LifeKeeper Single Server Protection

v9.3.1

Installation Guide

November 2018

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

Table of Contents

Installing the LifeKeeper Single Server Protection Software 5

Installing the LifeKeeper Single Server Protection Software 5

Chapter 1: Installation 6

How to Use the setup Script 6

Change the Configuration After Installing LifeKeeper SSP 7

Repair Installation 7

How to Use the Dialog Screen 7

Authentication Setting 10

Recovery Kit Selection 10

Confirmation before initiating the installation 11

setup Script Options 12

Resource Policy Management 15

Overview 15

LifeKeeper SSP Recovery Behavior 15

Custom and Maintenance-Mode Behavior via Policies 15

Standard Policies 16

Meta Policies 16

Important Considerations for Resource-Level Policies 16

The lkpolicy Tool 17

Example lkpolicy Usage 17

Authenticating With Local and Remote Servers 17

Listing Policies 18

Showing Current Policies 18

Setting Policies 18

Removing Policies 19

Verifying LifeKeeper Single Server Protection Installation 19

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, Amazon EC2). LifeKeeper SSP is built on the proven and stable architecture of SIOS 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 SIOS LifeKeeper technology, you will see references to LifeKeeper throughout the documentation as well as references to information found in the SIOS 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, PPATH and NEC SPS)

  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)

  Note: When operating on Amazon EC2, assign a secondary private IP address to the NIC using the Amazon EC2 Management Console prior to creating the IP resource. Next, create the IP resource as the private IP address on the NIC that is using the LifeKeeper GUI client. An Elastic IP can now be associated with the IP resource

For more information on the SIOS LifeKeeper product, on which LifeKeeper SSP is built, please see the SIOS 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.

Packages that LifeKeeper Single Server Protection is dependent on are now installed automatically because a setup of LifeKeeper 9.3 and later uses package manager `(yum or zypper)` to install packages.

IMPORTANT: If the dependent packages cannot be installed automatically, please refer to the topic Linux Dependencies and install the necessary packages in advance.

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 or non-interactive system setup tasks required to install LifeKeeper Single Server Protection on the 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.

Please refer to the LikeKeeper Single Server Protection Release Notes.

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*.

Installing the LifeKeeper Single Server Protection Software

Please refer to How to Use Setup Scripts for the installation activities.

For upgrading, please refer to Upgrading SSP.

Chapter 1: Installation

To install LifeKeeper SSP, perform the following activities using the setup script.

1. Collect information about the system environment

   Collect the information necessary for the script to start LifeKeeper SSP. It takes several tens of seconds to several minutes.

2. Determine configuration

   Determine the functionality to use and application to protect with LifeKeeper SSP. You can specify them individually via the dialog screen or determine them non-interactive way all at once using a configuration file which has been created beforehand.

3. Install the package and change the settings

   Install the package which requires the script and change the settings based on the configuration determined in Step 2.

How to Use the setup Script

1. Login as root user and mount `lkssp.img` with the following command:

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

   PATH: A path to the image
   IMAGE_NAME: Image name
   MOUNT_POINT: A path to the mount point
2. Go to the directory where `lkssp.img` is mounted and execute the following command:

   ```
   ./setup [command option]
   ```

   See "setup Script Options" for the available options.

3. Information about the system environment is corrected first when executing the script.

   In the dialog mode, when it is determined that there is a problem after collecting the system environment information, the screen "Pre-install check failed!!" or “Pre-install warning” is displayed depending on the severity.

   “Pre-install check failed!!” is displayed when a serious problem such as the environment where you want to install LifeKeeper does not satisfy the installation requirements of LifeKeeper SSP is detected. If this is displayed, the installation process cannot proceed and the script is stopped.

   You can use LifeKeeper SSP even when “Pre-install warning” is displayed: it is displayed when the manual setting change is required or when some functionalities are restricted. You can continue the installation even when this is displayed.

The menu screen is displayed when there is no problem or the installation process is continued with “Pre-install warning” displayed. Please refer to "How to Use the Dialog Screen".

When you install with the non-interactive way, the script ends displaying the results if a problem is detected. If the problem displays “Pre-install warning”, you can continue the installation by specifying "`-q y`" option when executing the script.

4. When the configuration is determined, the installation process is initiated.

   If any problem arises during the installation, an error message is displayed. Please resolve the problem first and re-execute the setup script. When "Important notice" is output after the installation is completed, please follow the instruction.

