



LifeKeeper Single Server Protection

v8.2

Installation Guide

October 2013

This document and the information herein is the property of SIOS Technology Corp. (previously known as SteelEye® Technology, Inc.) and all unauthorized use and reproduction is prohibited. SIOS Technology Corp. makes no warranties with respect to the contents of this document and reserves the right to revise this publication and make changes to the products described herein without prior notification. It is the policy of SIOS Technology Corp. to improve products as new technology, components and software become available. SIOS Technology Corp., therefore, reserves the right to change specifications without prior notice.

LifeKeeper, SteelEye and SteelEye DataKeeper are registered trademarks of SIOS Technology Corp.

Other brand and product names used herein are for identification purposes only and may be trademarks of their respective companies.

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

Copyright © 2013
By SIOS Technology Corp.
San Mateo, CA U.S.A.
All rights reserved

Table of Contents

Installing the LifeKeeper Single Server Protection Software	4
Installing the LifeKeeper Single Server Protection Software	5
Resource Policy Management	8
Overview	8
LifeKeeper SSP Recovery Behavior	8
Custom and Maintenance-Mode Behavior via Policies	8
Standard Policies	9
Meta Policies	9
Important Considerations for Resource-Level Policies	9
The lkpolicy Tool	10
Example lkpolicy Usage	10
Authenticating With Local and Remote Servers	10
Listing Policies	11
Showing Current Policies	11
Setting Policies	11
Removing Policies	12
Verifying LifeKeeper Single Server Protection Installation	12

LifeKeeper Single Server Protection (SSP) allows for application monitoring in a single node configuration (i.e., no cluster requirements or restraints). Single node environments may be physical or virtual (vSphere, KVM). LifeKeeper SSP is built on the proven and stable architecture of SteelEye LifeKeeper. LifeKeeper SSP provides superior application monitoring and can perform recovery of failed applications and system infrastructure items (e.g., NFS share, IP address, File System). If an application cannot be recovered for some reason, LifeKeeper SSP will initiate a restart of the node via a system reboot or via a VMware HA restart for VMware virtual machines configured for VM and Application Monitoring.

Note: Because LifeKeeper SSP is built using the SteelEye LifeKeeper technology, you will see references to LifeKeeper throughout the documentation as well as references to information found in the SteelEye Protection Suite for Linux documentation for topics common to both products. When referencing these common topics the following subject items do not apply to LifeKeeper SSP:

- Clustering
- Communication Paths

- Shared Storage (requirements, configuration, ...)
- Extending / Unextending resource hierarchies
- Storage Kits (DR, DMMP, HDLM, LVM, MD, and PPATH)

Note: Without the underlying storage kits in LifeKeeper SSP, steps must be taken to ensure the devices required to mount protected file systems are activated during system boot (e.g. if the file system is mounted on a logical volume the volume must be in the active state before LifeKeeper SSP starts)

- Resource/Machine failovers (by default with LifeKeeper SSP these result in a node restart)
- Resource switchovers
- Switchable IP Addresses (with LifeKeeper SSP Switchable IP addresses are required for some protected applications but since there is only a single node no switching actually takes place)

For more information on the SteelEye LifeKeeper product, on which LifeKeeper SSP is built, please see the [SteelEye Protection Suite for Linux documentation](#) for the common release number. This documentation will provide detailed information on resource hierarchy creation, resource types, states and relationships, Graphical User Interface (GUI), as well as common and advanced tasks.

Installing the LifeKeeper Single Server Protection Software

Install the LifeKeeper Single Server Protection software on each server in the LifeKeeper Single Server Protection configuration. Each LifeKeeper Single Server Protection server must have the packages necessary to support your configuration requirements, including any optional Recovery Kit packages.



IMPORTANT: Please review the [Linux Dependencies](#) topic prior to installing LifeKeeper Single Server Protection .

