
```

タスクの結果

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

次のタスク

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

- 保持と最適化がまだ行われていない、ソートや順序付けの結果をデータベースで直接保持するため。結果は処理のためにデータベースに一時的に保持されます。
- 次のいずれかの方式を使用して、データベースへの管理アクセス権を与えるため。
  - Db2 Open Database Connectivity (ODBC) クライアント
  - Oracle Java Database Connectivity (JDBC) クライアント
  - 管理クライアント・コマンド・ラインからサーバーへの構造化照会言語 (SQL)

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

データベース・サイズ	最小の一時スペース所要量
< 500 GB	50 GB
≥ 500 GB かつ < 1 TB	100 GB
≥ 1 TB かつ < 1.5 TB	150 GB
≥ 1.5 かつ < 2 TB	200 GB
≥ 2 かつ < 3 TB	250 - 300 GB
≥ 3 かつ < 4 TB	350 - 400 GB

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

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

データベース・マネージャーと一時スペース

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

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

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

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

- データベースに少量のスペースしかなく、一時スペースを必要とするサーバー操作によって、残りのフリー・スペースが使用される場合。
- ファイル・スペースが大きい、またはファイル・スペースに多数のファイル・バージョンを作成するポリシーが割り当てられている場合。
- 限られたメモリーで IBM Spectrum Protect サーバーを実行しなければならない場合。 データベースは、IBM Spectrum Protect サーバーのメイン・メモリーを使用して、データベース操作を実行します。しかし、使用可能なメモリーが不足している場合、IBM Spectrum Protect サーバーはデータベースに対してディスク上に一時スペースを割り振ります。例えば、10G のメモリーが使用可能で、データベース操作に 12G のメモリーが必要な場合、データベースは一時スペースを使用します。
- IBM Spectrum Protect サーバーをデプロイすると、「データベース・スペース不足 (out of database space)」エラーが表示される場合。サーバーのアクティビティー ・ログをモニターして、データベース・スペースに関連したメッセージを調べてください。

重要 : IBM Spectrum Protect インストール・パッケージおよびフィックスパックとともにインストールされている Db2 ソフトウェアは変更しないでください。データベースが損傷する可能性があるため、別のバージョン、リリース、またはフィックスパックの Db2 ソフトウェアをインストールしたり、それらにアップグレードしたりしないでください。

回復ログのスペース要件

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

活動ログとアーカイブ・ログのスペース

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

IBM Spectrum Protect サーバー V7.1 以降では、活動ログは最大サイズ 512 GB にすることができます。アーカイブ・ログ・サイズは、それがインストールされているファイル・システムのサイズに 制限されます。

活動ログのサイズを見積もる際に、以下の一般ガイドラインを使用してください。

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

アーカイブ・ログの推奨開始サイズは 48 GB です。

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

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

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

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

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

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

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

この計算は、以下の表の例で使用されます。

表 9. 基本クライアント保管操作

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

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

ログをモニターし、必要に応じてそれらのサイズを調整します。

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

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

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

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

この計算は、以下の表の例で使用されます。

表 *10.* 複数のクライアント・セッション

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

表 *10.* 複数のクライアント・セッション *(*続き*)*

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

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

活動ログをモニターし、必要に応じてそのサイズを調整します。

例*:* 同時書き込み操作の活動ログとアーカイブ・ログのサイズの見積もり

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

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

この計算は、以下の表の例で使用されます。

表 *11.* 同時書き込み操作

項目	値の例	説明
時間帯に関わらずファイルを同時にバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの最大数。	300	毎日夜間にファイルをバックアップ、アーカイブ、またはマイグレーションするクライアント・ノードの数。
各トランザクション中に保管されるファイル	4096	サーバー・オプション TXNGROUPMAX のデフォルト値は 4096 です。
各ファイルに必要なログ・スペース	3453 バイト	3053 バイトに加えて、コピー・ストレージ・プールごとに 200 バイト。 トランザクション内のファイルごとに 3053 バイトという値は、ファイル名が 12 から 120 バイトであるファイルを Windows クライアントからバックアップするときに必要なログ・バイト数を表しています。 この値は、実験室条件下で実行されたテストの結果に基づきます。これらのテストは、ランダム・アクセス・ディスク (DISK) ストレージ・プールに対するバックアップ操作を実行するバックアップ/アーカイブ・クライアントで構成されました。DISK プールは、順次アクセス・ストレージ・プールよりも多くのログの使用量の増加をもたらします。保管するデータのファイル名が 12 から 120 バイトよりも長い場合は、3053 バイトより大きい値を使用することを検討してください。
活動ログ: 推奨サイズ	20 GB [1]	活動ログのサイズを判別するには、以下の計算を使用します。1 GB は 1,073,741,824 バイトに相当します。 (300 クライアント x 各トランザクション時に保管される 4096 ファイル x ファイルごとに 3453 バイト) ÷ 1,073,741,824 バイト = 4.0 GB 以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。 4 + 16 = 20 GB
アーカイブ・ログ: 推奨サイズ	60 GB [1]	3 つのサーバー・データベース・バックアップ・サイクル全体でアーカイブ・ログを保管できるという要件があるため、活動ログの見積もりに 3 を掛けて、アーカイブ・ログの所要量を見積もります。 4 GB x 3 = 12 GB 以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。 12 + 48 = 60 GB

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

ログをモニターし、必要に応じてそれらのサイズを調整します。

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

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

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

```
300 clients  x 100,000 files for each client   x  110 bytes =  3.1 GB
```

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

例: 差異が大きい条件下での活動ログとアーカイブ・ログのサイズの見積もり

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

例: フル・データベース・バックアップのアーカイブ・ログ・サイズの見積もり

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

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

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

表 *12.* フル・データベース・バックアップ

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

表 12. フル・データベース・バックアップ (続き)

項目	値の例	説明
各ファイルに必要なログ・スペース	3453 バイト	ファイルごとの 3053 バイトに加えて、コピー・ストレージ・プールごとに 200 バイト。 トランザクション内のファイルごとに 3053 バイトという値は、ファイル名が 12 から 120 バイトであるファイルを Windows クライアントからバックアップするときに必要なログ・バイト数を表しています。 この値は、実験室条件下で実行されたテストの結果に基づきます。テストは、ランダム・アクセス・ディスク (DISK) ストレージ・プールに対するバックアップ操作を実行するクライアントで構成されました。DISK プールは、順次アクセス・ストレージ・プールよりも多くのログの使用量の増加をもたらします。保管するデータのファイル名が 12 から 120 バイトよりも長い場合は、3053 バイトより大きい値を使用することを検討してください。
活動ログ: 推奨サイズ	20 GB [1]	活動ログのサイズを判別するには、以下の計算を使用します。1 GB は 1,073,741,824 バイトに相当します。 (300 クライアント x トランザクションごとに 4096 ファイル x ファイルごとに 3453 バイト) ÷ 1,073,741,824 バイト = 4.0 GB 以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。 4 + 16 = 20 GB
アーカイブ・ログ: 毎日のフル・データベース・バックアップでの推奨サイズ	60 GB [1]	3 つのバックアップ・サイクル全体でアーカイブ・ログを保管できるという要件があるため、活動ログの見積もりに 3 を掛けて、アーカイブ・ログの合計所要量を見積もります。 4 GB x 3 = 12 GB 以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。 12 + 48 = 60 GB
アーカイブ・ログ: 毎週のフル・データベース・バックアップでの推奨サイズ	132 GB [1]	3 つのサーバー・データベース・バックアップ・サイクル全体でアーカイブ・ログを保管できるという要件があるため、活動ログの見積もりに 3 を掛けて、アーカイブ・ログの合計所要量を見積もります。 その結果に、フル・データベース・バックアップ間の日数を掛けます。 (4 GB x 3) x 7 = 84 GB 以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。 84 + 48 = 132 GB

表 12. フル・データベース・バックアップ (続き)		
項目	**値の例**	**説明**
[1] この表内の値の例は、活動ログとアーカイブ・ログのサイズの計算方法を示すためにのみ使用しています。重複排除を使用しない本番環境では、活動ログの推奨される最小サイズは 16 GB です。重複排除を使用しない本番環境では、アーカイブ・ログの推奨される開始サイズは 48 GB です。ご使用の環境から値を補完し、その結果 16 GB および 48 GB より大きくなった場合は、その結果を使用して活動ログとアーカイブ・ログのサイズを調整します。 ログをモニターし、必要に応じてそれらのサイズを調整します。		

例: データ重複排除操作の活動ログとアーカイブ・ログのサイズの見積もり

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

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

重複排除されるデータの量

活動ログとアーカイブ・ログのスペースに対するデータ重複排除の影響は、重複排除に適格なデータの割合に応じて異なります。 重複排除できるデータの割合が比較的高い場合は、より多くのログ・スペースが必要です。

エクステントのサイズと 数

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

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

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

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

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

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

重複識別プロセスのタイミングと数

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

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

ファイル・サイズ

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

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

もっと小さい他の重複識別プロセスが、単一のラージ・オブジェクトの重複識別プロセスと同時に生じる場合、活動ログには十分なスペースがない可能性があります。例えば、ストレージ・プールの重複排除が使用可能であるとします。このストレージ・プールには、10 KB から数百 KB までの範囲にわたる、比較的小さい多数のファイルを含めて、データの混合があります。また、このストレージ・プールには、重複エクステントの割合が高い、ラージ・オブジェクトはほとんどありません。

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

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

表 *13.* 平均の重複エクステント・サイズ *700 KB*

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

表 *13.* 平均の重複エクステント・サイズ *700 KB* (続き)

項目	値の例		説明

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

アーカイブ・ログ: 推奨サイズ	198 GB [1]	239.4 GB [1]	活動ログの見積もりサイズに係数 3 を掛けます。
			複数のトランザクションと 800 GB のオブジェクトには、以下の計算式が使用されました。
			`50 GB x 3 = 150 GB`
			以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。
			`150 + 48 = 198 GB`
			複数のトランザクションと 4 TB のオブジェクトには、以下の計算式が使用されました。
			`63.8 GB x 3 = 191.4 GB`
			以下のとおり、推奨される開始サイズ 48 GB を追加してこの量を増やします。
			`191.4 + 48 = 239.4 GB`

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

ログをモニターし、必要に応じてそれらのサイズを調整します。

表 *14.* 平均の重複エクステント・サイズ *256 KB*

項目	値の例		説明
重複排除対象の最大単一オブジェクトのサイズ	800 GB	4 TB	重複排除のための処理の細分性はファイル・レベルです。したがって、重複排除対象の最大の単一ファイルが、最大トランザクション、およびそれに応じた、活動ログとアーカイブ・ログ上の大きな負荷を表します。
エクステントの平均サイズ	256 KB	256 KB	重複排除アルゴリズムでは、可変ブロック方式を使用します。所定のファイルについて重複排除されるすべてのエクステントが同じサイズであるとは限らないので、この計算は、エクステントの平均サイズを前提としています。

所定ファイルのエクステント	3,276,800 ビット	16,777,216 ビット	これらの計算は、平均エクステント・サイズを使用して、所定オブジェクトのエクステントの 総数を表します。
			複数のトランザクションと 800 GB のオブジェクトには、以下の計算式が使用されました。
			`(800 GB ÷ 256 KB) = 3,276,800 bits`
			複数のトランザクションと 4 TB のオブジェクトには、以下の計算式が使用されました。
			`(4 TB ÷ 256 KB) = 16,777,216 bits`

活動ログ: 単一の重複識別プロセス時に単一のラージ・オブジェクトの重複排除に必要な推奨サイズ	4.5 GB	23.4 GB	このトランザクションに必要な活動ログ・スペースの見積もりサイズ。

活動ログ: 推奨合計サイズ	71.6 GB [1]	109.4 GB [1]	重複排除に加えてサーバーの作業負荷のその他の局面を検討した後、既存の見積もりに係数 2 を掛けます。これらの例では、単一のラージ・オブジェクトの重複排除に必要な活動ログ・スペースが、必要な活動ログ・サイズの前の見積もりと一緒に検討されます。
			複数のトランザクションと 800 GB のオブジェクトには、以下の計算式が使用されました。
			`(23.3 GB + 4.5 GB) x 2 = 55.6 GB`
			以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。
			`55.6 + 16 = 71.6 GB`
			複数のトランザクションと 4 TB のオブジェクトには、以下の計算式が使用されました。
			`(23.3 GB + 23.4 GB) x 2 = 93.4 GB`
			以下のとおり、推奨される開始サイズ 16 GB を追加してこの量を増やします。
			`93.4 + 16 = 109.4 GB`

表 *14.* 平均の重複エクステント・サイズ *256 KB* (続き)

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

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

ログをモニターし、必要に応じてそれらのサイズを調整します。

活動ログ・ミラー・スペース

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

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

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

アーカイブ・フェイルオーバー・ログ・スペース

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

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

データベースおよび回復ログのスペース使用率のモニター

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

活動ログ

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

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER
活動ログ・スペースが指定の最大サイズを超えると、このメッセージが表示されます。IBM Spectrum Protect サーバーはフル・データベース・バックアップを開始します。

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

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
活動ログ・スペースが指定の最大サイズを超えると、このメッセージが表示されます。手動でデータベースをバックアップする 必要があります。

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

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER
使用可能な活動ログ・スペースに対する、使用済みの活動ログ・スペースの比率が、ログ使用率のしきい値を超えました。フル・データベース・バックアップが少なくとも 1 回行われている場合、IBM Spectrum Protect サーバーは差分データベース・バックアップを開始します。 そうでない場合、サーバーはフル・データベース・バックアップを開始します。

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
使用可能な活動ログ・スペースに対する、使用済みの活動ログ・スペースの比率が、ログ使用率のしきい値を超えました。手動でデータベースをバックアップする 必要があります。

アーカイブ・ログ

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

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
使用可能なアーカイブ・ログ・スペースに対する、使用済みのアーカイブ・ログ・スペースの比率が、ログ使用率のしきい値を超えました。IBM Spectrum Protect サーバーは自動フル・データベース・バックアップを開始します。

データベース

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

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2
使用済みのデータベース・スペースが、データベース・スペース使用率のしきい値を超えました。データベースのスペースを増やすには、**EXTEND DBSPACE** コマンド、**EXTEND DBSPACE** コマンド、または **DBDIR** パラメーターを指定した DSMSERV FORMAT ユーティリティーを 使用してください。

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB
サーバー・データベース・ファイルが置かれているディレクトリー内の使用可能スペースが 1 GB 未満です。

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

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

インストール・ロールバック・ファイルの削除

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

このタスクについて

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

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

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

手順

1. IBM Installation Manager を開きます。

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

   ```
   ./IBMIM
   ```

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

コマンド・ラインを使用したインストール・ロールバック・ファイルの削除

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

手順

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

   ```
   eclipse/tools
   ```

   例えば次のとおりです。

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

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

   ```
   ./imcl -c
   ```

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

8. **Installation Manager を終了**するには X を入力します。

サーバー名の命名のベスト・プラクティス

IBM Spectrum Protect サーバーをインストールまたはアップグレードする 場合は、以下の説明を参照してください。

インスタンス・ユーザー ID

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

例えば次のとおりです: tsminst1

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

インスタンス・ユーザー ID のホーム・ディレクトリー

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

例: `/home/tsminst1`

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

データベース・インスタンス名

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

例: `tsminst1`

インスタンス・ディレクトリー

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

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

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

別の場所にディレクトリーを作成することもできます。例: `/tsmserver/tsminst1`

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

- サーバー・オプション・ファイルの `dsmserv.opt`
- サーバーの鍵データベース・ファイル `cert.kdb`、および `.arm` ファイル (クライアントおよび他のサーバーが、サーバーの Secure Sockets Layer 証明書をインポートする際に使用します)
- `DEVCONFIG` サーバー・オプションが完全修飾名を指定していない場合、装置構成ファイル
- `VOLUMEHISTORY` サーバー・オプションが完全修飾名を指定していない場合、ボリューム・ヒストリー・ファイル

- 装置クラスのディレクトリーが完全に指定されていない場合、または完全修飾でない場合、**DEVTYPE=FILE** ストレージ・プール
- ユーザー出口
- トレース出力 (完全修飾でない場合)

データベース名

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

サーバー名

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

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

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

例えば次のとおりです。

```
PAYROLL
SALES
```

データベース・スペースおよび回復ログ用のディレクトリー

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

例えばアーカイブ・ログの場合、次のような名前を指定します。

```
/tsminst1_archlog
```

インストール・ディレクトリー

IBM Spectrum Protect サーバー用のインストール・ディレクトリーには、サーバー、IBM Db2、デバイス、言語、およびその他のディレクトリーがあります。各ディレクトリーには、いくつかの追加のディレクトリーが含まれています。

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

Db2 サーバーのインストールの一部としてインストールされる IBM Spectrum Protect 製品は、Db2 情報源に記載されているディレクトリー構造を持っています。サーバー・ディレクトリーと同様に、これらのディレクトリーおよびファイルを保護してください。デフォルト・ディレクトリーは `/opt/tivoli/tsm/db2` です。

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

第 2 章 サーバー・コンポーネントのインストール

IBM Spectrum Protect サーバー・コンポーネントをインストールするには、インストール・ウィザード、またはコンソール・モードでのコマンド・ラインのどちらかを使用できます。

このタスクについて

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

- サーバー

  ヒント: サーバー・コンポーネントを選択するときに、データベース (IBM Db2)、Global Security Kit (GSKit)、および IBM Java ランタイム環境 (JRE) が自動的にインストールされます。
- サーバー言語
- ライセンス
- 装置
- IBM Spectrum Protect for SAN
- Operations Center

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

インストール・パッケージの入手

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

始める前に

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

1. 最大ファイル・サイズ値を照会するには、次のコマンドを発行します。

   ```
   ulimit -Hf
   ```
2. 最大ファイル・サイズのシステム ・ユーザー制限が無制限に設定されていない場合、ご使用のオペレーティング・システムの資料の指示に従って、無制限に変更してください。

手順

1. 以下のいずれかの Web サイトから該当するパッケージ・ファイルをダウンロードします。
   - パスポート・アドバンテージ または Fix Central からサーバー・パッケージをダウンロードします。
   - 最新情報、更新、および保守修正については、IBM サポート・ポータルにアクセスしてください。
2. IBM ダウンロード・サイトからパッケージをダウンロードした場合は、以下のステップを実行します。
   a. 製品パッケージからインストール・ファイルを抽出したときにそれらのファイルを保管するのに十分なスペースがあることを確認してください。 スペース要件については、ダウンロード文書を参照してください。
      - IBM Spectrum Protect 技術情報 588021
      - IBM Spectrum Protect Extended Edition 技術情報 588023
      - IBM Spectrum Protect for Data Retention 技術情報 588025

   b. パッケージ・ファイルを、選択したディレクトリーにダウンロードします。パスに含める文字数は 128 文字以下でなければならない。必ず、インストール・ファイルを空のディレクトリーに抽出しま

す。インストール・ファイルは、前に抽出したファイルやその他のファイルが含まれるディレクトリーには抽出しないでください。

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

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

d. 次のコマンドを発行して、パッケージを抽出します。

```
./package_name.bin
```

ここで、*package_name* は、次のようなダウンロード・ファイルの名前です。

```
8.1.x.000-IBM-SPSRV-AIX.bin
```

3. IBM Spectrum Protect 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。

4. IBM Spectrum Protect のインストール方式を次の中から 1 つ選択します。
   - 70 ページの『インストール・ウィザードを使用した IBM Spectrum Protect のインストール』
   - 71 ページの『コンソール・モードを使用した IBM Spectrum Protect のインストール』
   - 72 ページの『サイレント・モードで IBM Spectrum Protect をインストール』
5. IBM Spectrum Protect をインストールした後、使用目的に合わせてカスタマイズする前に、IBM サポート・ポータル にアクセスしてください。「**Support and downloads**」をクリックし、適用できる修正があれば適用します。

インストール・ウィザードを使用した IBM Spectrum Protect のインストール

IBM Installation Manager グラフィカル・ウィザードを使用して、サーバーをインストールできます。

始める前に

インストールを始める前に、次のアクションを実行します。

- 以下の RPM ファイルがシステムにインストールされていない場合は、インストールする必要があります。

  ヒント: コンソール・ウィザードを使用している場合は RPM ファイルをインストールする必要がありません。

  GTK2 ファイルのインストールについて詳しくは、IBM トピック Installing and configuring GTK2 on IBM AIX を参照してください。

```
atk-1.12.3-2.aix5.2.ppc.rpm
cairo-1.8.8-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm
fontconfig-2.4.2-1.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm
gettext-0.10.40-6.aix5.1.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm
gtk2-2.10.6-4.aix5.2.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
libpng-1.2.32-2.aix5.2.ppc.rpm
libtiff-3.8.2-1.aix5.2.ppc.rpm
```

```
pango-1.14.5-4.aix5.2.ppc.rpm
pixman-0.12.0-3.aix5.2.ppc.rpm
xcursor-1.1.7-3.aix5.2.ppc.rpm
xft-2.1.6-5.aix5.1.ppc.rpm
xrender-0.9.1-3.aix5.2.ppc.rpm
zlib-1.2.3-3.aix5.1.ppc.rpm
```

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

手順

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

オプション	説明
ダウンロードしたパッケージからソフトウェアをインストールする場合:	a. パッケージをダウンロードしたディレクトリーに変更します。 b. 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`

次のタスク

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

  インストール・ログ・ファイルは、Installation Manager ツールから「**ファイル**」 > 「**ログの表示**」をクリックすると表示できます。これらのログ・ファイルを収集するには、Installation Manager ツールから「**ヘルプ**」 > 「**問題分析のためのデータをエクスポート**」をクリックします。
- サーバーおよびコンポーネントをインストールした後、使用目的に合わせてカスタマイズする前に、IBM サポート・ポータルにアクセスしてください。「**Downloads (fixes and PTFs)**」をクリックして、適用できる修正があれば適用します。
- 新規サーバーをインストールした後、77 ページの『第 3 章 IBM Spectrum Protect のインストール後の最初のステップの実行』を参照して、サーバーの構成方法について確認します。

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

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

始める前に

インストールを始める前に、次のアクションを実行します。

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

手順

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

オプション	説明
ダウンロードしたパッケージからソフトウェアをインストールする場合:	a. パッケージをダウンロードしたディレクトリーに変更します。 b. 次のコマンドを発行して、コンソール・モードでインストール・ウィザードを開始します。

オプション	説明
	``` ./install.sh -c ``` **オプション :** コンソール・モードのインストールの一部として、応答ファイルを生成します。コンソール・モードのインストール・オプションを完了し、「**要約**」パネルで「G」を指定して、応答を生成します。

次のタスク

- インストール・プロセス中にエラーが発生した場合、それらのエラーは、IBM Installation Manager ログ・ディレクトリーに保管されている次のようなログ・ファイルに記録されます。

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

- サーバーおよびコンポーネントをインストールした後、使用目的に合わせてカスタマイズする前に、IBM サポート・ポータルにアクセスしてください。「**Downloads (fixes and PTFs)**」をクリックして、適用できる修正があれば適用します。
- 新規サーバーをインストールした後、77 ページの『第 3 章 IBM Spectrum Protect のインストール後の最初のステップの実行』を参照して、サーバーの構成方法について確認します。

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

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

始める前に

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

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

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

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

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

手順

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

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

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

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

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

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

   - `./install.sh -s -input response_file -acceptLicense`

次のタスク

- インストール・プロセス中にエラーが発生した場合、それらのエラーは、IBM Installation Manager ログ・ディレクトリーに保管されている次のようなログ・ファイルに記録されます。

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

- サーバーおよびコンポーネントをインストールした後、使用目的に合わせてカスタマイズする前に、IBM サポート・ポータルにアクセスしてください。「**Downloads (fixes and PTFs)**」をクリックして、適用できる修正があれば適用します。
- 新規サーバーをインストールした後、77 ページの『第 3 章 IBM Spectrum Protect のインストール後の最初のステップの実行』を参照して、サーバーの構成方法について確認します。

サーバー言語パッケージのインストール

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

始める前に

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

サーバー言語のロケール

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

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

- LANGUAGE en_US

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

以下に示す言語を使用できます。

表 *15. AIX* のサーバー言語

言語	**LANGUAGE のオプション値**
中国語 (簡体字)	zh_CN
中国語 (簡体字) (UTF-8)	ZH_CN
中国語 (繁体字) (Big5)	Zh_TW
中国語 (繁体字) (UTF-8)	ZH_TW
中国語 (繁体字) (euc_tw)	zh_TW
英語	en_US
英語 (UTF-8)	EN_US
フランス語	fr_FR

表 15. AIX のサーバー言語 (続き)	
言語	**LANGUAGE のオプション値**
フランス語 (UTF-8)	FR_FR
ドイツ語	de_DE
ドイツ語 (UTF-8)	DE_DE
イタリア語	it_IT
イタリア語 (UTF-8)	IT_IT
日本語、EUC	ja_JP
日本語、PC	Ja_JP
日本語、UTF8	JA_JP
韓国語	ko_KR
韓国語 (UTF-8)	KO_KR
ブラジル・ポルトガル語	pt_BR
ブラジル・ポルトガル語 (UTF-8)	PT_BR
ロシア語	ru_RU
ロシア語 (UTF-8)	RU_RU
スペイン語	es_ES
スペイン語 (UTF-8)	ES_ES

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

言語パッケージの構成

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

このタスクについて

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

- サーバー・オプション・ファイル内の LANGUAGE オプションをご使用のロケール名に設定します。 例えば次のとおりです。

  it_IT ロケールを使用するには、LANGUAGE オプションを it_IT に設定します。 73 ページの『サーバー言語のロケール』を参照してください。
- サーバーをフォアグラウンドで始動する場合は、LC_ALL 環境変数をサーバー・オプション・ファイルに設定されている値に一致するように設定します。 例えば、イタリア語の環境変数を設定するには、次の値を入力します。

```
export LC_ALL=it_IT
```

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

言語パッケージの更新

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

このタスクについて

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

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

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

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

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

このタスクについて

1. サーバー・インスタンス用のディレクトリーとユーザー ID を作成します。77 ページの『サーバー・インスタンスのユーザー ID とディレクトリーの作成』を参照してください。
2. サーバー・インスタンスを構成します。以下のいずれかのオプションを選択してください。
   - 推奨されている方法である構成ウィザードを使用します。79 ページの『構成ウィザードを使用した IBM Spectrum Protect の構成』を参照してください。
   - 手動で新規インスタンスを構成します。80 ページの『手動でのサーバー・インスタンスの構成』を参照してください。手動構成の間に次のステップを完了します。
     a. ディレクトリーをセットアップして IBM Spectrum Protect インスタンスを作成します。80 ページの『サーバー・インスタンスの作成』を参照してください。
     b. サーバーとクライアント間の通信をセットアップするために、サンプル・ファイルをコピーして新規のサーバー・オプション・ファイルを作成します。82 ページの『サーバーとクライアントの間の通信の構成』を参照してください。
     c. **DSMSERV FORMAT** コマンドを発行してデータベースをフォーマットします。84 ページの『データベースとログのフォーマット』を参照してください。
     d. データベース・バックアップのためにシステムを構成します。86 ページの『データベース・バックアップのためのデータベース・マネージャーの準備』を参照してください。
3. データベース再編成時に制御を行うためのオプションを構成します。88 ページの『サーバー・データベース保守のためのサーバー・オプションの構成』を参照してください。
4. サーバー・インスタンスがまだ始動していない場合は、始動します。

   89 ページの『サーバー・インスタンスの開始』を参照してください。
5. ライセンスを登録します。94 ページの『ライセンスの登録』を参照してください。
6. データベース・バックアップのためにシステムを準備します。94 ページの『データベース・バックアップ操作のためのサーバーの準備』を参照してください。
7. 将来何らかの問題が起きた場合のトラブルシューティングを容易にするために、必ず十分なスペースをコア・ダンプに割り振ってください。詳しくは、技術情報 6357399 を参照してください。
8. サーバーをモニターします。95 ページの『サーバーのモニター』を参照してください。

サーバー・インスタンスのユーザー ID とディレクトリーの作成

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

始める前に

このタスクを完了する前に、サーバーのスペースの計画についての情報を検討してください。48 ページの『サーバーの詳細を計画するためのワークシート』を参照してください。

手順

1. サーバー・インスタンスを所有するユーザー ID を作成します。

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

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

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

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

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

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

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

制約事項 : IBM Db2 は、LDAP を介した直接的なオペレーティング・システムのユーザー認証をサポートしていません。

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

2. サーバーに必要なディレクトリーを作成します。

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

項目	ディレクトリーを作成するためのコマンド例	ディレクトリー
サーバーのインスタンス・ディレクトリー。これは、特にこのサーバー・インスタンス用のファイル (サーバー・オプション・ファイルおよびその他のサーバー特有のファイル) を含むディレクトリーです)。	`mkdir /tsminst1`	

データベース・ディレクトリー	`mkdir /tsmdb001`
	`mkdir /tsmdb002`
	`mkdir /tsmdb003`
	`mkdir /tsmdb004`	

活動ログ・ディレクトリー	`mkdir /tsmlog`	
アーカイブ・ログ・ディレクトリー	`mkdir /tsmarchlog`	
オプション: 活動ログのログ・ミラーのディレクトリー	`mkdir /tsmlogmirror`	

次の表の各項目ごとに空のディレクトリーを作成して、ディレクトリーが先ほど作成した新規ユーザー ID によって所有されていることを確認します。活動ログ・ディレクトリー、アーカイブ・ログ・ディレクトリー、およびデータベース・ディレクトリーの各ディレクトリーに、関連するストレージをマウントします。 *(続き)*		
項目	**ディレクトリーを作成するためのコマンド例**	**ディレクトリー**
オプション: 2 次アーカイブ・ログ・ディレクトリー (アーカイブ・ログのフェイルオーバー・ロケーション)	`mkdir /tsmarchlogfailover`	

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

3. 新規ユーザー ID をログオフします。

IBM Spectrum Protect サーバーの構成

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

このタスクについて

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

- ローカル・システムで IBM Spectrum Protect 構成ウィザードを使用します。 79 ページの『構成ウィザードを使用した IBM Spectrum Protect の構成』を参照してください。
- 手動で新規 IBM Spectrum Protect インスタンスを構成します。 80 ページの『手動でのサーバー・インスタンスの構成』を参照してください。手動構成の間に次のステップを完了します。
  1. ディレクトリーをセットアップして IBM Spectrum Protect インスタンスを作成します。 80 ページの『サーバー・インスタンスの作成』を参照してください。
  2. IBM Spectrum Protect サーバーとクライアント間の通信をセットアップするために、サンプル・ファイルをコピーして新規のサーバー・オプション・ファイルを作成します。 82 ページの『サーバーとクライアントの間の通信の構成』 を参照してください。
  3. DSMSERV FORMAT コマンドを発行してデータベースをフォーマットします。 84 ページの『データベースとログのフォーマット』を参照してください。
  4. データベース・バックアップのためにシステムを 構成します。 86 ページの『データベース・バックアップのためのデータベース・マネージャーの準備』を参照してください。

構成ウィザードを使用した IBM Spectrum Protect の構成

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

始める前に

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

手順

1. 次の要件を満たしているようにしてください。

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

2. ウィザードのローカル・バージョンを開始するには、以下のようにします。

   /opt/tivoli/tsm/server/bin ディレクトリーで dsmicfgx プログラムを開きます。このウィザードは、root ユーザー ID を使用する場合のみ実行できます。

