



LifeKeeper Single Server Protection

v9.3.1

インストレーションガイド

2018年 11月

本書およびその内容は SIOS Technology Corp. (旧称 SteelEye® Technology, Inc.) の所有物であり、許可なき使用および複製は禁止されています。SIOS Technology Corp. は本書の内容に関していかなる保証も行いません。また、事前の通知なく本書を改訂し、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。SIOS Technology Corp. は、新しい技術、コンポーネント、およびソフトウェアが利用可能になるのに合わせて製品を改善することを方針としています。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留します。

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使用されており、各社の商標が含まれています。

出版物の品質を維持するために、弊社は本書の正確性、明瞭性、構成、および価値に関するお客様のご意見を歓迎いたします。

以下の宛先に電子メールを送信してください。

ip@us.sios.com

Copyright © 2018

By SIOS Technology Corp.

San Mateo, CA U.S.A.

All rights reserved

目次

はじめに	1
LifeKeeper Single Server Protection for Linux について	1
インストール	3
LifeKeeper Single Server Protection ソフトウェアのインストール	3
LifeKeeper Single Server Protection ソフトウェアのインストール	3
Chapter 2: インストール	4
セットアップの手順	4
インストール後の構成変更	5
修復インストール	5
対話画面の操作	5
認証の設定	6
リカバリキットの選択	7
インストール開始前の確認	8
setup スクリプトのオプション	9
Upgrade_LifeKeeper_Single_Server_Protection	10
SSP のアップグレード	10
リソースポリシー管理	12
概要	12
LifeKeeper SSP のリカバリ動作	12
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	13
標準ポリシー	13
メタポリシー	13
リソースレベルのポリシーに関する重要な考慮事項	14
lkpolicy ツール	14
lkpolicy の使用方法の例	14

ローカルおよびリモートサーバとの認証	14
ポリシーのリスト表示	15
現在のポリシーの表示	15
ポリシーの設定	16
ポリシーの削除	16
LifeKeeper Single Server Protection のインストールの検証	16

はじめに

LifeKeeper Single Server Protection for Linux について

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、システムのリポートまたは 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、NEC SPS)

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ー (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ー
- 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。

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 (SSP) 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。

9.3以降のセットアップはパッケージマネージャ (yum もしくは zypper) を使用してパッケージをインストールするため、LifeKeeper が依存するパッケージは自動的にインストールされるようになりました。



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もしくは非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一式を提供します。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ス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。

[LifeKeeper Single Server Protection リリースノート](#)を参照してください。

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

インストール作業は[セットアップスクリプトの操作](#)を参照してください。

アップグレード方法については、[SSP のアップグレード](#)を参照してください。

Chapter 2: インストール

セットアップスクリプトは、LifeKeeper SSPをインストールするために以下の作業を行います。

1. 環境情報の収集

スクリプトがLifeKeeper SSPを動作させるために必要な情報を収集します。
これには数十秒から数分程度かかります。

2. 構成の決定

使用する機能や保護対象アプリケーションを決定します。
対話画面で個別に決定していくか、あらかじめ用意した構成情報ファイルを用いて非対話で一括して決定することが可能です。

3. パッケージのインストールと設定変更

ステップ2で決定した構成を元に、スクリプトが必要なパッケージのインストール及び設定変更を行います。

セットアップの手順

1. root ユーザーでログイン後、次のコマンドを使用して、lkssp.img ファイルをマウントします。

```
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ます。