The LifeKeeper Single Server Protection core package and any optional recovery kits will be installed through the command line using the LifeKeeper Single Server Protection Installation Image File (*lkssp.img*). This image file provides a set of installation scripts designed to perform user-interactive system setup tasks that are necessary when installing LifeKeeper Single Server Protection on your system. The installation image file identifies what Linux distribution you are running and, through a series of questions you answer, installs various packages required to ensure a successful LifeKeeper Single Server Protection installation. A licensing package is also installed providing utilities for obtaining and displaying the Host ID of your server and your Entitlement ID once your licenses have been installed. The Entitlement ID is used to obtain valid licenses for running LifeKeeper Single Server Protection and was provided with your Software.

Note: These installation instructions assume that you are familiar with the Linux operating system installed on your servers.



IMPORTANT:

- LifeKeeper Single Server Protection does not provide shared storage support or I/O fencing. Each server must use local disk storage for application data.
- All LifeKeeper Single Server Protection packages are installed in the directory */opt/LifeKeeper*.
- If you are re-installing the existing version of LifeKeeper, you must remove the old LifeKeeper packages first. A standard LifeKeeper installation requires that you redefine any existing resource hierarchies. If you wish to retain your current resource hierarchy definitions, refer to the .
- If you receive an error message referencing the LifeKeeper Distribution Enabling package when you are installing LifeKeeper Single Server Protection you should run/re-run the **setup** script on the LifeKeeper Single Server Protection Installation Image File.

Installing the LifeKeeper Single Server Protection Software

LifeKeeper Single Server Protection will be installed through the command line regardless of the Linux distribution you are operating under.

1. Mount the `lkssp.img` file using the following command:

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

Where PATH is the path to the image
IMAGE_NAME is the name of the image
MOUNT_POINT is the path to mount location

2. Change to the `lkssp.img` mounted directory and type the following:

```
./setup
```

3. Text will appear explaining what is going to occur during the installation procedure. You will now be asked a series of questions where you will answer “**y**” for **Yes** or “**n**” for **No**. The type and sequence of the questions are dependent upon your Linux distribution.

Read each question carefully to ensure a proper response. It is recommended that you answer **Yes** to each question in order to complete all the steps required for a successful LifeKeeper Single Server Protection Installation.

4. Next, the LifeKeeper Single Server Protection Core Packages will be installed.
5. The setup script will then perform the installation of the licensing utilities. See [Obtaining and Installing the License](#) for details.

Installing the LifeKeeper Single Server Protection Software

6. After you have answered all the questions posed by the setup script, you will be informed that the installation was successful and then be presented with a list of all LifeKeeper Single Server Protection Recovery Kits available for installation.

Note: Trace information for execution of the setup scripts is saved in `/var/log/LK_install.log`.

7. Select the kits you would like installed by highlighting the kit and pressing the "space" bar. This will place an "i" next to each kit that will be installed. Then press **Enter**.

Note: To add kits at a later time, simply run setup again followed by -k:

```
./setup -k
```

LifeKeeper Single Server Protection requires a unique license for each server. The license is a run-time license, which means that you can install LifeKeeper Single Server Protection without it, but the license must be installed before you can successfully start and run the product.

The Installation script installs the Licensing Utilities package which obtains and displays all of the available Host IDs for your server during the initial install of your LifeKeeper Single Server Protection Software. Once your licenses have been installed the utility will return the Entitlement ID if it is available or the Host IDs if it is not.

Note: Host IDs, if displayed will always be based on the MAC address of the NICs.

Any LifeKeeper Single Server Protection licenses obtained from the SIOS Technology Corp. Licensing Operations Portal will contain your Entitlement ID and will not be locked to a specific node in the cluster. The Entitlement ID (Authorization Code) which was provided with your LifeKeeper Single Server Protection Software, is used to obtain the permanent license required to run the LifeKeeper Single Server Protection Software. The process is illustrated below.



Note: Each software package requires a license for each server.

Perform the following steps to obtain and install your license(s) for each server in the LifeKeeper Single Server Protection cluster:

1. **Ensure you have your LifeKeeper Entitlement ID** (Authorization Code). You should have received an email with your software containing the Entitlement ID needed to obtain the license.
2. **Obtain your licenses from the SIOS Technology Corp. Licensing Operations Portal.**
 - a. Using the system that has internet access, log in to the [SIOS Technology Corp. Licensing Operations Portal](#).
 - b. Select **Manage Entitlements**.

