SIOS Protection Suite for Windows
Microsoft SQL Server Recovery Kit
v8.6.4

管理ガイド

2019年4月

このドキュメントおよびその内容は SIOS Technology Corp. (旧称 SteelEye® Technology, Inc.) の所有物であり、いかなる無許可での使用および複製も禁じます。SIOS Technology Corp. はこのドキュメントの内容に関していかなる保証も行いません。また、事前の通知なくこの出版物を改訂し、本書に記載された製品に変更を加える権利を保有しています。最新のテクノロジー、コンポーネント、およびソフトウェアを使用して製品を改善するのが SIOS Technology Corp. の方針です。そのため、SIOS Technology Corp. は事前の通知なく仕様を変更する権利を保有しています。

LifeKeeper、SteelEye、および SteelEye DataKeeper は SIOS Technology Corp. の登録商標です。

本書で使用されるその他のブランド名および製品名は識別のみを目的としており、各社の商標である場合があります。

出版物の品質を維持するために、このドキュメントの正確さ、わかりやすさ、構成、および価値に関するお客様のご意見をお寄せください。

宛先:
ip@us.sios.com

Copyright © 2019
By SIOS Technology Corp.
San Mateo, CA U.S.A.
All rights reserved

目次

Chapter 1: はじめに **1**

SIOS Protection Suite Microsoft SQL Server **1**

SQL Server サービス **1**

SQL2008(R2), 2012, 2014, 2016 or 2017: 1

リカバリキットの要件 **2**

Chapter 2: SQL Server のインストール **3**

リカバリキットのインストール **3**

キットの削除 **3**

SIOS Protection Suite とともに SQL Server をインストールおよび設定する **3**

SQL Server をインストールする前に 3

インストール - 共有ストレージシステム **3**

プライマリサーバ上 3

バックアップサーバ上 4

プライマリサーバ上 4

SQL Server ソフトウェアのインストール 4

ターゲットシステムで管理者ではないローカルシステムアカウントを使用する 5

インストール - 複製ストレージシステム **5**

プライマリサーバ上 5

バックアップサーバ上 6

プライマリサーバ上 6

拡張構成の追加のセットアップ作業 **7**

SQL 階層の作成 **7**

SQL 階層の拡張 **8**

SQL 階層の拡張解除 **9**

SQL 階層の削除 **9**

Chapter 3: SQL Server 設定上の考慮事項 **11**

SQL 構成 11

フェイルオーバ 12

複数の SQL インスタンス 12

SQL Server の設定管理 **13**

プロセス設定メニュー **14**

データベース設定メニュー **15**

管理操作メニュー **15**

管理ユーザメニュー **15**

SQL リソース階層のテスト **16**

Chapter 4: SQL Server 階層の管理 **17**

保護されたコミュニケーションパス経由でアクセスする **17**

リモートアクセスにリソース名を使用する **17**

ボリュームを SQL 専用にする **17**

SQL Server 環境での手動スイッチオーバの制限について **17**

Microsoft SQL Management ツールの実行 **17**

SQL Server の起動と停止は SIOS Protection Suite 上で実行する **17**

Microsoft SQL Server ボリュームの追加 **18**

スイッチオーバ後にデータベースの「Suspect」状態から回復 **18**

Microsoft SQL Server (MSSQLServer) の一時停止 **19**

切り替え可能な IP アドレスで接続するように SQL Server を設定 **19**

SQL Server のログインおよびパスワードの管理 **19**

SQL 階層の監視 **19**

Chapter 5: トラブルシューティング **20**

マスタ、あるいはユーザデータベースがシステムドライブにある場合リソースの作成や拡張に失敗する **20**

現象 20

推奨される処置 20

SQL リソースの拡張に失敗する **20**

現象 20

推奨される処置 21

名前付きインスタンスで SQLAgent サービスを開始できない **21**
現象 21
推奨される処置 21
SQL Server の名前付きインスタンスへの ODBC クライアントの接続 **21**
現象 21
推奨される処置 22

Chapter 1: はじめに

SIOS Protection Suite Microsoft SQL Server

SIOS Protection Suite Microsoft SQL Server Recovery Kit ソフトウェアを使用すると、Microsoft SQL を使用したデータベースのデータの完全性と、SIOS Protection Suite for Windows による可用性の向上に結び付けることができます。

LifeKeeper GUI によって、SQL リソース階層を簡単に作成できるようになります。SIOS Protection Suite は、SQL Server インスタンスが使用するすべてのディスクリソースはもちろん、データベースアクセスに使用される IP ソケットリソースも保護します。

重要:本キットでは、SQL Serverの次の機能を利用できません: SQLレプリケーション(スナップショット、マージ、トランザクション) 、SQLのログ配布、SQLデータベースのミラーリング、SQL Server AlwaysOn 可用性グループ

SQL Server サービス

SIOS Protection Suite Microsoft SQL Server Recovery Kit は次のサービスを監視および保護します。

SQL2008(R2), 2012, 2014, 2016 or 2017:

コアサービス	オプションサービス
SQL Server (MSSQLSERVER)	SQL Server Agent
	SQL Server Reporting Services
	Distributed Transaction Coordinator
	SQL Server Browser
	SQL Server VSS Writer
	SQL Server Integration Services
	SQL Full-text Filter Daemon Launcher (SQL Server 2014 より利用可能)
	SQL Server Launchpad (SQL Server 2016 より利用可能)
	SQL Server PolyBase Data Movement (SQL Server 2016 より利用可能)
	SQL Server PolyBase Engine (SQL Server 2016 より利用可能)
	SQL Server CEIP service (SQL Server 2016 より利用可能)

注記 :「SQL Server Integration Services」は、SQL Server のオプションとしてのその機能をインストールする際に、保護するオプションサービスのリストに表示されます。

データファイルは共有ボリュームまたは複製ボリュームに格納されます。SIOS Protection Suite は障害を検出すると、データベースとともに、関連するボリュームとIP ソケットリソースをバックアップサーバに切り替えます。SIOS Protection Suite は、すべての依存リソースをバックアップサーバに切り替えると、SQL サービスおよび保護対象のオプションサービスを起動します。

リカバリキットの要件

SIOS Protection Suite Microsoft IIS Recovery Kit をインストールして設定する前に、構成が以下の要件を満たしていることを確認してください。

- SIOS Protection Suite は、SIOS Protection Suite for Windows リリースノートのオペレーティングシステムに記載されている Windows オペレーティングシステムをサポートします。
- **SIOS Protection Suite ソフトウェア**。クラスタ内のすべてのサーバに同じバージョンの SIOS Protection Suite for Windows をインストールする必要があります。共有ストレージではなく複製ボリュームで Microsoft SQL Server を使用する計画を立てている場合は、SIOS DataKeeper for Windows ソフトウェアを各サーバ上にインストールする必要があります。
- **Microsoft SQL Server RDBMS ソフトウェア**。このキットは Microsoft SQL2008(R2)、2012 または 2014 の全バージョンに対して互換性があります。ただし、クラスタ内のすべてのシステム上に同じバージョンの Microsoft SQL Server がインストールされている必要があります。
- **通信プロトコル**。Microsoft はクラスタ環境では TCP/IP を使用するように強く推奨しています。SIOS Protection Suite は LAN Manager をサポートしますが、このドキュメントはユーザが TCP/IP を使用していることを前提とし、設定の説明では LAN Manager リソースではなく切り替え可能 IP リソースについて説明しています。