Change the Configuration After Installing LifeKeeper SSP

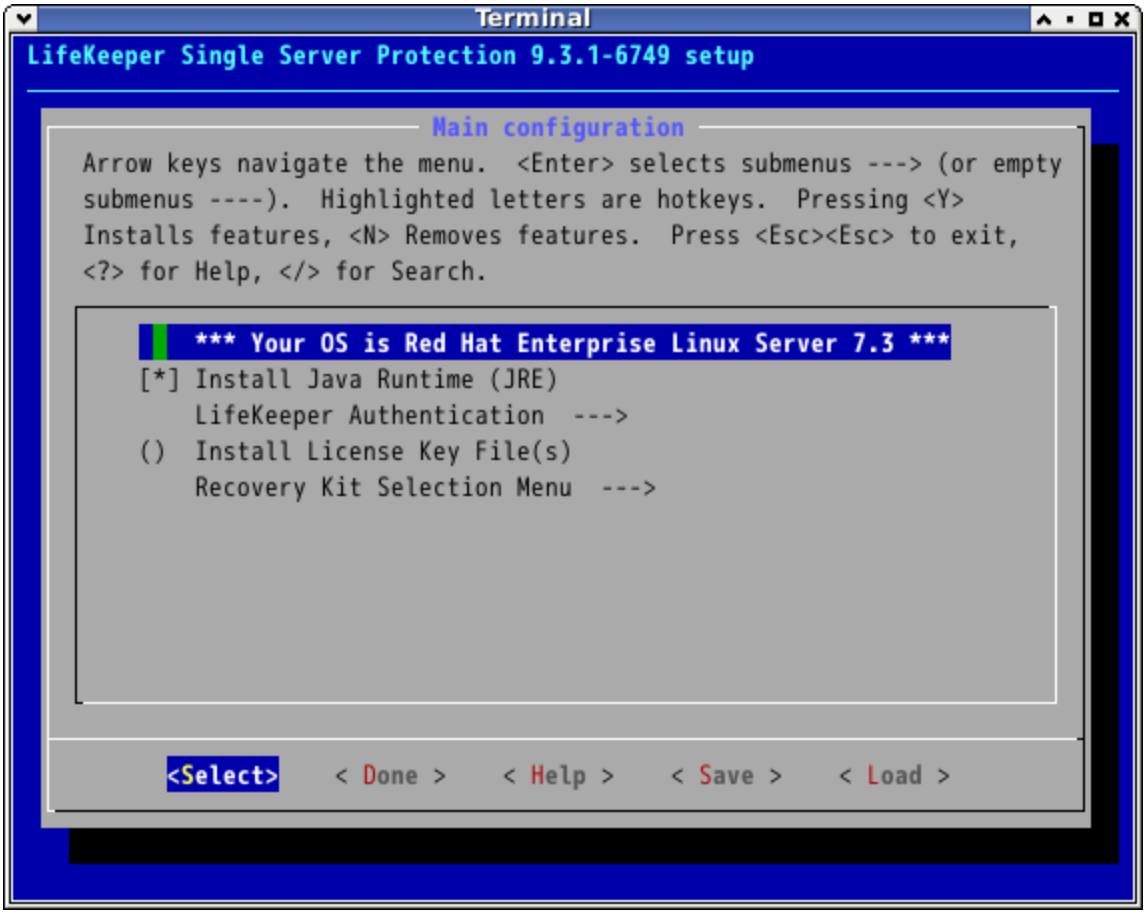
If you want to change the configuration after installing LifeKeeper SSP, please run the setup script again. The selected functions will be additionally installed and unselected functions will be uninstalled.

Repair Installation

To repair a LifeKeeper installation run setup with the "`--force`" option.

How to Use the Dialog Screen

Configure LifeKeeper SSP on the screen below.



>Use the following keys to navigate the menu.

↑ ↓	Navigate between menu items
TAB	Select the menu buttons at the bottom of the screen
SPACE / Enter	Execute the selected action

The menu buttons at the bottom of the screen are used for the following operations.

Select	The menu buttons at the bottom of the screen are used for the following operations.
Done	The menu buttons at the bottom of the screen are used for the following operations.
Help	Displays help for the highlighted item.
Save	Saves the configuration information in a configuration file. The saved configuration file can be used for non-interactive installations.
Load	Loads a saved configuration file.

For each option, you can configure the following functions. Options are displayed only when the configuration is required.

- **Install Java Runtime (JRE)**

  Install the Java runtime environment used by the LifeKeeper SSP GUI.

- **LifeKeeper authentication**

  Specify the users required to manage LifeKeeper SSP. Selecting this option will navigate you to the child screen.