   指示に従って構成を完了します。 ウィザードは停止と再始動ができますが、サーバーは構成プロセス全体が完了するまでは操作可能になりません。

手動でのサーバー・インスタンスの構成

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

サーバー・インスタンスの作成

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

このタスクについて

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

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

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

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

  - サーバー・オプション・ファイルの dsmserv.opt
  - サーバーの鍵データベース・ファイル cert.kdb、および .arm ファイル (クライアントおよび他のサーバーが、サーバーの Secure Sockets Layer 証明書をインポートする際に使用します)
  - DEVCONFIG サーバー・オプションが完全修飾名を指定していない場合、装置構成ファイル
  - VOLUMEHISTORY サーバー・オプションが完全修飾名を指定していない場合、ボリューム・ヒストリー・ファイル
  - 装置クラスのディレクトリーが完全に指定されていない場合、または完全修飾でない場合、**DEVTYPE=FILE** ストレージ・プール
  - ユーザー出口
  - トレース出力 (完全修飾でない場合)
- 以下のファイルのバックアップ・コピーは、安全でセキュアな場所に保管する必要があります。
  - マスター暗号鍵ファイル (dsmkeydb.*)
  - サーバー証明書と秘密鍵のファイル (cert.*)
- root ユーザーおよびインスタンス・ユーザーの ID は、シェル構成ファイルに対する書き込み権限を持っている必要があります。シェル構成ファイル (.profile など) がホーム・ディレクトリーに存在する。

詳しくは、Db2 製品情報を参照してください。Linux® および UNIX の環境変数の設定を検索してください。

1. root ユーザー ID を使用してログインし、IBM Spectrum Protect インスタンスを作成します。インスタンスの名前は、そのインスタンスを所有するユーザーと同じ名前でなければなりません。**db2icrt** コマンドを使用して、次のコマンドを 1 行で入力してください。

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

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

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

   要確認 : この時点から先は、IBM Spectrum Protect サーバーを構成する際には、この新規ユーザー ID を使用します。root ユーザー ID をログアウトし、新規インスタンス・ユーザー ID でログインします。
2. データベースのデフォルト・ディレクトリーを、サーバーのインスタンス・ディレクトリーと同じになるように変更します。複数のサーバーがある場合は、それぞれのサーバーのインスタンス ID でログインします。次のコマンドを出します。

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

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

   ```
   db2 update dbm cfg using dftdbpath /tsminst1
   ```
3. ライブラリー・パスを変更して、サーバー操作に必要なライブラリーを組み込むようにしてください。

   ヒント : 以下の例では、ディレクトリーを示します。

   - *server_bin_directory* は、サーバーのインストール・ディレクトリーのサブディレクトリーです。 例えば、/opt/tivoli/tsm/server/bin です。
   - *instance_users_home_directory* は、インスタンス・ユーザーのホーム・ディレクトリーです。例えば、/home/tsminst1 です。
   - 以下のコマンドを 1 行で指定して発行します。

     ```
     export LIBPATH=server_bin_directory/dbbkapi:
     /usr/opt/ibm/gsk8_64/lib64:$LIBPATH
     ```
   - 以下のいずれかのファイルを更新して、IBM Db2 またはサーバーの始動時のライブラリー・パスを設定します。インスタンス・ユーザーが使用するように構成されているシェルごとに更新します。

     Bash または Korn シェル:

     ```
     instance_users_home_directory/sqllib/userprofile
     ```

     C シェルの場合 :

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

     Bash または Korn シェル:

     次の項目を *instance_users_home_directory*/sqllib/userprofile ファイルに 1 行で追加します。

     ```
     export LIBPATH=server_bin_directory/
     dbbkapi:/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
     ```

C シェルの場合 :

次の項目を *instance_users_home_directory*/sqllib/usercshrc ファイルに 1 行で追加します。

```
setenv LIBPATH server_bin_directory/dbbkapi:
/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

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

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

4. 新規サーバー・オプション・ファイルを作成します。

サーバーとクライアントの間の通信の構成

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

このタスクについて

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

オプション・ファイルを編集する場合は、以下のガイドラインに従ってください。

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

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

次の通信方式を 1 つ以上指定できます。

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

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

TCP/IP オプションの設定

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

このタスクについて

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

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

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

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

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

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

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

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、TCP/IP または SSL 対応の通信要求を待つポート番号を指定します。 デフォルト値は TCPPORT です。

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

SSLTCPADMINPORT
(SSL のみ) サーバー TCP/IP 通信ドライバーがコマンド・ライン管理クライアントの SSL 対応セッションの要求を待機するポート・アドレスを指定します。

共用メモリー・オプションの設定

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

このタスクについて

以下の例は、共用メモリー設定を示したものです。

```
commmethod     sharedmem
   shmport     1510
```

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

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

```
commmethod tcpip
commmethod sharedmem
```

同時にサポートする共用メモリー・セッションの最大数は、使用可能なシステム・リソースに基づいて決まります。 各共用メモリー・セッションでは、IBM Spectrum Protect クライアント・レベルに応じて、最大 4 MB の共用メモリー領域が 1 つと、IPCS メッセージ・キューが 4 つ使用されます。

サーバーとクライアントが同じユーザー ID で稼働していない場合は、サーバーを root にする必要があります。 これにより、共用メモリー通信エラーが防止されます。

Secure Sockets Layer オプションの設定

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

始める前に

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

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

データベースとログのフォーマット

サーバーを手動で構成する場合、サーバー・データベースとリカバリー・ログをフォーマットする 必要があります。データベースは、クライアント・データとサーバー操作に関する情報を保管するために使用され、リカバリー・ログは、システムとメディアの 障害からのリカバリーするために使用できます。 **DSMSERV FORMAT** ユーティリティーは、サーバー・データベースおよびリカバリー・ログをフォーマットして初期化するために使用します。 データベースおよびリカバリー・ログを初期化中は、他のサーバー活動は許可されません。

サーバー通信をセットアップしたら、データベースを初期化することができます。 このディレクトリーは、スペース不足になる可能性のあるファイル・システム 上に指定しないでください。 アーカイブ・ログなど特定のディレクトリーが使用不可または満杯になった場合、サーバーが停止します。詳しくは、「キャパシティー計画」を参照してください。

出口リスト・ハンドラーの設定

各サーバー・インスタンスの **DB2NOEXITLIST** レジストリー変数を ON に設定します。インスタンス・ユーザー ID を使用してシステムにログオンし、以下のコマンドを実行します。

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

例えば次のとおりです。

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

サーバー・データベースとリカバリー・ログの初期化

DSMSERV FORMAT ユーティリティーは、サーバー・データベース (IBM Db2 データベース)、およびリカバリー・ログをフォーマットして初期化するために使用します。 例えば、サーバー・インスタンス・ディレクトリーが */tsminst1* である場合、以下のコマンドを実行します。

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

ヒント: 複数のディレクトリーを指定する場合、データベース操作での並列処理の整合度を確保するために、必ず基礎となるファイル・システムのサイズが 等しくなるようにしてください。 データベース用のディレクトリーの中に他のディレクトリーより小さいものが 1 つ以上ある場合、並列プリフェッ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。

DSMSERV FORMAT コマンドを実行しても Db2 データベースが開始しない場合、ファイル・システム・マウント・オプション NOSUID を使用不可に設定する必要がある場合があります。このオプションは、以下の環境でシステムを開始する場合には無効にする必要があります。

- このオプションが、Db2 インスタンス所有者ディレクトリーを含むファイル・システムで設定される場合。
- このオプションが、Db2 データベース、活動ログ、アーカイブ・ログ、フェイルオーバー・ログ、またはミラーリングされたログが含まれているファイル・システムで設定される場合。

NOSUID オプションを使用不可にした後、ファイル・システムを再マウントしてから、次のコマンドを実行して Db2 データベースを開始します。

```
db2start
```

管理ユーザーの作成

データベースとリカバリー・ログのフォーマットの完了後、サーバーにログインできる管理ユーザーを作成し、また IBM Spectrum Protect Operations Center でサーバーへの接続を有効にする必要があります。以下のコマンドをマクロで使用して、管理ユーザーをセットアップします。

REGISTER ADMIN

REGISTER ADMIN コマンドでは、以下のパラメーターを使用します。

```
register admin administrator_user_id administrator_user_password
```

パスワードは、長さに関する固有のルールを満たしている必要があります。詳しくは、REGISTER ADMIN (管理者 ID の登録) を参照してください。

GRANT AUTH

GRANT AUTH コマンドでは、以下のパラメーターを使用します。

```
grant auth administrator_user_id classes=administrator_user_class
```

詳しくは、GRANT AUTHORITY (管理者権限の追加) を参照してください。

管理ユーザーをセットアップするには、以下のステップを実行します。

1. 「setup.mac」などのマクロを作成します。
2. 以下の資格情報を使用してマクロを編集し、管理ユーザーを登録し、「システム」権限をユーザーに付与します。
   - 管理ユーザー ID: adminadmin
   - 管理ユーザーのパスワード: adminadmin1

   ```
   register admin adminadmin adminadmin1
   grant auth adminadmin classes=system
   ```

   管理ユーザーが、制限された特権で他の潜在的な管理ユーザーを作成できるように、**classes=system** オプションを使用して管理ユーザーを作成する必要があります。これらの管理ユーザーのいずれかが、IBM Spectrum Protect Operations Center に接続できます。
3. 管理ユーザーを作成して、「システム」権限をユーザーに付与するには、**runfile** オプションとマクロ・ファイルを指定して **DSMSERV** コマンドを実行します。

   ```
   dsmserv runfile setup.mac
   ```

管理ユーザーはサーバー・インスタンスを開始して、サーバーに接続し、他の必須ステップ (データベース・バックアップの設定など) を実行する必要があります。

データベース・バックアップのためのデータベース・マネージャーの準備

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

このタスクについて

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

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

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

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

1. データベース・インスタンスの IBM Spectrum Protect API 環境変数構成を設定します。
   a. `tsminst1` ユーザー ID を使用してログインします。
   b. ユーザー `tsminst1` がログインするときには、必ず IBM Db2 環境が正しく初期化されているようにしてください。Db2 環境は、`/home/tsminst1/sqllib/db2profile` スクリプトの実行によって初期化されます。通常このスクリプトは、ユーザー ID のプロファイルから自動的に実行されます。`.profile` ファイルが、インスタンス・ユーザーのホーム・ディレクトリー (例えば、`/home/tsminst1/.profile`) に存在することを確認してください。`.profile` が `db2profile` スクリプトを実行しない場合は、次の行を追加してください。

```
if [ -f /home/tsminst1/sqllib/db2profile ]; then
      . /home/tsminst1/sqllib/db2profile
  fi
```

   c. `instance_directory/sqllib/userprofile` ファイルに、以下の行を追加します。

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

   ここで、

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

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

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

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

```
. ~/.profile
```

ヒント : 最初のドット (.) 文字の後に必ずスペースを入力します。

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

```
SERVERNAME TSMDBMGR_TSMINST1
```

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

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

   server_bin_directory/dbbkapi/dsm.sys

```
servername TSMDBMGR_TSMINST1
commmethod tcpip
tcpserveraddr localhost
tcpport 1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

   ここで、

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

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

5. オプション: 共有メモリーを使用してデータベースをバックアップするようにサーバーを 構成します。これにより、プロセッサーの負荷を軽減し、スループットを向上できる可能性があります。次の手順を実行してください。

   a. dsmserv.opt ファイルを確認します。ファイルに以下の行がない場合は、追加してください。

```
commmethod sharedmem
shmport port_number
```

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

   b. dsm.sys 構成ファイルで、以下の行を見つけます。

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

      指定された行を、以下の行で置き換えます。

```
commmethod sharedmem
shmport port_number
```

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

サーバー・データベース保守のためのサーバー・オプションの構成

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

このタスクについて

表と索引の再編成には、かなりのプロセッサー・リソース、活動ログ・スペース、およびアーカイブ・ログ・スペースが必要です。 データベース・バックアップは再編成よりも優先するため、処理がオーバーラップせずに再編成が完了できるように、再編成の時刻と期間を選択してください。

サーバー・データベースの索引および表の再編成を最適化することができます。こうすると、予期しないデータベースの増加やパフォーマンスの問題を回避することができます。 方法については、技術情報 1683633 を参照してください。

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

手順

1. サーバー・オプションを変更します。

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

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

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

2. データ重複排除を使用する予定の場合は、**ALLOWREORGINDEX** サーバー・オプションを有効にしてください。

   次のオプションと値をサーバー・オプション・ファイルに追加します。

   ```
   allowreorgindex yes
   ```

3. 再編成の開始時刻と期間を制御する **REORGBEGINTIME** および **REORGDURATION** のサーバー・オプションを設定します。 サーバーが一番すいているときに再編成が実行されるように、時刻と期間を選択してください。

   これらのサーバー・オプションは、表と索引の両方の再編成処理を制御します。

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

   ```
   reorgbegintime 20:30
   ```

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

```
reorgduration 4
```

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

サーバー・インスタンスの開始

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

始める前に

アクセス許可とユーザー制限を正しく設定したことを確認します。

このタスクについて

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

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

手順

サーバーを始動するには、次のいずれかをアクションを実行します。

- インスタンス・ユーザー ID を使用して、サーバーを始動します。

  手順については、91 ページの『インスタンス・ユーザー ID からのサーバーの始動』を参照してください。
- root ユーザー ID を使用して、サーバーを始動します。

  サーバーを始動する権限を root ユーザー ID に与える方法については、サーバーを始動する権限の root ユーザー ID への付与 (V7.1.1)を参照してください。root ユーザー ID を使用したサーバーの始動方法については、root ユーザー ID からのサーバーの始動 (V7.1.1)を参照してください。
- サーバーを自動的に開始します。

  手順については、91 ページの『サーバーの自動始動』を参照してください。
- 保守モードでのサーバーの始動。

  手順については、92 ページの『保守モードでのサーバーの始動』を参照してください。

アクセス権限およびユーザー制限の確認

サーバーを開始する前にアクセス権限とユーザー制限を確認してください。

このタスクについて

ulimits とも呼ばれるユーザー限度を検証しないと、サーバーが不安定になったり、サーバーが応答できない状態を検出する可能性があります。また、オープン・ファイルの最大数に対するシステム全体の限度も確認する必要があります。 システム全体の限度は、ユーザー限度以上でなければなりません。

手順

1. サーバー・インスタンスのユーザー ID がサーバーを始動する許可を持っていることを確認します。
2. 始動する予定のサーバー・インスタンスについて、サーバー・インスタンス・ディレクトリー内のファイルの読み取りおよび書き込みの権限を持っていることを確認します。

   dsmserv.opt ファイルがサーバー・インスタンス・ディレクトリーに存在していること、およびそのファイルにサーバー・インスタンスのパラメーターが含まれていることを確認してください。
3. サーバーが磁気テープ・ドライブ、メディア・チェンジャー、または取り外し可能メディア・デバイスに接続されており、インスタンス・ユーザー ID を使用してサーバーを始動する予定の場合、インスタンス・ユーザー ID にこれらのデバイスに対する読み取り/書き込み権限を付与します。許可を設定するには、次のいずれかをアクションを実行します。

   - システムが IBM Spectrum Protect 専用で、IBM Spectrum Protect 管理者のみがアクセス権限を持っている場合、デバイス特殊ファイルを全ユーザーによる書き込みが可能になるようにします。 オペレーティング・システムのコマンド・ラインで、次のコマンドを発行します。

     ```
     chmod +w /dev/rmtX
     ```

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

     ```
     chmod u+w /dev/rmtX
     ```

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

     ```
     chmod g+w /dev/rmtX
     ```
4. 表に示された指針に基づいて、以下のユーザー制限を確認します。

表 *16.* ユーザー制限 *(ulimit)* 値

ユーザー制限タイプ	推奨値	値を照会するコマンド
作成されるコア・ファイルの最大サイズ	無制限	ulimit -Hc
プロセスのデータ・セグメントの最大サイズ	無制限	ulimit -Hd
最大ファイル・サイズ	無制限	ulimit -Hf
オープン・ファイルの最大数	65536	ulimit -Hn
最大プロセッサー時間 (秒単位)	無制限	ulimit -Ht

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

   ヒント : スクリプトを使用して自動的にサーバーを始動する予定の場合は、スクリプトでユーザー制限を設定できます。
5. 最大ユーザー・プロセス数 (nproc 設定) のユーザー制限が最小推奨値 16384 に設定されていることを確認します。

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

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

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

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

```
instance_user_id        -    nproc          16384
```

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

インスタンス・ユーザー ID からのサーバーの始動

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

始める前に

アクセス権限およびユーザー制限が正しく設定されていることを確認します。

手順

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

   ```
   . /home/tsminst1/sqllib/db2profile
   ```

   ヒント: db2profile スクリプトを自動的に実行するためのユーザー ID ログイン・スクリプトの更新方法については、Db2 製品情報を参照してください。
3. サーバー・インスタンス・ディレクトリーから次のコマンドを 1 行で発行して、サーバーを始動します。

   ```
   LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
   usr/bin/dsmserv
   ```

   必ず、SHMPSIZE=64K の後にスペースを入れてください。このコマンドを使用してサーバーを始動することにより、サーバー用に 64 KB のメモリー・ページを使用可能にします。この設定は、サーバーのパフォーマンスの最適化に役立ちます。

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

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

   ```
   cd /tsminst1
    . ~/sqllib/db2profile
   LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
   usr/bin/dsmserv
   ```

サーバーの自動始動

サーバーは、システムのスタートアップ時に自動的に始動するように構成できます。 **rc.dsmserv** スクリプトを使用します。これは、この目的のために用意されたファイルです。

始める前に

アクセス権限およびユーザー制限が正しく設定されていることを確認します。

このタスクについて

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

ヒント: 構成ウィザードを使用した場合は、システムの再始動時にサーバーを自動的に始動することを選択している可能性があります。その項目を選択した場合は、サーバーを始動するための項目が /etc/inittab ファイルに自動的に追加されています。

手順

ウィザードを使用してサーバーを構成しなかった場合は、自動的に始動したいサーバーごとに項目を /etc/inittab ファイルに追加します。

1. ネットワークを使用可能にして、実行レベルをマルチユーザー・モードに対応する値に設定します。オペレーティング・システムとその構成に応じて、通常、使用する実行レベルは 2、3、または 5 です。 /etc/inittab ファイル内の実行レベルが、オペレーティング・システムの実行レベルと一致するようにしてください。

   マルチユーザー・モードおよび実行レベルについて詳しくは、ご使用のオペレーティング・システムの資料を参照してください。
2. /etc/inittab ファイルの **rc.dsmserv** コマンドで、-u オプションを使用してインスタンス・ユーザー ID を指定し、-i オプションを使用してサーバー・インスタンス・ディレクトリーの場所を指定します。 複数のサーバーを自動的に始動したい場合は、サーバー・インスタンスごとに項目を追加してください。

   構文を確認するには、ご使用のオペレーティング・システムの資料を参照してください。

   ヒント: root ユーザー ID を使用してサーバー・インスタンスを自動的に始動するには、-U オプションを使用します。

例

例えば、インスタンス所有者が tsminst1 で、サーバー・インスタンス・ディレクトリーが /home/tsminst1/tsminst1 の場合は、次の項目を 1 行で /etc/inittab に追加します。

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
   -i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
```

この例では、プロセスの ID は tsm1 で、実行レベルは 2 に設定されています。

実行したいサーバー・インスタンスが複数ある場合は、それぞれのサーバー・インスタンスごとに項目を追加してください。例えば、インスタンス所有者 ID tsminst1 と tsminst2 がいて、インスタンス・ディレクトリー /home/tsminst1/tsminst1 と /home/tsminst2/tsminst2 がある場合は、次の項目を /etc/inittab に追加します。それぞれのエントリーは、1 行で入力します。

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
   -i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
tsm2:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst2
   -i /home/tsminst2/tsminst2 -q >/dev/console 2>&1
```

保守モードでのサーバーの始動

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

このタスクについて

MAINTENANCE パラメーターを指定して **DSMSERV** ユーティリティーを 実行し、サーバーを保守モードで始動します。

保守モードでは、以下の操作が使用不可になります。

- 管理コマンド・スケジュール
- クライアント・スケジュール
- サーバー上のストレージ・スペースのレクラメーション
- インベントリーの有効期限
- ストレージ・プールのマイグレーション

さらに、クライアントがサーバーとのセッションを 開始できなくなります。

ヒント:

- サーバーを保守モードで始動するために、サーバー・オプション・ファイル 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。

保守モード中に使用不可になっていた操作が再び使用可能になります。

サーバーの停止

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

このタスクについて

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

```
halt
```

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

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

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

```
cat /instance_dir/dsmserv.v6lock
```

サーバーを停止するには、次のコマンドを発行します。

```
kill -36 dsmserv_pid
```

ここで、*dsmserv_pid* は プロセス ID 番号です。

ライセンスの登録

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

このタスクについて

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

例: ライセンスの登録

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

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

データベース・バックアップ操作のためのサーバーの準備

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

手順

1. IBM Spectrum Protect サーバー構成が完了していることを確認します。

   ヒント: 構成ウィザード (dsmicfgx) を使用することによって、データベース・バックアップ用にサーバーを構成できます。また手動でステップを完了することもできます。構成の詳細については、IBM Knowledge Center の「サーバーの構成」セクションを参照してください。
2. データベースのバックアップに使用する装置クラスを選択し、マスター暗号鍵を保護して、パスワードを設定します。

   以下の鍵ファイルが発行済みであることを確認します。

   - マスター暗号鍵ファイル (dsmkeydb.*)
   - サーバー証明書と秘密鍵のファイル (cert.*)

   これらのアクションを実行するには、管理コマンド・ラインから **SET DBRECOVERY** コマンドを実行します。

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

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

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

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

   重要: パスワードは忘れないようにして、安全な場所にコピーを保管しておいてください。パスワードがないとデータをリカバリーできません。

例

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

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

単一システムでの複数のサーバー・インスタンスの実行

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

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

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

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

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

サーバーのモニター

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

手順

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

   サーバー作業負荷が通常予期されるレベルに達すると、活動ログによって使用されるスペースは、活動ログ・ディレクトリーの使用可能スペースの 80% から 90% になります。この時点で、スペースを増量する必要が生じることがあります。スペースの増量が必要かどうかは、サーバー作業負荷のトランザクションのタイプによって決まります。トランザクションの特性が、活動ログのスペースがどのように使用されるかに影響します。

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

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

- 比較的遅い接続で行われるバックアップ操作の場合、トランザクションは完了までにより長い時間がかかります。 これらのトランザクションは、より長時間、活動ログのスペースを使用します。

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

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

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

   次のパターンに気付く可能性があります。

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

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

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

   - アーカイブ・ログにスペースを追加します。 別のファイル・システムにアーカイブ・ログを移動する必要が生じることもあります。
   - フル・データベース・バックアップの頻度を増加します。そうすると、ログの整理がより頻繁に実行されます。

3. フェイルオーバー・アーカイブ・ログ用のディレクトリーを定義した場合は、通常操作中にそのディレクトリーに保管されたログがあるかどうかを判別します。 フェイルオーバー・ログ・スペースが使用されている場合は、アーカイブ・ログのサイズを増加することを検討してください。

   目標は、フェイルオーバー・アーカイブ・ログが、通常操作時ではなく、異常な状態の場合にのみ使用されることです。

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

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

始める前に

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

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

サーバーをアップグレードしてから 前のレベルに戻す場合は、 データベースをアップグレード 前の特定時点にリストアする必要があります。アップグレード・プロセス中に必要な手順を実行して、データベースをリストアできるようにしてください。必要な手順とは、データベース、ボリューム・ヒストリー・ファイル、装置構成ファイル、およびサーバー・オプション・ファイルをバックアップする操作です。

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

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

以下の情報については、IBM サポート・ポータルにアクセスしてください。

- 最新の保守修正とダウンロード修正のリスト。 「**Downloads**」をクリックし、適用可能な修正を適用します。
- 基本ライセンス・パッケージの入手方法に関する詳細。 「**Downloads > Passport Advantage**」を検索します。
- サポートされているプラットフォームとシステム 要件。「**IBM Spectrum Protect サポート対象オペレーティング・システム (supported operating systems)**」を検索します。

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

重要 : IBM Spectrum Protect インストール・パッケージおよびフィックスパックと一緒にインストールされる Db2 ソフトウェアは変更しないでください。別のバージョン、リリース、またはフィックスパックの Db2 ソフトウェアをインストールしたり、それらにアップグレードしたりしないでください。データベースが損傷する可能性があります。

手順

フィックスパックまたは暫定修正をインストールするには、以下のステップを実行します。

1. データベースのバックアップを取ります。 スナップショット・バックアップを使用する方法をお勧めします。 スナップショット・バックアップは、スケジュールされたデータベース・バックアップを中

断しない、フル・データベース・バックアップです。例えば、以下の IBM Spectrum Protect 管理コマンドを実行します。

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

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

```
backup devconfig filenames=file_name
```

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

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

```
backup volhistory filenames=file_name
```

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

4. サーバー・オプション・ファイル (通常、`dsmserv.opt` という名前) のコピーを保存します。ファイルはサーバー・インスタンス・ディレクトリーにあります。
5. フィックスパックまたは暫定修正をインストールする前にサーバーを停止します。

   HALT コマンドを使用します。
6. インストール・ディレクトリーに余分なスペースがあることを確認してください。

   このフィックスパックのインストールには、サーバーのインストール・ディレクトリーに追加の一時ディスク・スペースが必要な場合があります。 追加ディスク・スペースの量は、IBM Spectrum Protect インストールの一部として新規データベースをインストールするのに必要なのと同じ量にすることができます。IBM Spectrum Protect インストール・ウィザードは、フィックスパックのインストールに必要なスペース量と使用可能な量を表示します。 必要なスペース量が使用可能な量より多い場合、インストールは停止します。 インストールが停止する場合、必要なディスク・スペースをファイル・システムに追加し、インストールを再開してください。
7. root ユーザーとしてログインします。
8. インストールするフィックスパックまたは暫定修正は、IBM サポート・ポータル、パスポート・アドバンテージ、または Fix Central から入手してください。
9. 実行可能ファイルを置いたディレクトリーに変更して、次のステップを実行してください。

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

   a. 次のコマンドを入力してファイル許可を変更します。

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

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

   b. 次のコマンドを発行してインストール・ファイルを解凍します。

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

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

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

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

    インストール・ウィザード
    使用するオペレーティング・システムの指示に従って、以下を実行します。

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

    ヒント: ウィザードを開始した後、「**IBM Installation Manager**」ウィンドウで、「**更新**」アイコンをクリックします。「**インストール**」または「**変更**」アイコンをクリックしないでください。

    コンソール・モードのコマンド・ライン
    使用するオペレーティング・システムの指示に従って、以下を実行します。

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

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

タスクの結果

インストール・プロセス中に検出されたエラーを訂正します。

インストール・ウィザードを使用してサーバーをインストールした場合は、IBM Installation Manager ツールを使用してインストール・ログを表示できます。 「**ファイル**」 > 「**ログの表示**」をクリックします。ログ・ファイルを収集するには、IBM Installation Manager ツールから、「**ヘルプ**」 > 「**問題分析のためのデータのエクスポート**」をクリックします。

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

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

クラスター環境における IBM Spectrum Protect へのフィックスパックの適用

IBM Spectrum Protect 保守更新 (フィックスパックともいいます) により、サーバーを現行の保守レベルまで引き上げることができます。 AIX 用のクラスター環境にフィックスパックを適用することができます。

始める前に

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

手順

1. データベースのバックアップを取ります。 スナップショット・バックアップを使用する方法をお勧めします。 スナップショット・バックアップは、スケジュールされたデータベース・バックアップを中断しない、フル・データベース・バックアップです。例えば、次のコマンドを発行します。

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

   サーバーを前のレベルに戻す必要がある場合、データベースのバックアップと構成ファイルを使用して、サーバーを前のレベルに復元する必要があります。
2. 装置構成情報をバックアップします。 次のコマンドを出します。

   ```
   backup devconfig filenames=file_name
   ```

   ここで、*file_name* は、装置構成情報を保管するファイルの名前を示します。
3. ボリューム・ヒストリー情報をバックアップします。 次のコマンドを出します。

   ```
   backup volhistory filenames=file_name
   ```

   ここで、*file_name* は、ボリューム・ヒストリー情報を保管するファイルの名前を示します。
4. サーバー・オプション・ファイル (通常、`dsmserv.opt` という名前) のコピーを保存します。ファイルはサーバー・インスタンス・ディレクトリーにあります。
5. IBM Spectrum Protect サーバーのアプリケーション・レベルのモニターを使用する場合、1 次ノードから、dsmserv アプリケーション・リソースのモニターを中断します。 モニターを中断するには、smitty IBM PowerHA® メニューを使用します。
6. IBM Spectrum Protect サーバーを停止します。

7. データベース・マネージャーが実行中でないことを確認してください。
8. すべての共有リソースを 1 次ノードにマウントします。

   フィックスパックのインストール時に他のノードにこれらのリソースへの書き込み権限がないことを確認してください。ご使用の環境に IBM Spectrum Protect の複数のインスタンスが含まれている場合、フィックスパックのインストール中、すべてのインスタンスの共有リソースが 1 次ノードにアクセス可能でなければなりません。
9. 1 次ノードに IBM Spectrum Protect サーバーをインストールします。
10. IBM Spectrum Protect サーバーを開始します。
11. IBM Spectrum Protect サーバーを一時停止します。 2 次ノードに進みます。
12. 2 次ノードで IBM Spectrum Protect サーバーをインストールします。

第 5 章 V8.1 へのアップグレード

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

始める前に

3 ページの『サーバーのインストールまたはアップグレードの 前に認識する必要があるセキュリティーに関する事項』 に記載されているセキュリティー更新計画に関する情報を確認します。

このタスクについて

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

表 17. アップグレード手順

アップグレード元のバージョン	アップグレード先のバージョン	参照情報
V8.1	V8.1 フィックスパックまたは暫定修正	97 ページの『第 4 章 IBM Spectrum Protect サーバー・フィックスパックのインストール』
V7.1	V8.1	104 ページの『サーバーのインストールとアップグレードの検証』
V7.1	V8.1 フィックスパックまたは暫定修正	97 ページの『第 4 章 IBM Spectrum Protect サーバー・フィックスパックのインストール』
V5.5、V6.2、または V6.3	V8.1	IBM Spectrum Protect のアップグレードおよびマイグレーション・プロセス - よくあるご質問

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

クラスター環境におけるアップグレードについては、107 ページの『クラスター環境でのサーバーのアップグレード』を参照してください。

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

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

関連情報

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

V8.1 へのアップグレード

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

始める前に

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

ヒント : V8.1 以降では DVD の提供がなくなりました。

手順

サーバーを V8.1 にアップグレードするには、以下のタスクを実行します。

1. 102 ページの『アップグレードの計画』
2. 103 ページの『システムの準備』
3. 104 ページの『サーバーのインストールとアップグレードの 検証』

アップグレードの計画

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

このタスクについて

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

手順

1. 以下のハードウェア要件およびソフトウェア要件を確認します。

   AIX システムのシステム 要件

   システム 要件に関する最新の更新情報は、IBM Spectrum Protect サポート Web サイト (技術情報 1243309) を参照してください。
2. ご使用のオペレーティング・システムに対する特別な手順あるいは固有の情報については、サーバー・コンポーネントの関するリリース情報 (http://www.ibm.com/support/knowledgecenter/SSEQVQ_8.1.11/srv.common/r_relnotes_srv.html) および README ファイルを確認してください。
3. 3 ページの『サーバーのインストールまたはアップグレードの 前に認識する必要があるセキュリティーに関する事項』 に記載されているセキュリティー更新計画に関する情報を確認します。
4. 実動運用への影響を最小限に抑えるために、システムのアップグレードには 適切な日時を選んでください。システムの更新に要する時間は、データベースのサイズおよびその 他の多くの要因によって異なります。 アップグレード・プロセスを開始すると、新しいソフトウェアがインストールされて必要なライセンスがすべて再登録されるまで、クライアントはサーバーに 接続できません。
5. サーバーを V7 から V8.1 にアップグレードする 場合、IBM Db2 サーバーの IBM Spectrum Protect インスタンス用のシステム ID とパスワードがあることを確認してください。システムをアップグレードするには、これらの資格情報が必要です。