リリースおよびご注文につきましては、弊社の SIOS Protection Suite 営業担当者にお問い合わせください。

Chapter 2: SQL Server のインストール

SIOS Protection Suite Microsoft SQL Server Recovery Kit を適切に操作するには、ハードウェアとソフトウェアを正しくセットアップする必要があります。

最初に、このガイドの「階層の管理」セクションを参照してください。このセクションでは、SIOS Protection Suite 環境における Microsoft SQL Server の管理に役立つ一般的なガイドライン、設定の詳細、トラブルシューティングのヒントを提供します。

リカバリキットのインストール

SIOS Protection Suite Microsoft SQL Server Recovery Kit は FTP ダウンロードで配布されます。インストールは、標準のインストールインターフェースを提供する InstallShield を使用して、簡単にすばやく実行できます。

SIOS Protection Suite Microsoft SQL Server Recovery Kit ソフトウェアをインストールする前に、製品の前提条件をよく理解していることを確認してください。SIOS Protection Suite で SQL リソースを保護するには、SIOS Protection Suite Microsoft SQL Server Recovery Kit ライセンスキットをインストールする必要があります。

キットの削除

SIOS Protection Suite Microsoft SQL Server Recovery Kit ソフトウェアを削除するには、コントロールパネルの **[プログラムの追加と削除]** または **[プログラムと機能]** アプレットにある **Microsoft SQL Server Recovery Kit** を選択してください。

注意: キットを削除するときには、サービス中の SQL インスタンスおよびリソースが存在しないことを確認してください。キットが削除されると、これらのリソースは使用できなくなります。また、キットを削除する前にすべての SQL 階層を削除してください。

SIOS Protection Suite とともに SQL Server をインストールおよび設定する

SIOS Protection Suite Microsoft SQL Server Recovery Kit を適切に操作するには、ハードウェアとソフトウェアを正しくセットアップする必要があります。

このセクションでは、SIOS Protection Suite 環境における Microsoft SQL Server の管理に役立つ一般的なガイドライン、設定の詳細、トラブルシューティングのヒントを提供します。階層の管理作業についての再確認を忘れないでください。

SQL Server をインストールする前に

SQL Server ソフトウェアをインストールする前に、サーバとストレージが設定され、SIOS Protection Suite がクラスタ内の各サーバにインストールされている必要があります。

インストール - 共有ストレージシステム

プライマリサーバ上

1. バックアップサーバの電源を落とします。これは、共有ストレージへの同時アクセスが発生しないようにするためです。
2. **Windows ディスク管理** ツールを使用して、ディスクリソースを設定し、使用したい共有ボリュームを定義します。(ボリュームは適

切なサイズにしてください。)

3. **Windows エクスプローラ**を使用して、SQL Server インスタンスによって使用されるすべてのボリュームをネットワークから共有解除します。
4. ネットワークを、SIOS Protection Suite TCP/IP コミュニケーションパスと切り替え可能な IP アドレス(該当する場合)をサポートするように設定します。
5. SIOS Protection Suite Core ソフトウェア、SIOS Protection Suite SQL Server Recovery Kit の順にローカルディスクにインストールします。

バックアップサーバ上

1. バックアップサーバを起動し、**ディスク管理**ユーティリティを使用して、プライマリサーバに割り当てたものと同じドライブレターを共有ボリュームに割り当てます。
2. SIOS Protection Suite Core ソフトウェア、SIOS Protection Suite SQL Server Recovery Kit の順にローカルディスクにインストールします。

プライマリサーバ上

これで両方のサーバに SIOS Protection Suite がインストールされました。プライマリサーバに戻って、以下を実行してください。

1. SIOS Protection Suite で、プライマリサーバとバックアップサーバの間のコミュニケーションパスを作成します。
2. SIOS Protection Suite でボリュームリソースと IP コミュニケーションパスを作成し、それらをバックアップサーバに拡張します。その後、SQL Server リソース階層を作成するときに、SIOS Protection Suite は依存関係に従ってこれらのリソースを自動で階層内に移動します。

SQL Server ソフトウェアのインストール

1. 共有ボリュームを使用している場合は、LifeKeeper GUI を使用してバックアップサーバ上でボリュームリソース階層を[サービス開始]にします。
2. 以下のガイドラインに従って、バックアップサーバに Microsoft SQL Server をインストールします。
   - 追加の機能と共に、データベースエンジンをインストールします。インスタンスデータとログファイルを、SIOS Protection Suite によって保護されているボリュームに格納されるように設定します。
   - 「**混合モード**」のデータベース認証を選択し、SA アカウント用の空白でないパスワードを入力します。パスワードは、クラスター内のすべてのサーバーで同一にする必要があります。

   インストールが完了したら **Microsoft SQL Server Configuration Manager** を使用して、バックアップサーバ上で SQL Server が正しく起動されるかどうかを確認します。バックアップサーバ上の Microsoft SQL サービスをすべて停止してください。

   共有ボリュームに対して、以下の手順を実行してください。

   1. プライマリサーバ上で、ボリュームリソース階層を[サービス開始]にします。
   2. プライマリサーバ上で**エクスプローラ**を開き、共有ボリュームに関連付けられたドライブにアクセスします。

3. 以前に SQL データファイルをインストールしたディレクトリを削除します。(これらのディレクトリは次の手順で再インストールします。)
4. Microsoft SQL Server を、バックアップサーバとまったく同じ方法でプライマリサーバにインストールします (プログラムファイルをローカルディスク、データファイルを共有ボリュームにインストール)。

インストールが完了したら、**Microsoft SQL Server Configuration Manager** を使用して、プライマリサーバ上で SQL Server が正しく起動されるかどうかを確認します。

ターゲットシステムで管理者ではないローカルシステムアカウントを使用する

特定の状況で、SQL Server サービスアカウント (sql_svc) をローカル管理者グループまたはドメイン管理者グループに追加することができない場合があります。このような場合、そのサービスアカウントでファイルの権限の問題が発生します。ユーザには、以下のようなメッセージで「アクセス拒否」エラーが通知されます。

```
"Open failed: Could not open file E:\SQL1\MSSQL10_
50.SQL1\MSSQL\DATA\master.mdf for file number 1. OS error: 5 (Access is
denied)."
```

解決策: 以下を実行してください。

1. ファイル (例: c:\file.ksh) に以下のスクリプトコードをコピーします。

```
$LKROOT/bin/find .>$LKROOT/out/file
while read filename
do
icacls "${filename}" /grant $1:F
done < $LKROOT/out/file
$LKDROOT/bin/rm $LKROOT/out/file
```

2. 各ドライブ (E、F) で以下のコマンドを実行して、ボリュームで起動します。このコマンドは管理者 (ローカルまたはドメイン) として実行してください。これによって、当該ユーザのみにファイル権限が付与されます。SQL Server サービスユーザはファイルにアクセスできるようになり、管理者アカウントとして追加する必要はありません。

```
E:\>c:\lk\bin\sh c:\file.ksh domain\sql_svc
```

注記: この例では、SteelEye Protection Suite は c:\lk にインストールされており、domain\sql_svc は SQL Server サービスユーザ ID の名前です。