Note: If changing password, use the **Profile** button in the upper right corner of the display.
 - c. Find your **Entitlement ID** and select each **Activation ID** associated with that Entitlement ID by checking the box to the left of the line item.
 - d. Select the **Activate** tab.
 - e. Define the required fields and select **Next**.

- f. Click on **Add New Host** to create a new host.
 - g. Select **Any** from the Node Locked Host list and click **Okay**.
 - h. Check the box to the left of the **Host ID** and select **Generate**. The **Fulfillment ID** will display on the **License Summary** screen.
 - i. Check the box to the left of the **Fulfillment ID** and select the **Email License** tab.
 - j. Enter a valid email address to send the license to and select **Send**.
 - k. Select **Complete**.
 - l. Retrieve the email(s).
 - m. Copy the file(s) to the appropriate system(s).
3. Install your license(s). On each system, copy the license file(s) to `/var/LifeKeeper/license`, or on each system, run `/opt/LifeKeeper/bin/lkkeyins` and specify the filename (including full path) to the file.

Resource Policy Management

Overview

Resource Policy Management in LifeKeeper Single Server Protection (SSP) provides behavior management of resource local recovery and failover. Resource policies are managed with the **lkpolicy** command line tool (CLI).

LifeKeeper SSP Recovery Behavior

LifeKeeper SSP is designed to monitor individual applications and groups of related applications, periodically performing local recoveries or notifications when protected applications fail. Related applications, by example, are hierarchies where the primary application depends on lower-level storage or network resources. When an application or resource failure occurs, the default behavior is:

1. **Local Recovery**: First, attempt **local** recovery of the resource or application. An attempt will be made to restore the resource or application on the local server without external intervention. If local recovery is successful, then LifeKeeper SSP will not perform any additional action.
2. **Failover**: Second, if a local recovery attempt *fails* to restore the resource or application (or the *recovery kit* monitoring the resource has no support for local recovery), then a **failover** will be initiated (see [Failover](#) in the Standard Policies section below).

Please see [LifeKeeper Single Server Protection Fault Detection and Recovery Scenario](#) for more detailed information about our recovery behavior.

Custom and Maintenance-Mode Behavior via Policies

LifeKeeper SSP supports the ability to set additional policies that modify the default recovery behavior. There are four policies that can be set for individual resources (see the section below about

precautions regarding individual resource policies) or for an entire server. **The recommended approach is to alter policies at the server level.**

The available policies are:

Standard Policies

- **Failover** - For LifeKeeper SSP this policy setting can be used to turn on/off resource failover (which results in a reboot).
- **LocalRecovery** - LifeKeeper SSP by default, will attempt to recover protected resources by restarting the individual resource or the entire protected application prior to performing a failover (which would be a reboot). This policy setting can be used to turn on/off local recovery.
- **TemporalRecovery** - Normally, LifeKeeper SSP will perform local recovery of a failed resource. If local recovery fails, LifeKeeper SSP will perform a reboot. If the local recovery succeeds, failover (which would be a reboot) will not be performed.

There may be cases where the local recovery succeeds, but due to some irregularity in the server, the local recovery is re-attempted within a short time; resulting in multiple, consecutive local recovery attempts. This may degrade availability for the affected application.

To prevent this repetitive local recovery/failure cycle, you may set a temporal recovery policy. The temporal recovery policy allows an administrator to limit the number of local recovery attempts (successful or not) within a defined time period.

Example: If a user sets the policy definition to limit the resource to three local recovery attempts in a 30-minute time period, LifeKeeper SSP will failover(reboot) when a third local recovery attempt occurs within the 30-minute period.

Defined temporal recovery policies may be turned on or off. When a temporal recovery policy is off, temporal recovery processing will continue to be done and notifications will appear in the log when the policy would have fired; however, no actions will be taken.