システムの準備

システムを V7.1 から V8.1 にアップグレードする準備をするには、各 IBM Db2 インスタンスに関する情報を収集する必要があります。次に、サーバー・データベースをバックアップし、主要な構成ファイルを保存し、セッションを取り消して、サーバーを停止します。

手順

1. サーバーがインストールされているコンピューターにログオンします。

   インスタンス・ユーザー ID を使用してログオンしていることを確認してください。
2. Db2 インスタンスのリストを取得します。以下のシステム・コマンドを発行します。

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

   出力は、以下の例のようになります。

   ```
   tsminst1
   ```

   各インスタンスが、システム上で実行されているサーバーに対応していることを確認してください。
3. Db2 インスタンスごとに、そのインスタンスに対して構成されているデフォルト・データベース・パス、実際のデータベース・パス、データベース名、データベース別名、および Db2 変数を書き留めます。後で参照できるように、この記録を保持しておきます。この情報は、V7.1 データベースをリストアするために必要です。
4. 管理ユーザー ID を使用して、サーバーに接続します。
5. **BACKUP DB** のコマンドを使用してデータベースをバックアップします。

   推奨される方式は、スナップショット・バックアップを作成することです。これはスケジュール済みのデータベース・バックアップに割り込まないフル・データベース・バックアップです。

   例えば、次のコマンドを発行して、スナップショット・バックアップを作成することができます。

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

   ```
   backup devconfig filenames=file_name
   ```

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

   ヒント : V7.1 データベースをリストアする場合、このファイルが必要です。
7. ボリューム・ヒストリー・ファイルを、別のディレクトリーにバックアップします。以下の管理コマンドを発行します。

   ```
   backup volhistory filenames=file_name
   ```

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

   ヒント : V7.1 データベースをリストアする場合、このファイルが必要です。
8. サーバー・オプション・ファイル (通常は `dsmserv.opt` という名前) のコピーを保存します。ファイルはサーバー・インスタンス・ディレクトリーにあります。
9. 新規セッションを使用不可にして、サーバー上のアクティビティーを 防止します。以下の管理コマンドを発行します。

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

    ```
    query session
    ```

11. 次の管理コマンドを発行して、セッションを取り消します。

```
cancel session all
```

このコマンドは、現行セッションを除くすべてのセッションを取り消します。

12. 次の管理コマンドを発行して、サーバーを停止します。

```
halt
```

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

次のコマンドを出します。

```
ps -ef | grep dsmserv
```

14. インストール済み環境のサーバー・インスタンス・ディレクトリーで、NODELOCK ファイルを見つけて、それを構成ファイルを保存している別のディレクトリーに移動します。

NODELOCK ファイルには、ご使用のシステムの以前のライセンス情報が入っています。 アップグレードが完了すると、このライセンス情報は置き換えられます。

サーバーのインストールとアップグレードの検証

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

始める前に

root ユーザー ID を使用してシステムにログオンする必要があります。

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

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

1. 最大ファイル・サイズ値を照会するには、次のコマンドを実行します。

```
ulimit -Hf
```

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

このタスクについて

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

- サーバー

  ヒント: サーバー・コンポーネントを選択するときに、データベース (IBM Db2)、Global Security Kit (GSKit)、および IBM Java ランタイム環境 (JRE) が自動的にインストールされます。
- サーバー言語
- 使用許諾条件
- 装置
- IBM Spectrum Protect for SAN
- Operations Center

手順

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

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

2. 次の手順を実行してください。

   a. 製品パッケージからインストール・ファイルを抽出したときにそれらのファイルを保管するのに十分なスペースがあることを確認してください。 スペース所要量については、ご使用の製品のダウンロード資料を参照してください。

      - IBM Spectrum Protect 技術情報 588021
      - IBM Spectrum Protect Extended Edition 技術情報 588023
      - IBM Spectrum Protect for Data Retention 技術情報 588025

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

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

   c. 必要に応じて、次のコマンドを実行してファイル許可を変更します。

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

      ここで、*package_name* は、以下の例のようになります。

      ```
      8.1.x.000-IBM-SPSRV-AIX.bin
      ```

      例では、*8.1.x.000* は製品リリース・レベルを表します。

   d. 次のコマンドを実行して、インストール・ファイルを抽出します。

      ```
      ./package_name.bin
      ```

      このパッケージは大容量です。 そのため、抽出にはしばらく時間がかかります。

3. IBM Spectrum Protect ウィザードが正常に機能するようにするために、以下のコマンドが使用可能であることを確認します： `lsuser`
4. 以下のいずれかの方法を使用して、IBM Spectrum Protect ソフトウェアをインストールします。インストール処理時に IBM Spectrum Protect ライセンスをインストールしてください。

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

   インストール・ウィザード

   IBM Installation Manager のグラフィカル・ウィザードを使用してサーバーをインストールするには、70 ページの『インストール・ウィザードを使用した IBM Spectrum Protect のインストール』の指示に従ってください。

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

   コンソール・モードを使用したサーバーのインストール

   コンソール・モードを使用してサーバーをインストールするには、71 ページの『コンソール・モードを使用した IBM Spectrum Protect のインストール』の指示に従ってください。

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

   サイレント・モード

   サイレント・モードを使用してサーバーをインストールするには、72 ページの『サイレント・モードで IBM Spectrum Protect をインストール』の指示に従ってください。

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

ソフトウェアをインストールした後、システムを再構成する必要はありません。

5. インストール・プロセス中に検出されたエラーを訂正します。

   インストール・ウィザードを使用してサーバーをインストールした場合は、IBM Installation Manager ツールを使用してインストール・ログを表示できます。「**ファイル**」 > 「**ログの表示**」をクリックします。ログ・ファイルを収集するには、IBM Installation Manager ツールから、「**ヘルプ**」 > 「**問題分析のためのデータのエクスポート**」をクリックします。

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

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

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

   ```
   dsmadmc
   ```

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

   ```
   query system
   ```

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

   ```
   query db format=detailed
   ```

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

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

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

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

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

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

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

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

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

制約事項:

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

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

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

9. 自動および手動のデータベース・バックアップ操作のためにサーバーを準備します。

   手順については、94 ページの『データベース・バックアップ操作のためのサーバーの準備』を参照してください。
10. オプション: 追加の言語パッケージをインストールするには、IBM Installation Manager の変更機能を使用します。
11. オプション: 新規バージョンの言語パッケージにアップグレードするには、IBM Installation Manager の更新機能を使用します。
12. 将来何らかの問題が起きた場合のトラブルシューティングを容易にするために、必ず十分なスペースをコア・ダンプに割り振ってください。詳しくは、技術情報 6357399 を参照してください。

次のタスク

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

クラスター環境でのサーバーのアップグレード

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

手順

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

表 *18. AIX* オペレーティング・システムのクラスター環境でのサーバーのアップグレード手順

ソース・リリース	ターゲット・リリース	手順
V8.1	V8.1 フィックスパック	99 ページの『クラスター環境における IBM Spectrum Protect へのフィックスパックの適用』
V6.3 または V7.1	V8.1	• 108 ページの『共有データベース・インスタンスを使用する クラスター環境での IBM Spectrum Protect の V7.1 から V8.1 へのアップグレード』 • 別個のデータベース・インスタンスを使用する AIX のクラスター環境でのアップグレード
V5.5, V6.1, V6.2	V7.1.1 以降	IBM Spectrum Protect のアップグレードおよびマイグレーション・プロセス - よくあるご質問

共有データベース・インスタンスを使用する クラスター環境での IBM Spectrum Protect の V7.1 から V8.1 へのアップグレード

共有データベース・インスタンスを使用する AIX のクラスター環境で IBM Spectrum Protect サーバーを V7.1 から V8.1 にアップグレードできます。このようにして、IBM Spectrum Protect の新機能を利用できます。

始める前に

アップグレードする V7.1 サーバーの基本リリースのインストール・メディアを保持していることを確認してください。DVD から IBM Spectrum Protect をインストールした場合は、その DVD が使用可能であることを確認してください。ダウンロード・パッケージから IBM Spectrum Protect をインストールした場合は、ダウンロードしたファイルが使用可能であることを確認してください。アップグレードが失敗し、サーバーのライセンス・モジュールがアンインストールされた場合は、サーバーの基本リリースのインストール・メディアからライセンスを再インストールする必要があります。

このタスクについて

IBM Db2 インスタンス・ディレクトリーがクラスター内のノード間で共有されている場合は、以下の手順を使用します。Db2 インスタンス・ディレクトリーは。インストール・ディレクトリーにあります。

```
/home/tsminst1/sqllib
```

Db2 インスタンス・ディレクトリーがノード間で共有されていない場合は、110 ページの『別個のデータベース・インスタンスを使用するクラスター環境でのアップグレード』の指示に従ってください。

手順

1. **BACKUP DB** のコマンドを使用してデータベースをバックアップします。

   推奨される方式は、スナップショット・バックアップを使用することです。これはスケジュール済みのバックアップに割り込まずにフル・データベース・バックアップを作成します。

   例えば、次のコマンドを実行して、スナップショット・バックアップを作成することができます。

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

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

   ```
   backup devconfig filenames=file_name
   ```

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

3. 次の管理コマンドを実行して、ボリューム・ヒストリー・ファイルを別のディレクトリーにバックアップします。

   ```
   backup volhistory filenames=file_name
   ```

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

4. サーバー・オプション・ファイル (通常、`dsmserv.opt` という名前) のコピーを保存します。このファイルはサーバー・インスタンス・ディレクトリー内にあります。
5. サーバーのすべてのインスタンスを停止します。サーバー・プロセスが実行していないことを確認します。IBM Spectrum Protect サーバーのアプリケーション・レベルのモニターを使用している場合は、クラスター化ツールを使用して、**dsmserv** アプリケーション・リソースのモニターを中断します。
6. インスタンスに対してデータベース・マネージャーが実行中でないことを確認します。 `db2sysc` プロセスが実行中であるかどうかを判別します。

   実行中のプロセスの所有者は、どのインスタンスがアクティブになっているかを 示します。 サーバー・インスタンスの所有者ごとに、次のコマンドを実行して、Db2 を停止します。

   ```
   db2stop
   ```

7. 1 次ノードで、**./install.sh** コマンドを実行して、IBM Spectrum Protect サーバーをインストールします。手順については、69 ページの『第 2 章 サーバー・コンポーネントのインストール』を参照してください。

   ウィザードを開始した後、「**IBM Installation Manager**」ウィンドウで、「**更新**」または「**変更**」アイコンをクリックします。
8. 各サーバーをフォアグラウンドで始動します。
   a) インスタンス所有者 ID を使用してログインしていることを確認してください。
   b) インスタンス・ディレクトリーに移動して、次のコマンドを実行します。

   ```
   /opt/tivoli/tsm/server/bin/dsmserv
   ```

   サーバーが始動したことを示すサーバーのプロンプトが表示されるまで待ちます。
9. アップグレードしている各 IBM Spectrum Protect インスタンスのサーバーを停止します。次のコマンドを出します。

   ```
   halt
   ```

   ヒント: Db2 インスタンス・ディレクトリーがクラスター内のノード間で共有されているため、共有リソースをクラスター内の 2 次ノードに移動する必要はありません。
10. クラスター内の各 2 次ノードで、以下の手順を実行します。
    a) **./install.sh** コマンドを実行して、IBM Spectrum Protect サーバーをインストールします。手順については、69 ページの『第 2 章 サーバー・コンポーネントのインストール』を参照してください。
       i) インストール・ウィザードを実行する場合、「**IBM Installation Manager**」ウィンドウで、「**更新**」または「**変更**」アイコンをクリックします。
       ii) インストール・ウィザードを実行している場合は、「**インスタンスの資格情報**」パネルで、各インスタンスの「**このインスタンスを更新**」チェック・ボックスをクリアします。
       iii) コンソール・モードでサーバーをインストールしている場合、プロンプト「このインスタンスを更新しますか？」で、各インスタンスに NO を入力します。
       iv) サイレント・モードでサーバーをインストールしている場合、各インスタンスの user.*instance_name*_update 変数の値に FALSE を指定してください。
    b) 各 IBM Spectrum Protect サーバーが開始していることを確認します。アプリケーション・レベルのモニターを使用している場合は、クラスター化ツールを使用して、サーバーを始動します。

       サーバーの始動に関する説明は、89 ページの『サーバー・インスタンスの開始』を参照してください。
11. **REGISTER LICENSE** コマンドを実行して、システムにインストールされているサーバー・コンポーネントのライセンスを登録します。

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

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

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

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

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

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

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

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

制約事項 :

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

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

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

別個のデータベース・インスタンスを使用するクラスター環境でのアップグレード

別個のデータベース・インスタンスを使用する AIX のクラスター環境でサーバーをアップグレードできます。このようにして、新機能を利用できます。

始める前に

アップグレードする V7.1 サーバーの基本リリースのインストール・メディアを保持していることを確認してください。DVD から IBM Spectrum Protect をインストールした場合は、その DVD が使用可能であることを確認してください。ダウンロード・パッケージから IBM Spectrum Protect をインストールした場合は、ダウンロードしたファイルが使用可能であることを確認してください。アップグレードが失敗し、サーバーのライセンス・モジュールがアンインストールされた 場合は、サーバーの基本リリースのインストール・メディアからライセンスを 再インストールする必要があります。

このタスクについて

IBM Db2 インスタンス・ディレクトリーがクラスター内のノード間で共有されていない場合は、以下の手順を使用します。Db2 インスタンス・ディレクトリーは、次の場所にあります。

```
/home/tsminst1/sqllib
```

Db2 インスタンス・ディレクトリーがノード間で共有されている場合は、108 ページの『共有データベース・インスタンスを使用する クラスター環境での IBM Spectrum Protect の V7.1 から V8.1 へのアップグレード』の指示に従ってください。

手順

1. **BACKUP DB** のコマンドを使用してデータベースをバックアップします。

   推奨される方式は、スナップショット・バックアップを使用することです。これはスケジュール済みのバックアップに割り込まずにフル・データベース・バックアップを作成します。

   例えば、次のコマンドを実行して、スナップショット・バックアップを作成することができます。

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

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

   ```
   backup devconfig filenames=file_name
   ```

   ここで、*file_name* は、装置構成情報を保管するファイルの名前を示します。
3. 次の管理コマンドを実行して、ボリューム・ヒストリー・ファイルを別のディレクトリーにバックアップします。

```
backup volhistory filenames=file_name
```

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

4. サーバー・オプション・ファイル (通常、dsmserv.opt という名前) のコピーを保存します。このファイルはサーバー・インスタンス・ディレクトリー内にあります。
5. サーバーのすべてのインスタンスを停止します。サーバー・プロセスが実行していないことを確認します。IBM Spectrum Protect サーバーのアプリケーション・レベルのモニターを使用している場合は、クラスター化ツールを使用して、**dsmserv** アプリケーション・リソースのモニターを中断します。
6. インスタンスに対してデータベース・マネージャーが実行中でないことを確認します。 db2sysc プロセスが実行中であるかどうかを判別します。

   実行中のプロセスの所有者は、どのインスタンスがアクティブになっているかを 示します。 サーバー・インスタンスの所有者ごとに、次のコマンドを実行して、Db2 を停止します。

   ```
   db2stop
   ```

7. すべての IBM Spectrum Protect インスタンスの共有リソースが 1 次ノード上にあることを確認します。

   アップグレード時に他のノードにこれらのリソースの書き込み権限がないことを確認してください。環境にサーバーの複数のインスタンスが含まれている場合、すべてのインスタンスの共有リソースが 1 次ノードからアクセス可能でなければなりません。
8. 1 次ノードで、**./install.sh** コマンドを実行して、サーバーをインストールします。手順については、69 ページの『第 2 章 サーバー・コンポーネントのインストール』を参照してください。

   ウィザードを開始した後、「**IBM Installation Manager**」ウィンドウで、「**インストール**」アイコンをクリックします。「**更新**」または「**変更**」アイコンをクリックしないでください。アップグレードを実行するには、サーバーをインストールする必要があります。
9. 各サーバーをフォアグラウンドで始動します。
   a) インスタンス所有者 ID を使用してログインしていることを確認してください。
   b) インスタンス・ディレクトリーに移動して、次のコマンドを実行します。

      ```
      /opt/tivoli/tsm/server/bin/dsmserv
      ```

      サーバーが始動したことを示すサーバーのプロンプトが表示されるまで待ちます。
10. アップグレードしている 各 IBM Spectrum Protect インスタンスのサーバーを停止します。以下のコマンドを実行します。

    ```
    halt
    ```

11. クラスター内の各 2 次ノードで、以下の手順を実行します。
    a) すべての共有リソースを 2 次ノードに移動します。

       環境にサーバーの複数のインスタンスが含まれている場合、すべてのインスタンスの共有リソースが、アップグレード時に 2 次ノードからアクセス可能でなければなりません。
    b) サーバーのすべてのインスタンスを 停止します。サーバー・プロセスが実行していないことを確認します。
    c) インスタンスに対してデータベース・マネージャーが実行中でないことを確認します。 db2sysc プロセスが実行中であるかどうかを判別します。

       実行中のプロセスの所有者は、どのインスタンスがアクティブになっているかを 示します。 サーバー・インスタンスの所有者ごとに、次のコマンドを実行して、Db2 を停止します。

       ```
       db2stop
       ```

    d) **./install.sh** コマンドを実行して、サーバーをインストールします。手順については、69 ページの『第 2 章 サーバー・コンポーネントのインストール』を参照してください。

i) インストール・ウィザードを使用している場合は、「**IBM Installation Manager**」ウィンドウで、「**インストール**」アイコンをクリックします。「**更新**」または「**変更**」アイコンをクリックしないでください。

ii) インストール・ウィザードを使用している場合は、「**インスタンスの資格情報**」ページで、構成している各インスタンスの「**クラスターの 2 次ノードでこのインスタンスを構成**」チェック・ボックスを選択します。

iii) コンソール・モードでサーバーをインストールしている 場合、プロンプト「クラスターの 2 次ノードでこのインスタンスを構成しますか？（Configure this instance on a secondary node of the cluster?)」で、各インスタンスに YES を入力します。

iv) サイレント・モードでサーバーをインストールしている 場合、各インスタンスの user.*instance_name*_secondaryNode 変数の値に TRUE を指定してください。

e) 各 V8.1.7 サーバーが開始していることを確認します。アプリケーション・レベルのモニターを使用している場合は、クラスター化ツールを使用して、サーバーを始動します。

サーバーの始動に関する説明は、サーバー・インスタンスの開始を参照してください。

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

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

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

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

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

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

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

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

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

制約事項 :

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

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

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

第 6 章 リファレンス: IBM Db2 サーバー・データベースに使用する IBM Spectrum Protect コマンド

このリストは、IBM サポートによって、Db2 コマンドを発行するよう指示された場合に参照として使用してください。

目的

ウィザードを使用して IBM Spectrum Protect をインストールおよび構成した後、Db2 コマンドを実行する必要がある場合はめったにありません。表に、使用する、または実行するよう依頼される可能性がある一部の Db2 コマンドをリストします。

このリストは、補足資料としてのみ使用することを目的としたもので、包括的なリストではありません。また、IBM Spectrum Protect 管理者が、日常的または継続的にこのリストを使用することを示唆するものではありません。一部のコマンドについては、例が示されています。詳細な出力はリストされていません。

ここに記載されているコマンドの完全な説明および構文については、Db2 の製品資料を参照してください。

表 *19. Db2* コマンド

コマンド	説明	例
db2icrt	インスタンス所有者のホーム・ディレクトリーに Db2 インスタンスを作成します。 **ヒント:** IBM Spectrum Protect 構成ウィザードは、サーバーおよびデータベースによって使用されるインスタンスを作成します。構成ウィザードを使用してサーバーをインストールして構成した後は、通常、**db2icrt** コマンドは使用しません。 このユーティリティーは、DB2DIR/instance ディレクトリーにあります。ここで、DB2DIR は、Db2 データベース・システムの現行バージョンがインストールされているインストール場所を表します。	IBM Spectrum Protect インスタンスを手動で作成します。 次のコマンドを 1 行で入力します。 `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u instance_name instance_name`
db2set	Db2 変数を表示します。	Db2 変数をリストします。 `db2set`
CATALOG DATABASE	システム・データベース・ディレクトリーに、データベースのロケーション情報を保管します。 データベースは、ローカル・ワークステーションまたはリモート・データベース・パーティション・サーバーのいずれかにも配置できます。 サーバー構成ウィザードは、サーバー・データベースを使用するために必要なすべてのカタログを扱います。 サーバーを構成した後、実行しているときに、環境内で何らかの変更または損傷があった場合にのみ、このコマンドを手動で実行してください。	データベースをカタログします。 `db2 catalog database tsmdb1`
CONNECT TO DATABASE	コマンド・ライン・インターフェース (CLI) で使用するために、指定したデータベースに接続します。	IBM Spectrum Protect CLI から Db2 データベースに接続します。 `db2 connect to tsmdb1`

表 19. *Db2* コマンド (続き)

コマンド	説明	例

GET DATABASE CONFIGURATION	特定のデータベース構成ファイル内にある個々の項目の値を返します。
	重要 : このコマンドおよびパラメーターは、Db2 によって直接設定および管理されます。これらは、単に情報提供のため、および既存の設定を表示する手段として、ここにリストされています。 これらの設定の変更は、IBM サポート、または APAR や技術ガイダンス文書 (技術情報) などの業務広報によって指示される場合があります。これらの設定を手動で変更しないでください。 これらの設定は、IBM による指示があった場合にのみ、IBM Spectrum Protect サーバーのコマンドまたはプロシージャーを使用して変更してください。
		データベース別名についての構成情報を表示します。
		`db2 get db cfg for tsmdb1`
		データベース構成、ログ・モード、および保守などの設定を確認するために情報を取得します。
		`db2 get db config for tsmdb1 show detail`

GET DATABASE MANAGER CONFIGURATION	特定のデータベース構成ファイル内にある個々の項目の値を返します。 **重要 :** このコマンドおよびパラメーターは、Db2 によって直接設定および管理されます。これらは、単に情報提供のため、および既存の設定を表示する手段として、ここにリストされています。 これらの設定の変更は、IBM サポート、または APAR や技術ガイダンス文書 (技術情報) などの業務広報によって指示される場合があります。これらの設定を手動で変更しないでください。 これらの設定は、IBM による指示があった場合にのみ、IBM Spectrum Protect サーバーのコマンドまたはプロシージャーを使用して変更してください。	データベース・マネージャーの構成情報を取得します。 `db2 get dbm cfg`
GET HEALTH SNAPSHOT	データベース・マネージャーとそのデータベースのヘルス状況情報を検索します。 戻された情報は、コマンドが発行された時点でのヘルス状態のスナップショットを表しています。 IBM Spectrum Protect は、ヘルス・スナップショットおよび Db2 により提供されるその他のメカニズムを使用して、データベースの状態をモニターします。ヘルス・スナップショットまたはその他の文書で、項目またはデータベースがアラート状態である可能性があることが示される場合があります。そのような場合は、状態を改善するためにアクションを検討する必要があることを示しています。 IBM Spectrum Protect は、状態をモニターして、適切に対応します。 Db2 データベースによって宣言されたすべてのアラートに従って対処しなければならない訳ではありません。	Db2 ヘルス・モニター・インディケーターに関するレポートを受け取ります。 `db2 get health snapshot for database on tsmdb1`

GRANT (データベース権限)	データベース内の特定のオブジェクトに適用される特権ではなく、データベース全体に適用される権限を付与します。	ユーザー ID itmuser にアクセス権限を付与します。
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

表 *19. Db2* コマンド *(*続き*)*

コマンド	説明	例
RUNSTATS	表および関連する索引、または統計ビューの特性についての統計を更新します。 これらの特性には、レコード数、ページ数、および平均レコード長が含まれます。 表を見る場合は、表を更新または再編成した後、このユーティリティーを 実行します。 照会を最適化するためにビューの統計を使用する場合は、ビューを最適化に使用できるようにする必要があります。最適化で使用可能なビューを、統計ビューといいます。ビューを最適化に使用できるようにするには、Db2 **ALTER VIEW** ステートメントを使用します。基礎となる表への変更が、ビューによって返される行にかなり影響を与える場合は、**RUNSTATS** ユーティリティーを 実行します。 **ヒント:** サーバーは、必要に応じて **RUNSTATS** コマンドを実行するように Db2 を構成します。	単一の表で統計を更新します。 `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all`
SET SCHEMA	Db2 CLI から直接 SQL コマンドを実行するための準備として、**CURRENT SCHEMA** 特殊レジスターの値を変更します。 **ヒント:** 特殊レジスターは、データベース・マネージャーによってアプリケーション処理のために定義されるストレージ域です。これは、SQL ステートメントで参照可能な情報を保管するために使用されます。	IBM Spectrum Protect のスキーマを設定します。 `db2 set schema tsmdb1`
START DATABASE MANAGER	現在のデータベース・マネージャー・インスタンスのバックグラウンド・プロセスを開始します。 サーバーは、サーバーを開始および停止するたびに、インスタンスとデータベースを開始および停止します。 **重要:** IBM サポートから特に別の指示がない限り、サーバーがインスタンスとデータベースの開始および停止を管理できるようにしてください。	データベース・マネージャーを開始します。 `db2start`
STOP DATABASE MANAGER	現在のデータベース・マネージャー・インスタンスを停止します。 データベース・マネージャーは、明示的に停止されない限り、アクティブなままです。 このコマンドは、データベースに接続されたアプリケーションがある場合には、データベース・マネージャー・インスタンスを停止しません。 データベース接続がなく、インスタンス接続はある場合、このコマンドは最初にインスタンス接続を強制的に停止します。 その後に、データベース・マネージャーを停止します。 また、このコマンドは、データベース・マネージャーを停止する前に、未解決のデータベースの活動を非活動化します。 このコマンドはクライアントでは無効です。 サーバーは、サーバーを開始および停止するたびに、インスタンスとデータベースを開始および停止します。 **重要:** IBM サポートから特に別の指示がない限り、サーバーがインスタンスとデータベースの開始および停止を管理できるようにしてください。	データベース・マネージャーを停止します。 `db2 stop dbm`

第 7 章 IBM Spectrum Protect のアンインストール

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

始める前に

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

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

このタスクについて

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

次のタスク

IBM Spectrum Protect コンポーネントを再インストールします。

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

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

手順

1. Installation Manager を開始します。

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

   ```
   ./IBMIM
   ```

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

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

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

手順

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

   ```
   eclipse/tools
   ```

例えば次のとおりです。

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

2. tools ディレクトリーから以下のコマンドを発行します。

```
./imcl -c
```

3. アンインストールするには、5 を入力します。
4. IBM Spectrum Protect パッケージ・グループからアンインストールすることを 選択します。
5. 「N」(次へ) を入力します。
6. IBM Spectrum Protect サーバー・パッケージをアンインストールすることを 選択します。
7. 「N」(次へ) を入力します。
8. 「U」(アンインストール) を入力します。
9. 「F」(終了) を入力します。

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

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

始める前に

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

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

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

手順

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

```
eclipse/tools
```

例えば次のとおりです。

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

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

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

以下にコマンド例を示します。

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

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

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

このタスクについて

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

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

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

2. 各サーバー・インスタンスに次のコマンドを実行します。

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

   それぞれのインスタンスのデータベース・パスを記録します。

3. IBM Spectrum Protect をアンインストールします。
4. サポートされるバージョンの IBM Spectrum Protect (フィックスパックを含む) をアンインストールすると、インスタンス・ファイルが作成されます。 インスタンス・ファイルは、IBM Spectrum Protect の再インストールに役立つように作成されます。 再インストールの際にインスタンスの資格情報の入力を求めるプロンプトが出されたときに、このファイルを確認して情報を使用します。 サイレント・インストール・モードでは、INSTANCE_CRED 変数を使用して、これらの資格情報を指定します。

   インスタンス・ファイルは以下のロケーションにあります。

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

5. IBM Spectrum Protect を再インストールします。

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

   a. サーバー・インスタンスを再作成します。

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

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

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

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

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

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

      ```
      db2 list database directory
      ```

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

IBM Installation Manager のアンインストール

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

始める前に

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

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

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

手順

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

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

     ```
     ./uninstall
     ```

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

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

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

始める前に

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

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

このタスクについて

121 ページの表 20 は、Operations Center のインストールまたはアンインストールの 方法をリストし、関連の説明を検索する場所を示しています。

Operations Center のアップグレードについては、Operations Center のアップグレードを参照してください。

表 *20. Operations Center* をインストールまたはアンインストールするための方法

Method	**説明**
グラフィカル・ウィザード	• グラフィカル・ウィザードを使用した Operations Center のインストール • グラフィカル・ウィザードを使用した Operations Center のアンインストール
コンソール・モード	• コンソール・モードでの Operations Center のインストール • コンソール・モードでの Operations Center のアンインストール
サイレント・モード	• サイレント・モードでの Operations Center のインストール • 192 ページの『サイレント・モードでの Operations Center のアンインストール』

第 8 章 Operations Center のインストール計画

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

このタスクについて

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

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

Operations Center には、以下の機能があります。

複数のサーバー用のユーザー・インターフェース
Operations Center を使用して、1 つ以上の IBM Spectrum Protect サーバーを管理できます。

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

アラートのモニター

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

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

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

Operations Center のシステム要件

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

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

インストール中に検証される要件

123 ページの表 21 は、インストール中に検証される前提条件をリストし、これらの要件に関する詳しい情報の検索場所を示しています。

表 *21.* インストール中に検証される要件

要件	詳細
最小メモリー所要量	124 ページの『Operations Center のコンピューターの要件』
オペレーティング・システム要件	127 ページの『オペレーティング・システム要件』
Operations Center がインストールされるコンピューターのホスト名	131 ページの『インストール・チェックリスト』

表 21. インストール中に検証される要件 (続き)	
要件	**詳細**
Operations Center インストール・ディレクトリーの要件	131 ページの『インストール・チェックリスト』

Operations Center のコンピューターの要件

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

リソース要件

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

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

Operations Center でモニターされるハブ・サーバーおよびスポーク・サーバーは、124 ページの『ハブ・サーバーおよびスポーク・サーバーの要件』で説明しているように、追加のリソースが必要です。

ハブ・サーバーおよびスポーク・サーバーの要件

初めて Operations Center を開いたときに、Operations Center を、ハブ・サーバー として指定された 1 つの IBM Spectrum Protect サーバーと関連付ける必要があります。複数サーバー環境では、その他のサーバー (スポーク・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。

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

124 ページの表 22 は、Operations Center によって管理されるハブ・サーバーおよび各スポーク・サーバーにインストールする必要がある、IBM Spectrum Protect サーバーのバージョンを示しています。

表 22. ハブ・サーバーおよびスポーク・サーバー上の *IBM Spectrum Protect* サーバーのバージョン要件		
Operations Center	**ハブ・サーバー上のバージョン**	**各スポーク・サーバー上のバージョン**
V8.1.12	V8.1.12	V8.1.10 以降 ========== または V7.1.10 以降のバージョン 7 のリリース **制限 :** • V8.1.12 より前のバージョンを使用するサーバーでは、一部の Operations Center 機能を使用できません。 • スポーク・サーバーは、ハブ・サーバーより新しいバージョンを使用することはできません。

Operations Center の他のバージョンでのハブ・サーバーとスポーク・サーバーの互換性要件については、技術情報 496593 を参照してください。

ハブ・サーバーがサポートできるスポーク・サーバーの数

ハブ・サーバーがサポートできるスポーク・サーバーの数は、構成と各スポーク・サーバーの IBM Spectrum Protect のバージョンによって異なります。ただし、一般ガイドラインとして、VM などの別のシステム上のハブ・サーバーは V7.1 以降のスポーク・サーバーを数十台サポートできます。

ハブ・サーバーおよびスポーク・サーバー構成の設計上のヒント

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

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

パフォーマンスに影響を与える主な要因

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

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

ハブ・サーバーとスポーク・サーバーのグループ化の方法

ハブ・サーバーとスポーク・サーバーは、地理的位置によってグループ化することを検討してください。例えば、同じデータ・センター内でサーバーを管理すると、ファイアウォールや、異なるロケーション間での不十分なネットワーク帯域幅が原因で発生する問題を回避するのに役立ちます。必要な場合は、以下の 1 つ以上の特性に従って、さらにサーバーを分割することができます。