インストール - 複製ストレージシステム

プライマリサーバ上

1. **[Windows ディスク管理]** ツールを使用して、ディスクリソースを設定し、使用したい複製ボリュームを定義します。(ボリュームは適切なサイズにしてください。)
2. **Windows エクスプローラ**を使用して、SQL Server によって使用されるすべてのボリュームをネットワークから共有解除します。

3. ネットワークを、SIOS Protection Suite TCP/IP コミュニケーションパスと切り替え可能な IP アドレス (該当する場合) をサポートするように設定します。
4. SIOS Protection Suite Core ソフトウェア、SIOS Protection Suite SQL Server Recovery Kit の順にローカルディスクにインストールします。
5. SIOS DataKeeper ソフトウェアをローカルディスクにインストールします。詳細については、SIOS Protection Suite for Windows インストレーションガイドを参照してください。
6. LifeKeeper GUI を使用して、プライマリサーバとバックアップサーバの間のコミュニケーションパスを作成します。
7. SIOS Protection Suite で IP コミュニケーションパスを作成し、それらをバックアップサーバに拡張します。その後、SQL Server リソース階層を作成するときに、SIOS Protection Suite は依存関係に従ってこれらのリソースを自動で階層内に移動します。

   注記: SQL Server 階層が作成されるとき、SIOS DataKeeper リソースは自動的に作成され、依存関係に従って SQL Server リソース階層に移動されます。

バックアップサーバ上

1. **LifeKeeper GUI** を使用して、ボリュームリソース階層をサービス開始の状態にします。
2. 以下のガイドラインに従って、Microsoft SQL Server をインストールします。
   - 追加の機能と共に、データベースエンジンをインストールします。インスタンスデータとログファイルを、SIOS Protection Suite によって保護されているボリュームに格納されるように設定します。
   - 「**混合モード**」のデータベース認証を選択し、SA アカウント用の空白でないパスワードを入力します。パスワードは、クラスター内のすべてのサーバーで同一にする必要があります。
3. インストールが完了したら **Microsoft SQL Server Configuration Manager**を使用して、バックアップサーバ上で SQL Server が正しく起動されるかどうかを確認します。バックアップサーバ上の Microsoft SQL サービスをすべて停止してください。**注記**: 複製ボリュームの場合、*SQL tempdb* データベースを SIOS Protection Suite で保護されていないボリュームに移動してパフォーマンスを改善することもできます。
4. Microsoft SQL Server を、バックアップサーバとまったく同じ方法でプライマリサーバにインストールします (プログラムファイルをローカルディスク、データファイルを複製ボリュームにインストール)。
5. インストールが完了したら **Microsoft SQL Server Configuration Manager**を使用して、プライマリサーバ上で SQL Server が正しく起動されるかどうかを確認します。

   注記: データファイルが複製ボリュームにインストールされた場合、*SQL tempdb* データベースを SIOS Protection Suite で保護されていないボリュームに移動してパフォーマンスを改善することもできます。

プライマリサーバ上

1. プライマリサーバ上で、**通信リソース**をサービス中にします。
2. プライマリサーバ上で **SQL Server サービス**を開始します。
3. プライマリサーバ上に **SQL Server 階層**を作成して、バックアップサーバに拡張します。**ボリュームリソースの拡張**処理中に、**作成された複製のミラー**を選択し、**[次へ]** を選択してウィザードを終了します。設定はこれで完了です。詳細については、SQL 階層の作成を参照してください。

手動でフェイルオーバを実行し、新しい **SQL Server 階層**をテストしてください。

拡張構成の追加のセットアップ作業

ご利用の設定で共有のストレージデバイスを使用している場合、または SIOS DataKeeper を使用している場合は、3 番目 (またはそれ以上) のサーバに拡張する設定を選択することができます。

1. SIOS Protection Suite による SQL Server のインストールおよび設定に示されている手順で 2 つのシステムを設定します。
2. 保護対象ボリュームを 3 番目のサーバに切り替えます。
3. Microsoft SQL Server ソフトウェアをローカルドライブにインストールし、マスターデータベースを他のサーバが使用しているものと同じ共有ボリューム / 複製ボリューム上にインストールします。こうすることで、階層を拡張して SIOS Protection Suite のカスケーディング機能を使用できるようになります。

SQL 階層の作成

SIOS Protection Suite for Windows インストレーションガイドに記述されている必要なセットアップ作業が完了したら、以下の手順に従ってデータベースを保護する SQL Server 階層を定義してください。

重要	既存の SQL データベースがインストールされている場合、この手順を完了する前に SQL データベースにアクセスしているすべてのクライアントアプリケーション (ローカル、リモートにかかわらず) を閉じる必要があります。オペレーションは自動化されており、その間にデータベースの起動と再起動が複数回行われ、実行中アプリケーションは各サービス動作のコマンドの影響を受ける可能性があります。そのため、この手順が完了した後にアプリケーションを再起動してください。

1. LifeKeeper GUI メニューから **[編集]** を選択し、次に **[サーバ]** を選択します。メニューから **[リソース階層の作成]** を選択します。
2. **[保護するアプリケーションの作成]** ダイアログボックスが表示されます。プルダウンリストから**プライマリ**および**バックアップ**サーバを選択します。**[次へ]** を選択して続行します。
3. ダイアログボックスはクラスタ内にインストールされたすべての認証済みのリカバリキットが表示されたドロップダウンリストボックスとともに表示されます。**[MS SQL Server]** を選択し、**[次へ]** をクリックします。
4. 次の表に示す情報を入力するように求められます。ダイアログボックス内で **[戻る]** ボタンがアクティブになっているときは、直前のダイアログボックスに戻ることができます。これは、前に入力した情報を修正する必要があるエラーが発生した場合に便利です。いつでも **[キャンセル]** をクリックして、作成処理全体を取り消すことができます。

フィールド	説明
Microsoft SQL Server のインスタンスの選択	SIOS Protection Suite で保護する Microsoft SQL Server のインスタンスを選択します。 SIOS Protection Suite は、このインスタンスの設定データを読み込み、関連ボリュームを階層に組み込みます。
Microsoft SQL 管理ユーザ名の入力	このサーバで Microsoft SQL の管理権限を持つユーザの名前を入力してください。管理ユーザアカウントはマスタデータベースに対する SA 権限を持っている必要があります。
パスワードの入力	入力したユーザアカウントの管理パスワードを入力してください。

フィールド	説明
設定の確認	データベースファイルの現在の位置を示します。SIOS Protection Suite を使用して保護するインスタンスに関連するファイルがシステムドライブ (C:) に配置されていた場合、その場所をハイライトで示します。
以下のフィールドはデータベースの再配置が必要な場合にのみ表示されます。	
データベースを再配置するボリュームの選択	データベースのマイグレーションが必要な場合に、影響を受けるデータベースを保存するボリュームを選択してください。
MOVE オペレーションの確認	選択したデータベースの配置場所と内容について確認してください。
データベースの再配置	MOVE オペレーション時に、データベースを再配置する処理の経過を操作ウィンドウに表示します。
保護対象のオプショナルサービスの選択	この階層で保護されるオプションの SQL サービスを選択してください。このリストには LifeKeeper の保護に適したサービスのみが表示されます。
保護する IP アドレス	インスタンスで保護する IP アドレスを選択してください。名前付きパイプだけを使用する場合、IP アドレスは不要です。ただし、名前付きパイプだけの使用は避けてください。
名前付きパイプの別名	名前付きパイプの別名
Microsoft SQL Server のリソース名	固有のタグ名を入力します。自動で表示されるデフォルトのタグ名をそのまま使用することもできます。 **注意**：タグ名に使用できる文字はASCII印字可能文字のみです。