Note: It is possible to disable failover and/or local recovery with a temporal recovery policy also in place. This state is illogical as the temporal recovery policy will never be acted upon if failover or local recovery are disabled.

Meta Policies

The "meta" policies are the ones that can affect more than one other policy at the same time. These policies are usually used as shortcuts for getting certain system behaviors that would otherwise require setting multiple standard policies.

- **NotificationOnly** - This mode allows administrators to put LifeKeeper SSP in a "monitoring only" state. **Both local recovery and failover(reboot) of a resource (or all resources in the case of a server-wide policy) are affected.** The user interface will indicate a **Failure** state if a failure is detected; but no recovery or failover(reboot) action will be taken. **Note:** The administrator will need to correct the problem that caused the failure manually and then bring the affected resource(s) back in service to continue normal LifeKeeper SSP operations.

Important Considerations for Resource-Level Policies

Resource level policies are policies that apply to a specific resource only, as opposed to an entire resource hierarchy or server.

Example:

```
app
- IP
- file system
```

In the above resource hierarchy, app depends on both IP and file system. A policy can be set to disable local recovery or failover of a specific resource. This means that, for example, if the IP resource's local recovery fails and a policy was set to disable failover of the IP resource, then the IP resource will not fail over or cause a failover of the other resources. However, if the file system resource's local recovery fails and the file system resource policy does not have failover disabled, then the entire hierarchy will failover causing a reboot.

Note: It is important to remember that resource level policies apply only to the specific resource for which they are set.

This is a simple example. Complex hierarchies can be configured, so care must be taken when setting resource-level policies.

The lkpolicy Tool

The `lcpolicy` tool is the command-line tool that allows management (querying, setting, removing) of policies on servers running LifeKeeper SSP. `lcpolicy` supports setting/modifying policies, removing policies and viewing all available policies and their current settings. In addition, defined policies can be set on or off, preserving resource/server settings while affecting recovery behavior.

The general usage is :

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

The `<name value pair data...>` differ depending on the operation and the policy being manipulated, particularly when setting policies. *For example:* Most on/off type policies only require `-on` or `--off` switch, but the temporal policy requires additional values to describe the threshold values.

Example lcpolicy Usage

Authenticating With Local and Remote Servers

The `lcpolicy` tool communicates with LifeKeeper SSP servers via an API that the servers expose. This API requires authentication from clients like the `lcpolicy` tool. The first time the `lcpolicy` tool is asked to access a LifeKeeper SSP server, if the credentials for that server are not known, it will ask the user for credentials for that server. These credentials are in the form of a username and password and:

1. Clients must have LifeKeeper SSP admin rights. This means the username must be in the `lkadmin` group according to the operating system's authentication configuration (via `pam`). It

is **not** necessary to run as **root**, but the root user can be used since it is in the appropriate group by default.

2. The credentials will be stored in the *credential store* so they do not have to be entered manually each time the tool is used to access this server.

See [Configuring Credentials for SteelEye Protection Suite](#) for more information on the credential store and its management with the credstore utility.

An example session with `lkpolicy` might look like this:

```
[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 ~]#
```

Listing Policies

```
lkpolicy --list-policy-types
```

Showing Current Policies

```
lkpolicy --get-policies
```

```
lkpolicy --get-policies tag=\*
```

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

```
lkpolicy --get-policies tag=mytagonly
```

Setting Policies

```
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
```

Removing Policies

```
lkpolicy --set-policy NotificationOnly --on
```

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

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

Removing Policies

```
lkpolicy --remove-policy Failover tag=steve
```

Note: *NotificationOnly* is a policy alias. Enabling *NotificationOnly* is the equivalent of disabling the corresponding *LocalRecovery* and *Failover* policies.

Verifying LifeKeeper Single Server Protection Installation

You can verify that the LifeKeeper Single Server Protection packages were installed correctly by entering the following at the command line:

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

Note: If the package is installed correctly, no output will be displayed by this command.

To perform a query from the command line, type

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

Note: The expected output for this command is the package information.