LifeKeeper Single Server Protection

v9.0

テクニカルドキュメンテーション

2015年9月

To maintain the quality of our publications, we welcome your comments on the accuracy, clarity, organization, and value of this document.

Address correspondence to:
ip@us.sios.com

目次

Chapter 1: はじめに

LifeKeeper Single Server Protection (SSP) は、単一ノード構成におけるアプリケーション監視を可能にします (つまり、クラスタの要件または制約はありません)。単一ノード環境は、物理的なものでも仮想 (vSphere、KVM) でも構いません。LifeKeeper SSP は、実績がある安定した SIOS LifeKeeper アーキテクチャ上に構築されます。LifeKeeper SSP は優れたアプリケーション監視機能を提供し、障害が発生したアプリケーションおよびシステムインフラストラクチャ項目 (例: NFS 共有、IP アドレス、ファイルシステム) のリカバリを実行することができます。何らかの理由でアプリケーションをリカバリできない場合、LifeKeeper SSP は、システムのリブートまたは VM とアプリケーション監視を設定された VMware 仮想マシンの VMware HA 再起動によって、ノードの再起動を開始します。

注記: LifeKeeper SSP は SIOS LifeKeeper 技術を使用して構築されているため、ドキュメント全体で LifeKeeper を参照します。また、両製品に共通するトピックについては SIOS Protection Suite for Linux ドキュメンテーションの情報を参照します。これらの共通のトピックを参照する場合、LifeKeeper SSP には以下の話題は適用されません。

- クラスタリング
- コミュニケーションパス
- 共有ストレージ (要件、構成、...)
- リソース階層の拡張/拡張解除
- ストレージキット (DR、DMMP、HDLM、LVM、MD、PPATH)

  注記: LifeKeeper SSP にベースとなるストレージキットがない場合、保護されるファイルシステムのマウントに必要なデバイスがシステム起動時にアクティベートされるようにするための手順が必要です (例: ファイルシステムが論理ボリューム上でマウントされる場合、LifeKeeper SSP が起動する前にボリュームがアクティブな状態になっていなければなりません)。

- リソース/マシンのフェイルオーバ (LifeKeeper SSP のデフォルトでは、これによってノードが再起動されます)
- リソースのスイッチオーバ
- 切り替え可能な IP アドレス (LifeKeeper SSP では、保護されるアプリケーションの一部には切り替え可能な IP アドレスが必要ですが、単一ノードしかないため、実際には切り替えは行われません)

LifeKeeper SSP のベースになっている SIOS LifeKeeper 製品の詳細については、共通するリリース番号の SIOS Protection Suite for Linux ドキュメンテーションを参照してください。このドキュメンテーションは、リソース階層の作成、リソースタイプ、状態と関係、グラフィカルユーザインターフェース (GUI)、および共通の作業と高度な作業に関する詳細情報を提供します。

ドキュメンテーションとトレーニング

SIOS LifeKeeper Single Server Protection for Linux のインストール、設定、管理、およびトラブルシューティングの方法を説明する関連ドキュメントは、SIOS Technology Corp. ウェブサイトのドキュメンテーション セクションから参照できます。SIOS LifeKeeper Single Server Protection for Linux のあらゆる側面について、以下のセクションで説明しています。

セクション	説明
はじめにおよびインストール	LifeKeeper Single Server Protection 環境のプランニングと設定、LifeKeeper Single Server Protection のインストールとライセンス、LifeKeeper のグラフィカルユーザインターフェース (GUI) の設定に役立つ情報を提供します。
管理	サーバのプロパティの編集やリソースの作成などのサーバレベルの作業、およびリソースの編集、拡張、削除などのリソースレベルの作業について説明します。
ユーザガイド	LifeKeeper GUI で実行できる多数の作業を含めて、LifeKeeper の GUI に関する詳細情報があります。
トラブルシューティング	既知の問題と制限について説明し、SIOS LifeKeeper Single Server Protection for Linux のインストール、設定、および使用を行うときに発生する可能性がある問題に対する解決策を説明します。
Recovery Kit	LifeKeeper Single Server Protection で特定のアプリケーションを管理および制御するために必要なオプションの Recovery Kit のプランニングおよびインストール手順、管理、設定、およびユーザ情報が含まれます。

トレーニング

LifeKeeper Single Server Protection のトレーニングは、SIOS Technology Corp. または代理店から受講可能です。詳細については、営業担当者にお問い合わせください。

テクニカルサポート

SIOS Technology Corp. と有効なサポート契約を結んだお客様は、新しい SIOS Technology Corp. のセルフサービスサポートポータルにアクセスできます。

SIOS Technology Corp. のセルフサービスサポートポータルでは、以下のことができます。

- 弊社のソリューションナレッジベースから、問題の解決策と質問に対する回答を検索する。
- 次のメニューを選択して、年中無休の SIOS Technology Corp. のサポートチームにアクセスする。
- **Log a Case** - 新しいインシデントを報告する。
- **View Cases** - お客様の未解決と解決済みのインシデントをすべて表示する。
- **Review Top Solutions** - 弊社のお客様が表示した、最も一般的な問題の解決策の情報を表示する。

セルフサービスポータルを設定してアカウントを有効にする方法については、SIOS Technology Corp. のサポート (support@us.sios.com) にお問い合わせください。

また、SIOS Technology Corp. のサポートには、以下の方法でも連絡できます。

1-877-457-5113 (通話料無料)

1-803-808-4270 (米国以外のお客様)

電子メール: support@us.sios.com

VMware HA との連携

「はじめに」セクションで説明したように、LifeKeeper Single Server Protection は、物理環境と仮想環境の両方で使用できるように設計されています。LifeKeeper SSP を VMware VM にインストールした場合、VMware の HA 機能を LifeKeeper SSP と組み合わせて、保護対象リソースやノードの障害を監視し、復旧することができます。これらの機能を有効にする方法については、VMware HA と LifeKeeper Single Server Protection の連係の有効化を参照してください。さらに、LifeKeeper SSP には、VMware vCenter と連携する管理インターフェースを提供するオプションのコンポーネントが用意されています (SteelEye 管理コンソールトピックを参照)。

SteelEye 管理コンソール

SteelEye 管理コンソール (SMC) は、VMware HA の構成で LifeKeeper Single Server Protection を実行するときに使用するオプションのコンポーネントです。SMC は、VMware vCenter と連携する管理インターフェースを提供する専用システムです。

VMware vCenter Server、および SIOS LifeKeeper Single Server Protection と連係して使用するときの SteelEye 管理コンソールの設定、インストール、および動作については、以下のトピックが役立ちます。詳細は以下のカテゴリに分かれています。

インストールの概要

システム要件

セットアップの実行

vSphere Client プラグイン

vSphere Client プラグインの設定

vSphere Client ユーザインターフェース

認証情報の設定

インストールの検証

vSphere Client プラグインへの対処

LifeKeeper Single Server Protection API

カスタム証明書の使用

インストールの概 要

SteelEye 管 理コンソール (*SMC*) のインストールは、いくつかの重 要 な手 順 で構 成 されます。

1. SMC のホストサーバ (仮 想 または物 理) を指 定 する必 要 があります。サーバは **SMC を実 行 するための専 用 システム**である必 要 があります。SIOS Technology Corp. は現 在 、他 の目 的 に使 用 中 のサーバにおける SMC の実 行 をサポートしていません。小 型 の仮 想 マシンで十 分 であるため、このサーバが非 常 に強 力 である必 要 はありません。サーバの要 件 の詳 細 については、システム要 件 を参 照 してください。
2. SMC ソフトウェアは、`setup` スクリプトを CD メディアまたは `.img` ファイルから実 行 して、インストールする必 要 があります。このプロセスはシステムに必 要 な変 更 を行 い、SMC ソフトウェアコンポーネントをインストールして、SMC サービスを開 始 します。
3. VMware vSphere Client プラグインを vCenter サーバに登 録 する必 要 があります。**注 記** : SMC は、1 つの vCenter インスタンスのみと連 係 できます。このため、複 数 の vCenter インスタンスを展 開 する場 合 は、SMC ソフトウェアを個 々 の vCenter インスタンスにインストールする必 要 があります。
4. SMC には、vSphere Client が管 理 する個 々 の SIOS LifeKeeper Single Server Protection (または SMC 経 由 で管 理 されるサブセット) との通 信 に必 要 な認 証 情 報 を設 定 する必 要 があります。認 証 情 報 の特 定 のセットが、複 数 の LifeKeeper Single Server Protection システムに有 効 である場 合 、これらの認 証 情 報 を 1 回 で入 力 することができ、残 りの LifeKeeper Single Server Protection ノードを個 別 に追 加 する必 要 があります。詳 細 については、認 証 情 報 の設 定 を参 照 してください。