5. **[作成]** をクリックすると、**ウィザード** により SQL リソースが作成されます。SIOS Protection Suite によって入力データが検査されます。SIOS Protection Suite が問題を検出すると、情報ボックスにエラーメッセージが表示されます。
6. 別の情報ボックスが表示され、SQL リソース階層の作成に成功したこと、およびフェイルオーバによって保護するには、クラスタ内の別のサーバにリソース階層を**拡張**する必要があることを示すメッセージが表示されます。**[次へ]** をクリックします。
7. **[続行]** をクリックすると SIOS Protection Suite の**拡張前処理ウィザード** が起動されます。

SQL 階層の拡張

この操作は **[編集]** メニューから開始できますが、**[リソース階層の作成]** オプションの処理を完了すると自動的に開始されます。その場合は、下記の手順 2 を参照してください。

1. **[編集]** メニューの **[リソース]** から **[リソース階層の拡張]** を選択します。**[拡張前処理ウィザード]** が表示されます。**拡張**操作に慣れていない場合は、**[次へ]** をクリックしてください。
2. **[拡張前処理ウィザード]** では引き続き情報の入力を求めるメッセージが表示されます。**注記**: 最初の 2 つのフィールドは、**[編集]** メニューから**拡張**を開始した場合のみ表示されます。
3. 拡張前のチェックが正常に終了したというメッセージが表示されたら、**[次へ]** をクリックします。

フィールド	説明

バックアップの優先順位	1～999 の数値を入力して、このリソースのカスケーディングフェイルオーバシーケンスにおけるテンプレートサーバの優先順位を指定してください。小さい数値ほど優先順位が高くなります。SIOS Protection Suite は、階層が作成されたサーバに「1」を割り当てます。特定のリソースに関して 2 台のサーバが同じ優先順位を持つことはできません。

4. **[拡張]** をクリックします。

重要	データベースを移動させた後に、SQL アプリケーションとデータベースファイルにアクセスできることを確認する必要があります。すべてのファイルは、システムコピーユーティリティを使用して再配置されます。この手順が正常に完了していることを確認した後、関連するデータとログファイルを削除することができます。

SQL 階層の拡張解除

SIOS Protection Suite クラスタの 1 つのサーバからリソース階層を削除する場合は、次の手順を実行してください。

1. **[編集]** メニューの **[リソース]** から **[リソース階層の拡張解除]** を選択します。
2. SQL リソースの拡張解除の対象となる**ターゲットサーバ**を選択します。SQL リソースが現在 In Service のサーバは選択できません。(右側のペインにあるリソースインスタンスを右クリックして**拡張解除**作業を選択した場合、このダイアログボックスは表示されません。)**[次へ]** をクリックします。
3. 拡張解除する SQL 階層を選択し、**[次へ]** をクリックします。(左右どちらかのペインのリソースインスタンスを右クリックして**拡張解除**作業を選択した場合、このダイアログボックスは表示されません。)
4. 拡張解除するために選択したターゲットサーバと SQL リソース階層を確認する情報ボックスが表示されます。**[拡張解除]** をクリックします。
5. SQL リソースの拡張解除に成功したことを通知する情報ボックスが表示されます。**[完了]** をクリックして、**[リソース階層の拡張解除]** メニューを終了します。

SQL 階層の削除

SQL 階層または SQL インスタンスを削除する前に、プライマリサーバでその階層がアクティブ (緑色) になっていることを確認してください。階層を削除する前に依存関係を解除することもできます。依存関係を解除しないと、それも削除されます。

SIOS Protection Suite 環境のすべてのサーバからリソース階層を削除するには、次の手順を実行してください。

1. **[編集]** メニューの **[リソース]** を選択し、次に **[リソース階層の削除]** を選択します。
2. SQL リソース階層を削除する**ターゲットサーバ**の名前を選択し、**[次へ]** をクリックします。(左右どちらかのペインのリソースインスタンスを右クリックして**リソース削除**作業を選択した場合、このダイアログボックスは表示されません。)
3. **削除する階層**を選択します。(左右どちらかのペインのリソースインスタンスを右クリックして**リソース削除**作業を選択した場合は、このダイアログボックスは表示されません。)**[次へ]** をクリックします。
4. 選択したターゲットサーバと削除対象として選択した階層を確認する情報ボックスが表示されます。**[次へ]** をクリックします。

5. SQL リソースの削 除 に成 功したことを通 知 する情 報 ボックスが表 示 されます。
6. **[完 了]** をクリックして終 了 します。

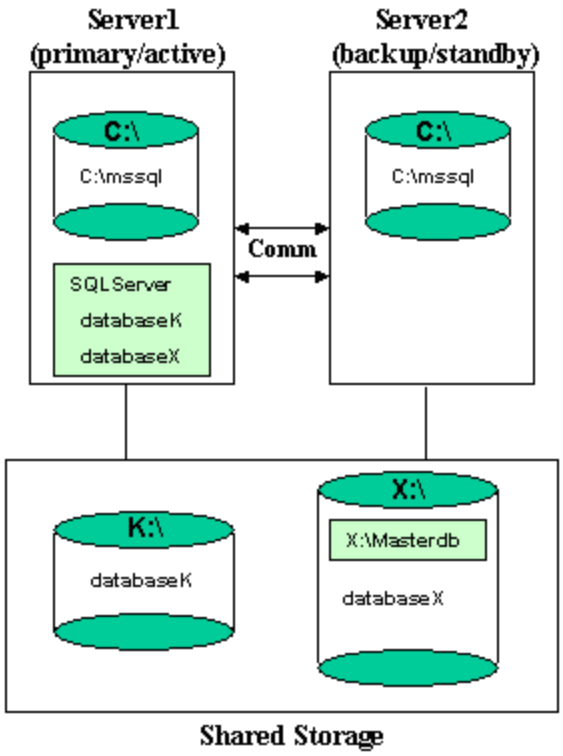
Chapter 3: SQL Server 設定上の考慮事項

クラスタをインストールして設定する前に、アクティブ/スタンバイ構成の概念と、複数のインスタンスを SQL 構成で設定する方法を理解することが重要です。

SQL 構成

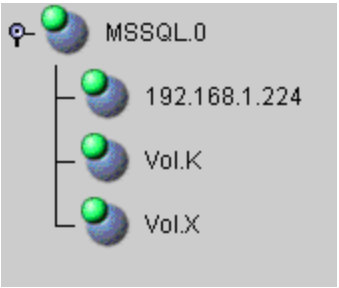
各 SQL Server にマスタデータベースが 1 つしかなく、それを共有ボリュームまたは複製ボリュームに配置した場合、クラスタはアクティブ/スタンバイ構成になります。サービスは一度に 1 つのシステムだけで実行されます。サーバには、SIOS Protection Suite 内部で優先順位が割り当てられ、特定の階層をフェイルオーバする順序が決定されます。