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

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

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

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

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

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

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

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

どのような場合に複数のハブ・サーバーを使用するか

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

制限 :

- 単一のサーバーが、ハブ・サーバーとスポーク・サーバーの両方になることはできません。
- 各スポーク・サーバーは、1 つのハブ・サーバーにのみ割り当てることができます。
- 各ハブ・サーバーには、別個の Web アドレスを持つ、Operations Center の別個のインスタンスが必要です。

ハブ・サーバーを選択するためのヒント

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

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

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

負荷が軽いサーバーを選択する

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

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

ネットワーク往復待ち時間が最短になるようにサーバーを配置する

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

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

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

ハブ・サーバーが状況モニターのリソース要件を満たしていることを確認する

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

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

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

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

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

ご使用の環境で複数のハブ・サーバーが必要かどうかを判別する

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

オペレーティング・システム要件

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

以下のシステム上で Operations Center を実行できます。

AIX および Linux のシステムの Operations Center サポートは、特に明記されていない限り、ビッグ・エンディアン・バージョンのみに限定されます。

- AIX システム:
  - IBM AIX V7.1 テクノロジー・レベル 5 およびサービス・パック 5 以降
  - IBM AIX V7.2 テクノロジー・レベル 3 およびサービス・パック 3 以降

要件に関する最新情報については、Software and Hardware Requirements を参照してください。

Web ブラウザーの要件

Operations Center では、Apple、Google、Microsoft、および Mozilla の各 Web ブラウザーを実行することができます。

Web ブラウザーで Operations Center の最適な表示ができるように、必ずシステムの 画面解像度を最小で 1024 X 768 ピクセルに設定してください。

最適なパフォーマンスのためには、JavaScript パフォーマンスが優れた Web ブラウザーを使用し、ブラウザーのキャッシュを有効にしてください。

Operations Center では、以下の Web ブラウザーを実行できます。

- iPad の Apple Safari

  制約事項 : iOS 8.x または iOS 9.x 上で Apple Safari を実行している場合、Operations Center とのセキュア通信に自己署名証明書を (証明書の追加構成なしで) 使用することはできません。 認証局 (CA) 認証を使用するか、必要に応じて自己署名証明書を構成してください。 手順については、技術情報 http://www.ibm.com/support/docview.wss?uid=swg21963153 を参照してください。
- Google Chrome 54 以降
- Microsoft Internet Explorer 11 以降
- Mozilla Firefox ESR 45 またはバージョン 48 以降

Transport Layer Security (TLS) 1.2 プロトコルを使用して Operations Center と Web ブラウザーの間の通信を保護する必要があります。 Web ブラウザーは TLS 1.2 をサポートしている必要があり、TLS 1.2 が有

効に設定されている必要があります。Web ブラウザーはこれらの要件を満たしていない場合、SSL エラーを表示します。

要件に関する最新情報については、Software and Hardware Requirements を参照してください。

言語要件

デフォルトにより、Operations Center では、Web ブラウザーで使用されている言語が使用されます。ただし、インストール処理では、オペレーティング・システムで使用されている言語が使用されます。Web ブラウザーとオペレーティング・システムが、ユーザーが必要とする言語に設定されていることを確認してください。

表 *23. AIX* システムで使用できる *Operations Center* の言語の値

言語	言語オプションの値
中国語 (簡体字)	zh_CN
中国語 (簡体字) (UTF-8)	ZH_CN
中国語 (繁体字) (Big5)	Zh_TW
中国語 (繁体字) (UTF-8)	ZH_TW
中国語 (繁体字) (euc_tw)	zh_TW
英語	en_US
英語 (UTF-8)	EN_US
フランス語	fr_FR
フランス語 (UTF-8)	FR_FR
ドイツ語	de_DE
ドイツ語 (UTF-8)	DE_DE
イタリア語	it_IT
イタリア語 (UTF-8)	IT_IT
日本語 (EUC)	ja_JP
日本語 (PC)	Ja_JP
日本語 (UTF-8)	JA_JP
韓国語	ko_KR
韓国語 (UTF-8)	KO_KR
ポルトガル語、ブラジル	pt_BR
ブラジル・ポルトガル語 (UTF-8)	PT_BR
ロシア語	ru_RU
ロシア語 (UTF-8)	RU_RU
スペイン語	es_ES
スペイン語 (UTF-8)	ES_ES

IBM Spectrum Protect クライアント管理サービスの要件と制限

IBM Spectrum Protect クライアント管理サービスは、クライアント・ログ・ファイルなどの診断情報を収集するためにバックアップ/アーカイブ・クライアントにインストールされるコンポーネントです。ご使用

のシステムでクライアント管理サービスをインストールする前に、要件と制限について理解しておく必要があります。

クライアント管理サービスの資料では、クライアント・システム はバックアップ/アーカイブ・クライアントがインストールされているシステムです。

診断情報は、Linux クライアントおよび Windows クライアントからのみ収集可能ですが、管理者は AIX、Linux、または Windows オペレーティング・システムの Operations Center で診断情報を参照できます。

ヒント: 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で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。

クライアント管理サービスの要件

クライアント管理サービスをインストールする前に、次の要件を確認してください。

- クライアントにリモート側からアクセスするには、Operations Center 管理者にシステム権限または次のいずれかのクライアント権限レベルが必要です。
  - ポリシー権限
  - クライアント所有者権限
  - クライアント・ノード・アクセス権限
- クライアント・システムが次の要件を満たしていることを確認します。
  - クライアント管理サービスは、Linux または Windows オペレーティング・システム上で実行されるクライアント・システムにのみインストールできます。
    - バックアップ/アーカイブ・クライアントでサポートされる Linux x86 64 ビット・オペレーティング・システム
    - バックアップ/アーカイブ・クライアントでサポートされる Windows 32 ビットおよび 64 ビット・オペレーティング・システム
  - クライアント管理サービス と Operations Center の間のデータ転送には、トランスポート層セキュリティー (TLS) バージョン 1.2 以降をインストールする必要があります。基本認証が提供され、データと認証情報は Secure Sockets Layer (SSL) チャネルを経由して暗号化されます。クライアント管理サービスをインストールすると、TLS は必要な SSL 証明書とともに自動的にインストールされます。

    IBM Spectrum Protect バージョン 8.1.11 からは、サーバー、クライアント、およびストレージ・エージェントの間の通信を保護するために、TLS 1.3 プロトコルはデフォルトで有効になっています。TLS 1.3 を使用するには、通信セッションの双方が TLS 1.3 を使用している必要があります。いずれかが TLS 1.2 を使用している場合、デフォルトで双方が TLS 1.2 を使用します。
- Linux クライアント・システムでは、クライアント管理サービスをインストールするために root ユーザー権限が必要です。
- Linux クライアント・システムなど、複数のクライアント・ノードを持つことができるクライアント・システムの場合は、それぞれのノード名がクライアント・システム上で固有であることを確認してください。

  ヒント: クライアント管理サービスをインストールした後は、再度インストールする必要はありません。このサービスでは、複数のクライアント・オプション・ファイルを検出できるからです。

クライアント管理サービスの制限

クライアント管理サービスは、バックアップ/アーカイブ・クライアントから診断情報を収集するための基本サービスを提供します。クライアント管理サービスには、以下の制限があります。

- クライアント管理サービスは、バックアップ/アーカイブ・クライアント (IBM Spectrum Protect for Virtual Environments: Data Protection for VMware のデータ・ムーバー・ノードにインストールされているバックアップ/アーカイブ・クライアントを含む) を使用するシステムにのみインストールできます。

- クライアント管理サービス は、その他の IBM Spectrum Protect クライアント・コンポーネントやバックアップ/アーカイブ・クライアントが含まれない製品にインストールすることはできません。
- バックアップ/アーカイブ・クライアントがファイアウォールに 保護されている場合、Operations Center は、クライアント管理サービス 用に構成されているポートを使用して、ファイアウォールを通過してバックアップ/アーカイブ・クライアントに接続できるようにしてください。デフォルト・ポートは 9028 ですが、これは変更できます。
- クライアント管理サービスは、すべてのクライアント・ログ・ファイルをスキャンして、過去 72 時間の期間にわたる項目を検出します。
- Operations Center の「**診断 (Diagnosis)**」ページには、バックアップ/アーカイブ・クライアントの基本トラブルシューティング情報が表示されます。ただし、一部のバックアップ問題では、管理者がクライアント・システムにアクセスして詳細な診断情報を入手することが必要になる場合があります。
- クライアント・システム上のクライアント・エラー・ログ・ファイルとスケジュール・ログ・ファイルの合計サイズが 500 MB を超えると、Operations Center へのログ・レコードの送信に遅れが生じることがあります。ログ・ファイルのサイズを制御するには、**errorlogretention** または **errorlogmax** クライアント・オプションを指定して、ログ・ファイルの整理または折り返しを有効にします。
- 同じサーバーにインストールされている 複数の IBM Spectrum Protect サーバーへの接続に同じクライアント・ノード名を使用すると、1 つのクライアント・ノードのログ・ファイルしか表示できません。

クライアント管理サービス に関連した利用可能な更新については、技術情報 534165 を参照してください。

関連タスク

169 ページの『IBM Spectrum Protect クライアント管理サービスでの診断情報の収集』
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。

Operations Center に必要な管理者 ID

管理者は、Operations Center にログインするためにハブ・サーバーに有効な ID とパスワードを持っている必要があります。Operations Center がサーバーをモニターできるように、管理者 ID は Operations Center にも割り当てられます。

Operations Center では、以下の IBM Spectrum Protect 管理者 ID が必要です。

ハブ・サーバーに登録されている管理者 ID

ハブ・サーバーに登録されている管理者 ID はすべて、Operations Center へのログインに使用できます。ID の権限レベルにより、どのタスクを実行できるかが決定されます。**REGISTER ADMIN** コマンドを使用して、新規の管理者 ID を作成することができます。

制約事項 : 複数サーバー環境で管理者 ID を使用するには、 同じパスワードと権限レベルを使用してこの ID をハブ・サーバーとスポーク・サーバーに登録する必要があります。

これらのサーバーの認証を管理するには、以下のいずれかの方法を使用することを検討してください。

- Lightweight Directory Access Protocol (LDAP) サーバー
- 管理者定義に対する変更を自動的に配布するためのエンタープライズ 構成機能。

モニター管理者 ID

最初にハブ・サーバーを構成すると、IBM-OC-*server_name* という名前の管理者 ID が、システム権限付きでハブ・サーバーに登録され、指定された初期パスワードに関連付けられます。この ID (モニター管理者と呼ばれることもある) は、Operations Center のみによって使用されるように意図されています。

この ID を削除、ロック、または変更しないでください。同じパスワードを持つ同じ管理者 ID が、追加されるスポーク・サーバーに登録されます。このパスワードは、90 日ごとにハブ・サーバーとスポーク・サーバーで自動的に変更されます。このパスワードを使用または管理する必要はありません。

制約事項 : Operations Center は、モニター管理者 ID とパスワードをスポーク・サーバー上で維持します。ただし、これらの資格情報を管理するためにエンタープライズ構成を使用する場合は除きます。資格情報を管理するためのエンタープライズ構成の使用について詳しくは、125 ページの『ハブ・サーバーおよびスポーク・サーバー構成の設計上のヒント』を参照してください。

IBM Installation Manager

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

IBM Installation Manager の必須バージョンがまだインストールされていない場合は、Operations Center をインストールした時に自動的にインストールまたはアップグレードされます。これは、Operations Center を後で必要に応じて更新またはアンインストールできるように、システムにインストールしたままにしておく必要があります。

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

オファリング
ソフトウェア製品のインストール可能単位。

Operations Center オファリングには、IBM Installation Manager が Operations Center をインストールするために必要なメディアのすべてが含まれます。

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

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

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

パッケージ・グループ
共通親ディレクトリーを共有するパッケージのセット。

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

Operations Center パッケージは、IBM Fix Central 上のリポジトリーに保管されています。

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

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

インストール・チェックリスト

Operations Center をインストールする前に、インストールの資格情報などの特定の情報を確認し、インストールのために IBM Installation Manager に指定する入力を判別する必要があります。

以下のチェックリストは、Operations Center をインストールする前に確認または決定する必要がある情報をハイライトで示し、132 ページの表 24 は、この情報の詳細を説明しています。

__ Operations Center がインストールされるコンピューターのホスト名を確認する。
__ インストールの資格情報を確認する。
__ Operations Center のインストール・ディレクトリーを決定する (デフォルト・パスを受け入れない場合)。
__ IBM Installation Manager のインストール・ディレクトリーを決定する (デフォルト・パスを受け入れない場合)。
__ Operations Center Web サーバーが使用するポート番号を決定する (デフォルトのポート番号を受け入れない場合)。
__ セキュア通信のためのパスワードを決定する。

表 *24. Operations Center* をインストールする前に確認または決定する情報

通知	**詳細**
Operations Center がインストールされるコンピューターのホスト名。	ホスト名は、以下の基準を満たしていなければなりません。 • 2 バイト文字セット (DBCS) 文字および下線文字 (_) を含めてはなりません。 • ホスト名にはハイフン文字 (-) を含めることができますが、名前の最終文字としてハイフンを使用することはできません。
インストールの資格情報	Operations Center をインストールするには、以下のユーザー・アカウントを使用する必要があります。 • root ユーザー

Operations Center のインストール・ディレクトリー	Operations Center は、インストール・ディレクトリーの `ui` サブディレクトリーにインストールされます。
	以下のパスは、Operations Center のインストール・ディレクトリーのデフォルト・パスです。
	• `/opt/tivoli/tsm`
	例えば、このデフォルト・パスを使用すると、Operations Center は以下のディレクトリーにインストールされます。
	`/opt/tivoli/tsm/ui`
	インストール・ディレクトリーのパスは、以下の基準を満たしている必要があります。
	• パスに含める文字数は 128 文字以下でなければならない。
	• パスには、ASCII 文字のみを含める必要がある。
	• パスに、表示できない制御文字を含めることはできない。
	• パスには、次のいずれの文字も使用できない。
	`% | < > ' " $ & ; *`

IBM Installation Manager のインストール・ディレクトリー	以下のパスは、IBM Installation Manager のインストール・ディレクトリーのデフォルト・パスです。 • `/opt/IBM/InstallationManager`

表 *24. Operations Center* をインストールする前に確認または決定する情報 *(*続き*)*

通知	詳細
Operations Center Web サーバーが使用するポート番号。	セキュア (https) ポート番号の値は、以下の基準を満たしていなければなりません。 • 番号は、1024 から 65535 の範囲の整数でなければなりません。 • 番号は、既に使用中であったり、別のプログラムに割り振られていてはなりません。 ポート番号を指定しない場合、デフォルト値は 11090 になります。 **ヒント:** • 1024 から 65535 までの範囲の整数を指定する必要がありますが、標準の TCP/IP セキュア・ポート (ポート 443) を使用するように Operations Center を後から構成することができます。詳しくは、148 ページの『標準 TCP/IP セキュア・ポートを使用するための Operations Center Web サーバーの構成』を参照してください。 • 後に、指定したポート番号を覚えていない場合は、以下のファイルを参照してください。ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを表します。 – *installation_dir*/ui/Liberty/usr/servers/guiServer/bootstrap.properties bootstrap.properties ファイルには、IBM Spectrum Protect サーバーの接続情報が入っています。
セキュア通信のためのパスワード	Operations Center は、Hypertext Transfer Protocol Secure (HTTPS) を使用して Web ブラウザーと通信します。 Operations Center では、サーバーと Operations Center 間のセキュア通信が必要です。通信を保護するには、ハブ・サーバーの Transport Layer Security (TLS) 証明書を Operations Center のトラストストア・ファイルを追加する必要があります。 Operations Center のトラストストア・ファイルには、Operations Center が Web ブラウザーとの HTTPS 通信に使用する証明書が入っています。Operations Center のインストール時に、トラストストア・ファイルのパスワードを作成する必要があります。Operations Center とハブ・サーバーの間にセキュア通信をセットアップする場合、同じパスワードを使用して、ハブ・サーバーの証明書をトラストストア・ファイルに追加する必要があります。 トラストストア・ファイルのパスワードは、以下の基準を満たしていなければなりません。 • パスワードには、最小 6 文字、最大 64 文字を含める必要があります。 • パスワードには、少なくとも以下の文字を含める必要があります。 – 1 つの大文字 (A – Z) – 1 つの小文字 (a – z) – 1 つの数字 (0 – 9) – 以下に示す非英数字文字のうち 2 つ: `~ @ # $ % ^ & * _ - + = ` |` `( ) { } [ ] : ; < > , . ? /`

第 9 章 Operations Center のインストール

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

始める前に

IBM Spectrum Protect サーバーをインストール、構成、および開始するまでは、Operations Center を構成することはできません。そのため、Operations Center をインストールする前に、124 ページの『ハブ・サーバーおよびスポーク・サーバーの要件』に記載されたサーバー・バージョンの要件に従って、該当するサーバー・パッケージをインストールしてください。

Operations Center は、IBM Spectrum Protect サーバーとともにコンピューターにインストールするか、別のコンピューターにインストールすることができます。

Operations Center インストール・パッケージの入手

インストール・パッケージは、IBM ダウンロード・サイト (IBM パスポート・アドバンテージまたは IBM Fix Central など) から入手できます。

このタスクについて

IBM ダウンロード・サイトからパッケージを入手した後、インストール・ファイルを抽出する必要があります。

手順

以下の手順を実行して、Operations Center インストール・ファイルを抽出します。以下の手順では、*version_number* を、インストールしている Operations Center のバージョンに置き換えます。

a. 次のパッケージ・ファイルを、選択したディレクトリーにダウンロードします。

```
version_number.000
-IBM-SPOC-AIX.bin
```

b. このパッケージ・ファイルの実行権限を持っていることを確認します。

必要な場合、次のコマンドを発行してファイル許可を変更します。

```
chmod a+x version_number.000-IBM-SPOC-AIX.bin
```

c. 次のコマンドを発行してインストール・ファイルを解凍します。

```
./version_number.000-IBM-SPOC-AIX.bin
```

自己解凍型のパッケージ・ファイルが、このディレクトリーに抽出されます。

グラフィカル・ウィザードを使用した Operations Center のインストール

IBM Installation Manager のグラフィカル・ウィザードを使用して、Operations Center をインストールまたは更新することができます。

始める前に

以下の RPM ファイルがコンピューターにインストールされていない場合は、 インストールしてください。手順については、136 ページの『グラフィカル・ウィザード用の RPM ファイルのインストール』を参照してください。

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

手順

1. Operations Center インストール・パッケージ・ファイルが抽出されたディレクトリーから、以下のコマンドを発行します。

   ```
   ./install.sh
   ```

2. ウィザードの指示に従って、IBM Installation Manager および Operations Center のパッケージをインストールします。

   ご使用のロケールで UTF-8 エンコード方式が使用されている場合、以下のメッセージが表示される可能性があり、インストール・ウィザードが遅くなる可能性があります。

   フォント・セットを作成できません

   メッセージが表示された場合、以下のアクションのいずれかを実行してください。

   - UTF-8 エンコード方式を使用しないロケールに変更します。UTF-8 エンコード方式を使用しない言語オプションの値については、128 ページの『言語要件』 を参照してください。
   - コンソール・モードでコマンド・ラインを使用して、Operations Center をインストールします。
   - サイレント・モードで Operations Center をインストールします。

次のタスク

143 ページの『Operations Center の構成』を参照してください。

グラフィカル・ウィザード用の RPM ファイルのインストール

IBM Installation Manager のグラフィカル・ウィザードを使用して Operations Center をインストールできるようにするには、 事前に特定の RPM ファイルをインストールしておく必要があります。

このタスクについて

135 ページの『グラフィカル・ウィザードを使用した Operations Center のインストール』 にリストされている RPM ファイルがインストールされていない場合は、ファイルをダウンロードしてインストールする必要があります。

手順

1. /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。

2. Operations Center 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。
3. IBM AIX Toolbox for Linux Applications Web サイトから現行ディレクトリーに RPM ファイルを自動的にダウンロードするには、次のコマンドを発行します。

```
download-prerequisites.sh
```

4. ファイルが含まれるディレクトリーから以下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
```

メッセージが、ファイルの 1 つが既にシステムにインストール済みであることを示している場合は、以下のアクションのいずれかを実行します。

- 次のコマンドを出します。

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

- 次の例に示すように、以前のバージョンのファイルを別のディレクトリーに移動し、**rpm** コマンドを再発行します。

```
mkdir already-installed
mv gettext*.rpm already-installed
rpm -Uvh *.rpm
```

コンソール・モードでの Operations Center のインストール

コンソール・モードでコマンド・ラインを使用して、Operations Center をインストールまたは更新することができます。

手順

1. インストール・パッケージ・ファイルを抽出したディレクトリーから、以下のプログラムを実行します。

```
./install.sh -c
```

2. コンソールの指示に従って、Installation Manager および Operations Center のパッケージをインストールします。

次のタスク

143 ページの『Operations Center の構成』を参照してください。

サイレント・モードでの Operations Center のインストール

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

始める前に

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

install_response_sample.xml
Operations Center をインストールするには、このファイルを使用します。

update_response_sample.xml
Operations Center をアップグレードするには、このファイルを使用します。

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

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

手順

1. 応答ファイルを作成します。
   サンプル応答ファイルを変更するか、または独自のファイルを作成することができます。

   ヒント: コンソール・モード・インストールの一部として応答ファイルを生成するには、コンソール・モード・インストールのオプションの 選択を完了してください。次に、前に選択されたオプションに従って応答ファイルを生成するには、「**要約**」 パネルで「G」を入力します。
2. 応答ファイルの Operations Center トラストストアのパスワードを作成します。

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

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

   このパスワードについて詳しくは、131 ページの『インストール・チェックリスト』を参照してください。

   パスワードを暗号化するには、138 ページの『サイレント・インストール応答ファイルのパスワードの暗号化』の手順に従います。

   ヒント: Operations Center をアップグレードする 際に、`update_response_sample.xml` ファイルを使用する場合はトラストストアのパスワードは不要です。
3. インストール・パッケージが抽出されたディレクトリーから次のコマンドを発行して、サイレント・インストールを開始します。値 *response_file* は、応答ファイル・パスとファイル名を示します。

   - ```
     ./install.sh -s -input response_file -acceptLicense
     ```

次のタスク

143 ページの『Operations Center の構成』を参照してください。

サイレント・インストール応答ファイルのパスワードの暗号化

Operations Center のサイレント・インストール中のセキュリティーを強化するために、応答ファイルのパスワードを暗号化できます。 応答ファイルのデータ・キー・フィールドに指定できるのは (暗号化または非暗号化された) パスワード 1 つのみです。

始める前に

IBM Installation Manager を開きます。IBM Installation Manager がインストールされているディレクトリーで、`eclipse` サブディレクトリーに移動します。デフォルトでは、サブディレクトリーは次の場所にあります。

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

手順

Operations Center のサイレント・インストールに使用される応答ファイルのパスワードを暗号化し、データ・キー・フィールドで確実に 1 つだけのパスワードを使用するには、以下の手順を実行します。

1. root ユーザーとして Operations Center をインストールする場合、tools サブディレクトリーに移動します。tools サブディレクトリーはデフォルトで 以下の場所にあります。

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

非 root ユーザーとして Operations Center をインストールする場合、以下のサブディレクトリーに移動します。

/home/*non_root_user*/IBM/InstallationManager/eclipse/tools

ここで、*non_root_user* は、インスタンス・ユーザー ID です。

2. 以下のコマンドを 1 行で指定して発行します。

```
./IBMIM -silent -noSplash encryptString string_to_encrypt
>encrypted_pwd
```

ここで *string_to_encrypt* は暗号化された値であり、*encrypted_pwd* は暗号化された値を含むファイルです。

3. 暗号化パスワード・ファイルを開き、値を応答ファイルのデータ・キー・フィールドにコピーします。次に、暗号化パスワード・ファイルをコメント化して削除します。
4. データ・キー・フィールドから非暗号化パスワードを削除するには、以下のステップを実行します。
   a. 非暗号化パスワード (user.SSL_PASSWORD) をコメント化して、次の例のようなパスワード行にします。

```
<!-- <data key='user.SSL_PASSWORD' value='${ssl.password}'/> -->
```

   b. パスワード行が次の例のようになるように、暗号化パスワード (user.SSL_PASSWORD_ENCRYPTED) からコメント・タグを削除します。

```
<data key='user.enableSP800_131' value='${enable.SP800131a}'/>
 <data key='user.SSL_PASSWORD_ENCRYPTED' value='${ssl.password.encrypted}'/>
```

制約事項 : 応答ファイルのデータ・キー・フィールドには、user.SSL_PASSWORD パスワードまたは user.SSL_PASSWORD_ENCRYPTED パスワードのいずれかの値 1 つのみを使用します。使用しないパスワードはコメント化する必要があります。さもないとエラー・メッセージが表示され、インストールが失敗します。

例

Installation Manager コマンド・ライン・ツールを使用してパスワード passw0rd を暗号化します。暗号化された値を my_pwd.txt ファイルに保存します。次のコマンドを出します。

```
./IBMIM -silent -noSplash encryptString passw0rd > my_pwd.txt
```

ここで my_pwd.txt ファイルには、暗号化された値 *rbN1IaMAWYYtQxLf6KdNyA==* が含まれています。

```
<variable name='ssl.password.encrypted' value=' rbN1IaMAWYYtQxLf6KdNyA==' />
```

第 10 章 Operations Center のアップグレード

Operations Center のアップグレードは、グラフィック・ウィザード、コンソール・モードのコマンド・ライン、またはサイレント・モードのいずれの方式を使用しても行えます。

始める前に

Operations Center をアップグレードする前に、システム要件とインストール・チェックリストを確認します。Operations Center の新しいバージョンでは、要件と考慮事項が、現在使用しているバージョンよりも多くなっているか、異なっている可能性があります。

このタスクについて

Operations Center のアップグレードの手順は、Operations Center のインストールの手順と同じですが、以下の例外があります。

- IBM Installation Manager の「**インストール**」機能ではなく、「**更新**」機能を使用します。

  ヒント: IBM Installation Manager では、更新 は、インストール済みソフトウェア・パッケージに対する更新および修正を検出してインストールすることを意味します。 この意味では、更新 とアップグレードは同義です。
- Operations Center をサイレント・モードでアップグレードする 場合は、トラストストア・ファイルのパスワードを作成するステップをスキップすることができます。

第 11 章 Operations Center の概要

Operations Center を使用してストレージ環境を管理するには、その前に構成を行う必要があります。

このタスクについて

Operations Center をインストールした後で、次の基本的な構成手順を行います。

1. ハブ・サーバーを指定する。
2. いくつかのスポーク・サーバーを追加する。
3. オプションで、ハブ・サーバーとスポーク・サーバー上で E メール・アラートを構成する

143 ページの図 1 には、Operations Center の構成を示します。

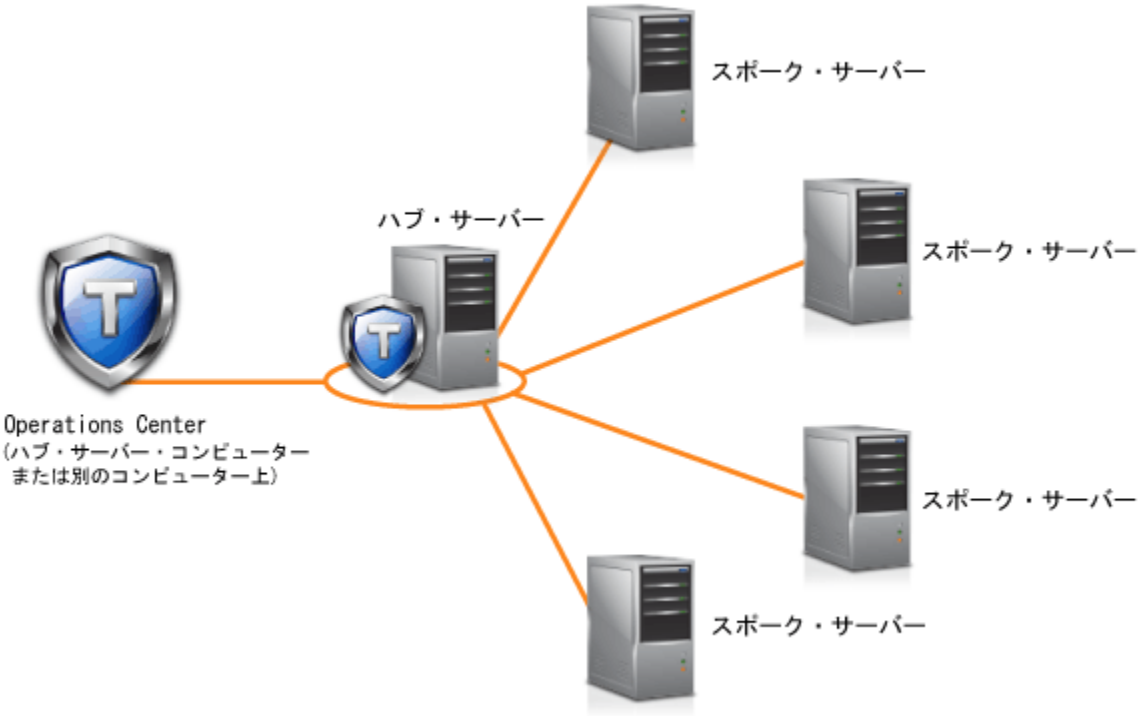


図 *1.* ハブ・サーバーとスポーク・サーバーを持つ *Operations Center* の構成の例

Operations Center の構成

初めて Operations Center を開いたときに、ストレージ環境を管理するように構成する必要があります。Operations Center を、ハブ・サーバーとして指定された IBM Spectrum Protect サーバーと関連付ける必要があります。その後で、追加の IBM Spectrum Protect サーバーをスポーク・サーバーとして接続できます。

ハブ・サーバーの指定

初めて Operations Center に接続するときに、どの IBM Spectrum Protect サーバーをハブ・サーバーにするかを指定する必要があります。

始める前に

Operations Center では、ハブ・サーバーと Operations Center 間のセキュア通信が必要です。通信を保護するには、ハブ・サーバーの Transport Layer Security (TLS) 証明書を Operations Center のトラストスト

ア・ファイルを追加する必要があります。詳しくは、150 ページの『自己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』を参照してください。

手順

Web ブラウザーで、次のアドレスを入力します。ここで、*hostname* は、Operations Center がインストールされているコンピューターの名前を表し、*secure_port* は、そのコンピューター上で Operations Center が HTTPS 通信用に使用するポート番号を表します。

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

ヒント:

- URL では大文字と小文字が区別されます。例えば、示されているように、「oc」を小文字で入力してください。
- ポート番号について詳しくは、インストール・チェックリストを参照してください。
- 初めて Operations Center に接続している場合は、以下の情報を提供する必要があります。
  - ハブ・サーバーとして指定するサーバーの接続情報
  - そのサーバーに定義される管理者 ID のログイン資格情報
- サーバーのイベント・レコードの保存期間が 14 日より少ない場合、そのサーバーをハブ・サーバーとして構成すると、期間が自動的に 14 日にリセットされます。

次のタスク

ご使用環境に複数の IBM Spectrum Protect サーバーがある場合は、他のサーバーをスポーク・サーバーとしてハブ・サーバーに追加します。

重要: ハブ・サーバーまたはスポーク・サーバーとして構成した後は、サーバーの名前を変更しないでください。

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。

メール・アラートの管理者への送信

アラートは、IBM Spectrum Protect サーバーに関連する問題の通知であり、サーバー・メッセージによって起動されます。アラートは、Operations Center に表示でき、サーバーから管理者に E メールで送信することができます。

