SIOS Protection Suite for Linux

v9.1.1

Installation Guide

Jan 2017

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

Chapter 1: SPS Installation Introduction

The SIOS Protection Suite (SPS) Installation Guide contains information on how to plan and install your SPS environment. In addition to providing the necessary steps for setting up your server, storage device and network components, it includes details for configuring your LifeKeeper graphical user interface (GUI).

Once you have completed the steps in this guide, you will be ready to configure your LifeKeeper and DataKeeper resources. The SPS for Linux Technical Documentation provides the information needed to complete your SPS configuration.

System Requirements

For a complete list of hardware and software requirements and versions, see the SPS for Linux Release Notes.

Also, before installing SPS, be sure that you have completed the planning and hardware configuration tasks described in this document.

Technical Notes

Refer to the Technical Notes and Troubleshooting sections of the SPS for Linux Technical Documentation for information detailing troubleshooting issues, restrictions, etc., pertaining to this software.

SIOS Protection Suite Software Packaging

The SIOS Protection Suite (SPS) for Linux software, including , is contained within a single image file (sps.img).

SPS for Linux Installation Image File

The SPS for Linux image file (sps.img) provides a set of installation scripts designed to perform user-interactive system setup tasks that are necessary when installing SPS 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 SPS installation, including the LifeKeeper API (steeleye-lkapi), which is used to allow communications between servers. **IMPORTANT NOTE: Currently, this API is reserved for internal use only but may be opened up to customer and third party usage in a future release.**

The type and sequence of the questions is dependent upon your Linux distribution. Read each question carefully to ensure a proper response. Under normal circumstances, you should be answering **Yes** to each question in order to complete all the steps required by the installation image file.

The SPS for Linux image file includes a core package cluster containing the following software packages:

SPS Core Package Cluster

- LifeKeeper (**steeleye-lk**). The LifeKeeper core packages provide recovery software for core system components, such as memory, CPUs, the operating system, the SCSI disk subsystem and file systems.
- LifeKeeper GUI (**steeleye-lkGUI**). The LifeKeeper GUI package provides a graphical user interface for LifeKeeper administration and monitoring.
- DataKeeper (**steeleye-lkDR**). The DataKeeper package provides data replication (synchronous or asynchronous mirrors) with intent logging.
- IP Recovery Kit (**steeleye-lkIP**). The LifeKeeper IP Recovery Kit provides switchover software for automatic recovery of IP addresses.
- Raw I/O Recovery Kit (**steeleye-lkRAW**). The LifeKeeper Raw I/O Recovery Kit provides support for applications that use raw i/o to bypass kernel buffering.
- Man Pages (**steeleye-lkMAN**). The LifeKeeper Man Page package provides reference manual pages for the LifeKeeper product.

Optional Recovery Software

Recovery kits are also released with the SPS Core software. During the installation, you will be presented with a complete, up-to-date, selectable list of available recovery kits. For information regarding these recovery kits, see the section of the SPS Technical Documentation.

Chapter 2: Planning Your SPS Environment

The following topics will assist in defining the SPS for Linux cluster environment.

Mapping Server Configurations

Document your server configuration using the following guidelines:

1. Determine the server names, processor types, memory and other I/O devices for your configuration. When you specify a backup server, you should ensure that the server you select has the capacity to perform the processing should a failure occur on the primary server.
2. Determine your communications connection requirements.

   Important: Potentially, clustered configurations have two types of communications requirements: cluster requirements and user requirements.

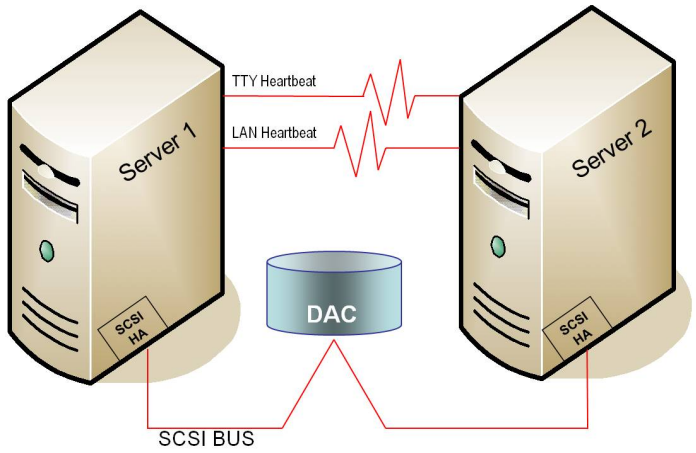
- **Cluster** - A LifeKeeper cluster requires at least two communication paths (also called “comm paths” or “heartbeats”) between servers. This redundancy helps avoid “split-brain” scenarios due to communication failures. Two separate LAN-based (TCP) comm paths using dual independent subnets are recommended, and at least one of these should be configured as a private network. Using a combination of TCP and TTY is also supported. A TTY comm path uses an RS-232 null-modem connection between the servers’ serial ports.