システム要 件

SteelEye 管 理コンソール (*SMC*) は専 用 サーバにインストールする必 要 があります。これは物 理 サーバでも仮 想 サーバでもかまいませんが、他 の目 的 に使 用 することはできません。SIOS Technology Corp. は現 在 、他 の目 的 に使 用 中 のサーバにおける SMC ソフトウェアの実 行 をサポートしていません。このサーバは、以 下 の最 小 要 件 を満 たす必 要 があります。

- Red Hat Enterprise Linux/CentOS 6.4 x86_64 を実 行 可 能 な Intel (または AMD) の 64 ビットシステムであること。ベアメタルシステムと仮 想 マシンのいずれでもかまいません。
- 512 MB 以 上 の RAM を装 備 していること。
- ディスク容 量 が 8 GB 以 上 であり、`/opt` ファイルシステムに 1 GB 以 上 が使 用 可 能 であること。
- ネットワークアダプタが 1 つ以 上 あること。
- TCP/IP 経 由 で、VMware vCenter Server (vSphere Client プラグインを使 用 する場 合)、および SMC が表 示 / 管 理 する LifeKeeper Single Server Protection サーバと直 接 通 信 可 能 であること。SMC のホストサーバを選 択 するときには、ネットワークセグメント / ルート / ファイアウォールの考 慮 事 項 がある場 合 もあります。
- OS に同 梱 されている openssl-devel がインストールされていること。

セットアップの前提条件

システムを選択した後、SMC をインストールする前に以下の前提条件を設定する必要があります。

- デフォルトの**ベース**ソフトウェアパッケージを使用してシステムをインストールする必要があります。特別なパッケージを選択する必要はありません。
- システムのコアオペレーティングシステムの **yum リポジトリを有効**にし、使用可能にする必要があります。これは、ベースシステムのインストールメディアリポジトリ、またはネットワークリポジトリを `/etc/yum.repos.d/` で有効にする必要があるということです。

サポートするオペレーティングシステムがシステム上で動作を開始した後、セットアップの実行の手順に従って、SMC ソフトウェアコンポーネントをインストールできます。

セットアップの実行

SteelEye 管理コンソールソフトウェアのコンポーネントは、CD/DVD、または CD イメージを持つ ISO img ファイルからインストールできます。この時点以降、すべてのソフトウェアの手順は `root` ユーザとして実行する必要があります。

いずれの場合でも、CD または ISO img ファイルをマウントする必要があります。CD は通常の方法でマウントできます。img ファイルは、以下のようなコマンドを使用して、ループバックデバイス経由でマウントできます。

```
mount -o loop <path-to>/smc.img /mnt
```

(/mnt は、イメージのマウントに適する任意の場所にすることが可能)

ソフトウェアのインストール

イメージをマウントした後、以下のコマンドでインストールを開始できます。

```
cd /mnt; ./setup
```

セットアップツールがインストールプロセスをガイドし、以下の動作を実行してソフトウェアコンポーネントをセットアップします。

- SMC コンポーネントと競合するパッケージがシステム上に存在しないように、システムパッケージのアップグレードまたはアンインストールが実行されます。このプロセスには、事前インストールされた Web サーバ、およびそれに依存するコンポーネントのアンインストールも含まれます。このプロセスには、数分かかることがあります。
- 次に、すべての SMC ソフトウェアコンポーネント用として、セットアップツールにより、SIOS パッケージのインストール / アップグレードが実行されます。これも数分かかることがあり、システムに必要なその他の変更、特にクライアントと SMC との通信を可能にする iptables ファイアウォール設定の変更が含まれます。HTTP トラフィックが SMC サーバのポート 80 および 443 を通過するように、iptables 設定が変更されます。
- 最後にセットアップツールにより、必要な VMware SDK パッケージがインストールされます。インストールするには、VMware SDK のエンドユーザライセンスに同意する必要があります。SDK のイン

ストールで、ツールのバイナリファイルのインストール先となるファイルパスを入力するように要求されます。これらのファイルについて、デフォルトの場所をそのまま使用することを推奨します。

ベースの vCenter と認証情報の設定

ソフトウェアコンポーネントのインストール後、セットアップツールは vSphere Client プラグイン、および SIOS LifeKeeper Single Server Protection ノードの通信に使用するデフォルトの認証情報を設定します。セットアッププロセスを完了するために、以下の動作が実行されます。

- セットアップツールにより、vCenter サーバ名、ユーザ、およびパスワードの入力が要求されます。この情報は、この SMC サーバが提供する vSphere Client プラグインを、指定した vCenter に登録するために使用されます。この手順の後、vCenter サーバはプラグイン用の追加のタブを表示します。最初のインストールの後はいつでも、プラグインの再登録または登録解除ができます。そのプロセスの詳細については、vSphere Client プラグインの設定 ページを参照してください。
- 最後に、セットアップツールは SIOS LifeKeeper Single Server Protection ノードとの通信に使用する***デフォルト***の認証情報の入力を要求します。これらの認証情報は SMC サーバに格納され、特定サーバに固有の認証情報が設定されていない限り、LifeKeeper Single Server Protection サーバとの通信に使用されます。SMC から LifeKeeper Single Server Protection システムをフルに管理できるようにするには、デフォルトの認証情報には LifeKeeper Single Server Protection ノードへの管理者のアクセス権限が必要です (代表的なインストールでは、ユーザがローカルの `/etc/group` ファイルの lkadmin グループに属する必要がある)。通常、***デフォルト***の認証情報は、インストールした LKSSP ノードの *root* ユーザとパスワードです。**注記**: パスワードのストレージは base64 でエンコードされていますが、LifeKeeper の credstore データベースでは**暗号化されません。** `lkadmin` グループのメンバシップを持つ別の LKSSP システムアカウントを使用することを推奨します。認証情報の設定 ページには、SMC で使用される認証情報を管理する方法の詳細が記載されています。

これで、セットアッププロセスが完了します。ソフトウェアのインストールと設定が正しく実行されたことを検証する方法の詳細については、インストールの検証 ページを参照してください。

認証情報の考慮事項

前述のセットアッププロセスの最後の手順では、LifeKeeper Single Server Protection システムにアクセスするためのデフォルトの認証情報を格納しています。この場合のデフォルトの認証情報とは、システムに固有の認証情報が設定されていないときに、LifeKeeper Single Server Protection システムでの認証に使用される認証情報を指します。SMC は常に、デフォルトの認証情報を使用するように戻ります。

このため、SMC の設定を簡略にするために、可能な限りすべての LifeKeeper Single Server Protection システムで同じ認証情報を使用することを推奨します。これは通常、LifeKeeper Single Server Protection システムの root ユーザを使用することを意味しますが、`lkadmin` グループに属するユーザである限り、すべてのシステムで共通な任意のユーザを使用できます。

SIOS LifeKeeper Single Server Protection vSphere Client プラグイン

SIOS LifeKeeper Single Server Protection vSphere Client プラグインは VMware vSphere クライアントと連係し、保護対象の仮想マシンのアプリケーション監視ステータスを提供します。プラグインを動作可能にするには、vCenter Server で登録する必要があります。

プラグインは、すべての転送動作にセキュリティで保護された HTTPS 通信を使用します。はじめてプラグインを vSphere クライアントにロードするときに **LK4Linux Valid SMC** の SSL 証明書のセキュリティ警告を受信しますが、これは正常な動作です。SSL 証明書を検査してローカル証明書ストアにインストールした後、セキュリティ警告を安全に無視できます。

プラグインの要件

- VMware vSphere バージョン 4 またはバージョン 5
- VMware vSphere Client
- クライアントシステムで Javascript とクッキーが有効であること

詳細については、vSphere Client プラグインの設定、および vSphere Client プラグインのセキュリティ警告への対処のトピックを参照してください。

vSphere Client プラグインの設定

インストール後にいつでも、vSphere Client プラグインの再登録、または認証情報の変更ができます。これは、必要に応じて別の vCenter サーバにプラグインを登録する操作も含みます。プラグインを別の vCenter サーバにインストールする場合、まず現在のサーバから登録解除する必要があります。

vSphere Client プラグインの登録

プラグインの登録は、/opt/LifeKeeper/bin/registerPlugin.pl ツールで行います。このツールは、vCenter サーバ、ユーザ名、およびパスワードの 3 つの引数をとります。vSphere Client プラグインを再登録するには、これらすべてが必須です。このツールの実行例は、以下のようになります (*すべてを 1 行に記述*)。

```
/opt/LifeKeeper/bin/registerPlugin.pl --server=myvcenter.mydomain.com --username=vcuser
--password=vcpassword
```

注記: shell の解釈を回避するために、shell 文字でもあるパスワード文字はエスケープする必要があります。

vSphere Client プラグインの登録解除

SMC サーバからインストールしたプラグインは、以下のコマンドを使用してリストできます。

```
/opt/LifeKeeper/bin/registerPlugin.pl --action=list
```

プラグインを削除するには、以下のコマンドを実行できます (*すべてを 1 行に記述*)。

```
/opt/LifeKeeper/bin/registerPlugin.pl --action=remove --key=com.sios.us.lkssp
```