1 組のサーバに 1 つの SQL インスタンスをインストールした状態を次図に示します。インスタンスには 2 つのデータベース (databaseK と databaseX) があり、各データベースは個別のボリュームに格納されています。マスタデータベースは 1 つであり、共有ボリューム X に格納されていることに注意してください。



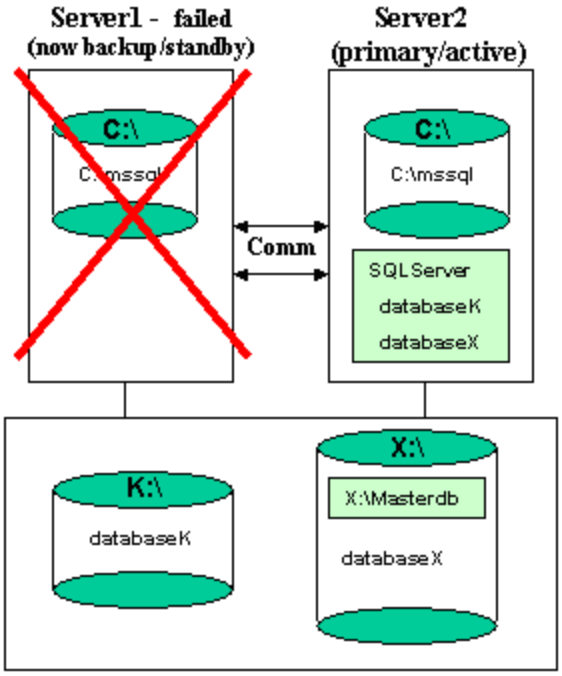
SIOS Protection Suite 内に SQL 階層を作成すると、保護する SQL インスタンス、およびデータベース接続に使用する IP リソースを指定するように求められます。SIOS Protection Suite は、そのインスタンスの設定データを読み込み、指定されたボリュームを階層に組み込みます。

作成した階層は、LifeKeeper GUI に次のように表示されます。



フェイルオーバ

SIOS Protection Suite は、障害が発生すると、バックアップサーバの SQL Server 階層をサービス中にします。バックアップサーバの SQL Server が起動して、定義済みデータベースの保護を引き継ぎます (次図参照)。

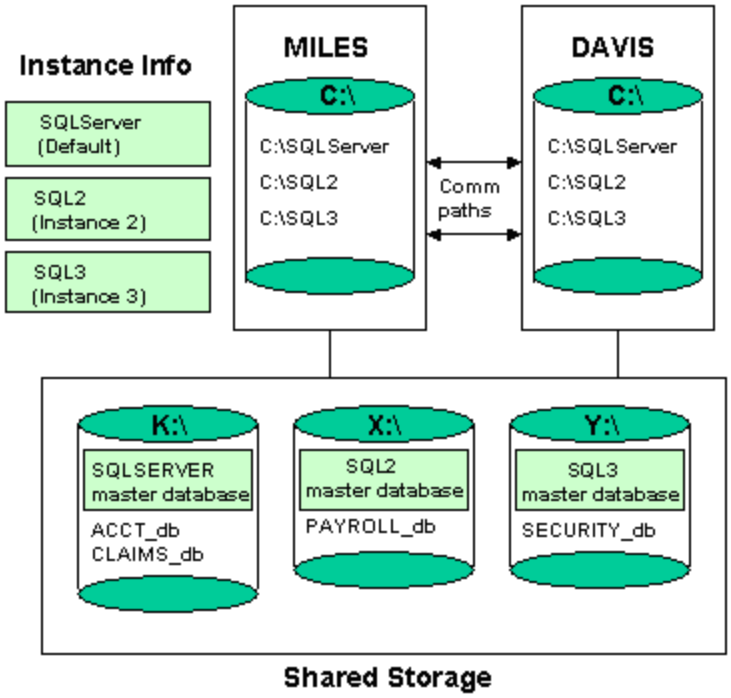


複数の SQL インスタンス

SQL Server を複数回インストールして、複数の SQL インスタンスを作成できます。SIOS Protection Suite は SQL Server の複数のインスタンスを保護できます。SIOS Protection Suite は、SQL のインストール時に指定された固有の名前でインスタンスを識別します。

1 つの SQL インスタンスには複数の SQL データベースを登録できます。各インスタンスは単一の SIOS Protection Suite 階層で保護されます。したがって、SQL インスタンスに 2 つのデータベースがある場合、対応する SIOS Protection Suite 階層は 2 つのデータベースと関連する IP とボリュームリソースを保護します。

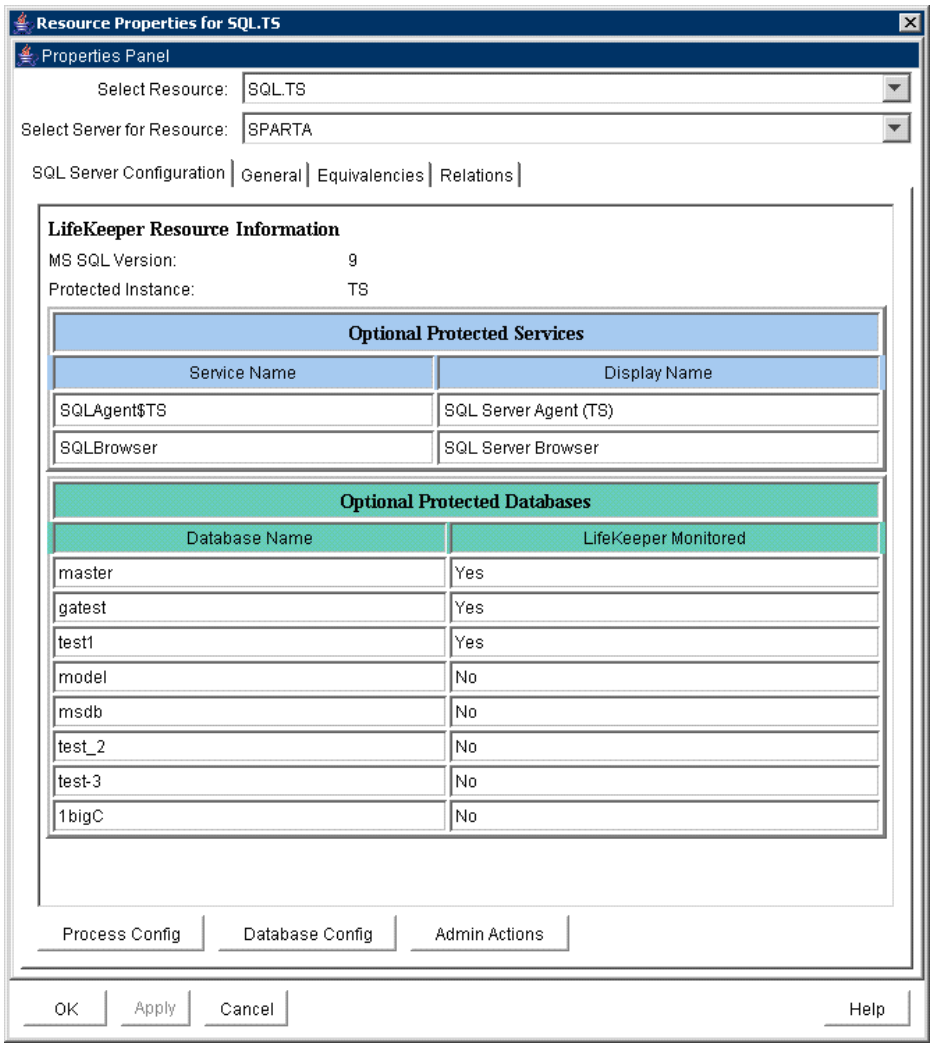
下の図は、SQLServer (デフォルトのインスタンス)、SQL2、SQL3 の 3 つの SQL インスタンスです。これらのインスタンスは 1 組のサーバ (MILES と DAVIS) にインストールされています。