  Note that using only one comm path can potentially compromise the ability of systems in a LifeKeeper cluster to communicate with each other. If a single comm path is used and the comm path fails, then LifeKeeper hierarchies may try to come into service on multiple systems simultaneously. This is known as a false failover or a “split-brain” scenario. In the “split-brain” scenario, each server believes it is in control of the application and thus may try to access and write data to the shared storage device. To resolve the split-brain scenario, LifeKeeper may cause servers to be powered off or rebooted or leave hierarchies out-of-service to assure data integrity on all shared data. Additionally, heavy network traffic on a TCP comm path can result in unexpected behavior, including false failovers and the failure of LifeKeeper to initialize properly.

- **User** - We recommend that you provide alternate LAN connections for user traffic - that is, a separate LAN connection than the one used for the cluster heartbeat. However, if two TCP comm paths are configured (as recommended), one of those comm paths can share the network address with other incoming and outgoing traffic to the server.
- **Note**: To help ensure that resources are brought into service only when necessary, you may elect to utilize the Quorum/Witness Server Support Package for LifeKeeper.

3. Identify and understand your shared resource access requirements. Clusters that use shared storage can utilize either shared SCSI buses or Fibre Channel loops. Because LifeKeeper locks resources to one server, you must ensure that only one server requires access to all locked resources at any given time. LifeKeeper device locking is done at the Logical Unit (LUN) level. For active/active configurations, each hierarchy must access its own unique LUN. All hierarchies accessing a common LUN must be active (in-service) on the same server.
4. Determine your shared memory requirements. Remember to take into account the shared memory requirements of third-party applications as well as those of LifeKeeper when configuring shared memory and semaphore parameters. See Tuning in Technical Notes for LifeKeeper's shared memory requirements.

Sample Configuration Map for LifeKeeper Pair



This sample configuration map depicts a pair of LifeKeeper servers sharing a disk array subsystem where, normally, Server 1 runs the application(s) and Server 2 is the backup or secondary server. In this case, there is no contention for disk resources because one server at a time reserves the entire disk storage space of the disk array. The disk array controller is labeled "DAC," and the SCSI host adapters (parallel SCSI, Fibre Channel, etc.) are labeled "SCSI HA."

A pair of servers is the simplest LifeKeeper configuration. When you plan a cluster consisting of more than two servers, your map is even more critical to ensure that you have the appropriate connections between and among servers. For example, in a multi-directional failover configuration, it is possible to define communications paths within LifeKeeper when the physical connections do not exist. Each server must have a physical communication path to every other server in the cluster in order to provide cascading failover capability.

Storage and Adapter Requirements

Determine your storage and host adapter requirements using the following guidelines:

Storage Devices - Based on your application's data storage requirements, you will need to determine the type and number of data storage devices required by your configuration. Your shared files should reside on a disk array subsystem (Redundant Array of Inexpensive Disks, or RAID). LifeKeeper supports a number of hardware RAID peripherals for use in LifeKeeper configurations. See Supported Storage List for a list of the supported peripherals.

Consider the following issues when planning the configuration of your storage devices:

- LifeKeeper manages resources at the physical disk or Logical Unit (LUN) level, making the resources on each physical disk or LUN available to only one server in the configuration at a time. As a result, it is a good idea to plan disk allocations before you begin to configure LifeKeeper. For example, each hierarchy in active/active configurations must access its own unique LUN, so a minimum of two LUNs is required for a two-node active/active configuration.
- Some model-specific issues and hardware configuration details are maintained at Supported Storage List.

Adapters - Based upon the type of configuration and the number of peripherals, determine the types and number of SCSI or Fibre Channel Host Adapters required. It is important that any adapter you choose be supported by LifeKeeper, as well as by your Linux distribution so that there is a driver available. Refer to Supported Adapter Models for a list of supported host adapters. For reference purposes, you should add the host adapter specifications to your configuration map.