注記: プラグインの登録解除に使用するキーは、list 動作で表示されるものと同一にする必要があります。

注記: セキュリティ警告の詳細については、vSphere Client プラグインのセキュリティ警告への対処を参照してください。

vSphere Client ユーザインターフェース

[LifeKeeper Single Server Protection] タブ

vSphere Client プラグインを登 録 すると、vSphere Client ユーザインターフェースに **[LifeKeeper Single Server Protection]** タブが表 示 されます。

コンテキストメニュー

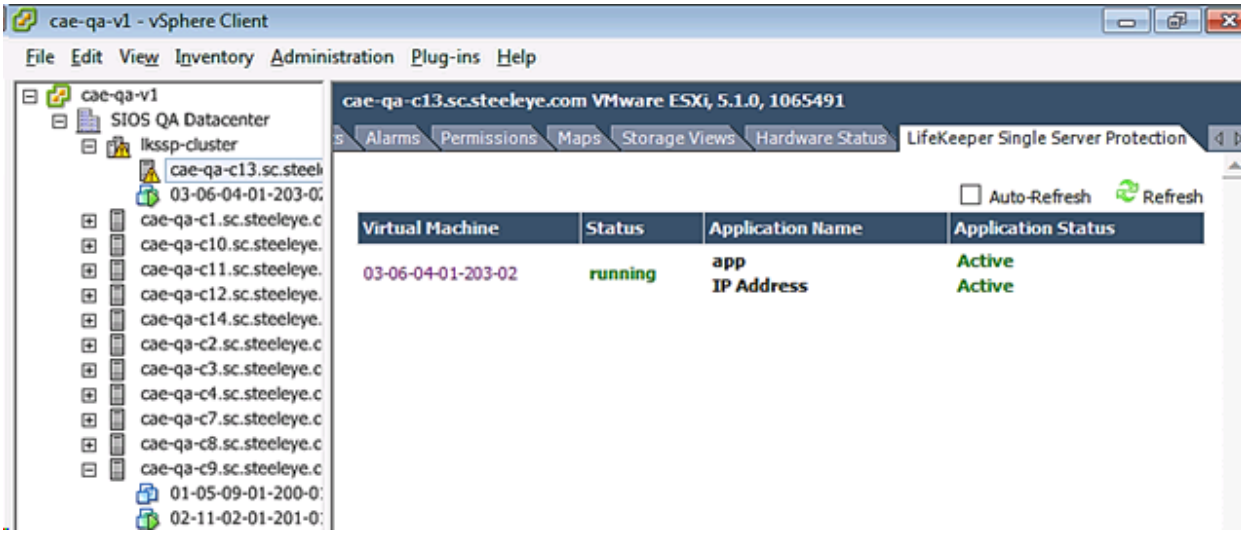
この vSphere Client プラグインにより、左 側 のインベントリツリーのクリック位 置 に合 わせて、[LifeKeeper Single Server Protection] タブに複 数 のコンテキストレベルが表 示 されます。

Datacenter Level

datacenter 内 にある仮 想 マシンを表 示 します。

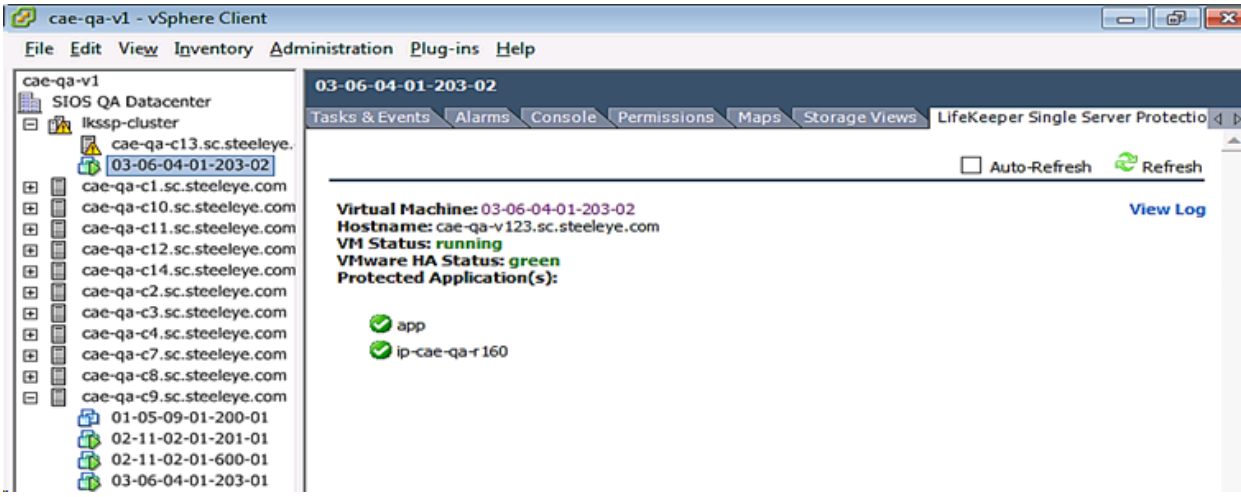
ESX or ESXi Level

特定ホストで動作中の仮想マシンのステータスを表示します。



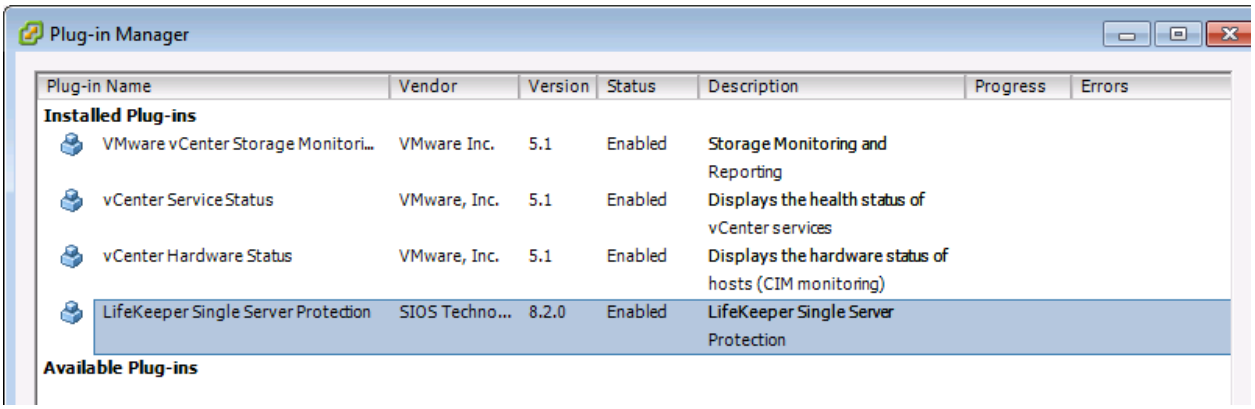
Virtual Machine Level

以下の特定ノードについて、情報を表示します。仮想マシン名、ホスト名、仮想マシンのステータス、VMware HA のステータス、保護対象のアプリケーション。また、LifeKeeper Single Server Protection のログを表示できる **[View Log]** リンクもあります。



Manage Plug-Ins

登録済みの LifeKeeper Single Server Protection vCenter プラグインのステータスを表示します。



.

その他の表示

LifeKeeper Single Server Protection プラグインは、**[Datacenter]**、**Virtual Application**、および **[Resource Pool]** のレベルでも表示できます。

認証情報の設定

SMC と LifeKeeper Single Server Protection ソフトウェアは、他のシステム (vCenter Server、または SIOS LifeKeeper Single Server Protection) との通信に使用する認証情報を*認証情報ストア*経由で管理します。このストアは、例えばプラグインの登録時に使用されます (vSphere Client プラグインの設定を参照)。このストアは、必要に応じて `/opt/LifeKeeper/bin/credstore` コマンドで管理できます。このコマンドを使用すると、サーバアクセスに必要な認証情報をサーバごとに設定、変更、削除することができます。

認証情報の追加または変更

認証情報の追加と変更は同じ方法で実行できます。代表的な例として、サーバ lkssp-server.mydomain.com の認証情報を追加または変更する場合は次のようになります。

```
/opt/LifeKeeper/bin/credstore -k lkssp-server.mydomain.com myuser
```

この例では、lkssp-server.mydomain.com へのアクセスに使用するユーザ名として *myuser* を指定しています。パスワードを入力 / 確認するプロンプト (*passwd* など) が表示されます。

注記: LifeKeeper Single Server Protection サーバの認証情報を格納するために SMC で使用するキー名は、LifeKeeper Single Server Protection サーバのホスト名と*完全に*一致する必要があります (その vSphere Client プラグインの **[Hostname:]** フィールドに表示されるものと一致)。ホスト名が FQDN の場合、認証キーは FQDN である必要があります。ホスト名が短縮名の場合、キーも短縮名にする必要があります。