```
./setup [コマンドオプション]
```

指定可能なオプションは「[setup スクリプトのオプション](#)」を参照してください。

3. スクリプトを実行すると、まず環境情報の収集を行います。

対話モードでは、収集した環境情報を収集した結果、問題があると判断された場合は重要度に応じて「Pre-install check failed!!」もしくは「Pre-install warning」の画面に切り替わります。

「Pre-install check failed!!」は、インストールを行う環境がLifeKeeper SSPのインストール要件を満たしていない等の重大な問題を検出した場合に表示されます。これが表示された場合にはインストールを続行することは出来ないので、スクリプトは中断されます。

「Pre-install warning」はLifeKeeper SSPを使用することは可能ですが、手動での設定変更が必要な場合や、一部機能が制限される場合などに表示されます。これが表示された場合でもインストールを継続することは可能です。

なにも問題がなかったか、「Pre-install warning」で継続した場合はメニュー画面に切り替わります。メニュー画面の操作は「[対話画面の操作](#)」を参照して下さい。

非対話モードでは、問題を発見した場合にはその結果を表示してスクリプトは終了します。「Pre-install warning」に相当する問題の場合はスクリプト実行時に"-qy" オプションを指定して再実行することで、インストールを継続することが出来ます。

4. 構成を決定すると、実際のインストール作業が開始されます。

インストール中に問題が発生した場合にはエラーメッセージが表示されるので、問題を解消してからセットアップスクリプトを再度実行してください。

また、インストール完了後に "Important notice" が出力された場合は、その指示に従ってください。

インストール後の構成変更

インストール後に構成変更を行う場合は setup を再実行して下さい。

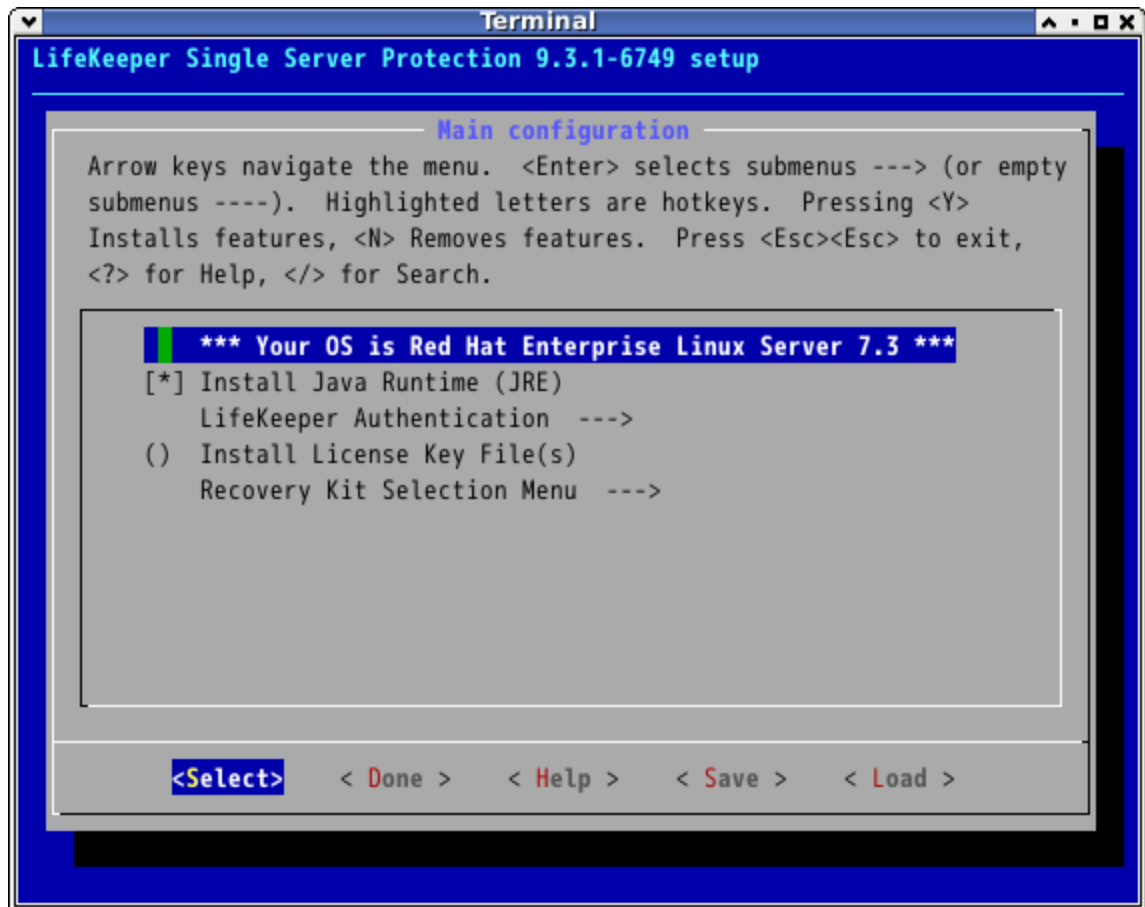
選択した機能は追加でインストールされ、選択を解除した機能はアンインストールされます。

修復インストール

何らかの理由で LifeKeeper SSP を再インストールする場合は「--force」オプションを指定して setup を再実行して下さい。

対話画面の操作

LifeKeeper SSP の構成を以下の画面で決定します。