- **Install license key file(s)**

  Specify the license file of LifeKeeper SSP. Input the full path name on a dialog to input the file name which will be displayed. Multiple files can be specified by separating them with spaces. Please refer to Obtaining and Installing the License topic for details.

- **Recovery Kit Selection**

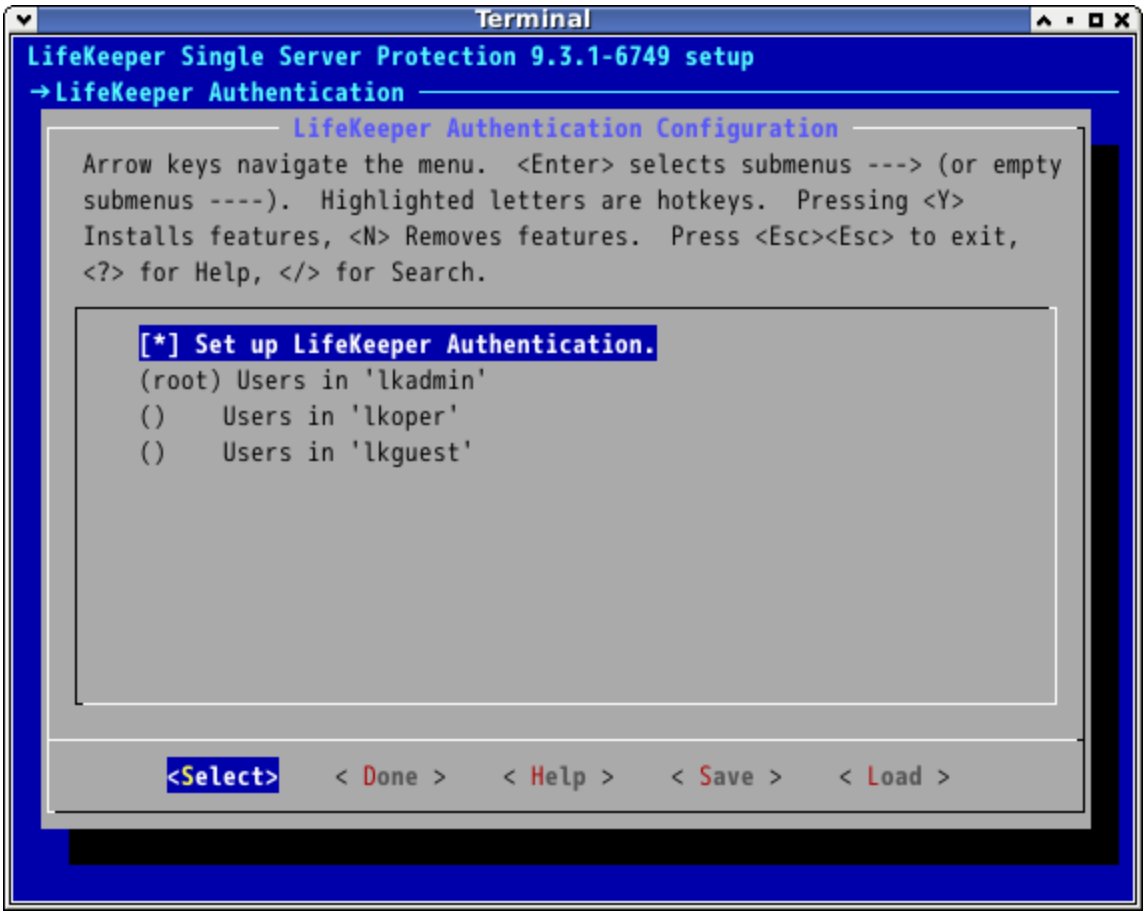
  Select a Recovery Kit to use.

  Select the Application Recovery Kit for the application protected by LifeKeeper SSP. Selecting this option will navigate you to the sub menu.

- **LifeKeeper startup after install**

  LifeKeeper SSP will be started when installation or update is completed. This option can be selected only when LifeKeeper SSP can be started.

Authentication Setting



The following items can be set on this screen.

- **Set up LifeKeeper Authentication.**

  Set up LifeKeeper Authentication.