注記	• データベースは 3 つの異なる共有ストレージボリューム (K、X、Y) に格納されています。デフォルトのインスタンスには 2 つのデータベース、残り 2 つのインスタンスにはそれぞれ 1 つのデータベースが格納されていることに注意してください。 • 各サーバは複数のインスタンスのプライマリサーバとバックアップサーバとして動作します。 • MILES がデフォルトインスタンスのプライマリサーバになり、DAVIS が SQL2 と SQL3 インスタンスのプライマリサーバになることも可能です。

SQL Server の設定管理

LifeKeeper GUI を使用して保護対象の SQL Server リソースを管理するには、LifeKeeper GUI の右側のペインで SQL Server リソースを右クリックし、**[プロパティ]**、**[SQL Server 設定]** タブの順にクリックします。**[SQL Server 設定]** ページでは、SQL リソースの情報を参照または変更できます。



プロセス設定メニュー

このメニューでは、リソース階層で保護されているオプションの SQL プロセス一覧を変更できます。SIOS Protection Suite は保護されているすべてのオプションサービスを監視します (SQL 階層の監視を参照してください)。

操作の選択

- *プロセスの追加* - 保護対象の構成にプロセスを追加します。SIOS Protection Suite は新しい SQL サービスの監視を開始します。
- *プロセスの削除* - 保護対象の構成からプロセスを削除します。

フィールド	説明
サービス名	保護対象の構成に**追加**または**削除**するサービス名を入力してください。
すべてのシステムを更新	該当のクラスタ内のすべてのシステムを更新する場合は、**[はい]**を選択してください。それ以外の場合は、**[いいえ]**を選択して現在のシステムだけを更新します。**[いいえ]**を選択した場合は、プロセスを手動でバックアップサーバに追加する必要があります。

データベース設定メニュー

このメニューでは、リソース階層で保護するオプションのSQLデータベースを変更します。SIOS Protection Suiteは SQLクエリを発行してデータベースとの接続をテストし、保護対象のSQLデータベース(オプション)を監視します (SQL階層の監視を参照してください)。

操作の選択:

- *データベースの追加* - 保護対象の設定にデータベースを追加します。**注記**: このオプションは、SQLリソースがアクティブ (サービス中) になっているサーバだけに使用できます。
- *データベースの削除* - 保護対象の設定からデータベースを削除します。

フィールド	説明
データベース名の入力	保護対象の設定に**追加**または**削除**するデータベースの名前を入力してください。
すべてのシステムを更新	該当のクラスタ内のすべてのシステムを更新する場合は、**[はい]**を選択してください。それ以外の場合は、**[いいえ]**を選択して現在のシステムだけを更新します。**[いいえ]**を選択した場合は、プロセスを手動でバックアップサーバに追加する必要があります。

管理操作メニュー

このメニューでは、SIOS Protection Suiteを操作するSQL管理ユーザを管理します。または階層を拡張する際、プライマリサーバとバックアップサーバとの間で発生したID競合も解決します。

[管理操作]の選択

- *ユーザ管理* - 保護対象のリソース階層が使用する現在のユーザ名を表示または更新します。

管理ユーザメニュー

管理作業の選択

- *現在のユーザを表示* - 保護対象のリソース階層で使用される現在のユーザ名を表示します。
- *パスワードの変更* - 保護対象のリソース階層に関連付けた現在のユーザのパスワードを変更します。

- *ユーザおよびパスワードの変更* - SIOS Protection Suite の操作の際に SQL インスタンスを管理監視するユーザとパスワードの両方を更新します。ユーザは、保護下にあるすべてのデータベースに対して sqladmin 権限を持つ必要があります。

注記: ユーザおよびパスワードを変更するには、SQL インスタンスが実行されている必要があります。

フィールド	説明
ユーザ名の入力	管理ユーザ名を入力してください。管理ユーザのアカウントには、SIOS Protection Suite で保護する全データベースに対する SA パーミッションを付与する必要があります。
パスワードの入力	更新するユーザアカウントの管理パスワードを入力してください。

ID 不一致の解決 (SQL 2005 のみ)

フィールド	説明
サービスの種類の選択	レジストリを修復して、SIOS Protection Suite による保護を許可するサービスを選択してください。 プライマリサーバとバックアップサーバの SQL Server サービス ID だけが異なる場合は、**[Sql]** を選択してください。 プライマリサーバとバックアップサーバの SQL OLAP Service ID だけが異なる場合は、**[Olap]** を選択してください。 プライマリサーバとバックアップサーバの SQL Reporting Service ID だけが異なる場合は、**[Rs]** を選択してください。 **Sql**、**Rs**、**Olap** サービスを同時に更新する場合は、**[All]** を選択してください。
テンプレートサーバの選択	修復するリソースのテンプレートサーバ (プライマリ) を選択します。テンプレートサーバは、サービス中 (ISP) のリソースを保持する必要があります。
ターゲットサーバの選択	修復するリソースのターゲット (バックアップ) サーバを選択します。ターゲットサーバは、サービス中 (ISP) のリソースを保持していてはなりません。
確認	上記で入力した情報が正確かどうかを確認します。処理を実行するには **[続行]**、情報を変更するには **[戻る]**、キャンセルする場合は **[キャンセル]** を選択してください。

SQL リソース階層のテスト

手動スイッチオーバを開始すると、SQL リソース階層をテストできます。これにより、リソースインスタンスのプライマリサーバからバックアップサーバへのフェイルオーバがシミュレートされます。

[編集]、**[リソース]**、**[サービス開始]** の順に選択。例えば、バックアップサーバでサービス開始要求を実行すると、アプリケーション階層はプライマリサーバでサービス停止になり、バックアップサーバではサービス開始となります。この時点で、元のバックアップサーバがプライマリサーバとなり、元のプライマリサーバがバックアップサーバとなります。

[サービス停止] の要求を実行した場合、このアプリケーションはサービス停止になり、別のサーバのアプリケーションはサービス開始になりません。

Chapter 4: SQL Server 階層の管理

SQL Server の管理は、以下のガイドラインどおりに行ってください。

保護されたコミュニケーションパス経由でアクセスする

サービスへのリモートアクセスは、リソース階層によって保護されている IP アドレスで行う必要があります。これにより、どのサーバが現在実行中かにかかわらず、ユーザは SQL サービスに確実にアクセスできます。

リモートアクセスにリソース名を使用する

アプリケーションがクラスタに対応していない場合、**Microsoft SQL Enterprise Manager** を使用してサービスを管理するときは、切り替え可能なリソース名 (TCP/IP アドレスを使用してユーザがサーバにアクセスできる名前) によってサービスを登録する必要があります。これにより、この処理のバイアビリティを継続的に監視できます。