Storage and Adapter Options

For a list of the disk array storage models currently supported by LifeKeeper in shared storage configurations, see the Supported Storage List. Refer to Storage and Adapter Configuration for details about driver versions and other configuration requirements for these arrays and adapters.

Note that a supported disk array and adapter are not required in LifeKeeper configurations involving non-shared storage with IP failover only or when using SIOS Data Replication or Network Attached Storage.

SIOS Technology Corp. does not specifically certify fibre channel hubs and switches, because there are no known LifeKeeper-specific restrictions or requirements on these devices. Unless otherwise noted for a given array in Storage and Adapter Configuration, LifeKeeper recommends the hubs and switches that the disk array vendor supports.

Chapter 3: Setting Up Your SPS Environment

Now that the requirements have been determined and LifeKeeper configuration has been mapped, components of this SPS environment can be set up.

Note: Although it is possible to perform some setup tasks in a different sequence, this list is provided in the recommended sequence.

Installing the Linux OS and Associated Communications Packages

Before attempting to install the SPS for Linux software, you must first ensure that your Linux operating system is successfully installed and operational. Please see the Linux installation instructions provided with your distribution of Linux for complete installation details.

Notes:

- Refer to the Linux Dependencies topic for further dependencies that may be necessary for the required packages.
- It is possible to install Linux *after* connecting and configuring your shared storage, but it may be simpler to have Linux installed and running before introducing new peripheral devices.
- The SPS for Linux Installation Image File provides a set of installation scripts designed to perform user-interactive system setup tasks and installation tasks for installing SPS on your system.

Linux Dependencies

Successful completion of the installation of SPS for Linux requires the installation of a number of prerequisite packages. To prevent script failures, these packages should be installed prior to attempting to run the installation setup script.

The prerequisite packages are broken down into the following three groups:

- General Package Dependencies
- Optional Recovery Kit Package Dependencies

Depending on the operating system version and the packages installed based on the operating system type selected (minimal, default, etc.), additional dependent packages may be required.

Note: You may want to consider using a repository-based package manager such as **yum** or **zypper** that is designed to automatically resolve dependencies by searching in predefined software repositories thereby easing the installation of these required packages.

rpm Install Example

```
rpm -ivh <package(s)>
```

yum Install Example

```
yum install <package(s)>
```

Zypper Install Example

```
zypper install <package(s)>
```

General Package Dependencies

The following packages are always required to successfully install SPS for Linux. The package architecture version of the installed package should always match the operating system architecture (x86 or x86_64):

Red Hat, CentOS and OEL (5.x, 6.x and 7.x)

- bzip2
- iproute
- iputils
- mktemp (5.x only)
- patch (version 2.5 or later)
- redhat-lsb

  Note: Some or all of these packages may already be installed depending on the selections made during the install of the operating system.

SLES 11 (SPx), SLES12 (SP1 or later)

- bzip2
- iproute2
- iptables
- iputils
- insserv
- patch (version 2.5 or later)
- lsb (SLES11 only)

  Note: Some or all of these packages may already be installed depending on the selections made during the install of the operating system.

Dependency with syslog daemon

LifeKeeper log information is recorded using the syslog daemon. LifeKeeper supports three implementations (standard syslog, rsyslog, and syslog-ng). Before installing LifeKeeper, one of syslog daemons must be installed and operating.

Note: In the distributions using systemd such as RHEL7 or SLES12, journald administrates the log collectively. Because LifeKeeper does log output using the syslog daemon, the syslog daemon also must be operating in these environments. Therefore, set up syslog daemon to operate when using LifeKeeper.

Note: journald records the log output to a temporary file system (tmpfs) mount on /run/log/journal by default. Thus, the system log is not saved at the time of the OS shutdown. Change the setup to let the journald log perpetuate.

Note: To let the journald log perpetuate, set up "Storage=persistent" in /etc/systemd/journald.conf, or, create the /var/log/journal directory with the set up "Storage=auto" (default). After changing the set up, restart systemd-journald.service.

Optional Recovery Kit Package Dependencies

Additionally, some of the SIOS Protection Suite for Linux optional Application Recovery Kits (ARKs) require supporting packages to be installed.