認証の設定

以下のキーで項目選択を行います。

↑↓	選択項目の移動
TAB	最下行ボタンの移動
SPACE / Enter	選択されているボタンの処理を実行

最下行ボタンは以下の動作を行います。

Select	選択項目のON / OFF・子画面へ移動
Done	現画面を終了して親画面に戻ります Main Configuration 画面の場合は、メニュー画面を終了して、インストールの確認画面へ移行します
Help	選択項目のヘルプ画面を表示します
Save	設定した構成情報をファイルに保存します 保存した構成情報ファイルは非対話モードでのインストールに使用できます
Load	保存済み構成情報ファイルの読み込み

各項目では以下の機能を設定できます。

なお、各項目は設定が必要な場合のみ表示されます。

- **Install Java Runtime (JRE)**

LifeKeeper SSP の GUI が使用する Java 実行環境をインストールします。

- **LifeKeeper Authentication**

LifeKeeper SSP を管理するために必要なユーザーの登録を行います。

子画面に移動します。

- **Install License Key File(s)**

LifeKeeper SSP のライセンスファイルを指定します。ファイル名を入力できるダイアログに切り替わるので、ライセンスファイルのフルパス名を入力して下さい。スペース区切りで複数のライセンスファイルを指定することが出来ます。

ライセンスの取得方法については[ライセンスの取得とインストール](#)を参照してください。

- **Recovery Kit Selection Menu**

保護対象アプリケーションに対応したリカバリキットを選択します。

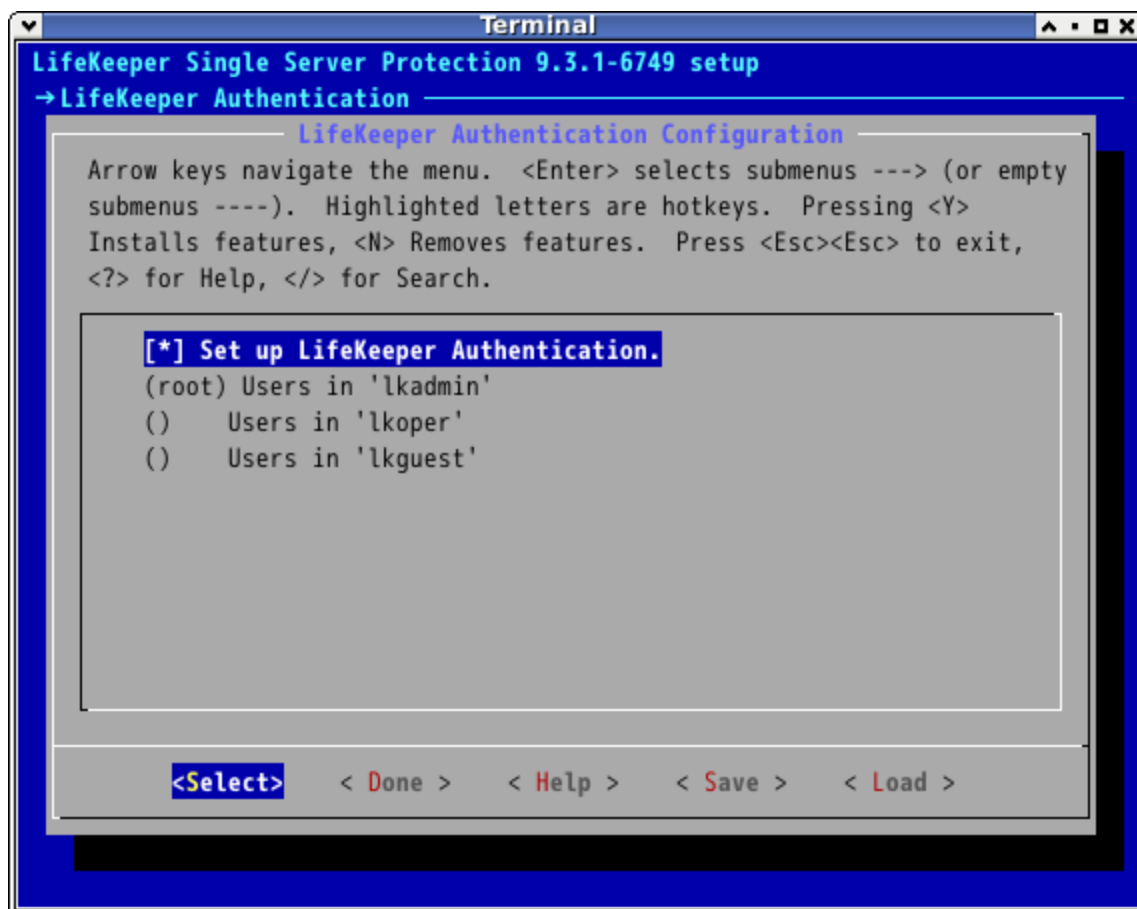
子画面に移動します。

- **LifeKeeper Startup After Install**

インストールもしくはアップデート完了後に LifeKeeper SSP を起動します。

LifeKeeper SSP が起動可能な場合のみ選択可能です。

認証の設定



以下の項目を設定可能です。

- **Set up LifeKeeper Authentication.**

選択するとユーザー情報の設定を行います。

リモートで認証する設定(NIS / LDAP など)の場合は選択しても反映されません。