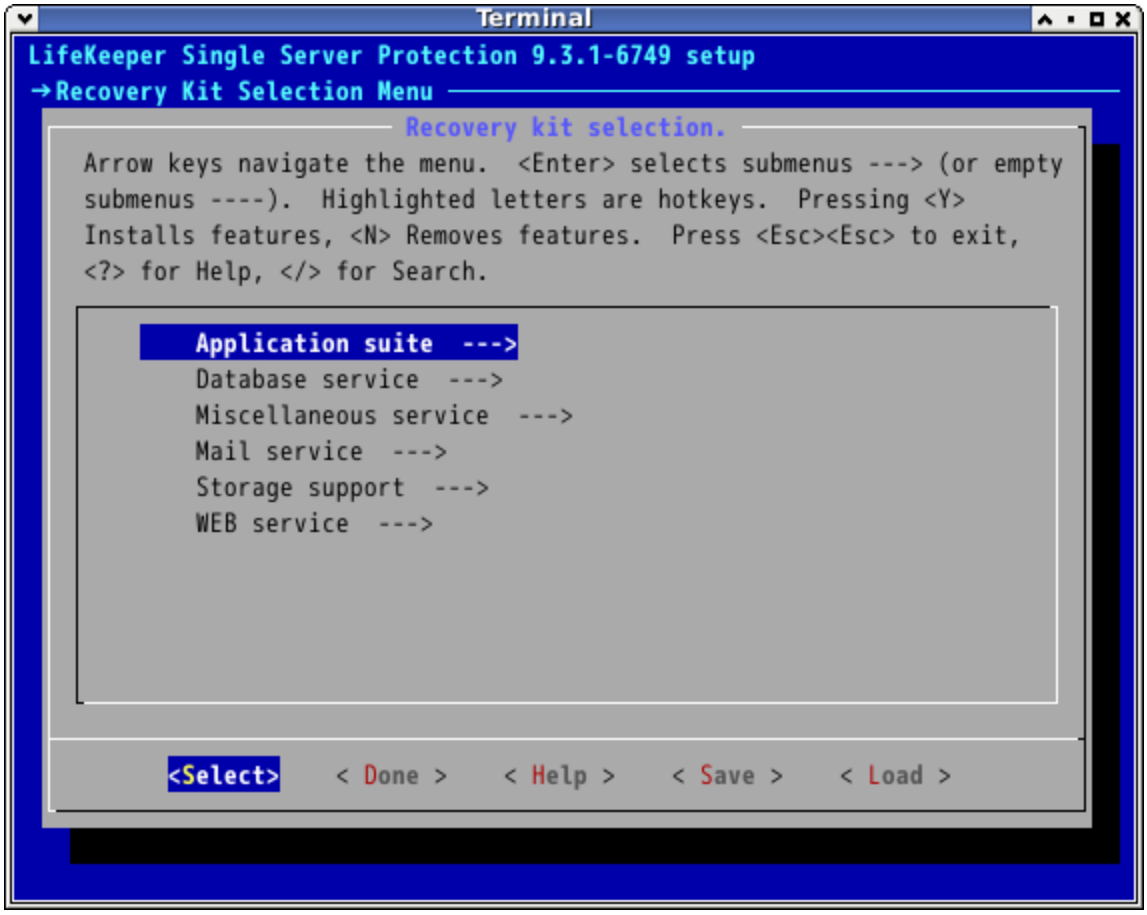
  By selecting this option, you can setup user information. When it is configured to authenticate remotely (e.g. NIS/LDAP), nothing will be updated even if you select this option.

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

  You can specify a name of users belong to each user group. Please refer to Configuring GUI Users topic in the Technical Documentation for the function of each group.