セットアップの実行時に以下の[Credential Considerations] (認証情報に関する考慮事項) が推奨された場合、特定のサーバキーが存在しないときには、対応するユーザ名とパスワードを持つ***デフォルト***キーが認証に使用されます。*デフォルト*キーを追加、変更するには以下のコマンドを実行してください。

```
/opt/LifeKeeper/bin/credstore -k default myuser
```

ストア内の認証情報のリスト表示

現在格納されている認証情報をリスト表示するには、以下のコマンドを実行します。

```
/opt/LifeKeeper/bin/credstore -l
```

これにより、認証情報ストア内に格納されているキーが表示されます。この場合の「キー」は、認証情報を使用する対象のサーバを示しています (認証情報自体は秘密情報のため、このコマンドが表示するのは、実際の認証情報の内容ではなくキーのみです)。

サーバの認証情報の削除

特定のサーバに対する認証情報を削除するには、以下のコマンドを実行します。

```
/opt/LifeKeeper/bin/credstore -d -k lkssp-server.mydomain.com
```

この例では、サーバ lkssp-server.mydomain.com の認証情報ストアがストアから削除されます。

追加情報

credstore ユーティリティの詳細については、以下のコマンドを実行してください。

```
/opt/LifeKeeper/bin/credstore --man
```

コマンドのマニュアルページがすべて表示されます。

インストールの検証

SteelEye 管理コンソールのインストールを検証するには、Web ブラウザを使用して、https://<smcserver>/ に接続します。インストールが正しく実行された場合、SMC サービスが利用可能であることを示すページが表示されます。**注記**: SMC は自己署名の SSL 証明書を使用するので、セキュリティ警告を受信するのは正常な動作です。この警告は安全に無視できます。

ブラウザにページの表示エラーが表示されるか、新規にインストールした SMC サーバへの接続に失敗した場合は、エラーが発生せずにすべてのインストール手順が完了したこと、および SMC サーバがネットワークにアクセス可能であることを確認してください。

トラブルシューティング

トラブルシューティングについては、SMC のトラブルシューティングセクションを参照してください。また、セキュリティ警告の詳細については、vSphere Client プラグインのセキュリティ警告への対処トピックを参照してください。

vSphere Client プラグインのセキュリティ警 告 への対 処

LifeKeeper Single Server Protection vSphere Client プラグインは、自 己 署 名 証 明 書を使 用して SSL 通 信を有 効にします。プラグインのコンテンツを表 示 するときに、セキュリティ警 告を受 信 するのは正 常 な動 作 です。セキュリティ警 告を低 減 するには、vSphere Client システムの証 明 書 ストアに「LK4Linux Valid SMC」証 明 書をインストールする必 要 があります。さらに、お使 いのシステムの「Trusted Root Certification Authorities」証 明 書 ストアに「SIOS Technology, Corp.」認 証 局 (CA) の証 明 書をインストールできます。

「LK4Linux Valid SMC」証 明 書をインストールするには、

1. セキュリティ警 告 が表 示 されたら、**[View Certificate]** を選 択 します。
2. **[Install Certificate]** ボタンをクリックします。
3. ウィザードの手 順 に従 って、証 明 書をインストールします。

「Trusted Root Certification Authorities」証 明 書 ストアに「SIOS Technology, Corp.」認 証 局 (CA) の証 明 書をインストールするには、

1. セキュリティ警 告 が表 示 されたら、**[View Certificate]** を選 択 します。
2. **[Certification Path]** タブをクリックします。
3. **SIOS Technology, Corp.** の証 明 書を選 択 します。
4. CA の証 明 書を表 示 するには、**[View Certificate]** をクリックします。
5. **[Install Certificate]** ボタンをクリックします。
6. **[Next]** をクリックします。
7. **[*Certificate Store Wizard*]** ペインの **[Place all certificates in the following store]** ラジオボタンを選 択 します。
8. **[Browse]** ボタンが有 効 になります。そのボタンをクリックします。
9. **[Select Certificate Store]** リストから、**[Trusted Root Certification Authorities]** を選 択 します。
10. **[OK]** をクリックします。
11. **[Next]** をクリックして、ウィザードを完 了 します。

LifeKeeper API

LifeKeeper API を使 用 すると、LifeKeeper Single Server Protection サーバと SteelEye 管 理 コンソール (SMC) との間 の通 信 を行 えるようになります。現 在 、この API は内 部 使 用 のみとして予 約 されていますが、将 来 のリリースではお客 様 とサードパーティが使 用 できるように公 開 される可 能 性 があります。

ネットワーク設 定

LifeKeeper Single Server Protection の各サーバは、ポート 778 の SSL 接続を使用してこの API を提供します。このポートは、`/etc/default/LifeKeeper` 内の設定変数 `API_SSL_PORT` を使用して変更できます。この変数は、SMC の `/etc/default/LifeKeeper.local.pl` に設定されます。(**注記**: この設定は、**API クライアントと LifeKeeper Single Server Protection サーバの間の通信**を制御します。SMC (常にポート 443) 自体へのアクセスは制御しません)。LifeKeeper Single Server Protection と SMC は両方とも、`API_SSL_PORT` に同じ値を使用する**必要があります。**

認証

LifeKeeper API は認証に PAM を使用します。API へのアクセス権限は、グループ *lkadmin*、*lkoper*、または *lkguest* のメンバーであるユーザにのみ付与されます。ユーザに権限を与えるには、システムの PAM 設定に応じて、ローカルシステムファイル (*/etc/passwd* および */etc/group*) を使用するか、ユーザを LDAP または Active Directory のグループに追加します。

注記: LifeKeeper API は、*lkpasswd* ユーティリティで管理されるユーザデータベースは使用しません。

SMC による API の使用

SMC は API を使用して、LifeKeeper Single Server Protection サーバからの情報を収集します。SMC は *credstore* ユーティリティを使用して、LifeKeeper Single Server Protection サーバのユーザアカウント情報を管理します。SMC は認証情報ストアのキーとして LifeKeeper Single Server Protection のサーバ名を使用するので、LifeKeeper Single Server Protection サーバの認証情報を指定するときには、LifeKeeper Single Server Protection サーバのシステム名を *-k* オプションとして *credstore* ユーティリティに渡す必要があります。また、指定したサーバの認証情報が見つからない場合、SMC は***デフォルト***キーに保存されている認証情報をチェックして使用します。

カスタム証明書の使用

LifeKeeper Single Server Protection では、異なるシステムとの通信に SSL/TLS が使用されます。デフォルトでは、ノード間で一定の身元確認が可能なデフォルト証明書が SPS と共にインストールされます。このドキュメントでは、デフォルト証明書を組織独自の認証局 (CA) が作成した証明書に置き換える方法を説明します。

証明書の使用方法

SteelEye 管理コンソール (SMC) と LifeKeeper Single Server Protection サーバとの通信では、転送するデータを保護するために SSL/TLS が使用されます。双方のシステムは自身を特定する証明書を提示し、証明書を提示されたシステムは、CA 証明書を使用して提示された証明書を SSL 接続経由で確認します。

以下の 4 種類の証明書が使用されます。

- /opt/LifeKeeper/etc/certs/LK4LinuxValidNode.pem (LifeKeeper Single Server Protection server certificate)
- /opt/LifeKeeper/etc/certs/LK4LinuxValidSMC.pem (SMC server certificate)
- /opt/LifeKeeper/etc/certs/LK4LinuxClient.pem (LifeKeeper Single Server Protection client

certificate, installed on all servers)

- /opt/LifeKeeper/etc/certs/LKCA.pem (certificate authority, installed on all servers)

最初の3つの証明書がサーバが実行する検証に合格するためには、4番目の証明書による署名が必要です。証明書の共通名は検証されません。証明書はCAによって署名されるのみということに注意してください。

独自の証明書の使用

運用環境によっては、デフォルト証明書を組織内部のCAが作成した証明書に置き換える必要がある場合があります。そのような場合は、上記の4種類の証明書を、*同じ証明書ファイル名*を持つ新しい証明書に置き換えます。これらの証明書はPEM形式です。LK4LinuxValidNode.pem、LK4LinuxValidSMC.pem、およびLK4LinuxValidClient.pemはそれぞれ、キーと証明書の両方を含んでいます。LK4LinuxValidNode.pemおよびLK4LinuxValidSMC.pemの証明書は、*サーバタイプ*の証明書です。LK4LinuxValidClient.pemは、*クライアントタイプ*の証明書です。

デフォルトの証明書を置換した場合、変更を反映するにはLifeKeeper Single Server ProtectionおよびSMCを再起動する必要があります。証明書の設定を間違えると、steeleye-lighttpdデーモンが起動に失敗し、LifeKeeper Single Server Protectionのログファイルにエラーが記録されます。問題が発生した場合、このログファイルを参照すると実行すべき完全なコマンドを見ることができます。

Chapter 2: インストール

LifeKeeper Single Server Protection ソフトウェアのインストール

LifeKeeper Single Server Protection 構成内の各サーバに LifeKeeper Single Server Protection ソフトウェアをインストールしてください。各 LifeKeeper Single Server Protection サーバには、オプションのリカバリキットパッケージを含む、設定要件をサポートするために必要なパッケージがインストールされている必要があります。