SQL Server をシステム名で登録すると、システムも監視できます。

ボリュームを SQL 専用にする

保護対象の SQL ファイルを含むボリュームは、SQL 専用にする必要があります。

SIOS Protection Suite の保護対象のボリュームにアプリケーション、プロセス、またはリモートユーザがアクセスすると、スイッチオーバに失敗する可能性があります。

SQL Server 環境での手動スイッチオーバの制限について

手動操作を実行する場合は、すべてのユーザが SQL Server リソースからログオフしている必要があります。

ボリュームに読み取り専用アクセスをしているローカルプロセスがあっても、サービスからリソースを削除できますが、スイッチバックしようとすると復元に失敗することがあります。例えば、パフォーマンスモニタは定期的に各ボリュームをポーリングし、共有ボリュームや複製ボリュームにインストールされた実行中のプロセスをチェックしています。この種の復元が失敗する可能性は、Microsoft SQL Server をローカルドライブにインストールして、データベースだけを共有ボリュームまたは複製ボリュームに置くことで、最小限に抑えることができます。

Microsoft SQL Management ツールの実行

Microsoft SQL Server Configuration Manager (SQL 2005) は、必要なときだけ実行してください。

Microsoft SQL Server Configuration Manager (SQL 2005) がオープンしていて、データベースレベルでアクティブな場合、SQL 階層が正しくサービス中の状態になるのが妨げられて、フェイルオーバが正常に完了しないことがあります。このような問題が発生した場合は、Microsoft SQL Server Configuration Manager (SQL 2005) を閉じて、SQL リソースを手動でサービス中にしてください。

SQL Server の起動と停止は SIOS Protection Suite 上で実行する

Microsoft SQL Server の管理の多くは Microsoft SQL Enterprise Manager を使用して行われますが、SIOS Protection Suite 管理オプ

ションを使用して Microsoft SQL Server をサービス開始およびサービス停止にすることによって、2 つの明確なメリットが得られます。

1. **一貫した表示**。SIOS Protection Suite が Microsoft SQL Server を停止して起動しても、設定内のすべてのノードについて、サーバの表示の一貫性が保たれます。
2. **詳細設定の保存**。Microsoft SQL Server 設定を変更した場合、SIOS Protection Suite によってサーバを停止および開始するか、または手動でのスイッチオーバを行うことができます。ペアノード上での設定変更は SIOS Protection Suite によって自動的に複製されます。

   注記: これらのオプションを使用してペアサーバ上の新しい設定情報を複製しないと、フェイルオーバの状況では、バックアップサーバによって古い設定情報が使用されます。
3. **コントロールパネルの「サービス」**ツールで、**保護対象の Microsoft SQL サービス**の起動モードを**手動**に設定する必要があります。

Microsoft SQL Server ボリュームの追加

環境の規模が拡大するにつれて、新しい Microsoft SQL Server データベースを新しい共有ボリュームまたは複製ボリュームに追加することが必要になります。その場合は、Microsoft SQL Server 内で新しいデータベースを管理する前に、次の作業を実行して、新しいボリュームを SIOS Protection Suite 階層に追加する必要があります。

新しいボリュームリソースを既存の SQL Server 階層に追加するには、次の作業を実行します。

1. **リソースの作成**。SQL Server 階層がサービス中のサーバ上で SQL 階層と優先順位が同じボリュームリソースを作成して拡張します。
2. **依存関係の作成**。SQL Server リソースを右クリックし、ポップアップメニューの [依存関係の作成] をクリックします。**[子リソース]** タグで新しいボリュームリソースを選択します。

この SIOS Protection Suite 作業を完了すると、管理作業を実行して、SQL Server データベースを追加できます。すでにリソース階層の一部であるボリュームに新しいデータベースを追加する場合は、SIOS Protection Suite 固有の管理は必要ありません。

スイッチオーバ後にデータベースの「Suspect」状態から回復

データベースを格納したボリュームがシステムで利用できない場合、Microsoft SQL Server を起動すると、データベースが suspect 状態になることがあります。SIOS Protection Suite を使用して SQL データベースを保護しているときは、SQL の起動と停止は、階層をサービス中またはサービス停止にする機能としてだけ実行する必要があります。データベースが suspect 状態になり、データベースに問題がないことがわかっている状況では、次の手順を実行してこの問題を解決してください。

プライマリまたはセカンダリサーバで suspect となったデータベースの場合

1. データベースが格納されているボリュームがアクティブ (緑) で、このサーバによって保護されていることを確認します。
2. `sp_resetstatus` を使用してデータベースの状態を変更します。次のコマンドをクエリウィンドウで実行し、suspect 状態のデータベースをリセットしてください。

```
While in master database, execute sp_configure 'allow updates', 1

Reconfigure with override

Sp_resetstatus 'dbname'

Sp_configure 'allow updates', 0

Reconfigure with override
```

3. Microsoft SQL Server を**停止**します。
4. Microsoft SQL Server を**開始**します。

Microsoft SQL Server (MSSQLServer) の一時停止

SQL 管理者は Microsoft SQL Server を手動で一時停止状態にできます。その場合、Microsoft SQL Server に対する既存の接続は処理を続行できますが、新しい接続は許可されません。この場合、SIOS Protection Suite は MSSQLServer サービスが実行中状態でないことを検出しますが、サービスをローカルで再起動したり、SQL 階層をバックアップサーバにフェイルオーバしたりすることはありません。どちらも適切な動作ではないため、Microsoft SQL Server が一時停止状態のときは、SQL リソースの監視は実質的に無効になります。

Microsoft SQL Server をこの状態にするには手動操作が必要であったため、SQL 管理者は SQL Server をこの状態から手動で変更する必要があります。一時停止状態でなくなると、SIOS Protection Suite は先に説明したように SQL リソースの監視を再開できます。

切り替え可能な IP アドレスで接続するように SQL Server を設定

SQL がインストールされている場合は、初期設定で TCP/IP ソケットがデフォルトのネットワークプロトコルとして設定されます。この設定を変更する場合は、**SQL Server Configuration Manager** ツールを使用し TCP/IP ネットワーク設定を再び有効にしてください。

SQL Server のログインおよびパスワードの管理

ユーザは SIOS Protection Suite SQL リソースを作成する際、Microsoft SQL Server のインスタンスにアクセスする SQL 管理ユーザ名とパスワードを入力する必要があります。管理ユーザ名とパスワードを変更した場合、SQL リソースは、クラスタ内のすべてのシステムで新しいパスワードを使用して更新する必要があります。新しいパスワードで更新しない場合は、これらのシステム上の SQL サーバに対して SIOS Protection Suite が十分な監視を行えなくなります。警告メッセージがアプリケーションイベントログに登録されますが、SQL リソースは障害とみなされません。

SIOS Protection Suite SQL リソースに関連付けた SQL 管理ユーザ名とパスワードは、LifeKeeper GUI の **[SQL Server 設定]** タブで変更できます。LifeKeeper GUI を使用して、保護対象の SQL Server リソースを管理するには、LifeKeeper GUI の右側のペインで SQL Server リソースを右クリックし、**[プロパティ]**、**[SQL Server 設定]** タブの順にクリックします。**[管理操作]** をクリックし、**[SQL Server 設定]** ページの [ユーザの管理] をクリックして、SQL リソース情報を参照または変更します。