始める前に

アラートに関する管理者への E メール通知を構成する前に、以下の要件を満たしていることを確認してください。

- E メールでアラートを送受信するには、SMTP サーバーが必要です。また、E メールでアラートを送信するサーバーは、SMTP サーバーへのアクセス権限が必要です。

  ヒント: Operations Center が別のコンピューターにインストールされている場合、そのコンピューターは SMTP サーバーへのアクセス権限は必要ありません。
- 管理者は、E メール通知を構成するためのシステム特権を持っていなければなりません。

このタスクについて

E メール通知は、アラートの最初の発生時のみ送信されます。また、E メール通知を構成する前にアラートが生成された場合、そのアラートの E メール通知は送信されません。

以下の方法で、E メール通知を構成できます。

- 個々のアラートの通知の送信
- アラート要約の送信

アラート要約には、現在のアラートに関する情報が含まれます。要約には、アラートの合計数、アクティブおよび非アクティブ・アラートの合計数、最も古いアラート、最も新しいアラート、および最も頻繁に発生しているアラートが含まれています。

E メールによるアラート要約を受信する最大 3 人の管理者を指定できます。アラート要約は、ほぼ毎時に送信されます。

手順

アラートに関する管理者への E メール通知を構成するには、E メール通知の発信元の各ハブ・サーバーおよびスポーク・サーバーに対して、以下の手順を実行します。

1. アラート・モニターがオンになっていることを確認するために、次のコマンドを発行します。

   ```
   QUERY MONITORSETTINGS
   ```

2. コマンド出力で、アラート・モニターがオフであることが示された場合は、次のコマンドを発行します。そうでなり場合は、次の手順に進みます。

   ```
   SET ALERTMONITOR ON
   ```

3. E メール通知の送信を有効にするために、次のコマンドを発行します。

   ```
   SET ALERTEMAIL ON
   ```

4. E メール通知の送信に使用する SMTP サーバーを定義するために、次のコマンドを発行します。

   ```
   SET ALERTEMAILSMTPHOST host_name
   ```

5. SMTP サーバーのポート番号を指定するために、次のコマンドを発行します。

   ```
   SET ALERTEMAILSMTPPORT port_number
   ```

デフォルトのポート番号は 25 です。

6. アラートの送信者の E メール・アドレスを指定するために、次のコマンドを発行します。

```
SET ALERTEMAILFROMADDR email_address
```

7. E メール通知を受信する必要がある管理者 ID ごとに、E メール通知をアクティブにして、E メール・アドレスを指定するために、次のコマンドのいずれかを発行します。

```
REGISTER ADMIN admin_name ALERT=YES EMAILADDRESS=email_address
```

```
UPDATE ADMIN admin_name ALERT=YES EMAILADDRESS=email_address
```

8. 以下のオプションの一方または両方を選択して、E メール通知を受信する管理者 ID を指定します。
   - 個々のアラートの通知の送信

     個々のアラートの E メール通知を受信する管理者 ID を指定または更新するには、次のコマンドのいずれかを発行します。

     ```
     DEFINE ALERTTRIGGER message_number
     ADmin=admin_name1,admin_name2
     ```

     ```
     UPDATE ALERTTRIGGER message_number
     ADDadmin=admin_name3 DELadmin=admin_name1
     ```

     ヒント: Operations Center の「**アラートの構成**」ページで、E メール通知を受け取る管理者を選択することができます。
   - アラート要約の送信

     E メールでアラート要約を受信する管理者 ID を指定または更新するには、次のコマンドを発行します。

     ```
     SET ALERTSUMMARYTOADMINS admin_name1,
     admin_name2,admin_name3
     ```

   アラート要約は受信するが、個々のアラートに関する通知は受信しない場合は、以下の手順を実行します。

   a. 147 ページの『メール・アラートの一時的な中断』の説明に従って、個々のアラートに関する通知を一時停止します。
   b. 個別の管理者 ID が次のコマンドにリストされていることを確認します。

      ```
      SET ALERTSUMMARYTOADMINS admin_name1,
      admin_name2,admin_name3
      ```

E メール・アラートの複数の管理者への送信

以下の例は、管理者 myadmin、djadmin、および csadmin にメッセージ ANR1075E に関するアラートが E メールで送信される原因となるコマンドを示しています。

```
SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
UPDATE ADMIN djadmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djadmin,csadmin
```

メール・アラートの一時的な中断

特定の状況では、E メール・アラートを一時的に中断したい場合があります。例えば、アラート要約は受け取りたいが、個々のアラートに関する通知は中断したい場合、あるいは管理者が休暇を取っているときは E メール・アラートを中断したい場合があります。

始める前に

145 ページの『メール・アラートの管理者への送信』の説明に従って、管理者への E メール通知を構成します。

手順

個々のアラートまたはアラート要約の E メール通知を中断します。

- 個々のアラートに関する通知の中断

  次のいずれかの方法を使用します。

  UPDATE ADMIN コマンド
  管理者への E メール通知をオフにするには、次のコマンドを発行します。

  ```
  UPDATE ADMIN admin_name ALERT=NO
  ```

  後に再び E メール通知をオンにするには、次のコマンドを発行します。

  ```
  UPDATE ADMIN admin_name ALERT=YES
  ```

  UPDATE ALERTTRIGGER コマンド
  特定のアラートが管理者に送信されないようにするには、次のコマンドを発行します。

  ```
  UPDATE ALERTTRIGGER message_number DELADMIN=admin_name
  ```

  管理者へのそのアラートの送信を再び開始するには、以下のコマンドを出します。

  ```
  UPDATE ALERTTRIGGER message_number ADDADMIN=admin_name
  ```

- アラート要約に関する通知の中断

  アラート要約が管理者に送信されないようにするには、次のコマンドのリストからその管理者 ID を除去します。

  ```
  SET ALERTSUMMARYTOADMINS admin_name1,admin_name2,admin_name3
  ```

  管理者 ID が上記のコマンドにリストされている場合、個別の管理者 ID への個々のアラートに関する通知が中断されても、その管理者は E メールによるアラート要約を受け取ります。

ログイン画面へのカスタマイズ・テキストの追加

組織のソフトウェアの利用条件などのカスタマイズ・テキストを Operations Center のログイン画面に追加して、Operations Center のユーザーがユーザー名とパスワードを入力する前にそれらのテキストを確認できるようにすることができます。

手順

ログイン画面にカスタマイズ・テキストを追加するには、以下のステップを実行します。

1. Operations Center がインストールされているコンピューター上で、次のディレクトリーに移動します。ここで、*installation_dir* は Operations Center がインストールされているディレクトリーを表します。

   installation_dir/ui/Liberty/usr/servers/guiServer

2. ディレクトリー内で、ログイン画面に追加するテキストが入った loginText.html というファイルを作成します。

   特殊な非 ASCII テキストは、UTF-8 でエンコードされている必要があります。

3. Operations Center のログイン画面で、追加したテキストを確認します。

   Operations Center を開くには、Web ブラウザーで次のアドレスを入力します。ここで、*hostname* は、Operations Center がインストールされているコンピューターの名前を表し、*secure_port* は、そのコンピューター上で Operations Center が HTTPS 通信用に使用するポート番号を表します。

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

標準 TCP/IP セキュア・ポートを使用するための Operations Center Web サーバーの構成

ポート 443 は、セキュアな Web ブラウザー通信のための標準ポートです。ユーザーがファイアウォール経由で Operations Center にアクセスする必要がある場合、この標準ポートを介して通信するように Operations Center を構成することができます。こうすると、ファイアウォールの別のポートを開かずにすみます。

このタスクについて

Operations Center をインストールする際に、Operations Center Web サーバーと Web ブラウザー間のセキュア通信のためのデフォルト・ポート番号は 11090 です。インストール時にデフォルト・ポートをそのまま使用することも、別のポート番号を範囲 1024 から 65535 の間で指定することも可能です。 1024 未満のポート番号は、特定のネットワーク・サービス用に予約されているためにインストール時に指定できません。

Operations Center のインストール後、Web サーバーは Web ブラウザーからの要求をその指定ポートで listen します。ポートがファイアウォールによってブロックされているために Operations Center を開けない場合、管理者はブラウザーが接続できるようにそのポートを開く必要があります。一部の実稼働環境では、システム・ポート 443 を使用することが効率的な場合があります。このシステム・ポートは安全に Web を参照するために予約されているため、ファイアウォールで既に開いている可能性があります。ポート 443 はインストール時に指定できませんが、インストール後に指定できます。

手順

ポート 443 を使用するように Operations Center Web サーバーを構成するには、Operations Center のインストール後に以下のステップを実行します。

1. Operations Center Web サーバーを停止します。

   Web サーバーの停止に関する説明は、168 ページの『Web サーバーの開始と停止』を参照してください。

2. 以下のディレクトリーに移動します。ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを表します。

   installation_dir/ui/Liberty/usr/servers/guiServer

3. bootstrap.properties ファイルを開きます。このファイルには、Operations Center Web サーバーがセキュア通信に使用するポート番号を指定するプロパティーが含まれています。

4. ポート 443 を指定するように tsm.https.port プロパティーを更新します。

   ```
   tsm.https.port=443
   ```

5. bootstrap.properties ファイルを保存して閉じます。

6. Operations Center Web サーバーを開始します。

   root ユーザーとして Operations Center を開始する必要があります。root ユーザーとして Operations Center を開始しないと、Operations Center は ポート 443 を介して通信できません。

Operations Center Web サーバーの始動に関する説明は、168 ページの『Web サーバーの開始と停止』を参照してください。

次のタスク

Operations Center では標準の TCP/IP セキュア・ポートを使用していることをユーザーに通知します。通常、ユーザーは URL にポート番号を指定して、各自のブラウザーで Operations Center を開きます。ポート 443 は、セキュア Web ブラウザー通信のためのデフォルト設定なので、ユーザーが URL にポート番号を指定する必要はありません。代わりに、以下の URL を使用できます。ここで *hostname* は、Operations Center がインストールされているコンピューターの名前を指定します。

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

Operations Center の開き方については、169 ページの『Operations Center の開始』を参照してください。

REST サービスの有効化

Representational State Transfer (REST) を使用するアプリケーションは、Operations Center に接続することで、ストレージ環境を照会および管理することができます。

このタスクについて

この機能を有効にすると、REST サービスは、以下のアドレスに呼び出しを送信することで、ハブ・サーバーおよびスポーク・サーバーと対話できるようになります。

```
https://oc_host_name:port/oc/api
```

ここで、*oc_host_name* は Operations Center ホスト・システムのネットワーク名または IP アドレス、*port* は Operations Center のポート番号です。 デフォルトのポート番号は 11090 です。

Operations Center で使用可能な REST サービスについては、技術情報 http://www-01.ibm.com/support/docview.wss?uid=swg21997347 を参照するか、以下の REST 呼び出しを発行します。

```
https://oc_host_name:port/oc/api/help
```

手順

1. Operations Center メニュー・バーで、設定アイコン  上にカーソルを移動し、「**設定**」をクリックします。
2. 「一般」ページで、「**管理 REST API の使用可能化**」チェック・ボックスを選択します。
3. 「**保存**」をクリックします。

セキュア通信の構成

Operations Center は、Hypertext Transfer Protocol Secure (HTTPS) を使用して Web ブラウザーと通信します。Transport Layer Security (TLS) により、Operations Center とハブ・サーバー間および、ハブ・サーバーと関連のスポーク・サーバー間の 通信を保護します。

このタスクについて

IBM Spectrum Protect サーバーと Operations Center 間、および ハブ・サーバーとスポーク・サーバー間のセキュア通信のために TLS バージョン 1.2 以降が必要です。

自己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

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

始める前に

Operations Center のトラストストア・ファイルは、Operations Center がアクセスできる証明書用のコンテナーです。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) により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を参照してください。

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オペレーティング・システムのコマンド・ラインに進みます。
3. **iKeycmd** ユーティリティーまたは **iKeyman** ユーティリティーを 使用して、Operations Center のトラストストア・ファイルに証明書を追加します。

   iKeycmd ユーティリティーは、コマンド・ライン・インターフェースであり 、**iKeyman** ユーティリティーは IBM Key Management グラフィカル・ユーザー・インターフェースを 開きます。

   iKeycmd ユーティリティーと **iKeyman** ユーティリティーは root ユーザーとして実行する必要があります。

   コマンド・ライン・インターフェースを 使用して、TLS 証明書を追加するには、以下の手順を実行します。

   a) 以下のディレクトリーに移動します。ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを表します。

   - *installation_dir*/ui/jre/bin

   b) **iKeycmd** コマンドを発行し、サーバーの cert256.arm 証明書を Operations Center トラストストアに追加します。

```
ikeycmd -cert -add
-db /installation_dir/ui/Liberty/usr/servers/guiServer/gui-truststore.jks
-file /server_instance_dir/cert256.arm
```

```
-label 'label_description'
-pw 'password' -type jks -format ascii -trust enable
```

ここで、

installation_dir
Operations Center がインストールされるディレクトリー。

server_instance_dir
IBM Spectrum Protect サーバー・インスタンス・ディレクトリー。

ラベルの説明
ラベルに割り当てる説明。

パスワード
Operations Center のインストール時に作成したパスワード。パスワードをリセットするには、Operations Center をアンインストールし、`.jks` ファイルを削除してから Operations Center を再インストールします。

「**IBM 鍵管理**」ウィンドウを使用して証明書を追加するには、以下の手順を実行します。

a) 以下のディレクトリーに移動します。ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを表します。

- *installation_dir*/ui/jre/bin

b) 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
```

c)「**鍵データベース・ファイル**」 > 「**オープン**」をクリックします。

d)「**オープン**」ウィンドウで、「**参照**」をクリックして、以下のディレクトリーに移動します。ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを 表します。

- *installation_dir*/ui/Liberty/usr/servers/guiServer

e) guiServer ディレクトリーで、gui-truststore.jks ファイルを選択します。

f)「**オープン**」をクリックして、「**OK**」をクリックします。

g) トラストストア・ファイルのパスワードを入力して、「**OK**」をクリックします。

h)「**IBM 鍵管理**」ウィンドウの「**鍵データベースの内容 (Key database content)**」域で、矢印をクリックして、リストから「**署名者証明書**」を選択します。

i)「**追加**」をクリックします。

j)「**オープン**」ウィンドウで、「**参照**」をクリックして、ハブ・サーバー・インスタンス・ディレクトリーに進みます。このディレクトリーには、cert256.arm 証明書が含まれています。

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

i) 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・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。

- *installation_dir*/ui/Liberty/usr/servers/guiServer

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

k) cert256.arm 証明書を選択します。

ヒント : 選択した証明書を、ハブ・サーバーの鍵データベース・ファイル内のデフォルト証明書として設定する必要があります。

l)「**オープン**」をクリックして、「**OK**」をクリックします。

m) 証明書のラベルを入力します。
例えば、ハブ・サーバーの名前を入力します。

n)「**OK**」をクリックします。

ハブ・サーバーの SSL 証明書がトラストストア・ファイルに追加され、そのラベルが「**IBM 鍵管理**」ウィンドウの「**鍵データベースの内容 (Key database content)**」域に表示されます。

o)「**IBM 鍵管理**」ウィンドウを閉じます。

4. Operations Center Web サーバーを始動します。
5. Operations Center への初回接続時に、ハブ・サーバーの IP アドレスまたはネットワーク名、およびハブ・サーバーと通信するためのポート番号を特定するようにプロンプトが出されます。TCPADMINPORT または SSLTCPADMINPORT のどちらかのサーバー・オプションで指定されたポート番号を入力します。

   Operations Center が以前に構成されていた場合は、`serverConnection.properties` ファイルの内容を表示して、接続情報を確認することができます。`serverConnection.properties` ファイルは、Operations Center がインストールされているコンピューターの以下のディレクトリーにあります。

   - *installation_dir*`/ui/Liberty/usr/servers/guiServer`

次のタスク

ハブ・サーバーとスポーク・サーバー間の TLS 通信のセットアップについては、153 ページの『ハブ・サーバーとスポーク・サーバー間の通信の保護』を参照してください。

関連タスク

166 ページの『Operations Center のトラストストア・ファイルのパスワードの削除と再割り当て』
Operations Center とハブ・サーバー間のセキュア通信をセットアップするには、Operations Center のトラストストア・ファイルのパスワードを知っている必要があります。このパスワードは、Operations Center のインストール時に作成します。パスワードが不明な場合は、パスワードを削除して新規パスワードを割り当てることができます。

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

CA 署名証明書を使用してハブ・サーバーを保護する場合、認証局 (CA) から送信される、ハブ・サーバーで使用するためのルート証明書および中間 CA 証明書のファイルを Operations Center のトラストストア・ファイルに追加する必要があります。

始める前に

以下の前提条件が満たされていることを確認します。

- 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。パスワードを覚えていない場合は、ここでトラストストア・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、166 ページの『Operations Center のトラストストア・ファイルのパスワードの削除と再割り当て』を参照してください。
- サーバーへの接続に必要な CA 署名証明書を認証局から受け取り、サーバーにインストールしておきます。SSL 接続を受け入れるためのサーバーの構成を参照してください。

以下の構成は、Operations Center とハブ・サーバーの間に Secure Sockets Layer (SSL) をセットアップするためのコンポーネントを示します。

このタスクについて

ハブ・サーバーから Operations Center に、各 IBM Spectrum Protect サーバーのルート証明書および CA 証明書をインポートするには、以下の手順を実行します。

ヒント: 自己署名証明書 (デフォルトでインストールされています) を使用する場合は、150 ページの『自己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』を参照してください。

手順

1. Operations Center がインストールされているオペレーティング・システムのコマンド・ラインにナビゲートします。
2. コマンド・ラインで、鍵ストアのロケーションのディレクトリーに移動します。
   installation_dir/ui/Liberty/usr/servers/guiServer
   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. ルート CA 証明書および中間 CA 証明書のファイルをこのロケーションにコピーします。
   ヒント: この証明書ファイルは、以前にハブ・サーバーのロケーションにコピーされています。
4. 168 ページの『Web サーバーの開始と停止』の説明に従って、Operations Center Web サーバーを停止します。
5. 元のバージョンに戻す必要がある場合に備えて Operations Center トラストストア・ファイルのバックアップ・コピーを作成します。Operations Center トラストストア・ファイルは、gui-truststore.jks という名前です。
6. CA 署名証明書を受信する手順を実行するには、以下のいずれかのコマンドを使用します。
   - **ikeyman** コマンド: 159 ページの『IBM 鍵管理を使用した署名付き証明書の受信』を参照して、署名証明書を受け取る手順に進んでください。
   - **ikeycmd** コマンド: 165 ページの『ikeycmd を使用した署名付き証明書の受信』を参照して、署名証明書を受け取る手順に進んでください。
7. Operations Center Web サーバーを開始します。

次のタスク

ハブ・サーバーとスポーク・サーバー間の TLS 通信のセットアップについては、153 ページの『ハブ・サーバーとスポーク・サーバー間の通信の保護』の指示に従ってください。

関連タスク

159 ページの『署名付き証明書の受信』
CA は、トラストストア・ファイルに追加する証明書ファイルを送信する必要があります。

ハブ・サーバーとスポーク・サーバー間の通信の保護

Transport Layer Security (TLS) プロトコルを使用してハブ・サーバーとスポーク・サーバーの間の通信を保護するには、ハブ・サーバーに対してスポーク・サーバーの証明書、そしてスポーク・サーバーに対してハブ・サーバーの証明書を定義する必要があります。 また、スポーク・サーバーをモニターするように Operations Center を構成することも必要です。

このタスクについて

ハブ・サーバーは、スポーク・サーバーから状況およびアラートの情報を受信して、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。

Operations Center と Web ブラウザー間の SSL 通信の構成

Operations Center のインストール時、自己署名デジタル証明書が生成され、Web ブラウザー・セッションに使用されます。 オプションで、自己署名証明書ではなくサード・パーティーの認証局によって署名された証明書を使用できます。

このタスクについて

Operations Center は、Web ブラウザーと通信するために常に HTTPS プロトコルを使用します。ご使用のブラウザーと Operations Center との間のすべての通信は、TLS プロトコルのバージョン 1.2 以降を使用して暗号化されます。

デフォルトでは、ブラウザーと Operations Center の間でセキュア接続を形成するために、自己署名証明書が使用されます。 証明書が自己署名証明書であるため、Web ブラウザーではサーバーの ID を検証できず、警告が表示されます。自己署名証明書は、イントラネット Web サイトでよく使用されます。そこでは接続の傍受やサーバーに偽装による危険が重大な脅威とは見なされないことがあります。ブラウザーのセキュリティー警告をバイパスして自己署名証明書を使用することも、自己署名証明書を信頼できる認証局 (CA) の証明書と置き換えることも可能です。

自己署名証明書を使用する場合、これ以上の構成は不要です。

CA によって署名された証明書を使用するには、複数のステップを実行する必要があります。

手順

1. 証明書署名要求を作成します。
2. 署名を得るために証明書署名要求を認証局に送信します。
3. Operations Center のトラストストア・ファイルに証明書を追加します。

証明書署名要求の作成

サード・パーティーによって署名された証明書を取得するには、証明書署名要求 (CSR) を作成して CA に送信する必要があります。

始める前に

Operations Center のトラストストア・ファイルは、Operations Center がアクセスできる SSL/TLS 証明書用のコンテナーです。トラストストア・ファイルには、Operations Center が Web ブラウザーとの HTTPS 通信に使用する証明書が入っています。

Operations Center のインストール時に、トラストストア・ファイルのパスワードを作成します。トラストストア・ファイルを処理するには、トラストストアのパスワードを知っておく必要があります。パスワードを覚えていない場合は、166 ページの『Operations Center のトラストストア・ファイルのパスワードの削除と再割り当て』の手順に従ってください。

手順

CSR を作成するには、以下の手順を実行します。

1. コマンド・ラインで、鍵ストアのロケーションのディレクトリーに移動します。
   installation_dir/ui/Liberty/usr/servers/guiServer

2. **ikeyman** コマンドまたは **ikeycmd** コマンドを使用して認証要求 (証明書要求) を作成します。**ikeyman** コマンドは IBM 鍵管理のグラフィカル・ユーザー・インターフェースを 開き、**ikeycmd** はコマンド・ライン・インターフェースを 開きます。

   ヒント : ikeyman コマンドや **ikeycmd** コマンドには絶対パスを指定することが必要な場合があります。コマンドはディレクトリーにあります。ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを表します。

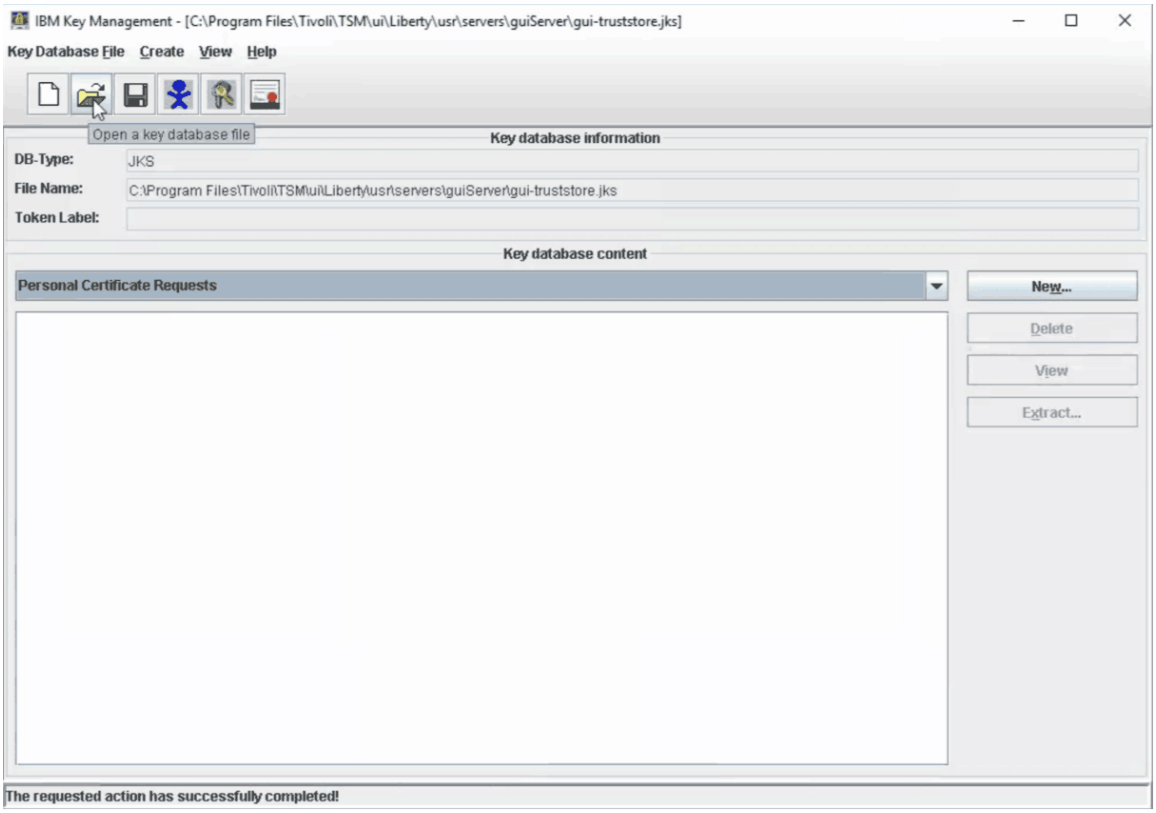
   installation_dir/ui/jre/bin

   - **ikeyman** グラフィカル・ユーザー・インターフェースを 使用して認証要求 (証明書要求) を作成するには、以下のステップを実行します。

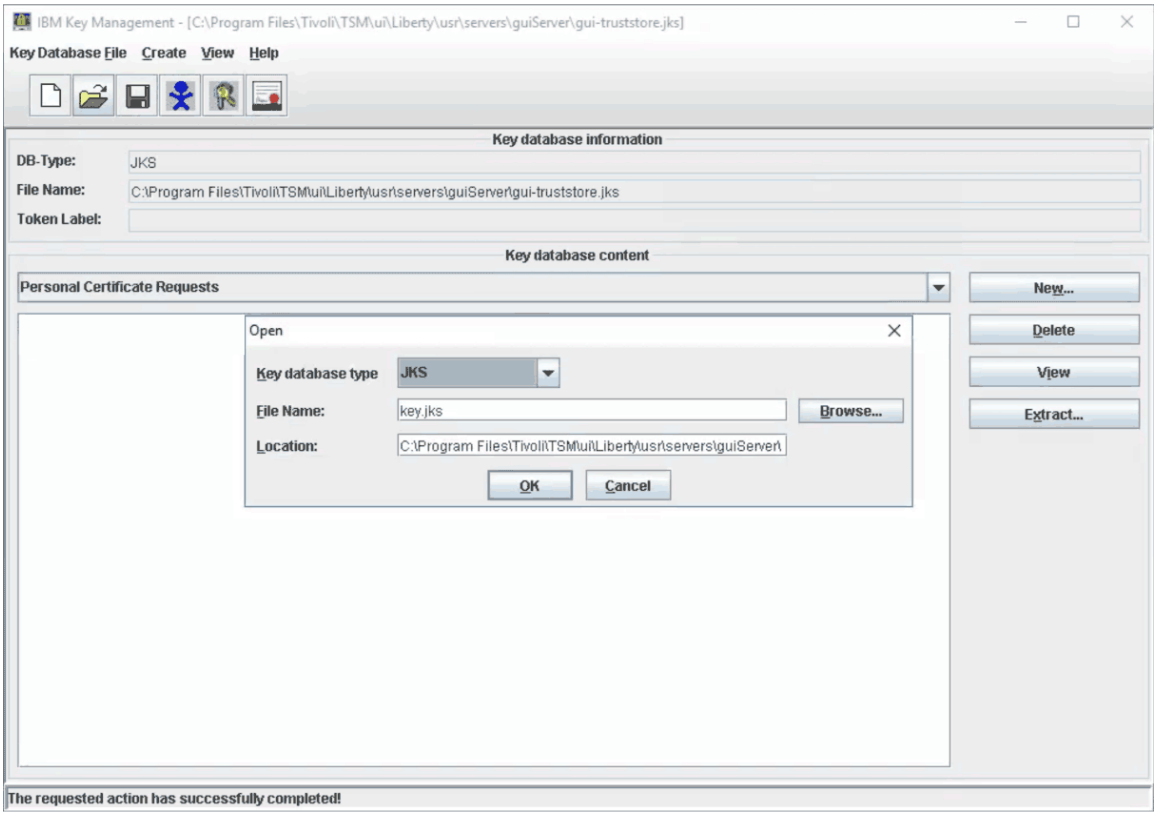
     a. 次のコマンドを発行して、「IBM 鍵管理」ツールを開きます。

     ```
     ikeyman
     ```

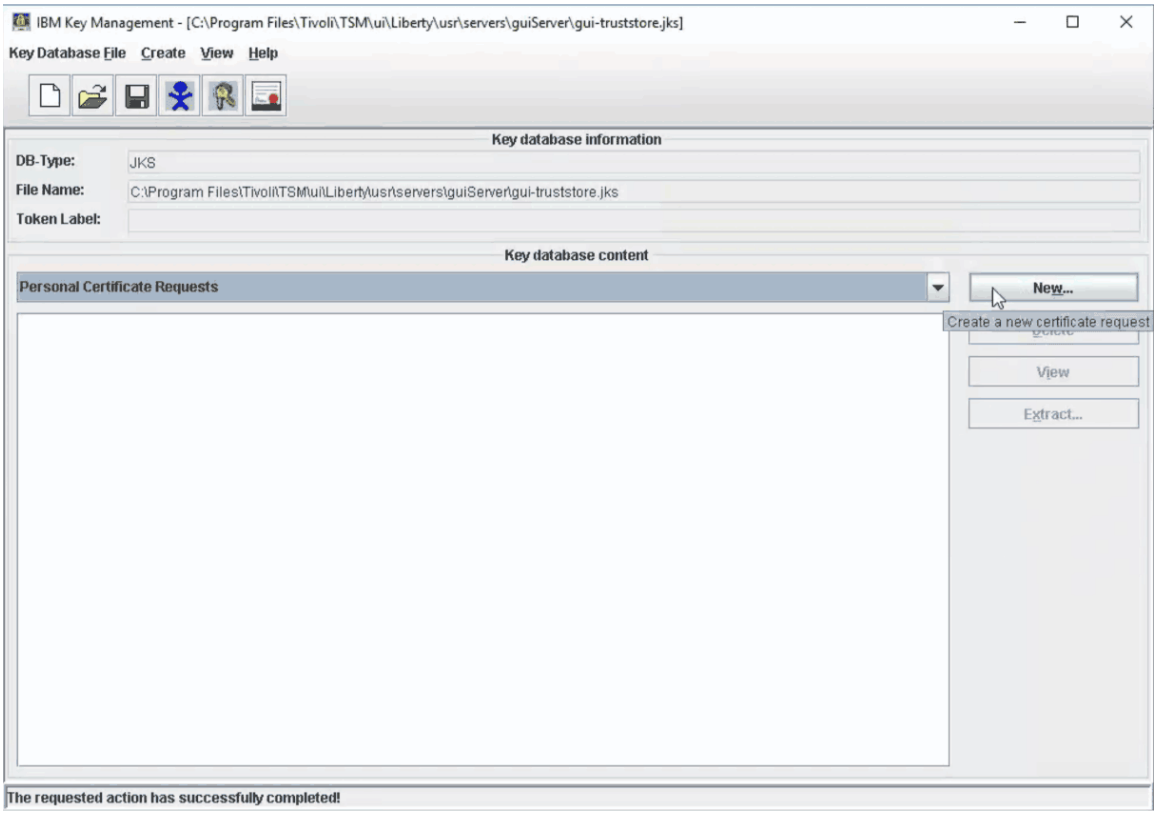
     b.「**鍵データベース・ファイル**」 > 「**オープン**」をクリックします。

     「**開く**」ウィンドウで「**参照**」をクリックしてディレクトリーを開き、`gui-truststore.jks` ファイルを選択します。「**OK**」をクリックします。



c. 証明書要求を作成します。「**鍵データベースの内容**」エリアで、「**新規**」をクリックします。



d.「鍵および認証要求の新規作成」ダイアログ・ボックスで、CA および組織の必要に応じてフィールドに入力します。以下の情報を指定します。

鍵ラベル
トラストストア・ファイルの証明書に固有のラベルを指定します。ラベル名 (*usr-cert-name* など) はトラストストアの証明書を特定します。

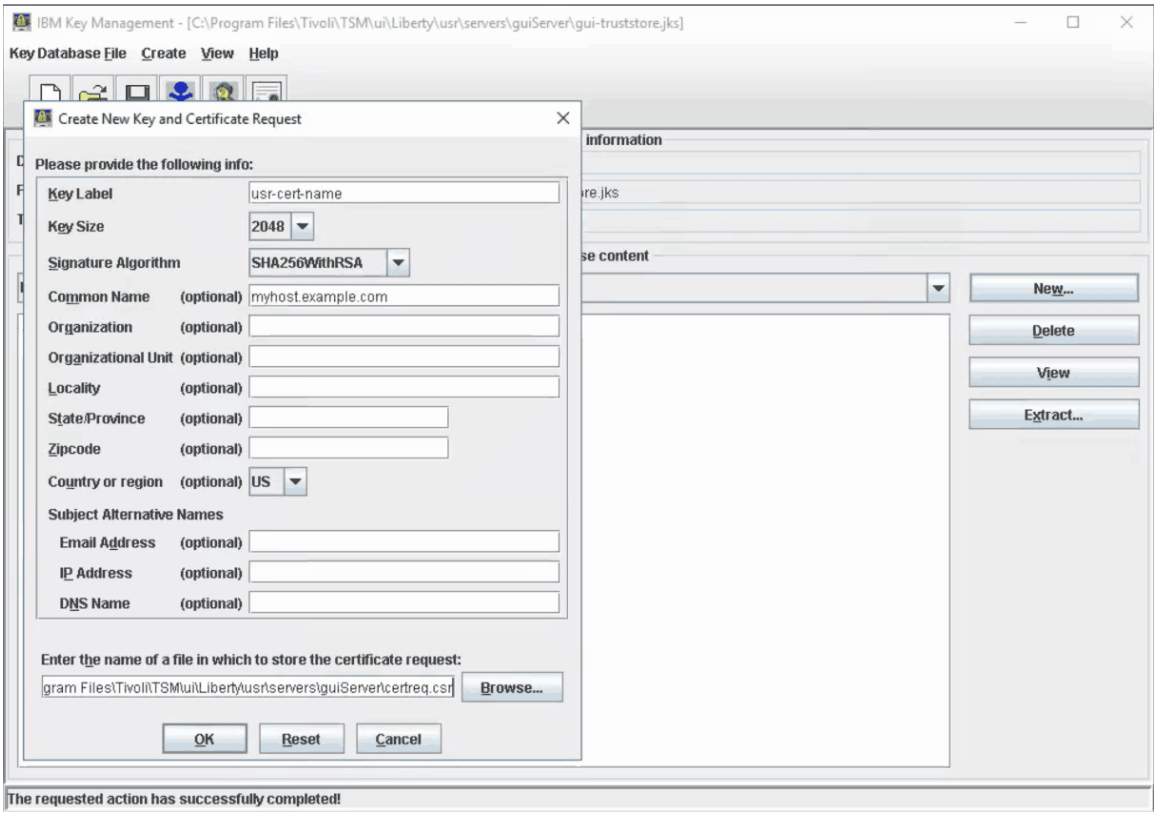
鍵サイズ
2048 ビット以上の鍵サイズを選択してください。

署名アルゴリズム
「**SHA256WithRSA**」を選択します。

共通名
Operations Center がインストールされているネットワーク上のシステムの完全修飾ドメイン名 (FQDN) を指定します。

要確認 : ネットワーク上のシステムの FQDN は、システムの Operations Center の URL で使用されます。URL は Web ブラウザーで Operations Center にアクセスするために使用されます。

認証要求を保管するファイルの名前を入力
`guiServer` ディレクトリーの `certreq.csr` という名前のファイルを指定します。



e.「**開く**」ウィンドウを閉じます。

- **ikeycmd** コマンドを使用して認証要求を作成するには、以下のコマンドを発行します。