重要: LifeKeeper Single Server Protection をインストールする前に、Linux の依存関係トピックを参照してください。

LifeKeeper Single Server Protection Core パッケージおよび他のオプションのリカバリキットは、LifeKeeper Single Server Protection インストールイメージファイル (*lkssp.img*) を使用して、コマンドラインでインストールします。このイメージファイルは、LifeKeeper Single Server Protection をシステムにインストールするときに必要なユーザ対話型のシステムセットアップ作業を実行するよう設計されたインストールスクリプトー式を提供します。インストールイメージファイルは、実行中の Linux ディストリビューションを特定し、一連の質問へのユーザの回答に基づいて、LifeKeeper Single Server Protection を正常にインストールするために必要なさまざまなパッケージをインストールします。ライセンスがインストールされた後にサーバの Host ID と Entitlement ID を取得して表示するユーティリティを提供するライセンシングパッケージもインストールされます。Entitlement ID は LifeKeeper Single Server Protection を実行するための有効なライセンスの取得に使用され、ソフトウェアに付属しています。

注記: これらのインストール手順は、読者がサーバにインストールされた Linux オペレーティングシステムに精通していることを前提としています。

重要:

- LifeKeeper Single Server Protection は共有ストレージサポートまたは I/O フェンシングを提供しません。各サーバはアプリケーションデータにローカルディスクストレージを使用する必要があります。
- すべての LifeKeeper Single Server Protection パッケージは、*/opt/LifeKeeper* ディレクトリにインストールされます。
- LifeKeeper の既存バージョンを再インストールする場合、最初に、古い LifeKeeper パッケージを削除する必要があります。標準の LifeKeeper のインストールには、既存のリソース階層の再定義が必要になります。現在のリソース階層定義を保持するには、を参照してください。
- LifeKeeper Single Server Protection のインストール中に、LifeKeeper Distribution Enabling Package を参照するエラーメッセージが表示された場合、LifeKeeper Single Server Protection インストールイメージファイル上の **setup** スクリプトを実行または再実行する必要があります。

LifeKeeper Single Server Protection ソフトウェアのインストール

LifeKeeper Single Server Protection は、使用している Linux ディストリビューションに関わらず、コマンドラインでインストールされます。

1. 次のコマンドを使用して、`lkssp.img` ファイルをマウントしてください。

   ```
   mount PATH/IMAGE_NAME MOUNT_POINT -t iso9660 -o loop
   ```

   ここで、PATH はイメージへのパスです
   IMAGE_NAME はイメージの名前です
   MOUNT_POINT はマウント位置へのパスです

2. `lkssp.img` がマウントされたディレクトリに移動して、次のコマンドを入力してください。

   ```
   ./setup
   ```

3. インストール手順の間に何が行われるかを説明するテキストが表示されます。ここで行われる一連の質問に対して、**Yes** の場合は「**y**」、**No** の場合は「**n**」と答えます。質問の種類と順序は、お使いの Linux ディストリビューションによって異なります。

   各質問をよく読んで、適切に回答してください。LifeKeeper Single Server Protection インストールを正常に行うために必要なすべての手順を最後まで行うには、各質問に **Yes** と答えることを推奨します。

4. 次に、LifeKeeper Single Server Protection Core パッケージがインストールされます。

5. ここで setup スクリプトが、ライセンスユーティリティのインストールを実行します。詳細については、ライセンスの取得とインストールを参照してください。

6. setup スクリプトが提示するすべての質問に回答した後、インストールが成功したことが通知され、インストール可能なすべての LifeKeeper Single Server Protection Recovery Kit の一覧が表示されます。

   注記: setup スクリプトの実行に関する追跡情報が、*/var/log/LK_install.log* に保存されます。

7. インストールするキットを反転選択し、「スペース」キーを押してください。インストール予定のキットの横に「i」のマークが付きます。**Enter** を押してください。

   注記: 後でキットを追加するには、-k を付けて setup スクリプトを実行します。

   ```
   ./setup -k
   ```

LifeKeeper Single Server Protection では、サーバごとに別々のライセンスが必要です。ライセンスは、ランタイムライセンスです。つまり、LifeKeeper Single Server Protection のインストールはライセンスなしでも可能ですが、正常に製品を起動して実行するためには、事前にライセンスをインストールする必要があります。

インストールスクリプトによってインストールされるライセンスユーティリティパッケージは、LifeKeeper Single Server Protection ソフトウェアの初期インストール時にサーバの使用可能なすべての Host ID を取得して表示します。ライセンスがインストールされると、このユーティリティは Entitlement ID (使用可能な場合) または Host ID (使用できない場合) を返します。

注記: Host ID が表示される場合は常に NIC の MAC アドレスに基づいています。

SIOS Technology Corp. ライセンス管理ポータルから取得した LifeKeeper Single Server Protection ライセンスには Entitlement ID が含まれ、クラスタ内の特定のノードにロックされることはありません。LifeKeeper Single Server Protection ソフトウェアと一緒に提供された Entitlement ID (認証コード) は、LifeKeeper Single Server Protection ソフトウェアを実行するために必要なパーマネントライセンスを取得するために使用されます。このプロセスを以下の図に示します。

注記: ソフトウェアパッケージごとに、サーバごとのライセンスが必要になります。

LifeKeeper Single Server Protection クラスタ内の各サーバについてライセンスを取得してインストールするには、次の手順を行います。

1. **LifeKeeper Entitlement ID (認証コード) があることを確認してください。**ライセンスの取得に必要な Entitlement ID を含むソフトウェアをメールで受け取っているはずです。
2. **SIOS Technology Corp. ラインセンス管理ポータルでライセンスを取得してください。**
   a. インターネットアクセスが可能なシステムを使用して、SIOS Technology Corp. ラインセンス管理ポータルにログインしてください。
   b. **[Manage Entitlements]** を選択してください。

      注記: パスワードを変更する場合は、画面の右上隅にある **[Profile]** ボタンを使用してください。

   c. **[Entitlement ID]** を探して、行項目の左にあるボックスをオンにすることで、その Entitlement ID に関連付けられた各 **[Activation ID]** を選択してください。
   d. **[Activate]** タブを選択してください。
   e. 必要なフィールドを定義して、**[Next]** を選択してください。
   f. **[Add New Host]** をクリックして、新しいホストを作成してください。
   g. [Node Locked Host] リストから **[Any]** を選択して、**[Okay]** をクリックしてください。
   h. **[Host ID]** の左にあるボックスをオンにして、**[Generate]** を選択してください。**[Fulfillment ID]** が **[License Summary]** 画面に表示されます。
   i. **[Fulfillment ID]** の左にあるボックスをオンにして、**[Email License]** タブを選択してください。
   j. ラインセンスの送信先となる有効なメールアドレスを入力して、**[Send]** を選択してください。
   k. **[Complete]** を選択してください。
   l. メールを取得してください。
   m. ファイルを適切なシステムにコピーにしてください。
3. ラインセンスをインストールしてください。各システムで、ライセンスファイルを */var/LifeKeeper/license* にコピーするか、または各システムで、`/opt/LifeKeeper/bin/lkkeyins` を実行してファイルに対するファイル名 (フルパスを含む) を指定してください。

リソースポリシー管理

概要

LifeKeeper Single Server Protection (SSP) のリソースポリシー管理では、リソースのローカルリカバリとフェイルオーバの動作管理機能が提供されます。リソースポリシーは、**lkpolicy** コマンドラインツール (CLI) を使用して管理できます。

LifeKeeper SSP のリカバリ動作

LifeKeeper SSP には、個々のアプリケーションおよび関連し合うアプリケーションのグループを監視する機能があり、定期的にローカルリカバリを実行したり、保護下のアプリケーションに障害が発生したときに通知したりすることができます。関連し合うアプリケーションの例としては、主アプリケーションが下位のストレージまたはネットワークリソースに依存する階層などがあります。アプリケーションまたはリソースに障害が発生した場合のデフォルトの動作は以下の通りです。

1. **ローカルリカバリ:** 最初に、リソースまたはアプリケーションの**ローカル**でリカバリを試みます。このときは、外部の介入なしにローカルサーバ上でリソースまたはアプリケーションをリストアしようとします。ローカルリカバリが成功した場合、LifeKeeper SSP は追加のアクションを実行しません。
2. **フェイルオーバ:** 次に、ローカルリカバリでリソースまたはアプリケーションのリストアに*失敗した* (またはリソースを監視する*リカバリキット*がローカルリカバリをサポートしていない) 場合、***フェイルオーバ***が開始されます (下記の標準ポリシーセクションの Failover を参照)。