[SQL Server 設定] ページの詳細については、SQL Server の設定管理を参照してください。

SQL 階層の監視

SIOS Protection Suite は、すべての SQL リソースに対しても、MS SQL Server サービス、および SQL 階層作成時とそれ以降に選択されたオプションサービスを監視します。いずれかのサービスが停止した場合、SQL リソースに関連付けられた監視プロセスがそれを検出して、ローカルリカバリが有効な場合は、ローカルサーバ上でサービスの再起動が試みられます。ローカルリカバリが無効に設定されている場合、リソースをバックアップサーバにフェイルオーバします。

SIOS Protection Suite は SQL クエリを発行して、保護対象の SQL データベースとの接続を確認します。SQL クエリがマスタデータベースとの接続に失敗すると、SQL リソースに関連付けられた監視プロセスは、問題を検出して、ローカルリカバリが有効に設定されていれば、サービスを再起動します。ローカルリカバリが無効に設定されている場合、リソースをバックアップサーバにフェイルオーバします。保護対象のデータベースを SQL 階層の作成後に追加した場合、エラーは **Application Event ログ**に記録されます。

Chapter 5: トラブルシューティング

このセクションでは、SIOS Protection Suite ソフトウェアには特別な関係がない、全体的な環境に関連する現象についての解決案と考えられる原因を提示します。

マスタ、あるいはユーザデータベースがシステムドライブにある場合リソースの作成や拡張に失敗する

現象

マスタデータベースやユーザデータベースが SIOS Protection Suite で保護できないシステムドライブやボリュームに配置されている場合、Microsoft SQL Server リソースの**作成**および**拡張**に失敗します。SIOS Protection Suite は *tempdb* データベースを SIOS Protection Suite で保護されたボリュームに配置することを必須としておらず、このデータベースは SQL Server が起動されるたびに再構成されます。

推奨される処置

以下のサイトにマスタデータベースやユーザデータベースの保存先をボリュームへ移動させる方法が掲載されています。SIOS Protection Suite はそのボリュームを保護します。

http://support.microsoft.com/kb/224071/en-us

http://www.databasejournal.com/features/mssql/article.php/3379901

SQL リソースの拡張に失敗する

現象

プライマリサーバとバックアップサーバの設定が一致しない場合 (例: Microsoft SQL ID の不一致)、Microsoft SQL リソースの拡張は失敗します。拡張時に LifeKeeper GUI に表示されるエラーメッセージの例を次に示します。

```
Process: canextend.ksh(1292)

*ERROR* (No. 14003) The target value for Database file location does not match the
template value (target=-
DQ:\SQLDEFAULT\MSSQL.1\MSSQL\DATA\MASTER.MDF,template=DQ:\SQLDEFAULT\MSSQL.4\MSSQL\DA
TA\MASTER.MDF)

Process: canextend.ksh(1572)

*ERROR* (No. 14003) The target value for Temp DB location does not match the template
value (target=-EQ:\SQLDEFAULT\MSSQL.1\MSSQL\LOG\ERRORLOG,template=-
EQ:\SQLDEFAULT\MSSQL.4\MSSQL\LOG\ERRORLOG)

Process: canextend.ksh(1156)
```

```
*ERROR* (No. 14003) The target value for Log file location does not match the
template value (target=-LQ:\SQLDEFAULT\MSSQL.1\MSSQL\DATA\MASTLOG.LDF,template=-
LQ:\SQLDEFAULT\MSSQL.4\MSSQL\DATA\MASTLOG.LDF)

Error - extmgr (HAWK, MSSQL.0, MSSQL.0, OSPREY) - canextend failed
```

推奨される処置

ID Conflict Resolution オプションを使用して、プライマリサーバとバックアップサーバの Microsoft SQL ID が一致しないトラブルを解決してください。LifeKeeper GUI の右ペインに移動し、**[SQL Server リソース]** を右クリックしてください。続いて、**[プロパティ]** をクリックし、**[SQL Server 設定]** タブをクリックしてください。**[管理操作]** をクリックし、**[SQL Server 設定]** ページの **[ID Conflict Resolution]** を選択してください。

[SQL Server 設定] ページの詳細については、SQL Server の設定管理を参照してください。

名前付きインスタンスで SQLAgent サービスを開始できない

現象

SIOS Protection Suite が SQLAgent サービスを保護している Microsoft SQL Server の名前付きインスタンスでは、リソースが最初にサービス中になると、このサービスの起動を SQL 問題によって妨げられ、この SQL が SQLAgent サービス開始の試みを放棄するまでに MAXWAIT 状況 (300 秒の遅延) が強制されます。

このメッセージは、SQL リソースの INFO フィールドが壊れていることを示しています。SQL リソースを削除して再作成する必要があります。リソースを削除する前に、すべての IP およびボリュームの依存関係を削除する必要があります。依存関係は新しい SQL リソースを作成した時点で SIOS Protection Suite によって再作成されます。

SQLAgent サービスが開始しようとしているシステム上で Microsoft SQL Server サービスがすでに開始している場合は、このシナリオに遭遇することがあります。

SQL 階層の作成時に SQLAgent サービスと Microsoft SQL Server サービスが両方とも開始している場合は、この問題は発生しません。

推奨される処置

Microsoft SQL Server サービスの停止と開始を行うと、通常この問題は解決し、続いて SQLAgent サービスが開始されます。ただし、SQL Server サービスの停止は適切な選択とはいえません。

デフォルトのインスタンスまたは名前付きインスタンスで、MSSQLServer サービスおよび SQLServerAgent サービスはいずれも、ローカルシステムアカウントを使用して正しく起動する必要があります。各システム上でローカル管理者グループにドメイン管理者アカウントを追加した場合、この 2 つのサービスはともにドメイン管理者アカウントを使用して起動します。

SQL Server の名前付きインスタンスへの ODBC クライアントの接続

現象

保護された IP アドレスを介して SIOS Protection Suite クラスタに ODBC 接続を作成した後で、SQL リソースをバックアップサーバに切り替えると、接続に失敗します。

推奨される処置

1. プライマリ上で各インスタンスをサービス休止中にしてから、In Service 状態に戻します。アプリケーションイベントログを調べて、その特定の SQL Server のインスタンスがどの IP:PORT で listen しているのか確認します。
2. セカンダリサーバで各階層の In Service を行い、各 SQL のインスタンスが listen している IP:PORT を記録します。
3. クライアントが ODBC を介していずれかのサーバに接続可能であることを確実にするには、各インスタンスが listen しているポートがプライマリサーバおよびセカンダリサーバのいずれでも同一であることを確認します。
4. この確認を行うには、Microsoft SQL Server ネットワークユーティリティを使用します。SQL インスタンスを選択し (当該マシン上で動作している必要があります)、TCP/IP プロトコルを強調表示し、プロパティを確認して SQL インスタンスが listen しているデフォルトのポートを特定します。
5. このインスタンスについてデフォルトのポートが両方のシステムで同一になるようにこの値を変更します。
6. 手順 5 で設定した、保護された IP:PORT を使用して、各インスタンスの ODBC 接続を作成します。