```
ikeycmd -certreq -create -db gui-truststore.jks -size 2048
-sig_alg SHA256WithRSA -dn "CN=myhost.example.com" -file certreq.csr -label usr-cert-name
-san_dnsname myhost.example.com,myhost
-san_ipaddr 192.0.2.1,192.0.2.2
```

ここで、

-dn "CN=*myhost.example.com*"
識別名を指定します。指定 CN=*myhost.example.com* を含む引用符付きストリングとして入力します。ここで *myhost.example.com* は、Operations Center がインストールされている、ネットワーク上のシステムの FQDN を指定します。

要確認 : ネットワーク上のシステムの FQDN は、システムの Operations Center の URL で使用されます。URL は Web ブラウザーで Operations Center にアクセスするために使用されます。

-label *usr-cert-name*
トラストストア・ファイルの証明書に固有のラベル *usr-cert-name* を指定します。

-san_dnsname *myhost.example.com,myhost* (オプション)
Operations Center がインストールされているシステムのドメイン・ネーム・サーバー (DNS) 名を指定します。CN と dnsname は通常同じ値です。

-san_ipaddr *192.0.2.1,192.0.2.2* (オプション)
Operations Center がインストールされているシステムの IP アドレスを指定します。

認証局への証明書署名要求の送信

認証要求ファイル (certreq.csr) の作成後、それを署名のために CA に送信する必要があります。CA の手順に従います。

署名付き証明書の受信

CA は、トラストストア・ファイルに追加する証明書ファイルを送信する必要があります。

手順

署名付き証明書を受信するには、以下の手順を実行します。

1. コマンド・ラインで、鍵ストアのロケーションのディレクトリーに移動します。
   installation_dir/ui/Liberty/usr/servers/guiServer
2. CA から受信したファイルを、このロケーションにコピーします。これらのファイルには、Operations Center の CA ルート証明書、中間 CA 証明書 (ある場合)、および署名付き証明書が含まれています。
3. 168 ページの『Web サーバーの開始と停止』の説明に従って、Operations Center Web サーバーを停止します。
4. 元のトラストストアに戻す必要がある場合に備えて Operations Center トラストストアのバックアップ・コピーを作成します。Operations Center トラストストアは、gui-truststore.jks という名前です。
5. 署名付き証明書を受信する手順を実行するには、以下のいずれかのコマンドを使用します。
   - **ikeyman** コマンド: 159 ページの『IBM 鍵管理を使用した署名付き証明書の受信』 の手順を実行します。
   - **ikeycmd** コマンド: 165 ページの『ikeycmd を使用した署名付き証明書の受信』 の手順を実行します。

IBM 鍵管理を使用した署名付き証明書の受信

グラフィカル・ユーザー・インターフェースの IBM 鍵管理ツールを使用して、証明書鍵を管理し、署名付き証明書を受け取ることができます。

手順

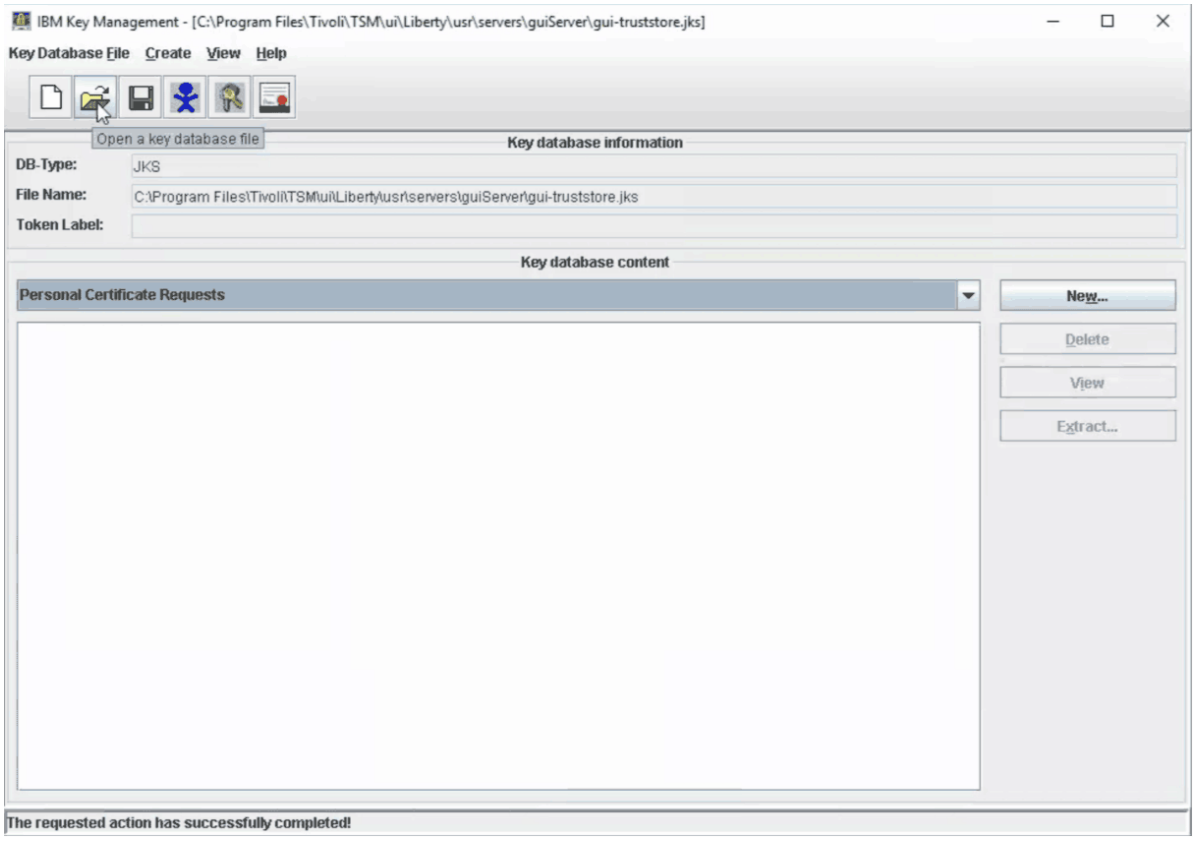
1. **ikeyman** コマンドを使用して個人署名証明書が適切なディレクトリー内にあることを確認します。次の手順を実行してください。
   a) 次のコマンドを発行して、「IBM 鍵管理」ツールを開きます。

   ```
   ikeyman
   ```

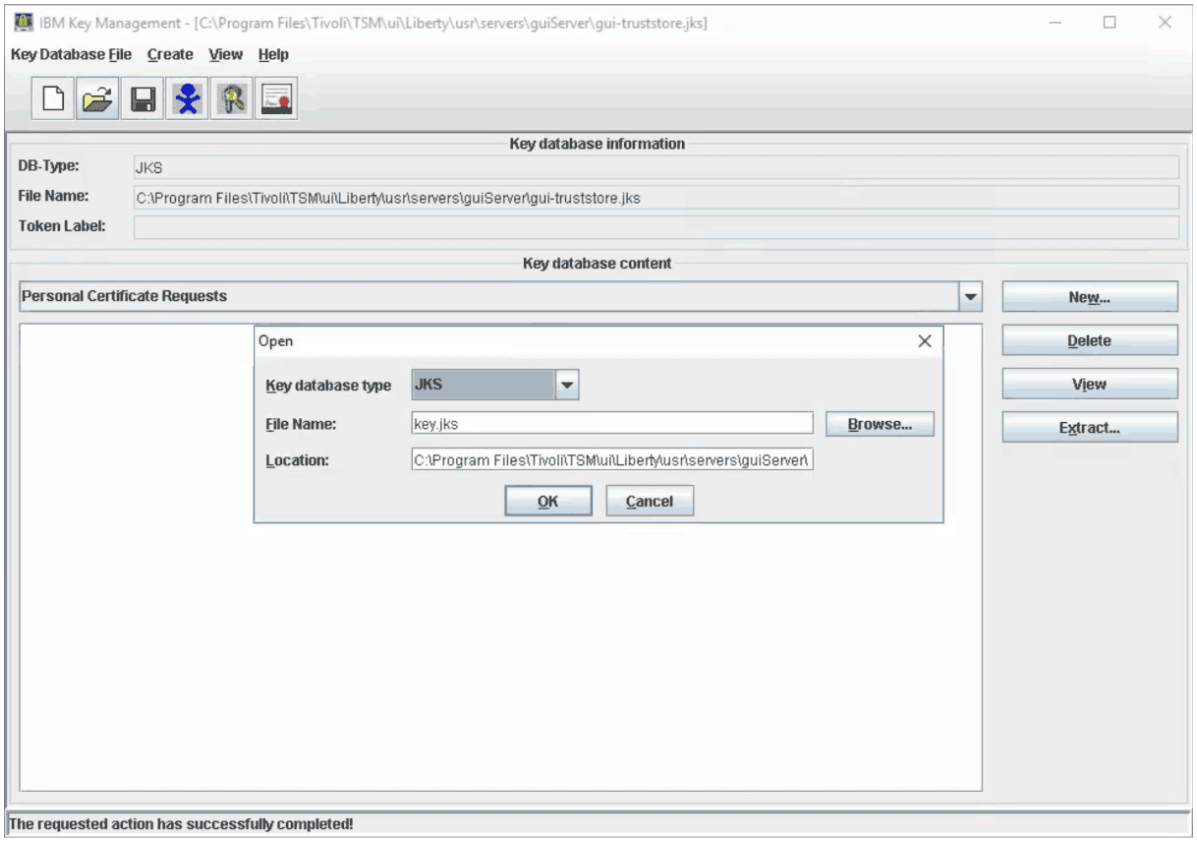
   ヒント : ikeyman コマンドには絶対パスを指定することが必要な場合があります。コマンドはディレクトリーにあります。ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを表します。

   installation_dir/ui/jre/bin

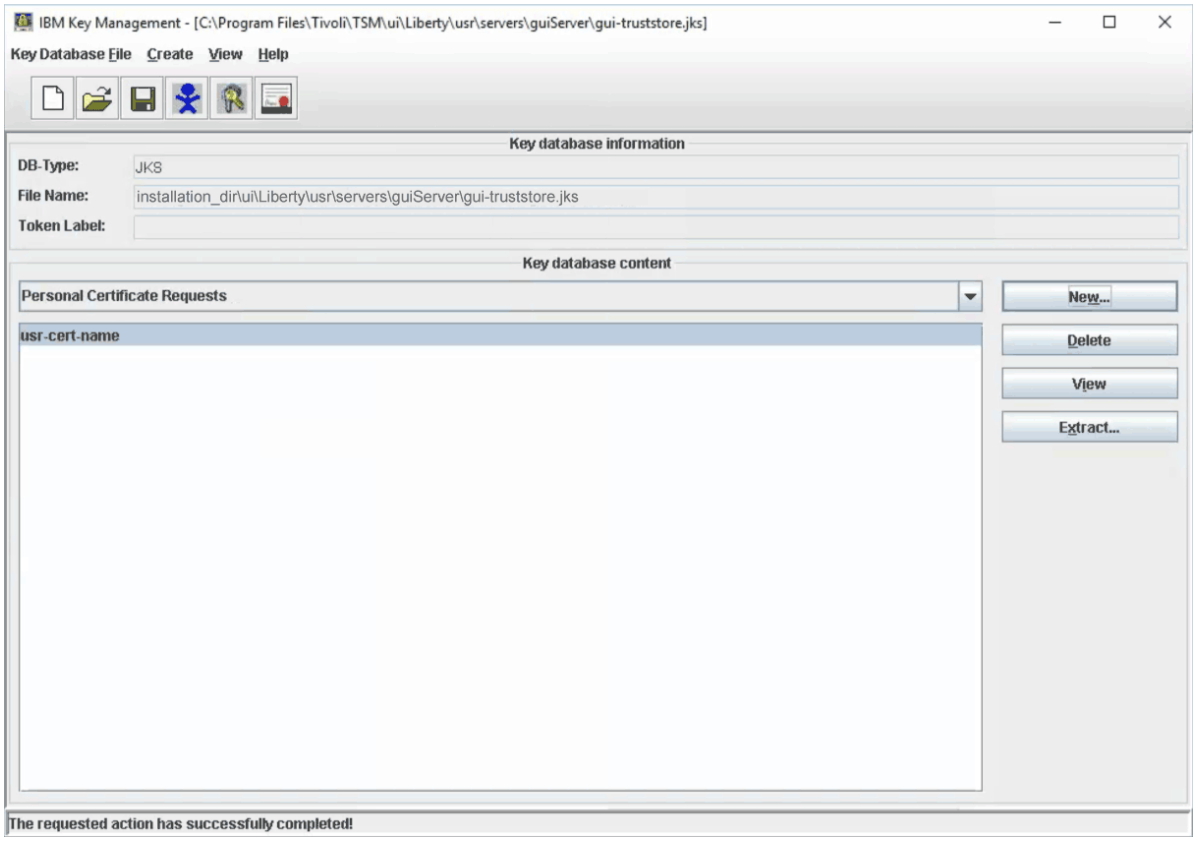
b)「**鍵データベース・ファイル**」 > 「**オープン**」をクリックします。



「**開く**」ダイアログ・ボックスで「**参照**」をクリックしてディレクトリーを開き、gui-truststore.jks ファイルを選択します。「**OK**」をクリックします。



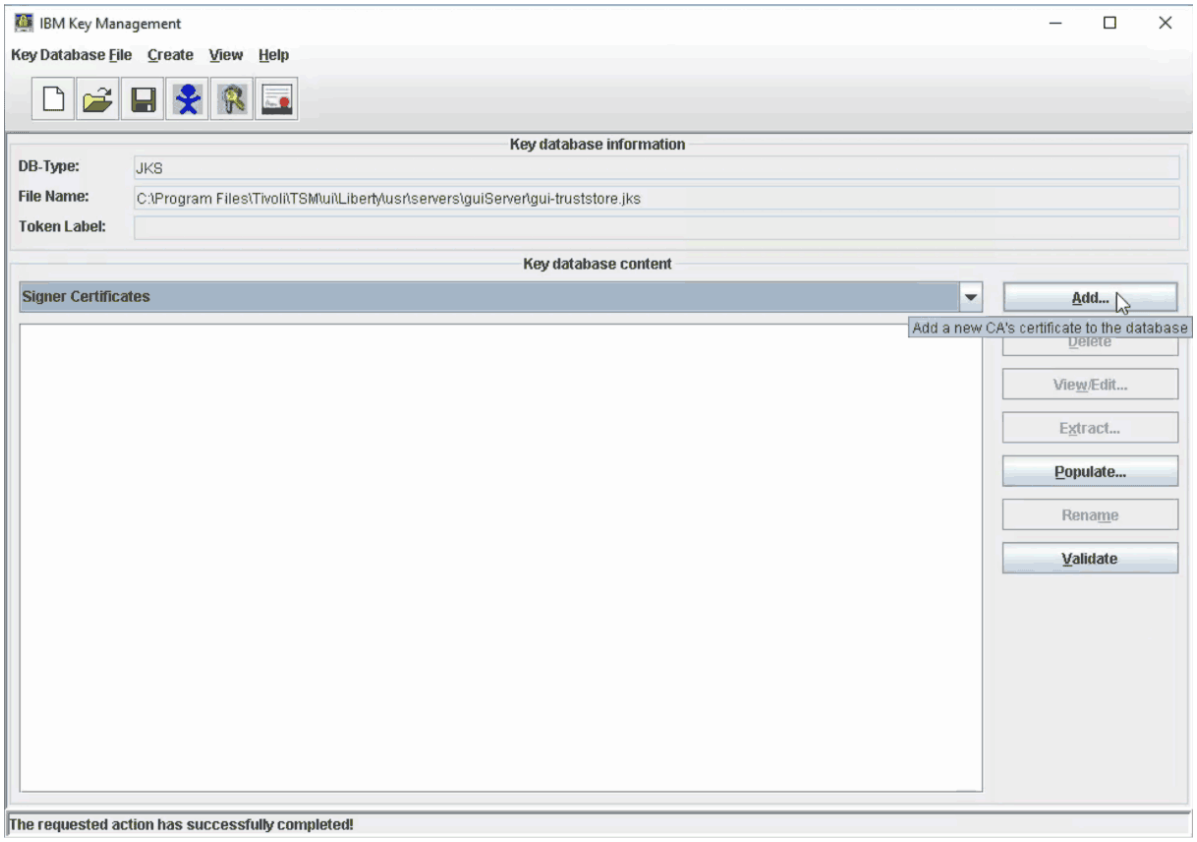
c)「**鍵データベースの内容**」エリアで、「**個人認証要求**」を選択し、「**usr-cert-name**」ラベルが表示されていることを確認します。



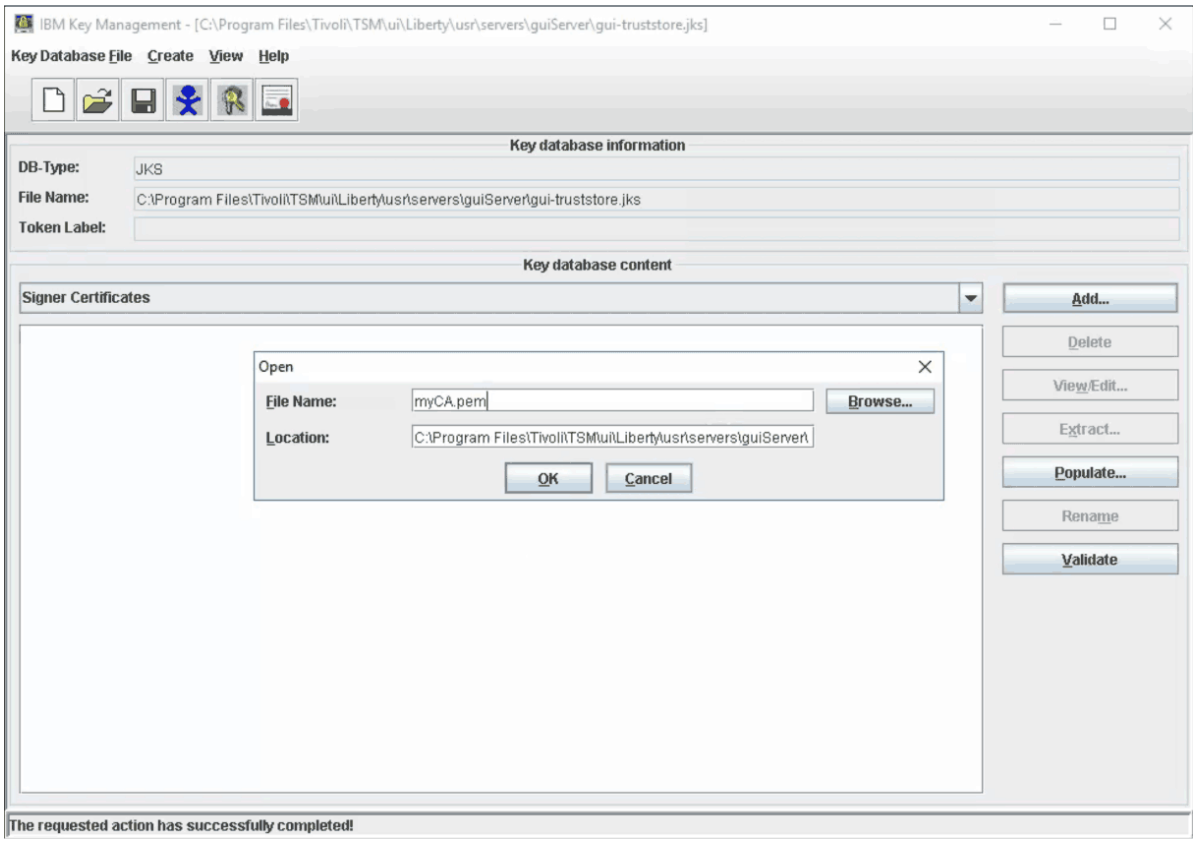
2. CA ルート証明書および任意の中間証明書をトラストストア・ファイルに追加します。CA から中間証明書を受け取った場合は、各証明書をトラストストア・ファイルに追加してから、CA ルート証明書を追加する必要があります。各中間証明書と CA ルート証明書に対して、以下のステップを実行します。

   重要 : CA は 1 つのルート証明書、署名付き証明書、また場合によっては 1 つ以上の中間証明書を送信します。CA によっては証明書ファイルが 1 ファイルになることも、複数ファイルになることもあります。1 ファイルで証明書ファイルを受け取った場合、個別のファイルに証明書を抽出する必要があります。証明書の抽出方法が不明な場合は、CA にお問い合わせください。

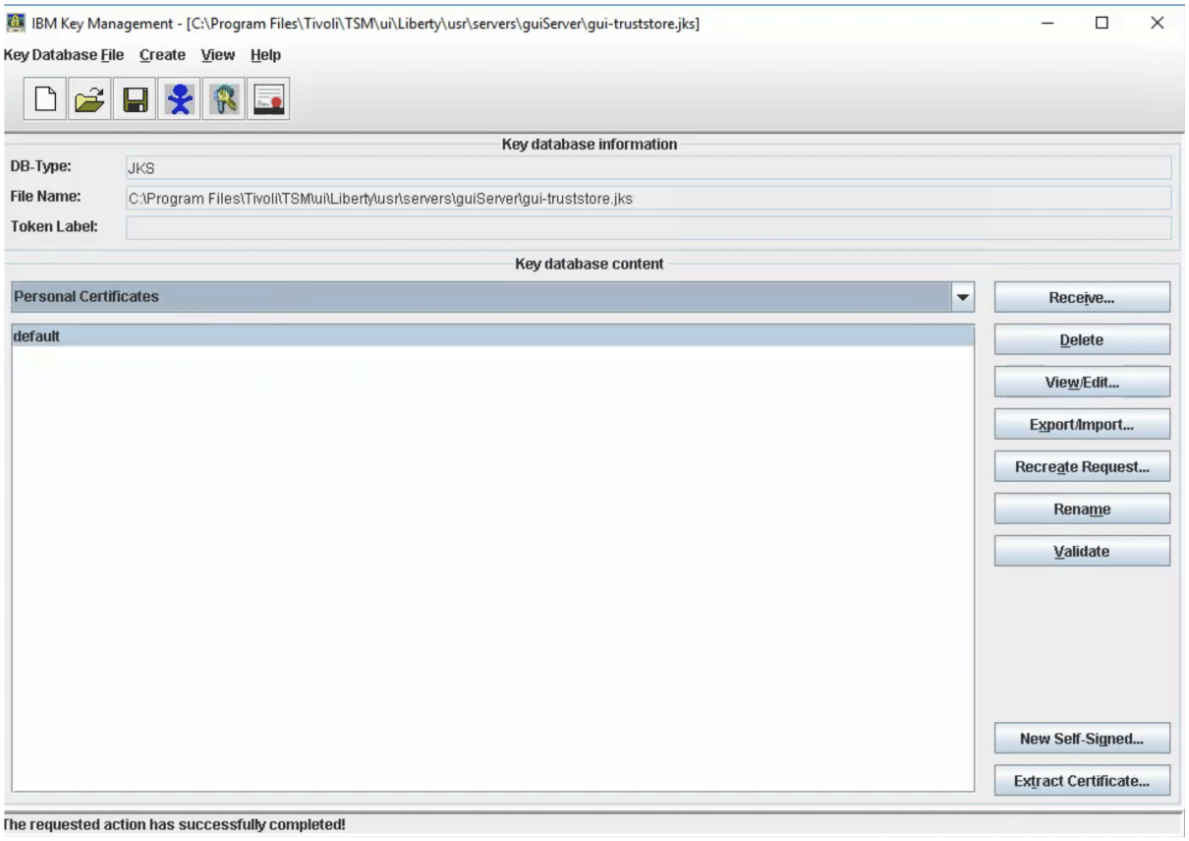
   a)「**鍵データベースの内容**」エリアで「**署名者証明書**」を選択し、「**追加**」をクリックします。



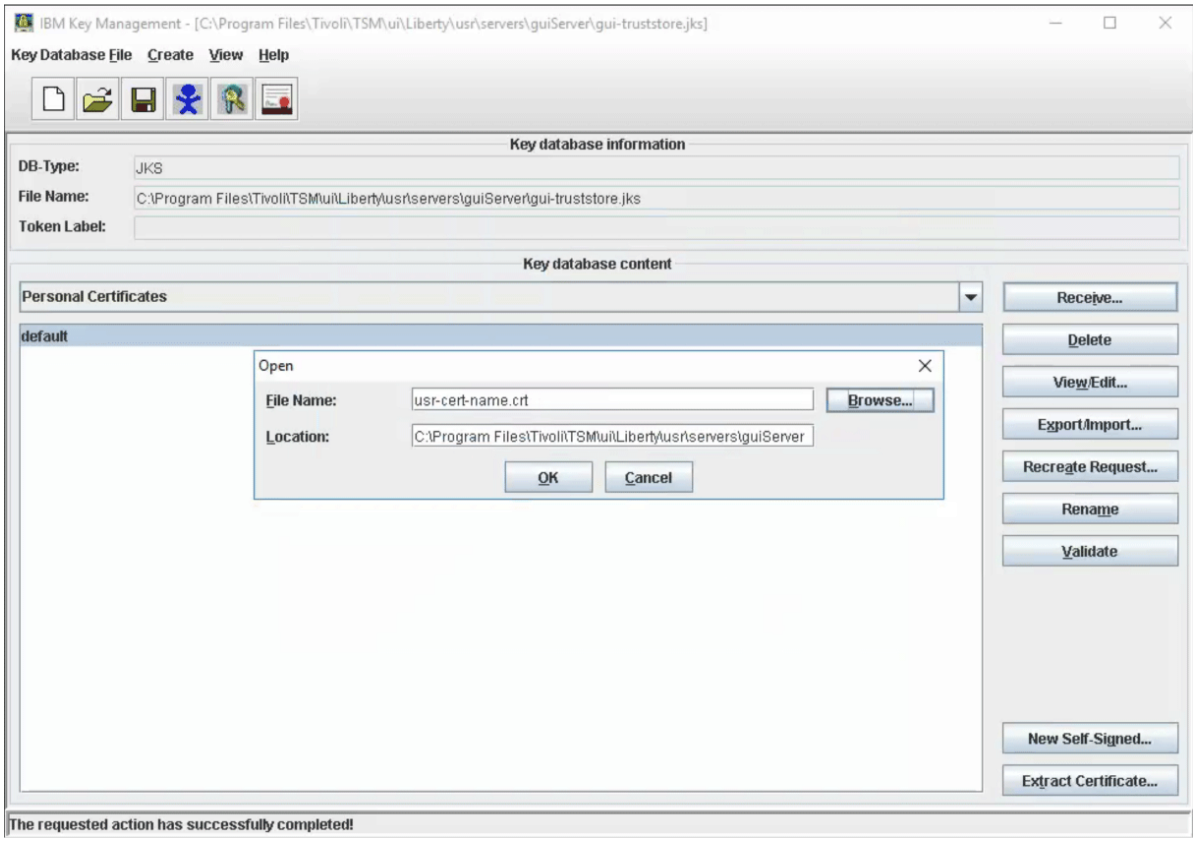
b)「開く」ダイアログで、CA ルート証明書または中間証明書を指定し、「**OK**」 をクリックします。



3. 以下の手順を実行して署名付き証明書を受け取ります。
   a)「**鍵データベースの内容**」エリアで、「**個人証明書**」を選択し、「**受信**」をクリックします。

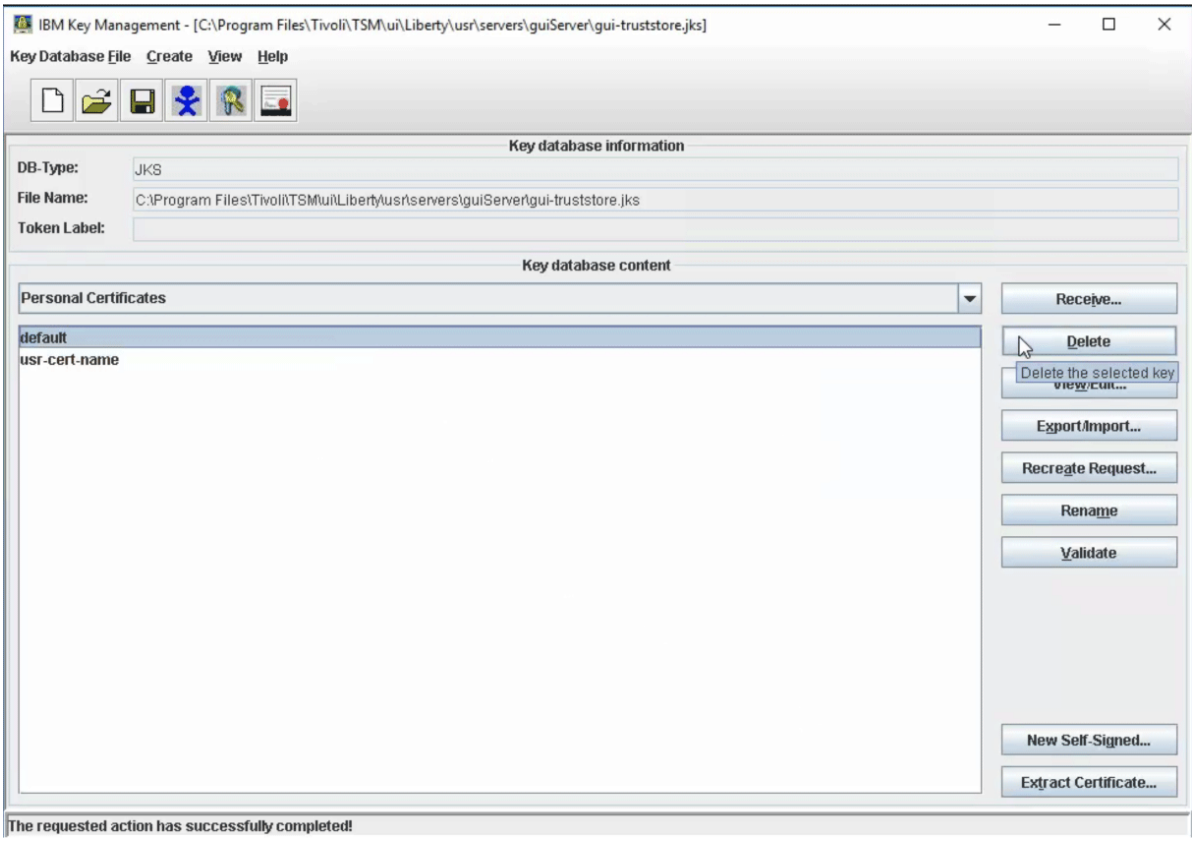


b)「開く」ダイアログ・ボックスで、署名付き証明書を指定し、「**OK**」 をクリックします。

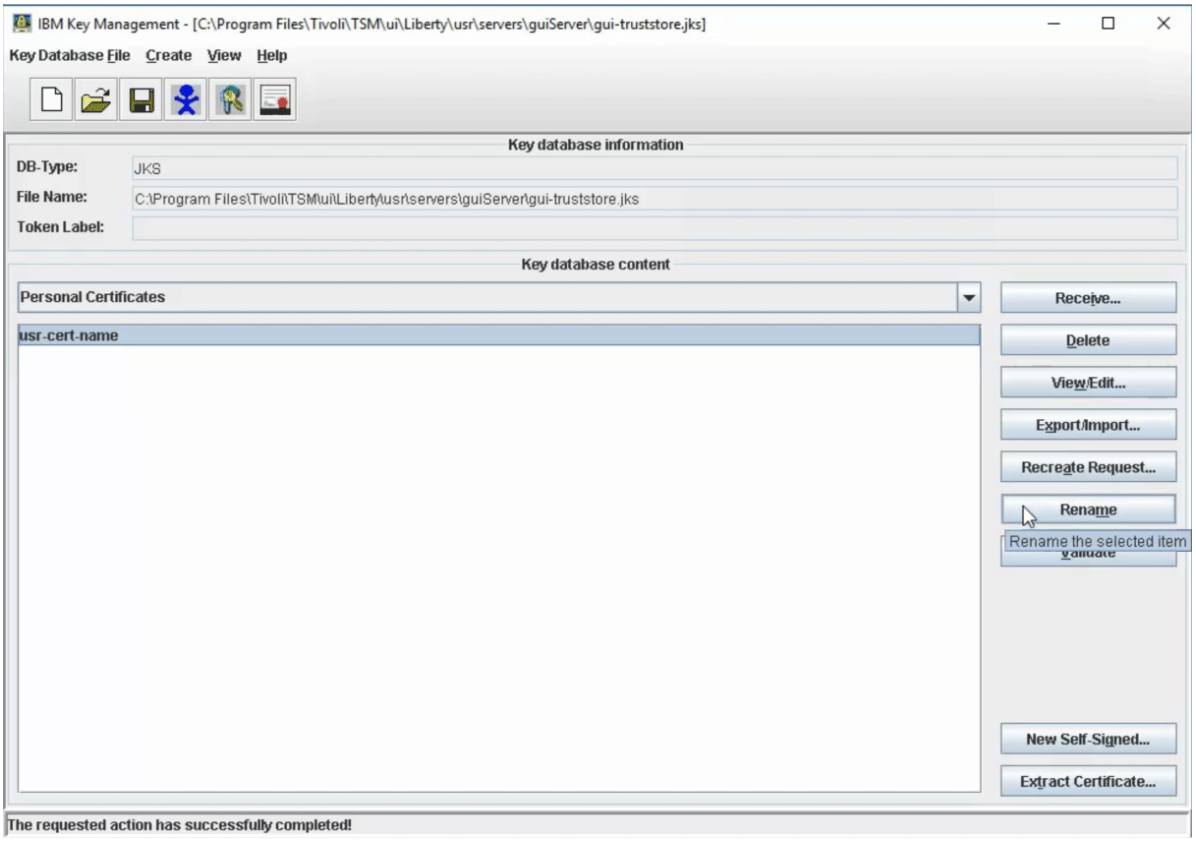


4. 現在 Operations Center によって使用されている自己署名証明書を削除し、それを CA 署名証明書に置き換えるには、以下の手順を実行します。
   a)「**鍵データベースの内容**」エリアで、「**個人証明書**」を選択します。

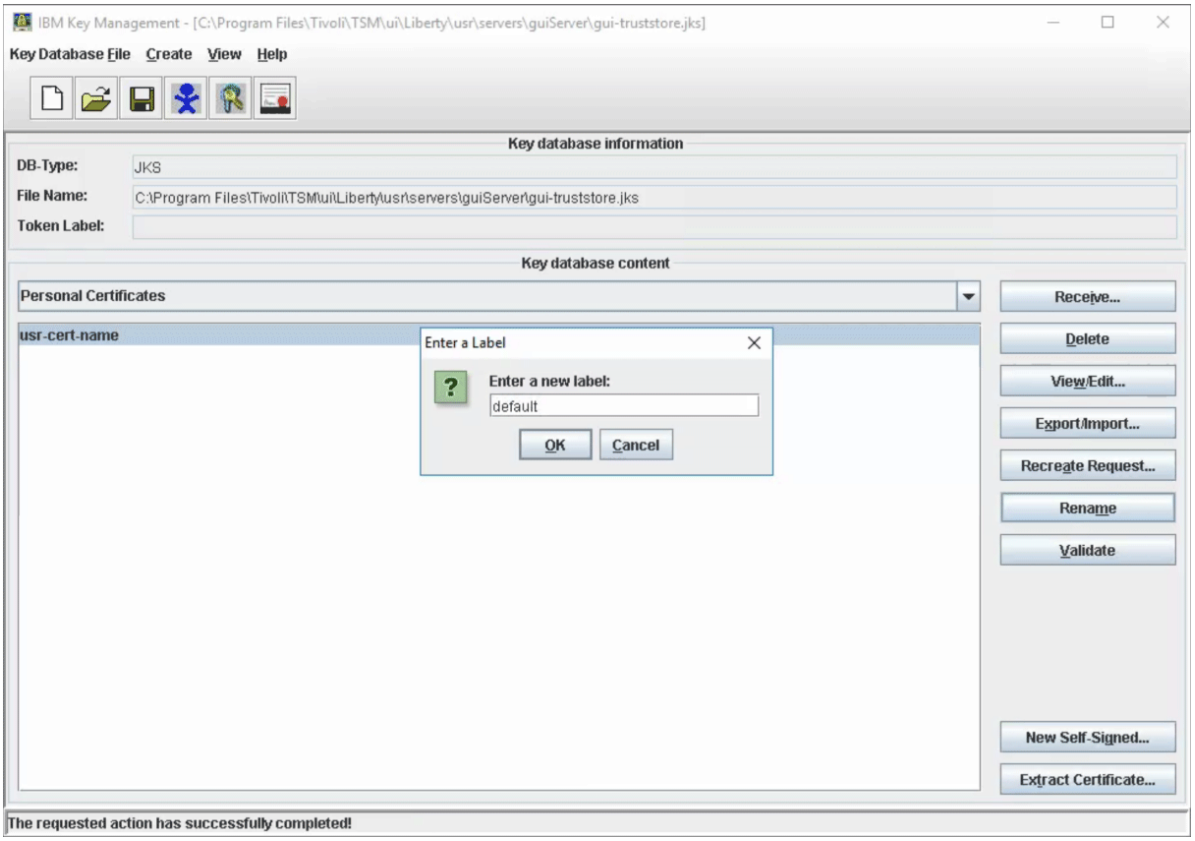
b) **default** というラベルの証明書を選択し、「**削除**」をクリックします。 確認ダイアログ・ボックスの「**はい**」をクリックします。



c) CA 署名証明書の **usr-cert-name** を選択し、「**名前変更**」をクリックします。



d)「名前変更」ダイアログで、その署名証明書 (usr-cert-name) を default に名前変更して、「**OK**」をクリックします。



5. 以下の手順を実行して、default 証明書を検証します。
   a)「**鍵データベースの内容**」エリアで、「**個人証明書**」を選択します。
   b) **default** というラベルの証明書を選択し、「**検証**」をクリックします。 確認ダイアログ・ボックスで「**OK**」をクリックします。
6. 168 ページの『Web サーバーの開始と停止』の説明に従って、Operations Center Web サーバーを開始します。

ikeycmd を使用した署名付き証明書の受信

ikeycmd コマンドを使用して、コマンド・ラインを開き、証明書鍵の管理と署名付き証明書を受信を行うことができます。

手順

1. **ikeycmd** コマンドを使用して個人署名証明書が適切なディレクトリー内にあることを確認します。次の手順を実行してください。
   a) 次のコマンドを出します。