リカバリ動作の詳細については、LifeKeeper Single Server Protection 障害検出とリカバリのシナリオを参照してください。

ポリシーによるカスタム動作およびメンテナンスモード動作

LifeKeeper SSP は、デフォルトのリカバリ動作を変更する追加ポリシーを設定する機能をサポートします。リソース単位またはサーバ単位で、4 つのポリシーが設定可能です (リソース単位のポリシーに関する注意については下のセクションを参照してください)。**サーバレベルでポリシーを変更する方法を推奨します。**

利用可能なポリシーは以下の通りです。

標準ポリシー

- **Failover** - LifeKeeper SSP では、このポリシー設定を使用すると、リソースフェイルオーバを有効 / 無効にできます (これによって再起動されます)。
- **LocalRecovery** - LifeKeeper SSP は、デフォルトでは、フェイルオーバ (再起動) を実行する前に、個々のリソースまたは保護対象アプリケーション全体を再起動することにより、保護対象リソースのリカバリを試みます。このポリシー設定を使用すると、ローカルリカバリを有効 / 無効にできます。
- **TemporalRecovery** - 通常、LifeKeeper SSP は、障害リソースのローカルリカバリを実行します。ローカルリカバリに失敗すると、LifeKeeper SSP は再起動を実行します。ローカルリカバリに成功した場合は、フェイルオーバ (再起動) は実行されません。

ローカルリカバリに成功した場合でも、サーバの何らかの異常によって短時間の間にローカルリカバリが再試行される場合があり、結果として何度も連続してローカルリカバリが試行されることになります。これが発生すると、問題のアプリケーションは可用性が悪化します。

この反復的なローカルリカバリ / 障害サイクルを回避するために、時間的リカバリポリシーを設定できます。時間的リカバリポリシーを使用すると、管理者は指定した時間内に試行するローカルリカバリの回数を (成功かどうかにかかわらず) 制限することができます。

> ソースが試行するローカルリカバリの回数を 30 分間で 3 回に限定するポリシー定義をユーザが設定した場合、30 分以内に 3 回目のローカルリカバリが試行されると、LifeKeeper SSP はフェイルオーバ (再起動) を実行します。

定義した時間的リカバリポリシーは有効または無効にできます。時間的リカバリポリシーが無効の場合、時間的リカバリ処理は継続して実行され、ポリシーが適用されるはずの時間に通知がログに表示されますが、実際のアクションは実行されません。

注記: 時間的リカバリポリシーを設定した状態で、フェイルオーバとローカルリカバリの一方または両方を無効にすることは可能です。フェイルオーバまたはローカルリカバリを無効にした場合に、時間的リカバリポリシーは実行されることがないため、この状態は非論理的です。

メタポリシー

「メタ」ポリシーは、他の複数のポリシーに影響を与える可能性があるポリシーです。通常、これらのポリシーは、標準ポリシーであれば複数個の設定が必要になるような特定のシステム動作を実現するためのショートカットとして使用します。

- **NotificationOnly** - このモードでは、管理者は LifeKeeper SSP を「監視専用」状態にすることができます。**1 つのリソース (または、サーバ単位のポリシーの場合はすべてのリソース) の**ローカルリカバリ**および**フェイルオーバ (再起動) **の両方が影響を受けます。**障害が検知されると、ユーザインターフェースには **Failure** 状態が表示されます。ただし、リカバリもフェイルオーバ (再起動) も実行されません。**注記:** 管理者は、障害の原因となった問題を手動で修正し、障害が起きたリソースを復帰させて通常の LifeKeeper SSP の運用を継続する必要があります。

リソースレベルのポリシーに関する重要な考慮事項

リソースレベルのポリシーとは、リソース階層全体またはサーバレベルのポリシーとは異なり、特定のリソースにのみ適用されるポリシーです。

> *例:*
>
> アプリケーション
>
> - IP
>
> - file system
>
> 上記のリソース階層では、アプリケーションは IP とファイルシステムの両方に依存しています。ポリシーは、特定のリソースのローカルリカバリまたはフェイルオーバを無効にするように設定できます。これは、例えば、IP リソースのローカルリカバリが失敗し、IP リソースのフェイルオーバが無効に設定されていた場合、IP リソースはフェイルオーバを実行せず、他のリソースのフェイルオーバも発生させないことを意味します。ただし、ファイルシステムリソー

スのローカルリカバリが失敗し、ファイルシステムリソースのポリシーのフェイルオーバが無効化されていない場合、階層全体が再起動を伴うフェイルオーバを実行します。

注記: 重要事項として、リソースレベルのポリシーは設定対象の特定のリソースにのみ適用されることに注意してください。

上記は単純な例です。複雑な階層を構成することもできるため、リソースレベルのポリシーを設定するときは注意してください。

lkpolicy ツール

`lkpolicy` ツールは、LifeKeeper SSP が稼働するサーバのポリシーを管理 (参照、設定、削除) するためのコマンドラインツールです。`lkpolicy`は、ポリシーの設定および修正、ポリシーの削除、利用可能なポリシーと現在の設定値の表示をサポートします。さらに、設定したポリシーは、有効または無効に設定できるため、リカバリ動作に影響を与えながらリソース / サーバ設定を保持できます。

全体的な使用方法は次の通りです。

```
lkpolicy [--list-policies | --get-policies | --set-policy | --remove-policy] <name value pair data...>
```

`<name value pair data...>` は、運用方法および対象のポリシーによって異なります (特にポリシーを設定する場合)。*たとえば、以下のようになります。*有効 / 無効タイプのポリシーのほとんどでは、必要なのは `-on or --off` のスイッチのみですが、時間的ポリシーの場合は、しきい値を設定するための値も必要です。

lkpolicy の使用方法の例

ローカルおよびリモートサーバとの認証

`lkpolicy` ツールは、サーバが公開する API を通じて LifeKeeper SSP サーバと通信します。この API は、`lkpolicy` ツールなどのクライアントに対して認証を要求します。`lkpolicy` ツールで LifeKeeper SSP サーバに最初にアクセスしようとしたときに、そのサーバに対する認証情報がまだ保存されていない場合、ユーザは認証情報を求められます。認証情報はユーザ名とパスワードの形式であり、さらに以下の条件があります。

1. クライアントには LifeKeeper SSP の管理者権限が必要です。したがって、そのユーザ名は、(PAM による) オペレーティングシステムの認証設定によって `lkadmin` グループに属する必要があります。必ずしも **root** で実行する**必要はありません**が、root ユーザはデフォルトで適切なグループに属しているため、root を使用することもできます。
2. 認証情報は*認証情報ストア*に保存されるため、ツールを使用してこのサーバにアクセスするたびに手動で認証情報を入力する必要はありません。

認証情報ストアと credstore ユーティリティによる管理の詳細については、SIOS Protection Suite の認証情報の設定を参照してください。

`lkpolicy` によるセッションの例は以下のようになります。

```
[root@thor49 ~]# lkpolicy -l -d v6test4
```

```
Please enter your credentials for the system 'v6test4'.
Username: root
Password:
Confirm password:
Failover
LocalRecovery
TemporalRecovery
NotificationOnly
[root@thor49 ~]# lkpolicy -l -d v6test4
Failover
LocalRecovery
TemporalRecovery
NotificationOnly
[root@thor49 ~]#
```

ポリシーのリスト表示

lkpolicy --list-policy-types

現在のポリシーの表示

lkpolicy --get-policies

lkpolicy --get-policies tag=*

lkpolicy --get-policies --verbose tag=mysql* # all resources starting with mysql

lkpolicy --get-policies tag=mytagonly

ポリシーの設定

lkpolicy --set-policy Failover --off

lkpolicy --set-policy Failover --on tag=myresource

lkpolicy --set-policy Failover --on tag=*

lkpolicy --set-policy LocalRecovery --off tag=myresource

lkpolicy --set-policy NotificationOnly --on

lkpolicy --set-policy TemporalRecovery --on recoverylimit=5 period=15

lkpolicy --set-policy TemporalRecovery --on --force recoverylimit=5 period=10

ポリシーの削除

lkpolicy --remove-policy Failover tag=steve

注記:*NotificationOnly* はポリシーのエイリアスです。*NotificationOnly* を有効にすることは、対応する LocalRecovery および Failover ポリシーを無効にすることと同じです。

LifeKeeper Single Server Protection のインストールの検証

LifeKeeper Single Server Protection パッケージが正常にインストールされたことを確認するには、コマンドラインで次のように入力してください。

```
rpm -V <package name>
```

注記: パッケージが正しくインストールされている場合、このコマンドは何も出力しません。

コマンドラインから照会を実行するには、次のように入力してください。

```
rpm -qi <package name>
```

注記: このコマンドの予想される出力は、パッケージ情報です。

Chapter 3: 管理

LifeKeeper Single Server Protection の管理の概要

LifeKeeper Single Server Protection は操作時に管理を必要としません。LifeKeeper Single Server Protection は、保護されたリソースを監視し、障害が発生した場合に指定されたリカバリアクションを実行するように、自動的に機能します。以下のケースでは LifeKeeper Single Server Protection GUI を使用します。