- **Users in 'lkadmin' / Users in 'lkoper' / Users in 'lkguest'**

各グループに所属するユーザー名を指定できます。

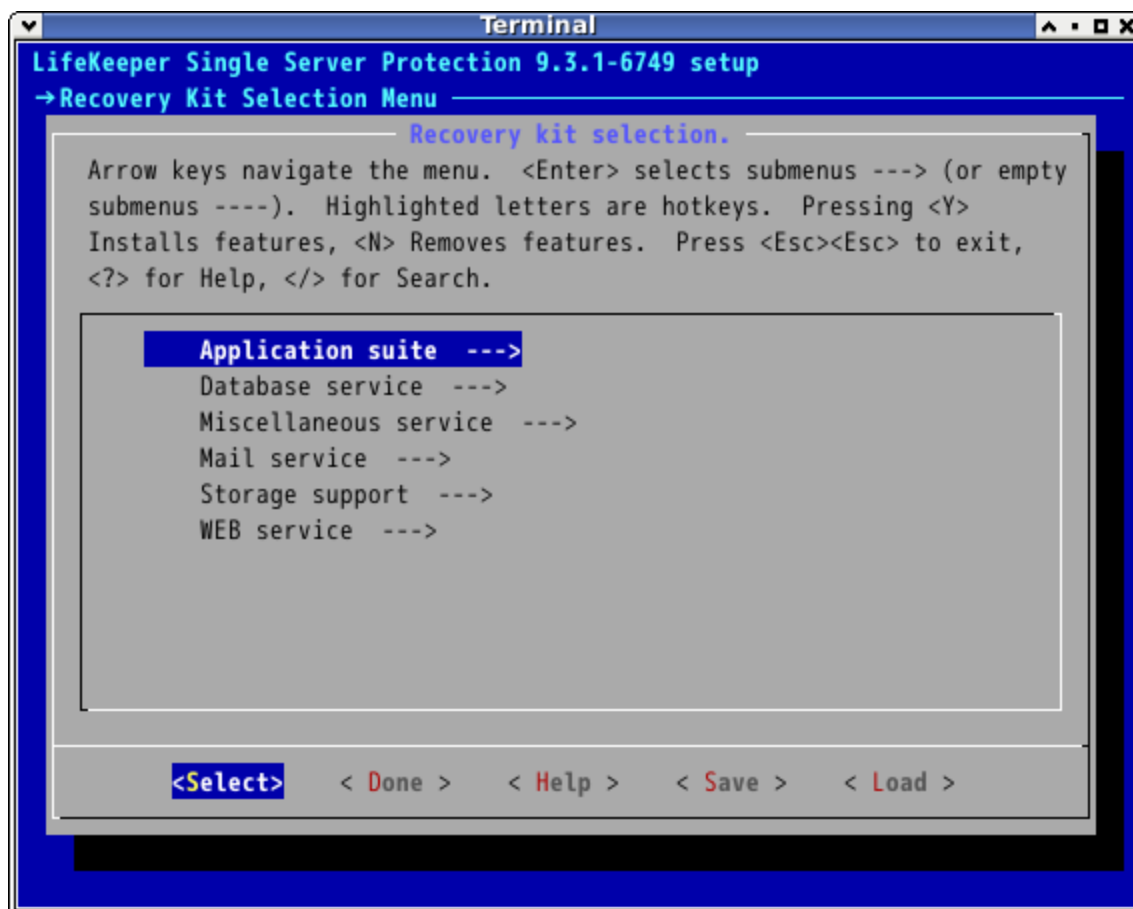
各グループの機能はテクニカルドキュメンテーションの[GUI ユーザー設定](#)を参照してください。

リカバリキットの選択

各リカバリキットはカテゴリごとに分類されています。

カテゴリを選択して、その中から個々のリカバリキットを選択して下さい。

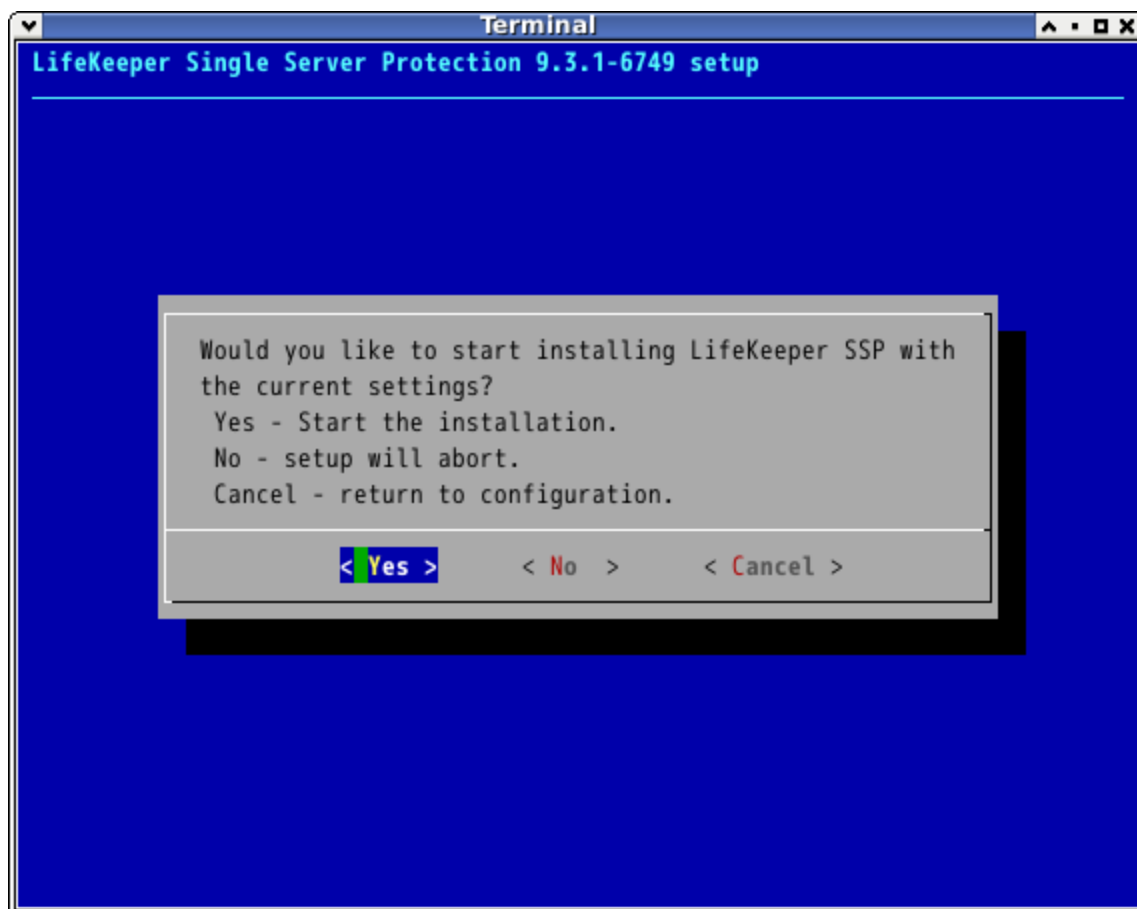
インストール開始前の確認



各カテゴリは以下の意味を持ちます。

カテゴリ	説明
Application suite	SAP/MQ など上位のアプリケーションを保護するリカバリキットが所属します
Network / Communication	ネットワークサービスに関係するリカバリキット及び IP リカバリキットと協調して動作するリカバリキットが所属します
Database service	各種データベースを保護するリカバリキットが所属します
Miscellaneous service	ファイルサーバーなど、汎用的なサービスを保護するリカバリキットが所属します
Mail service	メールサーバーを保護するリカバリキットが所属します
Storage support	ファイルシステム・ストレージに関係するリカバリキットが所属します
WEB service	WEBサーバーを保護するリカバリキットが所属します

インストール開始前の確認



Main Configuration 画面で Done を選択すると、この画面に移動します。

ここで実際のインストールを行うための最終確認が行われます。TAB キーでボタンを移動してEnter で確定します。

各ボタンは以下の動作を行います。

Yes	インストールを開始します
No	インストールを中断してスクリプトを終了します
Cancel	Main Configuration に戻ります

setup スクリプトのオプション

setup スクリプトは以下のオプションを指定して実行することができます。

- -f <file>

非対話的にインストールを行います。file は対話画面で Save することで保存される構成ファイルを指定します。

- -q <y/n>

非対話モードでインストールする時に、確認項目に対する応答を指定します。
現在は "y" を指定すると、Pre-install warning に了解しインストールを継続という意味を持ちます。