```
ikeycmd -certreq -list -db gui-truststore.jks
```

   ヒント : ikeycmd コマンドには絶対パスを指定することが必要な場合があります。コマンドはディレクトリーにあります。ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを表します。

   installation_dir/ui/jre/bin

   b) メッセージには、トラストストア・ファイル内にある個人署名証明書 usr-cert-name の名前が表示されます。

2. 以下のコマンドを発行して CA ルート証明書および任意の中間証明書をトラストストア・ファイルに追加します。CA から中間証明書を受け取った場合は、その証明書をトラストストア・ファイルに追加してから、CA ルート証明書を追加する必要があります。

```
ikeycmd -cert -add -db gui-truststore.jks
    -file intermediate_certificate_file
```

```
ikeycmd -cert -add -db gui-truststore.jks
    -file root_certificate_file
```

ここで、

-file *certificate_file*
証明書を含むファイルの名前を指定します。

3. 次のコマンドを発行して、署名付き証明書を受け取ります。

```
ikeycmd -cert -receive -db gui-truststore.jks
-file signer_certificate_file
```

ここで、

-file *signer_certificate_file*
署名証明書を含むファイルの名前を指定します。

4. 現在 Operations Center によって使用されている自己署名証明書を削除し、それを CA 署名証明書に置き換えるには、以下の手順を実行します。

a) 既存の自己署名証明書を削除するには、 次のコマンドを発行します。

```
ikeycmd -cert -delete -db gui-truststore.jks -label default
```

b) CA 署名証明書 *usr-cert-name* の名前を `default` に変更するには、 次のコマンドを発行します。

```
ikeycmd -cert -rename -db gui-truststore.jks -label usr-cert-name
-new_label default
```

ここで、

-label *usr-cert-name*
CA 署名証明書をそのラベルで識別します。

5. 以下のコマンドを発行して、`default` 証明書を検証します。

```
ikeycmd -cert -validate -db gui-truststore.jks -label default
```

6. 168 ページの『Web サーバーの開始と停止』の説明に従って、Operations Center Web サーバーを開始します。

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

Operations Center とハブ・サーバー間のセキュア通信をセットアップするには、Operations Center のトラストストア・ファイルのパスワードを知っている必要があります。このパスワードは、Operations Center のインストール時に作成します。パスワードが不明な場合は、パスワードを削除して新規パスワードを割り当てることができます。

このタスクについて

新規パスワードを再割り当てするには、新規パスワードを作成し、Operations Center のトラストストア・ファイルを削除して、 Operations Center Web サーバーを再始動する必要があります。

重要 :

トラストストア・パスワードを忘れた場合は、新規署名付き証明書を CA から取得する必要があります。詳しくは、159 ページの『署名付き証明書の受信』を参照してください。

トラストストアのパスワードが不明な場合のみ、以下のステップを実行してください。トラストストアのパスワードが分かっている上で、パスワードを変更する場合には、以下の手順を実行しないでください。パスワードを削除して再割り当てするには、トラストストア・ファイルを削除する必要があります。これにより、トラストストア・ファイルに保管済みの証明書はすべて削除されます。トラストストアのパスワードが分かっている場合、**ikeycmd** または **ikeyman** のユーティリティーを使用してパスワードを変更できます。

手順

1. Operations Center Web サーバーを停止します。
2. 以下のディレクトリーに移動します。ここで、*installation_dir* は、Operations Center がインストールされているディレクトリーを表します。

   installation_dir/ui/Liberty/usr/servers/guiServer
3. bootstrap.properties ファイルを開きます。このファイルには、トラストストア・ファイルのパスワードが入っています。

   パスワードが暗号化されていない場合、そのパスワードを使用してトラストストア・ファイルを開くことができます。パスワードを再割り当てする必要はありません。

   以下の例は、暗号化されたパスワードと暗号化されていないパスワード間の相違を示しています。

   暗号化されたパスワードの例

   暗号化されたパスワードには、先頭にテキスト・ストリング {xor} が付いています。

   次の例は、**tsm.truststore.pswd** パラメーターの値として、暗号化されたパスワードを示しています。

   ```
   tsm.truststore.pswd={xor}MiYPPiwsKDAtOw==
   ```

   暗号化されていないパスワードの例

   次の例は、**tsm.truststore.pswd** パラメーターの値として、暗号化されていないパスワードを示しています。

   ```
   tsm.truststore.pswd=J8b%^B
   ```
4. bootstrap.properties ファイル内のパスワードを新規パスワードに置き換えます。

   パスワードは、暗号化パスワードで置き換えることも、非暗号化パスワードで置き換えることもできます。後で使用するために、暗号化されていないパスワードを覚えておいてください。

   暗号化されたパスワードを作成する場合、以下の手順を実行します。

   a. 暗号化されていないパスワードを作成します。

      トラストストア・ファイルのパスワードは、以下の基準を満たしていなければなりません。

      - パスワードには、最小 6 文字、最大 64 文字を含める必要があります。
      - パスワードには、少なくとも以下の文字を含める必要があります。
        - 1 つの大文字 (A – Z)
        - 1 つの小文字 (a – z)
        - 1 つの数字 (0 – 9)
        - 以下に示す非英数字文字のうち 2 つ:

          ```
          ~ @ # $ % ^ & * _ - + = ` |
          ```

          ```
          ( ) { } [ ] : ; < > , . ? /
          ```

   b. オペレーティング・システムのコマンド・ラインから、以下のディレクトリーに移動します。

      installation_dir/ui/Liberty/bin

c. パスワードを暗号化するには、次のコマンドを発行します。ここで、*myPassword* は、暗号化されていないパスワードを表します。

```
securityUtility encode myPassword --encoding=aes
```

5. bootstrap.properties ファイルを保存します。
6. 次のディレクトリーに移動します。

   installation_dir/ui/Liberty/usr/servers/guiServer
7. gui-truststore.jks ファイルを削除します。これは Operations Center のトラストストア・ファイルです。
8. Operations Center Web サーバーを開始します。

   以下の手順を実行して、Operations Center Web サーバーを開始します。

   a. 以下のコマンドを発行して、Operations Center Web サーバーを開始します。

   ```
   /opt/tivoli/tsm/ui/Liberty/bin/server start guiServer
   ```

   Operations Center の新しいトラストストア・ファイルが自動的に作成され、Operations Center の TLS 証明書がそのトラストストア・ファイルに自動的に入れられます。ただし、Operations Center は使用できません。

   b. 以下のコマンドを発行して、Operations Center Web サーバーを停止します。

   ```
   /opt/tivoli/tsm/ui/Liberty/server stop guiServer
   ```

   c. 以下のコマンドを発行して、Operations Center Web サーバーを再始動します。

   ```
   /opt/tivoli/tsm/ui/utils/startServer.sh
   ```

タスクの結果

Operations Center の新しいトラストストア・ファイルが自動的に作成され、Operations Center の TLS 証明書がそのトラストストア・ファイルに自動的に入れられます。

Web サーバーの開始と停止

Operations Center の Web サーバーは、サービスとして実行され、自動的に開始します。例えば、構成変更を行う場合などに、Web サーバーを停止および開始する必要がある場合があります。

手順

Web サーバーを停止および開始します。

- */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示します) から以下のコマンドを発行します。
  - サーバーを停止する場合:

    ```
    ./stopserver.sh
    ```

  - サーバーを開始する場合:

    ```
    ./startserver.sh
    ```

Operations Center の開始

Operations Center を開始すると、デフォルトで「**概要**」ページが表示されます。 ただし、Web ブラウザーで、Operations Center にログインしたときに開くページをブックマークすることができます。

手順

1. Web ブラウザーで、次のアドレスを入力します。ここで、*hostname* は、Operations Center がインストールされているコンピューターの名前を表し、*secure_port* は、そのコンピューター上で Operations Center が HTTPS 通信用に使用するポート番号を表します。

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

   ヒント：

   - URL では大文字と小文字が区別されます。例えば、示されているように、「oc」を小文字で入力してください。
   - HTTPS 通信用のデフォルト・ポート番号は 11090 ですが、別のポート番号を 1024 から 65535 までの範囲で Operations Center のインストール時に指定できます。インストール後に管理者が Operations Center を構成して、HTTPS 通信用に標準の TCP/IP セキュア・ポート (ポート 443) を使用するように設定できます。ポート 443 を使用するように Operations Center を構成すると、Operations Center を開いたときにセキュア・ポート番号を組み込む必要がなくなります。代わりに以下のアドレスを入力します。ここで *hostname* は Operations Center がインストールされているコンピューターの名前を示します。

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

     ポート 443 を使用するための Operations Center の構成方法については、148 ページの『標準 TCP/IP セキュア・ポートを使用するための Operations Center Web サーバーの構成』を参照してください。
2. ハブ・サーバーに登録されている管理者 ID を使用してログインします。

   「**概要**」ページで、クライアント、サービス、サーバー、ストレージ・プール、およびストレージ・デバイスの要約情報を表示することができます。 項目をクリックするか、Operations Center メニュー・バーを使用して、詳細を表示することができます。

   モバイル・デバイスからのモニター：ストレージ環境をリモートからモニターするには、モバイル・デバイスの Web ブラウザーで Operations Center の「**概要**」ページを表示します。 Operations Center は、iPad の Apple Safari Web ブラウザーをサポートします。 その他のモバイル・デバイスも使用できます。

IBM Spectrum Protect クライアント管理サービスでの診断情報の収集

クライアント管理サービス は、バックアップ/アーカイブ・クライアントに関する診断情報を収集し、その情報を基本モニター機能のために Operations Center が使用できるようにします。

このタスクについて

クライアント管理サービスをインストールした後、Operations Center の「**診断 (Diagnosis)**」ページを表示して、バックアップ/アーカイブ・クライアントのトラブルシューティング 情報を入手できます。

ヒント：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で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。

診断情報は、Linux クライアントおよび Windows クライアントからのみ収集可能ですが、管理者は AIX、Linux、または Windows オペレーティング・システムの Operations Center で診断情報を参照できます。

データ・ムーバーに関する診断情報を収集するため、IBM Spectrum Protect for Virtual Environments: Data Protection for VMware のデータ・ムーバー・ノードに クライアント管理サービス をインストールすることもできます。

ヒント: クライアント管理サービスの資料では、クライアント・システム はバックアップ/アーカイブ・クライアントがインストールされているシステムです 。

グラフィカル・ウィザードを使用したクライアント管理サービスのインストール

クライアント・ログ・ファイルなど、バックアップ/アーカイブ・クライアントに関する診断情報を収集するには、管理するクライアント・システムにクライアント管理サービスをインストールする必要があります。

始める前に

128 ページの『IBM Spectrum Protect クライアント管理サービスの要件と制限』を確認します。

このタスクについて

クライアント管理サービスは、バックアップ/アーカイブ・クライアントと同じコンピューターにインストールする必要があります。

手順

1. クライアント管理サービス用のインストール・パッケージを IBM ダウンロード・サイト (IBM パスポート・アドバンテージや IBM Fix Central など) からダウンロードします。 *<version>*-IBM-SPCMS-*<operating system>*.bin のようなファイル名を探します。

   次の表に、インストール・パッケージの名前を示します。

クライアント・オペレーティング・システム	インストール・パッケージ名
Linux x86 64 ビット	8.1.x.000-IBM-SPCMS-Linuxx64.bin
Windows 32 ビット	8.1.x.000-IBM-SPCMS-Windows32.exe
Windows 64 ビット	8.1.x.000-IBM-SPCMS-Windows64.exe

2. 管理するクライアント・システム上にディレクトリーを作成して、そこにインストール・パッケージをコピーします。
3. インストール・パッケージ・ファイルの内容を抽出します。
   - Linux クライアント・システム上で、次の手順を実行します。
     a. 次のコマンドを発行して、ファイルを実行可能ファイルに変更します。

     ```
     chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
     ```

     b. 次のコマンドを出します。

     ```
     ./8.1.x.000-IBM-SPCMS-Linuxx64.bin
     ```

   - Windows クライアント・システム上で、Windows エクスプローラーに表示されているインストール・パッケージ名をダブルクリックします。

   ヒント: 以前にパッケージをインストールしてアンインストールした 場合、プロンプトが表示されたときに「**All**」と選択して、既存のインストール・ファイルを置き換えます。

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 170 ページの『2』 で作成したディレクトリーです。
   - Linux クライアント・システムでは、次のコマンドを発行します。

   ```
   ./install.sh
   ```

- Windows クライアント・システムでは、「**install.bat**」をダブルクリックします。

5. クライアント管理サービスをインストールするには、IBM Installation Manager ウィザードの説明に従ってください。

   IBM Installation Manager がまだクライアント・システムにインストールされていない場合は、「**IBM Installation Manager**」と「**IBM Spectrum Protect Client Management Services**」の両方を選択する必要があります。

   ヒント: 共有リソース・ディレクトリーと IBM Installation Manager のインストール・ディレクトリーのデフォルトの場所を受け入れることができます。

次のタスク

インストールを確認します。

サイレント・モードでの クライアント管理サービス のインストール

クライアント管理サービス をサイレント・モードでインストールすることができます。サイレント・モードを使用する場合は、応答ファイルにインストール値を指定してから、インストール・コマンドを実行します。

始める前に

128 ページの『IBM Spectrum Protect クライアント管理サービスの要件と制限』を確認します。

170 ページの『グラフィカル・ウィザードを使用したクライアント管理サービスのインストール』の説明に従って、インストール・パッケージを抽出します。

このタスクについて

クライアント管理サービスは、バックアップ/アーカイブ・クライアントと同じコンピューターにインストールする必要があります。

インストール・パッケージが抽出されたディレクトリー内の `input` ディレクトリーに、次のサンプル応答ファイルが入っています。

`install_response_sample.xml`

このサンプル・ファイルをデフォルト値で使用することも、カスタマイズすることもできます。

ヒント: サンプル・ファイルをカスタマイズする場合は、サンプル・ファイルのコピーを作成し、名前を変更して、そのコピーを編集してください。

手順

1. サンプル・ファイルに基づいて応答ファイルを作成するか、あるいはサンプル・ファイル `install_response_sample.xml` を使用します。

   どちらの場合も、応答ファイルでクライアント管理サービスのポート番号を必ず指定します。デフォルト・ポートは 9028 です。例えば次のとおりです。

   ```
   <variable name='port' value='9028'/>
   ```

2. コマンドを実行して、クライアント管理サービスをインストールし、使用条件に同意します。インストール・パッケージ・ファイルが抽出されたディレクトリーから、以下のコマンドを発行します。ここで、*response_file* は、ファイル名を含む応答ファイル・パスを表します。

   Linux クライアント・システム:

   ```
   ./install.sh -s -input response_file -acceptLicense
   ```

   例えば次のとおりです。

```
./install.sh -s -input /cms_install/input/install_response.xml
-acceptLicense
```

Windows クライアント・システム:

```
install.bat -s -input response_file -acceptLicense
```

例えば次のとおりです。

```
install.bat -s -input c:¥cms_install¥input¥install_response.xml -acceptLicense
```

次のタスク

インストールを確認します。

クライアント管理サービスが正しくインストールされていることの確認

クライアント管理サービスを使用してバックアップ/アーカイブ・クライアントに関する診断情報を収集する前に、クライアント管理サービスのインストールと構成が正しく行われていることを確認できます。

手順

クライアント・システムのコマンド・ラインで、次のコマンドを実行して、クライアント管理サービスの構成を表示します。

- Linux クライアント・システムでは、次のコマンドを発行します。

```
client_install_dir/cms/bin/CmsConfig.sh list
```

ここで、*client_install_dir* はバックアップ/アーカイブ・クライアントがインストールされているディレクトリーです。例えば、デフォルトのクライアント・インストールでは、次のコマンドを発行します。

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

出力は、以下のテキストのようになります。

```
Listing CMS configuration

server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
    Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

- Windows クライアント・システムでは、次のコマンドを発行します。

```
client_install_dir¥cms¥bin¥CmsConfig.bat list
```

ここで、*client_install_dir* はバックアップ/アーカイブ・クライアントがインストールされているディレクトリーです。例えば、デフォルトのクライアント・インストールでは、次のコマンドを発行します。

```
C:¥"Program Files"¥Tivoli¥TSM¥cms¥bin¥CmsConfig.bat list
```

出力は、以下のテキストのようになります。

```
Listing CMS configuration

server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
    Opt Path: C:¥Program Files¥Tivoli¥TSM¥baclient¥dsm.opt

    Log File: C:¥Program Files¥Tivoli¥TSM¥baclient¥dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

```
Log File: C:¥Program Files¥Tivoli¥TSM¥baclient¥dsmsched.log
    en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

クライアント管理サービスのインストールと構成が正しく行われている場合、出力にはエラー・ログ・ファイルの場所が表示されます。

出力テキストは、次の構成ファイルから抽出されます。

- Linux クライアント・システム:

```
client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- Windows クライアント・システム:

```
client_install_dir¥cms¥Liberty¥usr¥servers¥cmsServer¥client-configuration.xml
```

出力に項目が含まれていない場合は、`client-configuration.xml` ファイルを構成する必要があります。 このファイルの構成方法については、カスタム構成のためのクライアント管理サービスの構成を参照してください。**CmsConfig verify** コマンドを使用して、ノード定義が `client-configuration.xml` ファイル内で正しく作成されていることを確認することができます。

クライアント管理サービスを使用するための Operations Center の構成

クライアント管理サービスのデフォルト構成を使用しなかった場合、クライアント管理サービスにアクセスするように Operations Center を構成する必要があります。

始める前に

クライアント管理サービスがクライアント・システムにインストールされ、開始されていることを確認します。128 ページの『IBM Spectrum Protect クライアント管理サービスの要件と制限』を確認します。

デフォルト構成が使用されているかどうかを確認します。以下のいずれかの条件に該当する場合、デフォルト構成は使用されていません。

- クライアント管理サービスがデフォルトのポート番号 (9028) を使用していない。
- バックアップ/アーカイブ・クライアントが、バックアップ/アーカイブ・クライアントのインストール先のクライアント・システムと同じ IP アドレスでアクセスされない。 例えば、以下の状態では、異なる IP アドレスが使用される可能性があります。
  - コンピューター・システムに 2 つのネットワーク・カードがある。バックアップ/アーカイブ・クライアントは 1 つのネットワークで通信するように構成されており、一方、クライアント管理サービスはもう 1 つのネットワークで通信します。
  - クライアント・システムが動的ホスト構成プロトコル (DHCP) を使用して構成されている。その結果、クライアント・システムに IP アドレスが動的に割り当てられ、その IP アドレスが、前のバックアップ/アーカイブ・クライアント操作中に IBM Spectrum Protect サーバーに保存されます。クライアント・システムが再始動すると、クライアント・システムには別の IP アドレスが割り当てられる可能性があります。Operations Center が常にクライアント・システムを確実に検出できるようにするには、完全修飾ドメイン・ネームを指定します。

手順

クライアント管理サービスを使用するように Operations Center を構成するには、以下の手順を実行します。

1. Operations Center の「**クライアント**」ページで、クライアントを選択します。
2. 「**詳細**」をクリックします。
3. 「**プロパティー**」タブをクリックします。
4. 「**一般**」セクションの「**リモート診断 URL**」フィールドに、クライアント・システム上のクライアント管理サービスの URL を指定します。

   アドレスの先頭は `https` でなければなりません。次の表に、リモート診断 URL の例を示します。

URL のタイプ	例
DNS ホスト名とデフォルト・ポート 9028 を使用	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

5. 「**保存**」をクリックします。

次のタスク

Operations Center の「**診断**」タブから、クライアント・ログ・ファイルなどのクライアント診断情報にアクセスできます。

クライアント管理サービス の始動と停止

クライアント管理サービスは、クライアント・システムにインストールされた後に自動的に開始されます。状況によっては、サービスを停止して開始する必要が生じることがあります。

手順

- Linux クライアント・システム上でクライアント管理サービスを停止、開始、または再始動するには、次のコマンドを発行します。
  - システムに **systemctl** がインストールされている場合は、以下のコマンドを発行します。
    - サーバーを停止する場合:

      ```
      systemctl stop cms.service
      ```

    - サーバーを開始する場合:

      ```
      systemctl start cms.service
      ```

    - サーバーを再始動するには、次のコマンドを実行します。

      ```
      systemctl restart cms.service
      ```

    - サーバーが稼働しているかどうかを判別するには、次のコマンドを発行します。

      ```
      systemctl status cms.service
      ```

  - システムに **systemctl** がインストールされていない場合は、以下のコマンドを発行します。
    - サーバーを停止する場合:

      ```
      service cms.rc stop
      ```

    - サーバーを開始する場合:

      ```
      service cms.rc start
      ```

    - サーバーを再始動するには、次のコマンドを実行します。

      ```
      service cms.rc restart
      ```

    - サーバーが稼働しているかどうかを判別するには、次のコマンドを発行します。

      ```
      service cms.rc status
      ```

- Windows クライアント・システムで、「**サービス**」ウィンドウを開き、IBM Spectrum Protect Client Management Services サービスの停止、開始、または再始動を行います。

クライアント管理サービス のアンインストール

クライアント 診断情報の収集が不要になった場合、クライアント 管理サービスをクライアント・システムからアンインストールできます。

このタスクについて

クライアント 管理サービスをアンインストールするには、IBM Installation Manager を使用する必要があります。IBM Installation Manager をもう使用する予定がない場合には、これもアンインストールできます。

手順

1. クライアント 管理サービスをクライアント・システムからアンインストールします 。
   a) 次のようにして、IBM Installation Manager を開きます。
      - Linux クライアント・システム 上の IBM Installation Manager がインストールされているディレクトリーで、eclipse サブディレクトリー (例えば、/opt/IBM/InstallationManager/eclipse) に移動し、次のコマンドを発行します。

        ```
        ./IBMIM
        ```

      - Windows のクライアント・システムでは、「**スタート**」メニューから IBM Installation Manager を開きます。

   b)「**アンインストール**」をクリックします。
   c)「**IBM Spectrum Protect Client Management Services**」を選択し、 「**次へ**」をクリックします。
   d)「**アンインストール**」をクリックしてから、「**終了**」をクリックします。
   e)「**IBM Installation Manager**」ウィンドウを閉じます。
2. IBM Installation Manager を、もはや必要でない場合は、クライアント・システムからアンインストールします。
   a) IBM Installation Manager アンインストール・ウィザードを開きます。
      - Linux クライアント・システムでは、IBM Installation Manager のアンインストール・ディレクトリー (例えば、/var/ibm/InstallationManager/uninstall) に移動し、次のコマンドを発行します。

        ```
        ./uninstall
        ```

      - Windows のクライアント・システムでは、「**スタート**」 > 「**コントロール パネル**」をクリックします。次に、「**プログラムのアンインストール**」 > 「**IBM Installation Manager**」 > 「**アンインストール**」をクリックします。

   b)「**IBM Installation Manager**」ウィンドウで、まだ選択されていない場合は「**IBM Installation Manager**」を選択して、「**次へ**」をクリックします。
   c)「**アンインストール**」をクリックしてから、「**終了**」をクリックします。

カスタム・クライアント・インストールのためのクライアント管理サービスの構成

クライアント 管理サービスは、クライアント 構成ファイル (client-configuration.xml) 内の情報を使用して、診断情報を検出します。クライアント 管理サービスがログ・ファイルの場所を検出できない場合は、**CmsConfig** ユーティリティーを 実行して、ログ・ファイルの場所を client-configuration.xml ファイルに追加する必要があります。

このタスクについて

クライアント 管理サービス をインストールする前に、バックアップ・アーカイブ・クライアントとサーバーの間で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。

CmsConfig ユーティリティー

デフォルトのクライアント構成を使用していない場合は、クライアント・システムで **CmsConfig** ユーティリティーを実行して、クライアント・ログ・ファイルの場所を検出し、client-configuration.xml ファイルに追加することができます。 構成の完了後、クライアント管理サービス は、クライアント・ログ・ファイルにアクセスし、それらを Operations Center での基本的な診断機能に使用できるようにすることができます。

また、**CmsConfig** ユーティリティーを 使用して、クライアント管理サービスの構成を表示したり、client-configuration.xml ファイルからノード名を削除したりすることもできます。

client-configuration.xml ファイルは、次のディレクトリーにあります。

- Linux クライアント・システム:

```
client_install_dir/cms/Liberty/usr/servers/cmsServer
```

- Windows クライアント・システム:

```
client_install_dir¥cms¥Liberty¥usr¥servers¥cmsServer
```

ここで、*client_install_dir* はバックアップ/アーカイブ・クライアントがインストールされているディレクトリーです。

CmsConfig ユーティリティーは以下の場所にあります。

クライアント・オペレーティング・システム	ユーティリティーの 場所と名前
Linux	*client_install_dir*/cms/bin/CmsConfig.sh
Windows	*client_install_dir*¥cms¥bin¥CmsConfig.bat

CmsConfig ユーティリティーを 使用するには、ユーティリティーに 含まれている任意のコマンドを発行します。必ず、各コマンドを 1 行に入力してください。

CmsConfig discover コマンド

CmsConfig discover コマンドを使用すると、オプション・ファイルおよびログ・ファイルを自動的に検出し、それらをクライアント構成ファイル client-configuration.xml に追加することができます。これにより、クライアント管理サービスがクライアント・ログ・ファイルにアクセスして、それらを Operations Center での診断に確実に使用できるようにすることができます。

通常、クライアント管理サービスのインストーラーは **CmsConfig discover** コマンドを自動的に実行します。 しかし、バックアップ/アーカイブ・クライアントの変更 (クライアントの追加や、サーバー構成またはログ・ファイルの場所の変更など) を行った場合は、手動でこのコマンドを実行する必要があります。

クライアント管理サービスが client-configuration.xml 内にログ定義を作成するには、IBM Spectrum Protect のサーバー・アドレス、サーバー・ポート、およびクライアント・ノード名を入手する必要があります。クライアント・オプション・ファイル (通常は、Linux クライアント・システム上の dsm.sys、および Windows クライアント・システム上の dsm.opt) でノード名が定義されていない場合は、クライアント・システムのホスト名が使用されます。

クライアント構成ファイルを更新するには、クライアント管理サービスは 1 つ以上のログ・ファイル (dsmerror.log や dsmsched.log など) にアクセスする必要があります。 最良の結果を得るために、**CmsConfig discover** コマンドは、バックアップ/アーカイブ・クライアントのコマンド **dsmc** の場合と同じディレクトリーで、同じ環境変数を使用して実行してください。 これにより、正しいログ・ファイルが検出される可能性が高くなります。

クライアント・オプション・ファイルがカスタムの場所にあるか、標準的なオプション・ファイル名が付いていない場合には、検出の対象範囲を絞るためにクライアント・オプション・ファイルのパスを指定することもできます。

構文

パラメーター

configPath
クライアント・オプション・ファイルのパス (通常は dsm.opt)。クライアント・オプション・ファイルがデフォルトの場所にない場合、またはデフォルトの名前ではない場合は、構成パスを指定します。クライアント管理サービス は、クライアント・オプション・ファイルをロードし、そこからクライアント・ノードおよびログを検出します。このパラメーターはオプションです。

Linux クライアント・システムでは、クライアント管理サービス は常にクライアント・ユーザー・オプション・ファイル (dsm.opt) をロードし、次にクライアント・システム・オプション・ファイル (通常は dsm.sys) を検索します。 ただし、*configPath* パラメーターの値は、常にクライアント・ユーザー・オプション・ファイルになります。

Linux クライアント・システムの例

- クライアント・ログ・ファイルを検出し、ログ定義を自動的に client-configuration.xml ファイルに追加します。

  /opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

  コマンド:
  ```
  ./CmsConfig.sh discover
  ```
  出力:
  ```
  Discovering client configuration and logs.

  server.example.com:1500 SUSAN
      /opt/tivoli/tsm/client/ba/bin/dsmerror.log

  Finished discovering client configuration and logs.
  ```

- /opt/tivoli/tsm/client/ba/bin/daily.opt ファイルに指定されている構成ファイルとログ・ファイルを検出し、ログ定義を client-configuration.xml ファイルに自動的に追加します。

  /opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

  コマンド:
  ```
  ./CmsConfig.sh discover /opt/tivoli/tsm/client/ba/bin/daily.opt
  ```
  出力:
  ```
  Discovering client configuration and logs

  server.example.com:1500 NO_SSL SUSAN
  Capabilities: [LOG_QUERY]
      Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Log File:  /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

  Finished discovering client configuration and logs.
  ```

Windows クライアント・システムの例

- クライアント・ログ・ファイルを検出し、ログ定義を自動的に client-configuration.xml ファイルに追加します。

  C:¥Program Files¥Tivoli¥TSM¥cms¥bin ディレクトリーから、次のコマンドを発行します。

  コマンド:
  ```
  cmsconfig discover
  ```
  出力:
  ```
  Discovering client configuration and logs.

  server.example.com:1500 SUSAN
      C:¥Program Files¥Tivoli¥TSM¥baclient¥dsmerror.log

  Finished discovering client configuration and logs.
  ```

- c:¥program files¥tivoli¥tsm¥baclient¥daily.opt ファイルに指定されている構成ファイルおよびログ・ファイルを検出し、ログ定義を client-configuration.xml ファイルに自動的に追加します。

  C:¥Program Files¥Tivoli¥TSM¥cms¥bin ディレクトリーから、次のコマンドを発行します。

  コマンド:
  ```
  cmsconfig discover "c:¥program files¥tivoli¥tsm¥baclient¥daily.opt"
  ```
  出力:
  ```
  Discovering client configuration and logs

  server.example.com:1500 NO_SSL SUSAN
  Capabilities: [LOG_QUERY]
      Opt Path: C:¥Program Files¥Tivoli¥TSM¥baclient¥dsm.opt

      Log File: C:¥Program Files¥Tivoli¥TSM¥baclient¥dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Log File: C:¥Program Files¥Tivoli¥TSM¥baclient¥dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

  Finished discovering client configuration and logs.
  ```

CmsConfig addnode コマンド

CmsConfig addnode コマンドを使用して、client-configuration.xml 構成ファイルにクライアント・ノード定義を手動で追加します。このノード定義には、IBM Spectrum Protect サーバーと通信するために クライアント管理サービス が必要とする情報が含まれています。

このコマンドは、クライアント・オプション・ファイルまたはクライアント・ログ・ファイルがクライアント・システム上のデフォルト以外の場所に保管されている場合にのみ使用してください。

構文

パラメーター

nodeName
ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。 ただし、Linux クライアント・システムなどの 複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

serverIP
クライアント 管理サービス の認証を行う IBM Spectrum Protect サーバーの TCP/IP アドレス。このパラメーターは必須です。

サーバーに 1 文字から 64 文字の TCP/IP アドレスを指定できます。サーバー・アドレスは、TCP/IP ドメイン・ネームまたは数値 IP アドレスにすることができます。数値 IP アドレスは TCP/IP v4 または TCP/IP v6 のアドレスにすることができます。IPv6 アドレスを使用できるのは、クライアント・システムに対して **commmethod V6Tcpip** オプションが指定されている場合だけです。

例:

- server.example.com
- 192.0.2.0
- 2001:0DB8:0:0:0:0:0:0

serverPort
IBM Spectrum Protect サーバーとの通信に使用される TCP/IP ポート番号。 1 から 32767 の範囲の値を指定できます。このパラメーターは必須です。

例: 1500

serverProtocol
クライアント管理サービスと IBM Spectrum Protect サーバー間の通信に使用されるプロトコル。 このパラメーターは必須です。

以下のいずれかの値を指定できます。

値	意味
NO_SSL	SSL セキュリティー・プロトコルは使用されません。
SSL	SSL セキュリティー・プロトコルが使用されます。
FIPS	連邦情報処理標準 (FIPS) モードで TLS 1.2 プロトコルが使用されます。 **ヒント:** あるいは、TLS_1.2 と入力して、TLS 1.2 プロトコルが FIPS モードで使用されることを指定できます。

optPath
クライアント・オプション・ファイルの完全修飾パス。 このパラメーターは必須です。

例 (Linux クライアント): /opt/backup_tools/tivoli/tsm/baclient/dsm.sys

例 (Windows クライアント): C:¥backup tools¥Tivoli¥TSM¥baclient¥dsm.opt

Linux クライアント・システムの例

クライアント・ノード SUSAN のノード定義を client-configuration.xml ファイルに追加します。ノードが通信する IBM Spectrum Protect サーバーは、サーバー・ポート 1500 上の server.example.com です。 SSL セキュリティー・プロトコルは使用されません。クライアント・システム・オプション・ファイルのパスは /opt/tivoli/tsm/client/ba/bin/custom_opt.sys です。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh addnode SUSAN server.example.com 1500 NO_SSL /opt/tivoli/tsm/
client/ba/bin/custom_opt.sys
```

出力:

```
Adding node.

Finished adding client configuration.
```

Windows クライアント・システムの例

クライアント・ノード SUSAN のノード定義を client-configuration.xml ファイルに追加します。ノードが通信する IBM Spectrum Protect サーバーは、サーバー・ポート 1500 上の server.example.com

です。 SSL セキュリティー・プロトコルは使用されません。クライアント・オプション・ファイルのパスは c:¥program files¥tivoli¥tsm¥baclient¥custom.opt です。

C:¥Program Files¥Tivoli¥TSM¥cms¥bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig addnode SUSAN server.example.com 1500 NO_SSL "c:¥program files
¥tivoli¥tsm¥baclient¥custom.opt"
```

出力:

```
Adding node.

Finished adding client configuration.
```

CmsConfig setopt コマンド

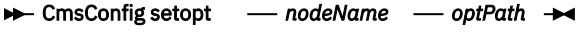
CmsConfig setopt コマンドを使用して、最初にクライアント・オプション・ファイルの内容を読み取らずに、クライアント・オプション・ファイルのパス (通常は dsm.opt) を、既存のノード定義に設定します。

このコマンドは、クライアント・オプション・ファイルが標準的な名前でないか、デフォルト以外の場所にある場合に役立ちます。

要件 : ノード定義が存在しない場合、最初に **CmsConfig addnode** コマンドを発行してノード定義を作成する必要があります。

CmsConfig discover コマンドとは異なり、**CmsConfig setopt** コマンドでは、client-configuration.xml ファイル内に関連付けられたログ定義が作成されません。**CmsComfog addlog** コマンドを使用して、ログ定義を作成する必要があります。

構文



パラメーター

nodeName

ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。 ただし、Linux クライアント・システムなどの複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

optPath

クライアント・オプション・ファイルの完全修飾パス。 このパラメーターは必須です。

例 (Linux クライアント): /opt/backup_tools/tivoli/tsm/baclient/dsm.opt

例 (Windows クライアント): C:¥backup tools¥Tivoli¥TSM¥baclient¥dsm.opt

Linux クライアント・システムの例

ノード SUSAN のクライアント・オプション・ファイル・パスを設定します。クライアント・オプション・ファイルのパスは /opt/tivoli/tsm/client/ba/bin/dsm.opt です。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.opt
```

出力:

```
Adding node configuration file.
```

```
Finished adding client configuration file.
```

Windows クライアント・システムの例

ノード SUSAN のクライアント・オプション・ファイル・パスを設定します。クライアント・オプション・ファイルのパスは c:¥program files¥tivoli¥tsm¥baclient¥dsm.opt です。

C:¥Program Files¥Tivoli¥TSM¥cms¥bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig setopt SUSAN "c:¥program files¥tivoli¥tsm¥baclient¥dsm.opt"
```

出力:

```
Adding node configuration file.
Finished adding client configuration file.
```

CmsConfig setsys コマンド

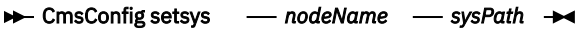
Linux クライアント・システム上で、**CmsConfig setsys** コマンドを使用して、最初にクライアント・システム・オプション・ファイルの内容を読み取ることなく、クライアント・システム・オプション・ファイルのパス (通常は dsm.sys) を既存のノード定義に設定します。

このコマンドは、クライアント・システム・オプション・ファイルが標準的な名前でないか、デフォルト以外の場所にある場合に役立ちます。

要件 : ノード定義が存在しない場合、最初に **CmsConfig addnode** コマンドを発行してノード定義を作成する必要があります。

CmsConfig discover コマンドとは異なり、**CmsConfig setsys** コマンドでは、client-configuration.xml ファイル内に関連ログ定義が作成されません。**CmsComfog addlog** コマンドを使用して、ログ定義を作成する必要があります。

構文



パラメーター

nodeName
ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。 ただし、Linux クライアント・システムなどの 複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

sysPath
クライアント・システム・オプション・ファイルの完全修飾パス。 このパラメーターは必須です。

例: /opt/backup_tools/tivoli/tsm/baclient/dsm.sys

例

ノード SUSAN のクライアント・システム・オプション・ファイル・パスを設定します。クライアント・システム・オプション・ファイルのパスは /opt/tivoli/tsm/client/ba/bin/dsm.sys です。

/opt/tivoli/tsm/cms/bin ディレクトリーから、以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.sys
```

出力:

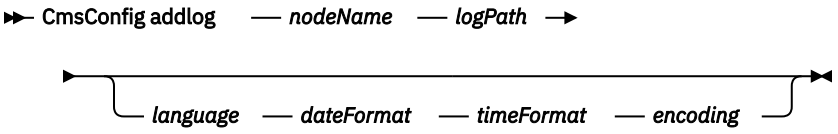
```
Adding node configuration file.
Finished adding client configuration file.
```

CmsConfig addlog コマンド

CmsConfig addlog コマンドを使用して、クライアント・ログ・ファイルの場所を client-configuration.xml 構成ファイルの既存のノード定義に手動で追加してください。このコマンドは、クライアント・ログ・ファイルがクライアント・システム上のデフォルト以外の場所に保管されている場合にのみ使用してください。

要件 : ノード定義が存在しない場合、最初に **CmsConfig addnode** コマンドを発行してノード定義を作成する必要があります。

構文



パラメーター

nodeName
ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。 ただし、Linux クライアント・システムなどの複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

logPath
ログ・ファイルの完全修飾パス。このパラメーターは必須です。

例 (Linux クライアント): /opt/backup_tools/tivoli/tsm/baclient/dsmerror.log

例 (Windows クライアント): C:¥backup tools¥Tivoli¥TSM¥baclient¥dsmerror.log

language
ログ・ファイルの言語ロケール。このパラメーターはオプションです。 ただし、このパラメーターを指定する場合は、**dateFormat**、**timeFormat**、および **encoding** の各パラメーターも指定する必要があります。以下の言語のロケールを指定する必要があります。

言語	ロケール
ブラジル・ポルトガル語	pt_BR
中国語 (簡体字)	zh_CN
中国語 (繁体字)	zh_TW
チェコ語	cs_CZ
英語	en_US
フランス語	fr_FR
ドイツ語	de_DE
ハンガリー語	hu_HU
イタリア語	it_IT
日本語	ja_JP

言語	ロケール
韓国語	ko_KR
ポーランド語	pl_PL
ロシア語	ru_RU
スペイン語	es_ES

dateFormat
クライアント・ログ・ファイルのタイム・スタンプ項目の日付形式。このパラメーターはオプションです。 ただし、このパラメーターを指定する場合は、**language**、**timeFormat**、および **encoding** の各パラメーターも指定する必要があります。

次の表に、言語の日付形式を示します。

ヒント: 表にリストされているいずれかの日付形式を使用する代わりに、バックアップ/アーカイブ・クライアントの **dateformat** オプションを使用して日付形式を指定できます。

言語	日付形式
中国語 (簡体字)	yyyy-MM-dd
中国語 (繁体字)	yyyy/MM/dd
チェコ語	dd.MM.yyyy
英語	MM/dd/yyyy
フランス語	dd/MM/yyyy
ドイツ語	dd.MM.yyyy
ハンガリー語	yyyy.MM.dd
イタリア語	dd/MM/yyyy
日本語	yyyy-MM-dd
韓国語	yyyy/MM/dd
ポーランド語	yyyy-MM-dd
ブラジル・ポルトガル語	dd/MM/yyyy
ロシア語	dd.MM.yyyy
スペイン語	dd.MM.yyyy

timeFormat
クライアント・ログ・ファイルのタイム・スタンプ項目の時刻形式。 このパラメーターはオプションです。 ただし、このパラメーターを指定する場合は、**language**、**dateFormat**、および **encoding** の各パラメーターも指定する必要があります。

次の表に、ユーザーが指定できるデフォルトの時刻形式とクライアント・オペレーティング・システムの例を示します。

ヒント: 表にリストされているいずれかの時刻形式を使用する代わりに、バックアップ/アーカイブ・クライアントの **timeformat** オプションを使用して時刻形式を指定できます。

言語	Linux クライアント・システムの時刻形式	Windows クライアント・システムの時刻形式
中国語 (簡体字)	HH:mm:ss	HH:mm:ss
中国語 (繁体字)	HH:mm:ss	ahh:mm:ss

言語	Linux クライアント・システムの時刻形式	Windows クライアント・システムの時刻形式
チェコ語	HH:mm:ss	HH:mm:ss
英語	HH:mm:ss	HH:mm:ss
フランス語	HH:mm:ss	HH:mm:ss
ドイツ語	HH:mm:ss	HH:mm:ss
ハンガリー語	HH.mm.ss	HH:mm:ss
イタリア語	HH:mm:ss	HH:mm:ss
日本語	HH:mm:ss	HH:mm:ss
韓国語	HH:mm:ss	HH:mm:ss
ポーランド語	HH:mm:ss	HH:mm:ss
ブラジル・ポルトガル語	HH:mm:ss	HH:mm:ss
ロシア語	HH:mm:ss	HH:mm:ss
スペイン語	HH:mm:ss	HH:mm:ss

encoding
クライアント・ログ・ファイルの項目の文字エンコード。 このパラメーターはオプションです。 ただし、このパラメーターを指定する場合は、**language**、**dateFormat**、および **timeFormat** の各パラメーターも指定する必要があります。

Linux クライアント・システムの場合は、標準の文字エンコードは UTF-8 です。Windows クライアント・システムの場合は、デフォルトのエンコード値が次の表に示されています。 クライアント・システムが異なる形式にカスタマイズされている場合は、**encoding** パラメーターを使用して、デフォルト以外の値を指定します。

言語	エンコード
中国語 (簡体字)	CP936
中国語 (繁体字)	CP950
チェコ語	Windows-1250
英語	Windows-1252
フランス語	Windows-1252
ドイツ語	Windows-1252
ハンガリー語	Windows-1250
イタリア語	Windows-1252
日本語	CP932
韓国語	CP949
ポーランド語	Windows-1250
ブラジル・ポルトガル語	Windows-1252
ロシア語	Windows-1251
スペイン語	Windows-1252

Linux クライアント・システムの例

クライアント・ログ・ファイルの場所を client-configuration.xml ファイル内のクライアント・ノード SUSAN の既存の定義に追加します。 クライアント・ログ・ファイルのパスは /usr/work/logs/dsmerror.log です。言語の指定、時刻形式、およびフランス語地域の日付形式を追加します。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh addlog SUSAN /usr/work/logs/dsmerror.log fr_FR yyyy/MM/dd
HH:MM:ss UTF-8
```

出力:

```
Adding log.

Finished adding log.
```

Windows クライアント・システムの例

クライアント・ログ・ファイルの場所を client-configuration.xml 内のクライアント・ノード SUSAN の既存の定義に追加します。 クライアント・ログ・ファイルのパスは c:¥work¥logs¥dsmerror.log です。言語の指定、時刻形式、およびフランス語地域の日付形式を追加します。

C:¥Program Files¥Tivoli¥TSM¥cms¥bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig addlog SUSAN c:¥work¥logs¥dsmerror.log fr_FR yyyy/MM/dd HH:MM:ss
UTF-8
```

出力:

```
Adding log.

Finished adding log.
```

CmsConfig remove コマンド

CmsConfig remove コマンドは、クライアント構成ファイル (client-configuration.xml) からクライアント・ノード定義を削除するために使用します。クライアント・ノード名に関連付けられているすべてのログ・ファイル項目も削除されます。

構文

パラメーター

nodeName
ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。 ただし、Linux クライアント・システムなどの複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

Linux クライアント・システムの例

client-configuration.xml ファイルから SUSAN のノード定義を削除します。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh remove SUSAN
```

出力:

```
Removing node.

Finished removing node.
```

Windows クライアント・システムの例

client-configuration.xml ファイルから SUSAN のノード定義を削除します。

C:¥Program Files¥Tivoli¥TSM¥cms¥bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig remove SUSAN
```

出力:

```
Removing node.

Finished removing node.
```

CmsConfig verify コマンド

CmsConfig verify コマンドを使用して、ノード定義が client-configuration.xml ファイル内で正しく作成されていることを確認します。 ノード定義にエラーがある場合、あるいはノードが正しく定義されていない場合は、適切な **CmsConfig** コマンドを使用してノード定義を修正する必要があります。

構文

パラメーター

nodeName
ログ・ファイルに関連付けられたクライアント・ノード名。大半のクライアント・システムでは、1 つのノード名のみが IBM Spectrum Protect サーバーに登録されています。 ただし、Linux クライアント・システムなどの複数のユーザーがいるシステムでは、複数のクライアント・ノード名がある場合があります。このパラメーターは必須です。

cmsPort
クライアント管理サービス との通信に使用される TCP/IP ポート番号。 クライアント管理サービス のインストール時にデフォルトのポート番号を使用しなかった場合は、ポート番号を指定します。デフォルトのポート番号は 9028 です。このパラメーターはオプションです。

Linux クライアント・システムの例

ノード SUSAN のノード定義が client-configuration.xml ファイル内に正しく作成されていることを確認します。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh verify SUSAN
```

検査プロセス中に、クライアント・ノード名または管理ユーザー ID とパスワードの入力を求められます。

出力:

```
Verifying node.


Verifying the CMS service configuration for node SUSAN.
The CMS configuration looks correct.
```

```
Verifying the CMS service works correctly on port 9028.

Enter your user id: admin
Enter your password:

Connecting to CMS service and verifying resources.
The CMS service is working correctly.
Finished verifying node.
```

Windows クライアント・システムの例

ノード SUSAN のノード定義が client-configuration.xml ファイル内に正しく作成されていることを確認します。

C:¥Program Files¥Tivoli¥TSM¥cms¥bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig verify SUSAN
```

検査プロセス中に、クライアント・ノード名または管理ユーザー ID とパスワードの入力を求められます。

出力:

```
Verifying node.


Verifying the CMS service configuration for node SUSAN.
The CMS configuration looks correct.

Verifying the CMS service works correctly on port 9028.

Enter your user id: admin
Enter your password:

Connecting to CMS service and verifying resources.
The CMS service is working correctly.
Finished verifying node.
```

CmsConfig list コマンド

CmsConfig list コマンドは、クライアント管理サービス構成を表示するために使用します。

構文

Linux クライアント・システムの例

クライアント管理サービスの構成の表示。次に、出力を表示して、コマンドを正しく入力したことを確認します。

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

コマンド:

```
./CmsConfig.sh list
```

出力:

```
Listing CMS configuration

server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
    Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Windows クライアント・システムの例

クライアント管理サービスの構成の表示。次に、出力を表示して、コマンドを正しく入力したことを確認します。

C:¥Program Files¥Tivoli¥TSM¥cms¥bin ディレクトリーから、次のコマンドを発行します。

コマンド:

```
cmsconfig list
```

出力:

```
Listing CMS configuration

server.example.com:1500 NO_SSL SUSAN
Capabilities: [LOG_QUERY]
    Opt Path: C:¥Program Files¥Tivoli¥TSM¥baclient¥dsm.opt

    Log File: C:¥Program Files¥Tivoli¥TSM¥baclient¥dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252

    Log File: C:¥Program Files¥Tivoli¥TSM¥baclient¥dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

CmsConfig help コマンド

CmsConfig ユーティリティー・コマンドの構文を表示するには、**CmsConfig help** コマンドを使用します。

構文

Linux クライアント・システムの例

/opt/tivoli/tsm/cms/bin ディレクトリーから以下のコマンドを発行します。

```
./CmsConfig help
```

Windows クライアント・システムの例

C:¥Program Files¥Tivoli¥TSM¥cms¥bin ディレクトリーから、次のコマンドを発行します。

```
CmsConfig help
```

クライアント管理サービスの拡張機能

デフォルトでは、IBM Spectrum Protect クライアント管理サービスは、クライアント・ログ・ファイルからのみ情報を収集します。 その他のクライアント・アクションを開始するには、クライアント管理サービスに組み込まれている Representational State Transfer (REST) API にアクセスします。

API 開発者は、REST アプリケーションを作成して、以下のクライアント・アクションを開始することができます。

- クライアント・オプション・ファイル (例えば、Linux クライアントの dsm.sys ファイルや、Linux および Windows クライアントの dsm.opt ファイルなど) の照会および更新。
- IBM Spectrum Protect クライアント・アクセプターおよびスケジューラーの 状況の照会。
- クライアント・ノードのファイルのバックアップおよびリストア。
- スクリプトを使用したクライアント管理サービスの機能の拡張。

クライアント管理サービス REST API について詳しくは、Client Management Services REST API Guide を参照してください。

第 12 章 Operations Center のインストールのトラブルシューティング

Operations Center のインストールで問題が発生し、それを解決できない場合は、既知の問題の説明を参照して可能な解決策を探すことができます。

AIX システムでグラフィカル・インストール・ウィザードを開始できない

グラフィカル・ウィザードを使用して AIX システム上に Operations Center をインストールしているときに、インストール・プログラムが開始しません。

解決策

135 ページの『グラフィカル・ウィザードを使用した Operations Center のインストール』 にリストされている RPM ファイルをコンピューターにインストールする必要があります。RPM ファイルがインストールされていることを確認してください。

第 13 章 Operations Center のアンインストール

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

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

IBM Installation Manager のグラフィカル・ウィザードを使用して、Operations Center をアンインストールすることができます。

手順

1. IBM Installation Manager を開きます。

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

   ```
   ./IBMIM
   ```

2. 「**アンインストール**」をクリックします。
3. Operations Center のオプションを選択して、「**次へ**」をクリックします。
4. 「**アンインストール**」をクリックします。
5. 「**終了**」をクリックします。

コンソール・モードでの Operations Center のアンインストール

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

手順

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

   ```
   eclipse/tools
   ```

   例えば次のとおりです。

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

2. tools ディレクトリーから以下のコマンドを発行します。

   ```
   ./imcl -c
   ```

3. アンインストールするには、5 を入力します。
4. IBM Spectrum Protect パッケージ・グループからアンインストールすることを 選択します。
5. 「N」(次へ) を入力します。
6. Operations Center パッケージをアンインストールすることを 選択します。
7. 「N」(次へ) を入力します。
8. 「U」(アンインストール) を入力します。
9. 「F」(終了) を入力します。

サイレント・モードでの Operations Center のアンインストール

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

始める前に

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

Operations Center をアンインストールするには、応答ファイル内の Operations Center 項目について、`modify="false"` を設定したままにします。

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

手順

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

   ```
   eclipse/tools
   ```

   例えば次のとおりです。

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

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

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

   以下にコマンド例を示します。

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

第 14 章 Operations Center の前のバージョンへのロールバック

デフォルトでは、IBM Installation Manager は、更新、フィックス、またはパッケージの以降のバージョンで問題が発生した場合にロールバックするために、パッケージの前のバージョンを保存します。

始める前に

ロールバック機能は、Operations Center が更新された後にのみ使用可能です。

このタスクについて

IBM Installation Manager がパッケージを前のバージョンにロールバックすると、現行バージョンのパッケージ・ファイルがアンインストールされ、前のバージョンが再インストールされます。

前のバージョンにロールバックするには、IBM Installation Manager は、そのバージョンのファイルにアクセスする必要があります。デフォルトでは、それぞれの連続するインストール中に、これらのファイルが保存されます。保存されるファイルの数は、各バージョンのインストールに伴い増加するため、定期的なスケジュールでファイルをシステムから削除することが必要になる場合があります。しかし、ファイルを削除すると、前のバージョンにロールバックできなくなります。

保存されたファイルを削除するか、今後のインストール時にこれらのファイルを保存するためにプリファレンスを更新するには、以下の手順を実行します。

1. IBM Installation Manager で、「**ファイル**」 > 「**プリファレンス**」をクリックします。
2. 「**プリファレンス**」ページで、「**ロールバックのファイル**」をクリックして、プリファレンスを指定します。

手順

- Operations Center の前のバージョンにロールバックするには、IBM Installation Manager の「**ロールバック**」機能を使用します。

付録 A インストール・ログ・ファイル

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

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

付録 B IBM Spectrum Protect 製品ファミリーのアクセシビリティー機能

アクセシビリティー機能は、運動障害または視覚障害など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]

[ワ行]

A

B

C

D

E

F

H

I

K

L

O

R

S

T

U

W

プログラム番号: 5725-W99
5725-W98
5725-X15