- **リソースおよび階層の定義**。LifeKeeper Single Server Protection は次のインターフェースオプションを提供します。
    - LifeKeeper Single Server Protection GUI。
    - LifeKeeper Single Server Protection コマンドラインインターフェース。
- **リソース監視。**LifeKeeper Single Server Protection GUI は、リソースステータス情報および LifeKeeper Single Server Protection ログへのアクセスを提供します。
- **手動での処理。**メンテナンスやその他の管理アクションのために、サーバまたは特定のリソースを停止することが必要になる場合があります。LifeKeeper Single Server Protection GUI には、特定のリソースを稼動させたり停止させたりすることができるメニュー機能が用意されています。アプリケーションが LifeKeeper Single Server Protection の保護下に置かれると、これらの LifeKeeper Single Server Protection のインターフェースを介してのみアプリケーションを起動および停止させることができます。LifeKeeper Single Server Protection の起動および停止は、コマンドラインを介してのみ行われます。

リソース階層の作成など、管理、設定、およびメンテナンス操作を実行する詳細な手順については、SPS for Linux ドキュメンテーションの管理作業、GUI の作業、およびメンテナンス作業を参照してください。

※Lifekeeperが提供しているコマンド(実行可能なスクリプトやプログラム)を実行するには、スーパーユーザ権限が必要です。

su コマンドや sudo でスーパーユーザ権限を付与したユーザで、LifeKeeper のコマンドを実行することは可能ですが、SIOS Technology Corp では、root ユーザ以外で LifeKeeper のコマンドのテストはしていません。

VMware HA と LifeKeeper Single Server Protection の連携を有効にする

デフォルトでは、VMware VM 上にインストールした場合、LifeKeeper Single Server Protection と VMware HA の連携は無効になっています。連携を有効にするには、以下の手順が必要です。

1. LifeKeeper Single Server Protection VM に VMware Tools をインストールしてください。
2. */etc/default/LifeKeeper* を編集して、VMware HA 連携を調整する `HA_DISABLE` の値を 1 から 0 に変更します。
3. LifeKeeper Single Server Protection を再起動します。LifeKeeper Single Server Protection が実行中の場合、`/etc/default/LifeKeeper` の上記の変更内容が検出されるように、停止してから再起動する必要があります。
4. SteelEye 管理コンソールをインストールします (オプション)。

VMware HA を有効化した障害検出およびリカバリシナリオ

アプリケーション内の問題を検出して通知する機能は、最適な総合的耐障害性ソリューションを構築する上で非常に重要です。すべての個々のアプリケーションは、障害発生のメカニズムと形式によって異なるため、一般的なメカニズムを示すことはできません。ただし、一般的に、多くのアプリケーションの設定は、LifeKeeper Single Server Protection に用意されている Core システムのエラー検出機能を利用することができます。このトピックでは、LifeKeeper Single Server Protection Core の機能について説明します。

アプリケーションに障害が発生したときに LifeKeeper Single Server Protection が障害を検出しリカバリを実行する仕組みを説明したリカバリシナリオを以下に示します。

1. LifeKeeper Single Server Protection は最初に、アプリケーションを再起動することでリカバリを試みます。
2. リカバリが成功した場合、アプリケーションは正常動作を継続します。
3. リカバリに失敗した場合、以下の処理が実行されます。
   a. LifeKeeper Single Server Protection が HA を有効 (/etc/default/LifeKeeper で HA_DISABLE=0) にした VMware ゲスト OS にインストールされている場合にリカバリに失敗すると、LifeKeeper Single Server Protection がアプリケーション監視インターフェースに送信するハートビートを抑制することで VMware HA がトリガされます。VMware HA はサーバを再起動することで応答します。

   b. LifeKeeper Single Server Protection が VMware ゲスト OS にインストールされていないか、HA を無効 (/etc/default/LifeKeeper で HA_DISABLE=1) にした VMware ゲスト OS にインストールされている場合にリカバリに失敗すると、システムが強制的に再起動されます。

必要に応じて、LifeKeeper Single Server Protection を**通知のみ**モードにすることができます。このモードでは、システム再起動の自動トリガは無効になります (以下の VMware HA と通知のみモードセクションを参照)。**通知のみ**モードでは、ユーザがシステムにログインし、障害の原因になった問題を修正する必要があります。

VMware HA と通知のみモード

1. VMware ゲスト OS で HA が有効にされ、LifeKeeper SSP vCenter プラグインがインストールされた**通知のみ**モードでは、障害が検出された場合、LifeKeeper Single Server Protection はアプリケーションの再起動を行いません。その代わりに、リソースは **[Failed]** とマークされます。vCenter プラグインダッシュボードのステータス表示画面には障害が表示されます (**[Application Status] : [Failed]**)。

Application Name	Application Status
Login failed: Couldn't resolve host name (6)	N/A
Apache	**Failed**
Login failed: Couldn't connect to server (7)	N/A
Login failed: Couldn't connect to server (7)	N/A
N/A	N/A
Login failed: Couldn't resolve host name (6)	N/A

2. サーバにログインして、障害の原因になった問題を修正します。
3. **CLI** を使用するか、**vSphere Client ユーザインターフェース**内の保護対象仮想マシンをクリックして、**LifeKeeper 管理コンソール**を開いてください。

4. アプリケーションを In Service に戻します。
5. **vSphere Client ユーザインターフェース**内の**ダッシュボード**表示に移動します。
6. **[Refresh]** をクリックします。**[Application Status]** は **[Active]** に戻ります。

Application Name	Application Status
Login failed: Couldn't resolve host name (6)	N/A
Apache	**Active**
Login failed: Couldn't connect to server (7)	N/A
Login failed: Couldn't connect to server (7)	N/A
N/A	N/A
Login failed: Couldn't resolve host name (6)	N/A

LifeKeeper Single Server Protection ハートビートと VMware HA

LifeKeeper Single Server Protection ハートビートは、保護対象のアプリケーションが正常であることを示すために、(VMware ゲスト OS で動作し、HA が有効である場合、10 秒ごとに) VMware HA に送信される信号です。アプリケーションで障害が発生すると、LifeKeeper Single Server Protection は最初にアプリケーションを復旧しようとします。復旧に失敗すると、LifeKeeper Single Server Protection はハートビートを抑制し、VMware HA に VM の再起動を指示します。

LifeKeeper Single Server Protection で保護するシステムのメンテナンス

LifeKeeper Single Server Protection で保護されているサーバでシステムまたはアプリケーションのメンテナンスを実行するときには、LifeKeeper Single Server Protection による監視を停止するか、保護対象のリソースをメンテナンスモードにしてください。これにより、アプリケーションのリカバリ、および VMware HA の障害イベントのトリガが無効になるので、LifeKeeper Single Server Protection がシステムやアプリケーションのメンテナンス作業に干渉しなくなります。

LifeKeeper Single Server Protection を停止して再起動するには、以下の操作を実行してください。

1. **LifeKeeper Single Server Protection を停止します。** `/etc/init.d/lifekeeper stop-daemons` コマンドを使用して、LifeKeeper Single Server Protection を停止してください。リソースは継続して動作しますが、LifeKeeper Single Server Protection からは監視されなくなります。障害は手動で処理する必要があります。
2. **メンテナンスを実行します。** 必要なメンテナンスを実行します。
3. **SIOS LifeKeeper Single Server Protection を起動します。** `/etc/init.d/lifekeeper start` コマンドを使用して、LifeKeeper Single Server Protection を開始してください。リソースが保護されている状態になります。

別の方法 - リソースをメンテナンス (「通知のみ」とも呼ばれる) モードにします。以下の操作を実行してください。

1. **リソースをメンテナンスモードにします。** `/opt/LifeKeeper/bin/lkpolicy -s NotificationOnly --On` コマンドを使用してください。リソースは復旧されなくなり、VMware HA の障害イベントがトリガされなくなります。
2. **メンテナンスを実行します。** 必要なメンテナンスを実行します。
3. **メンテナンスモードをオフにします。** `/opt/LifeKeeper/bin/lkpolicy -s NotificationOnly --Off` コマンドを使用してください。リソースが保護されている状態になります。