- `--force`

すでにインストール済みのパッケージを強制的に再インストールします。

Upgrade_LifeKeeper_Single_Server_Protection

SSP のアップグレード

LifeKeeper Single Server Protection (SSP) は、既存の階層を保ちながら将来のリリースにアップグレードすることができます。

注記: 最新バージョンの LifeKeeper Single Server Protection にアップグレードできるのは、2 世代前までのバージョンです。それより前のバージョンからアップグレードする場合、古いバージョンをアンインストールし、LifeKeeper Single Server Protection を再インストールする必要があります。旧バージョンをアンインストールする代わりに、旧バージョンを 1 世代前もしくは 2 世代前のバージョンにアップグレードした上で、最新バージョンにアップグレードする方法もあります。

注記: アップグレード中に lkbakcup を使用する場合は、[lkbakcup の既知の問題](#)を参照してください。

1. 必要な場合、SSP をアップグレードする前に、Linux オペレーティングシステムをアップグレードしてください。
2. [セットアップスクリプトの操作](#)を参照してLifeKeeperをアップグレードします。

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が。
2. **SIOS Technology Corp. ライ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ー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. **フェイルオーバー:** 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、**フェイルオーバー** 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ーを有効 / 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、フェイルオーバー(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、フェイルオーバー(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 はフェイルオーバー(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、フェイルオーバー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。フェイルオーバー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ー(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ー(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ー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ー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ーを実行せず、他のリソースのフェイルオーバー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ー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ーを実行します。

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。

lcpolicy ツール

lcpolicy 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。lcpolicy 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。

```
lcpolicy [--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。

lcpolicy 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

lcpolicy 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、lcpolicy ツールなどのクライアントに対して認証を要求します。lcpolicy 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

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。