If NFS exports are to be protected via the SIOS Protection Suite for Linux NFS Application Recovery Kit, then the following dependent packages are required:

- nfs-utils (Red Hat, CentOS, Oracle 5.x, 6.x and 7.x)
- nfs-client (SLES 11)
- nfs-kernel-server (SLES 11)

If multipath devices are to be protected via Device Mapper Multipath (DMMP), Hitachi Dynamic Link Manager Software (HDLM), Power Path or NEC iStorage StoragePathSavior (NECSPS), then the following dependent package is required:

- sg3_utils (All multipath kits)
- sg3_utils-libs (All multipath kits)
- HDLM (Hitachi Dynamic Link Manager Software Kit)
- EMCpower.LINUX (Power Path Kit)
- sps (NEC iStorage StoragePathSavior Kit **4.2.0 or prior**)
- sps-utils and sps-driver (NEC iStorage StoragePathSavior Kit **4.2.1 or later**)

If Websphere MQSeries queue managers are to be protected via the SIOS Protection Suite for Linux Websphere MQ/MQSeries Application Recovery Kit, then the following dependent Websphere MQ packages are required:

- MQSeriesServer
- MQSeriesSamples
- MQSeriesClient
- MQSeriesRuntime
- MQSeriesSDK

If Software RAID devices are to be protected via the SIOS Protection Suite for Linux Software RAID (md) Recovery Kit, then the following dependent package is required:

- mdadm

yum/Zypper Package Lists

The following list of rpm packages, for each distribution listed and installed with the corresponding package installer, is the minimum list of packages that will resolve all the required dependencies for SIOS Protection Suite for Linux:

Red Hat, CentOS and OEL (5.x, 6.x and 7.x)

```
yum install libXtst libstdc++ bzip2-libs pam zlib patch
redhat-lsb
```

SLES11, SLES12

```
zypper install libstdc++ bzip2 pam pam-modules zlib lsb
```

Connecting Servers and Shared Storage

If you are planning to use LifeKeeper in a non-shared storage environment, then you may skip this information. If you are using LifeKeeper in a data replication (mirroring) environment, see the DataKeeper section of this documentation. If you are using LifeKeeper in a network attached storage environment, see LifeKeeper Network Attached Storage Recovery Kit Administration Guide.

Once Linux is installed, you should set the host adapter and shared peripheral addressing. Refer to the documentation accompanying your adapter and storage device for specific details.

Configuring Shared Storage

LifeKeeper configurations may use the facilities of shared Small Computer System Interface (SCSI) host adapters and shared disk hardware to switch resources from a failed server to a designated backup server. A Fibre Channel Storage Area Network (SAN) may also be used to switch resources from a failed server to a designated backup server.

Perform the following tasks before creating disk-based application resource hierarchies that enable LifeKeeper to provide failover protection.

1. Partition disks and LUNs. Because all disks placed under LifeKeeper protection must be partitioned, your shared disk arrays must now be configured into logical units, or LUNs. Use your disk array management software to perform this configuration. You should refer to your disk array software documentation for detailed instructions.

   Note: Remember that LifeKeeper locks **its disks** at the LUN level. Therefore, one LUN may be adequate in an Active/Standby configuration. But, if you are using an Active/Active configuration, then you must configure at least two separate LUNs, so that each hierarchy can access its **own unique** LUN.

2. Verify that both servers recognize the shared disks (for example, using the **fdisk** command). If Linux does not recognize the LUNs you have created, then LifeKeeper will not either.
3. Create file systems on your shared disks from the system you plan to use as the primary server in your LifeKeeper hierarchy. Refer to the Linux documentation for complete instructions on the administration of file systems.

Verifying Network Configuration

It is important to ensure that your network is configured and working properly *before* you install LifeKeeper. There are several tasks you should do at this point to verify your network operation:

1. If your server installation has a firewall enabled, you will either need to accommodate the LifeKeeper ports or disable the firewall. Please refer to the topic "Running LifeKeeper With a Firewall".
2. From each server, ping the local server, and ping the other server(s) in the cluster. If the ping fails, then do the necessary troubleshooting and perform corrective actions before continuing.
3. If your server has more than one network adapter, you should configure the adapters to be on different subnets. If the adapters are on the same subnet, TCP/IP cannot effectively utilize the second adapter.
4. Ensure that *localhost* is resolvable by each server in the cluster. If DNS is not implemented, edit the */etc/hosts* file and add an entry for the *localhost* name. This entry can list either the IP address for the local server, or it can list the default entry (127.0.0.1). If *localhost* is not resolvable, the LifeKeeper GUI may not work.
5. If DNS is implemented, verify the configuration to ensure the servers in your LifeKeeper cluster can be resolved using DNS.
6. Ensure each server's hostname is correct and will not change after LifeKeeper is installed. If you later decide to change the hostname of a LifeKeeper system, you should follow these steps *on all servers in the cluster*.
    a. Stop LifeKeeper on all servers in the cluster using the command:

        ```
        /etc/init.d/lifekeeper stop-nofailover
        ```

    b. Change the server's hostname using the Linux **hostname** command.
    c. Before continuing, you should ensure that the new hostname is resolvable by each server in the cluster (see the previous bullets).
    d. Run the following command on every server in the cluster to update LifeKeeper's hostname. (Refer to `lk_chg_value(1M)` for details.)

        ```
        /opt/LifeKeeper/bin/lk_chg_value -o oldhostname -n newhostname
        ```

    e. Start LifeKeeper using the command:

        ```
        /etc/init.d/lifekeeper start
        ```

LifeKeeper for Linux v7.x supports VLAN interface for Communication Paths and IP resources. The type of VLAN interface can be chosen as described below.

VLAN Interface Support Matrix

- not supported \ x supported

LK Linux v7.1 or Prior Version

VLAN_NAME_TYPE	CommPath	IP resource
DEV_PLUS_VID (eth0.0100)	-	x
DEV_PLUS_VID_NO_PAD (eth0.100)	-	x
VLAN_PLUS_VID (vlan0100)	x	x
VLAN_PLUS_VID_NO_PAD (vlan100)	x	x

LK Linux v7.2 or Later Version

VLAN_NAME_TYPE	CommPath	IP resource
DEV_PLUS_VID (eth0.0100)	x	x
DEV_PLUS_VID_NO_PAD (eth0.100)	x	x
VLAN_PLUS_VID (vlan0100)	x	x
VLAN_PLUS_VID_NO_PAD (vlan100)	x	x

Creating Switchable IP Address

A switchable IP address is a “virtual” IP address that can be switched between servers. It is separate from the IP address associated with the network interface card of each server. Applications under LifeKeeper protection are associated with the switchable IP address. Then, if there is a failure on the primary server, that IP address “switches” to the backup server.

If you plan to configure resource hierarchies for switchable IP addresses, you must do the following on each server in the cluster:

- Verify that the computer name is correct and will not be changed.
- Verify that the switchable IP addresses are unique using the ping command.
- Edit the */etc/hosts* file to add an entry for each switchable IP address.

Refer to the LifeKeeper for Linux IP Recovery Kit Technical Documentation for additional information.

Installing and Setting Up Database Applications

If your environment includes a protected database application such as Oracle or MySQL, you should install

the application using the documentation provided with the database. Ensure that the database is on a shared file system and that the configuration files are on a shared file system. The executables may either be on each local or a shared file system.

Although it is possible to install your application *after* LifeKeeper is installed, you should test the application to ensure it is configured and operating properly before placing it under LifeKeeper protection. Please reference the specific for additional installation and setup considerations.

Configuring GUI Users

GUI Authentication with PAM

SPS for Linux now leverages the Pluggable Authentication Module (PAM) provided in the Linux Standard Base (LSB). SPS no longer uses its private password file once located in */opt/LifeKeeper/website/passwd*. Instead, users are identified and authenticated against the system's PAM configuration. Privilege levels are determined from group membership as provided through PAM.

In order to access the GUI, a user must be a member in one of the three LifeKeeper groups: `lkadmin`, `lkoper` or `lkguest`. Membership in these groups should be set by the system administrator using whatever technique is appropriate for the type of user account database that is being used throughout the cluster.

These three LifeKeeper groups provide three different sets of permissions (see Permissions Table).

1. Users with ***Administrator*** permission (`lkadmin`) throughout a cluster can perform all possible actions through the GUI.
2. Users with ***Operator*** permission (`lkoper`) on a server can view LifeKeeper configuration and status information and can bring resources into service and take them out of service on that server.
3. Users with ***Guest*** permission (`lkguest`) on a server can view LifeKeeper configuration and status information on that server.