Chapter 4: FAQ

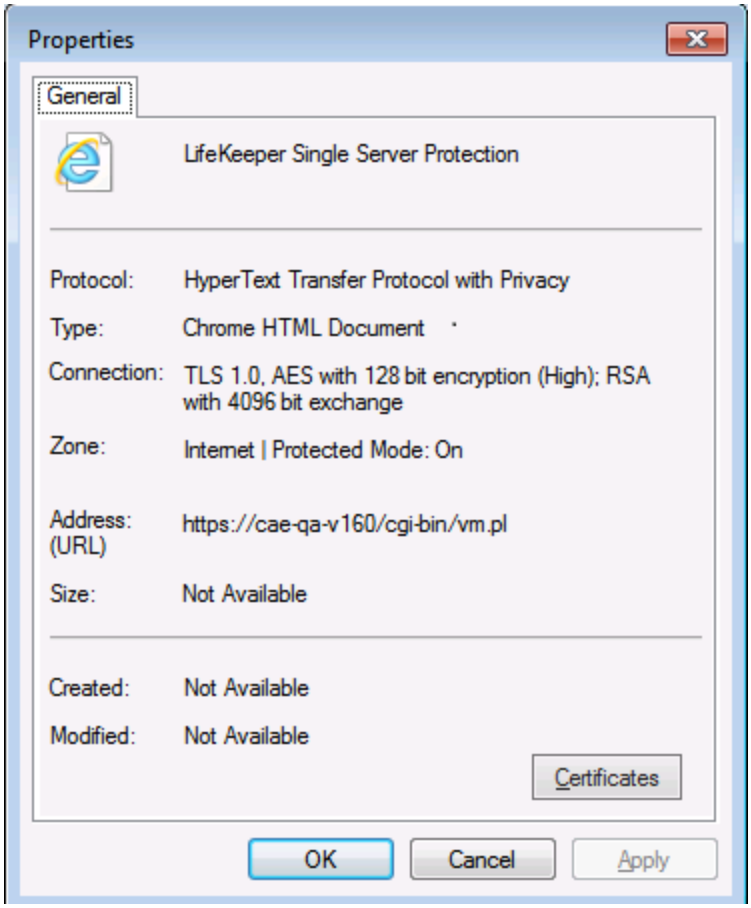
SMC

質問

(プラグインから) 使用している SMC を調べる方法はありますか。

回答

右クリックして、プラグイン Web ページの **[Properties]** を表示します。



回答

Chapter 5: トラブルシューティング

このセクションには、LifeKeeper Single Server Protection の制限または既知の問題と、SMC のトラブルシューティングのヒントが記載されています。

トラブルシューティング情報の詳細については、の LifeKeeper テクニカルノートおよびトラブルシューティングの各トピックを参照してください。

既知の問題と回避策

下記に、LifeKeeper Single Server Protection で明らかになっている制限または既知の問題を示します。

Core

バグ 2257

LifeKeeper Single Server Protection および SIOS Protection Suite のノードに

credstore 経由でアクセスするときに、正しい credstore キーが必要です

解決方法: `credstore` を使用して、LifeKeeper Single Server Protection または SIOS Protection Suite のノードの認証情報を保存するときに、credstore の認証情報キーについてホスト名の正しい形式 (`credstore -k <hostname>`) を使用する必要があります。

LifeKeeper Single Server Protection プラグインの場合、LifeKeeper Single Server Protection プラグイン画面の **[Hostname:]** フィールドに表示されるシステムのホスト名を使用して `credstore` を実行する必要があります。

SIOS Protection Suite の場合、認証情報の保存に使用するホスト名は、コマンドラインツール (`lkpolicy` など) の -d 引数に使用するものと同じである必要があります。例えば、**`lkpolicy -d mynode1`**, を実行する場合、**`credstore -k mynode1`** を使用して認証情報を保存する必要があります。この場合、認証情報の保存に FQDN を使用することはできません。FQDN を使用する場合は、**`lkpolicy -d`** *FQDN* を実行する必要があります。

対応策: LifeKeeper Single Server Protection または SIOS Protection Suite のすべてのノードで機能するデフォルトの認証情報セット (**`credstore -k default`**) を保存した場合、この問題の影響を受けることはありません。

バグ 2408

HA ハートビートが不正に有効になります

2 番目のリソースに障害が発生した後、lkvmhad が HA ハートビートを不正に有効にします。

対応策: */etc/default/LifeKeeper* の LKCHECKINTERVAL に、VMware HA の [VM Monitoring Failure Interval] (VM の障害監視間隔) よりも大きい値を設定してください。**注記:** LKCHECKINTERVAL のデフォルト値は 120 秒です。また、これは、VMware HA の VM 監視の監視感度「low」のデフォルト値でもあります。

openssl-develがインストールされていない場合SMCをインストールできません。

v8.3.2のSMCをインストールする際には、あらかじめopenssl-develがインストールされている必要があります。インストールしてない場合、以下のようなメッセージを出力してSMCのインストールに失敗します。

ld -shared -o ./lib/Crypt-SSLeay-0.55-0.9.8/lib/auto/Crypt/SSLeay/SSLeay.so ./lib/Crypt-SSLeay-0.55-0.9.8/lib/auto/Crypt/SSLeay/SSLeay.o -lcrypto -lssllld: cannot find -lcrypto

Unable to link the Crypt::SSLeay Perl module. Secured connections will be unavailable until you install the Crypt::SSLeay module.

So required libcrypt.a in system library.

setupスクリプトを実行した際に、上記のようなメッセージが出力された場合、OSに同梱されているopenssl-develをインストールしてから、再度setupスクリプトを実行してください。

GUI

LifeKeeper Single Server Protection GUI の更新の問題

GUI のリソースツリーが不規則に表示されることがあります (リソースの依存関係が正しく表示されない)。

対応策: GUI の更新を実行してください。

IP

バグ 2398

bonding NIC に割り当てられているものの、「暫定的な」状態のアドレスでは、IPv6 リソースが ISP としてレポートされます

LifeKeeper Single Server Protection の IPv6 保護リソースが、'active-backup' (1) 以外のモード、かつ 2.6.21 以前の Linux カーネルの bonding インターフェース上にある場合、SLES システムでは、この IPv6 保護リソースが、「In Service Protected」 (ISP: in service の保護) と不正に識別されます。
IPv6 の bonding リンクは、解決できないアドレスを持つ「暫定的な」状態のままになります。

対応策: bonding インターフェースモードを 'active-backup' (1) に設定します。または、'active-backup' (1) 以外のモードの場合、リンク状態を「tentative (暫定的)」から「valid (有効)」に設定する更新したカーネルで操作します。

Apache

Apache リソースの作成に失敗する

エラーメッセージの例:

Error: valid_http_root: Since "/usr/sbin/httpd" is shareable on "/usr", "/etc/httpd" must be also

原因:

不具合のため、マウントポイント"/"(root)にあるファイルを正しく検索できません。

例えば、マウントポイント"/"と同じファイルシステムに/etc/httpdがある場合、リソースの作成に失敗します。

対応策:

次のいずれかのようにマウントすることにより、エラーを回避することができます。

(a) /etc/httpdなどを別のマウントポイント以下に移動する

(b) /etcを/dev/sdb1などにマウントする

Oracle

バグ 2387

LifeKeeper Single Server Protection 環境の root ファイルシステムに、Oracle 階層を作成できません。

対応策: 以下の手順に従って、Oracle を新しいファイルシステムにコピーしてください。

Oracle データを格納できる十分に大きい新しいディスク (例: /dev/sdb) を作成してください。(注記: ディスクの大きさを見積もるために、/oracle ディレクトリの大きさを参考にできます。ログを含めるために、50 % 以上増加してください)。

fdisk を使用して、そのディスクに新しいパーティションを作成してください。

```
fdisk /dev/sdb
```

ファイルシステムを作成してください。

mkfs -t ext3 /dev/sdb1

このファイルシステムをマウントしてください (この例では /mnt/oracle を使用)。

mkdir /mnt/oracle

mount /dev/sdb1 /mnt/oracle

Oracle と Listener を停止してください。

Oracle を新しいファイルシステムにコピーしてください。

cd /oracle

cp -a * /mnt/oracle

(**注記**: データ量により、この手順には時間がかかることがあります)

新しいファイルシステムをアンマウントしてください。

umount /mnt/oracle

新しいファイルシステムを /oracle にマウントしてください。

mount /dev/sdb1 /oracle

Listener を開始し、次に Oracle を開始してください。

SAP

バグ 2388

SAP の場合、GUI を使用して階層を作成することはできません。

対応策: コマンドラインオプションを使用して、階層を作成してください。ただし、以下に示すように、コマンドラインの最後に番号 76 を指定してください。

```
$LKROOT/lkadm/subsys/appsuite/sap/bin/create <primary sys> <tag> <SAP SID>
<SAP Instance> <switchback type> <IP Tag> <Protection Level> <Recovery
Level> <Additional SAP Dependents> 76
```

コマンドラインの詳細については、「コマンドラインによる SAP の設定」を参照してください。

SMC のトラブルシューティング

以下に、トラブルシューティングに関するヒントを示します。

LifeKeeper Single Server Protection が監視するゲストの仮想マシンには、VMware Tools がインストール済みである必要があります。

LifeKeeper Single Server Protection は、VMware Tools が有効にインストールされていない仮想マシンに接続できません。SteelEye 管理コンソールはこれらのマシンに接続できないので、マシンとそのリソースの完全なステータスを取得できません。vSphere Client 内の LifeKeeper Single Server Protection プラグインは、これらのゲスト (ツールがインストールされていない場合) に関するエラーメッセージを表示します。

解決方法: LifeKeeper Single Server Protection が保護するゲストマシンには、必ず VMware Tools をインストールしてください。