Recovery Kit Selection

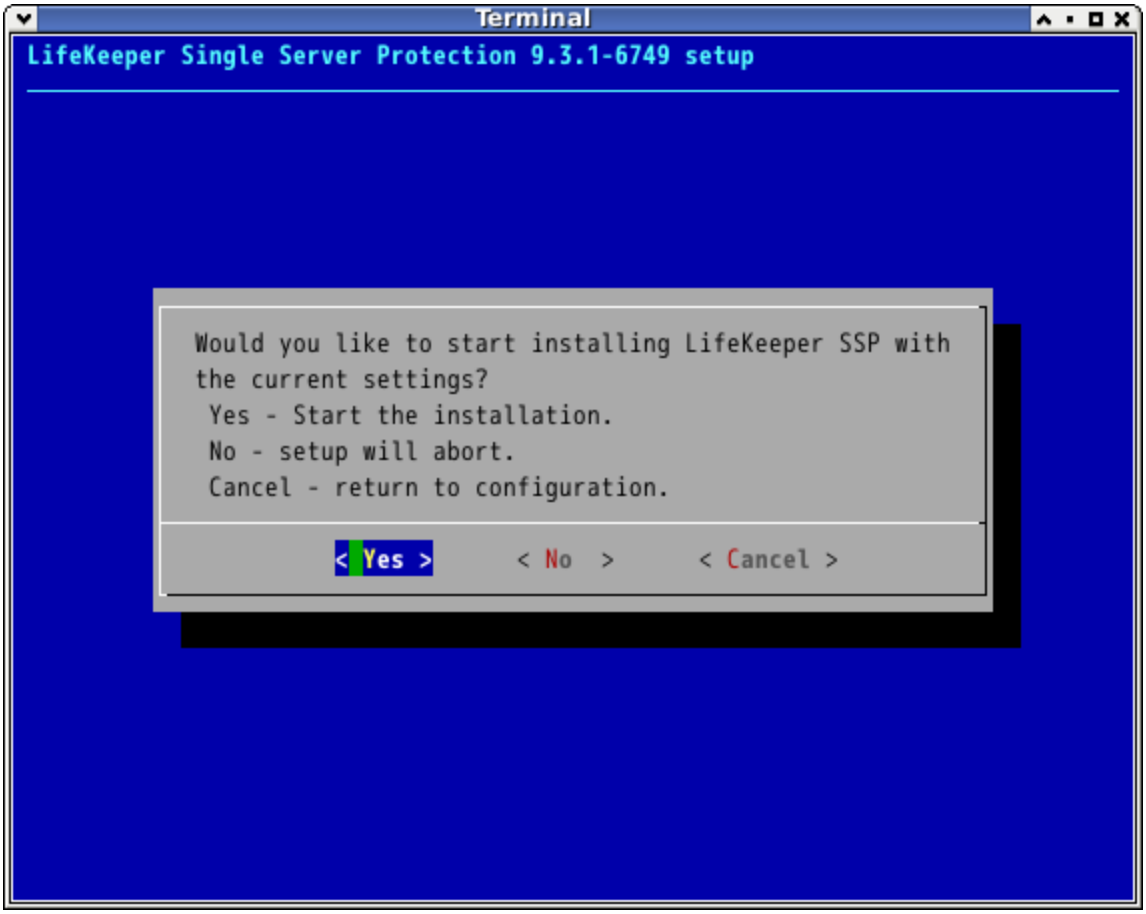
Application Recovery Kits are broken into several categories based on common functionality. Choose the category and select the Application Recovery Kits to install.



Details of each category are described in the table below.

Category	Description
Application suite	A group of recovery kits that protect application such as SAP and IBM MQ.
Network / Communication	A group of recovery kits that protect network services in the cloud such as EC2.
Database service	A group of recovery kits that protect database applications such as Oracle, PostgreSQL, and MaxDB.
Miscellaneous service	A group of recovery kits that protect general-purpose services such NFS and Samba.
Mail service	A group of recovery kits that protect email services such as Postfix.
Storage support	A group of recovery kits that protect file systems and data storage methods.
WEB service	A group of recovery kits that protect Web services.

Confirmation before initiating the installation



This screen is displayed when Done is selected on the Main Configuration screen.

You need to make a final decision to install LifeKeeper here. Navigate between options with TAB key and select with Enter.

Each button is used for the following operations.

Yes	Starts installation
No	Stops the installation and ends the script.
Cancel	Return to Main Configuration screen

setup Script Options

The setup script can be executed with the following options:

- `-f <file>`

  Install non-interactively. <file>> is the configuration file saved on the interactive screen.

- `-q <y/n>`

Specifies the response to any confirmation questions that may arise during non-interactive installation. Currently, specifying “y” means that you understand “Pre-install warning” and continue the installation.

- `--force`

  Forcibly reinstall LifeKeeper.

LifeKeeper Single Server Protection (SSP) can be upgraded to future releases while maintaining existing hierarchies.

Note:Only the previous two generations of LifeKeeper Single Server Protection can be upgraded to the latest version. If you are upgrading from older versions, you will need to uninstall the old version and reinstall LifeKeeper Single Server Protection. Instead of uninstalling the old version, you can also upgrade to the latest version after upgrading the older version to either of the previous two generations.

Note:For details on using lkbackup during the upgrade, please refer to lkbackup Known Issues.

1. Upgrade your Linux operating system before upgrading SSP If necessary.
2. Upgrade LifeKeeper referring to How to Use Setup Scripts.

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 `lkpolicy` tool is the command-line tool that allows management (querying, setting, removing) of policies on servers running LifeKeeper SSP. `lkpolicy` 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 :

```
lkpolicy [--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 lkpolicy Usage

Authenticating With Local and Remote Servers

The `lkpolicy` tool communicates with LifeKeeper SSP servers via an API that the servers expose. This API requires authentication from clients like the `lkpolicy` tool. The first time the `lkpolicy` 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 SIOS 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

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.