During installation of the GUI package, the *root* user on the system is automatically added to the `lkadmin` group in the system's local group database allowing *root* to perform all LifeKeeper tasks on that server via the GUI application or web client. If you plan to allow users other than *root* to use LifeKeeper GUI clients, then these LifeKeeper GUI users will need to be configured by adding them to the appropriate group.

If PAM is configured to use a non-local database such as NIS, LDAP or AD, then the system administrator must ensure that the accounts are correctly configured in those databases. The groups listed above must exist and users who are allowed to log into the LifeKeeper GUI must be a member of one of these groups. These groups should be created in the remote database only and they should be removed from the local */etc/group* file.

When upgrading from a version of LifeKeeper prior to 8.1.1, an attempt will be made to add any entries from the old */opt/LifeKeeper/website/passwd* to the new group membership mechanism. If the users do not get re-created, they will not be assigned to the corresponding LifeKeeper groups and will have to be added manually.

After upgrading to LifeKeeper 8.1.1 (or later), the default LifeKeeper GUI login will be ‘root’ (with the system’s ‘root’ password). The LifeKeeper GUI requires passwords on each system in the cluster to be the same.

If any system in the cluster is using an LK GUI password other than the system’s ‘root’ password, the LK GUI login will fail. Once the root passwords are the same on each system in the cluster, the LK GUI login for ‘root’ will succeed.

Note: To avoid confusion and maintain consistency if leveraging more complex PAM configurations such as LDAP, NIS or AD, it is recommended that all user and LifeKeeper group accounts exist prior to installing or upgrading SPS.

The best practice is to always grant permissions on a cluster-wide basis. It is possible to grant permissions on a single-server basis, but that is confusing to users and makes it impossible to perform administrative tasks.

Chapter 4: Installing the SIOS Protection Suite Software

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

	**IMPORTANT**: Please review the Linux Dependencies topic prior to installing SPS for Linux.

The SPS core package cluster and any optional recovery kits will be installed through the command line using the SPS Installation Image File (*sps.img*). This image file provides a set of installation scripts designed to perform user-interactive system setup tasks that are necessary when installing SPS 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 SPS installation. A licensing utilities package is also installed providing utilities for obtaining and displaying the Host ID or Entitlement ID of your server. Host IDs and/or Entitlement IDs are used to obtain valid licenses for running SPS.

Refer to the SPS for Linux Release Notes for additional information.

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

	**IMPORTANT**: • Installing SPS on your shared storage is not supported. Each server should have its own copy installed on its local disk. • All SPS packages are installed in the directory */opt/LifeKeeper*. • If you are re-installing the existing version of LifeKeeper, you should 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 SPS for Linux Release Notes and Upgrading SPS for upgrade instructions. • If you receive an error message referencing the LifeKeeper Distribution Enabling package when you are installing SPS, you should run/re-run the **setup** script on the SPS Installation Image File.

Installing the SPS Software

SPS will be installed through the command line regardless of the Linux distribution you are operating under.

1. Mount the `sps.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 `sps.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 SPS Installation.

   Note: The Installation image file may install kernel modules to support shared storage devices or the optional NFS Recovery Kit.

   Note: Beginning with SPS 8.1, when performing a kernel upgrade on Red Hat Enterprise Linux systems, it is no longer a requirement that the setup script (`./setup`) from the installation image be rerun. Modules should be automatically available to the upgraded kernel without any intervention as long as the kernel was installed from a proper Red Hat package (rpm file).

4. Next, the SPS 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.

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 SPS Recovery Kits available for installation.

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

   Note: During an upgrade, please make sure to stop LifeKeeper before running setup.

   Note: Previous to SPS for Linux Version 8.1, recovery kits would need to be installed from their individual image files once the core package install was completed. Now, once the packages have been installed, you are presented with a list of available kits for selection.

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
   ```

8. Execute the following command by a user with root authorization if the NFS Recovery Kit is being used on RHEL7, CentOS7, OEL7 or SLES12 (i.e systemd environments).

   ```
   systemctl stop var-lib-nfs-rpc_pipefs.mount
    systemctl disable var-lib-nfs-rpc_pipefs.mount
   ```

9. Install the SPS software, as appropriate, on the other server(s) in the cluster using the same procedure.

For upgrade installations, see Upgrading SPS.

Chapter 5: Obtaining and Installing the License

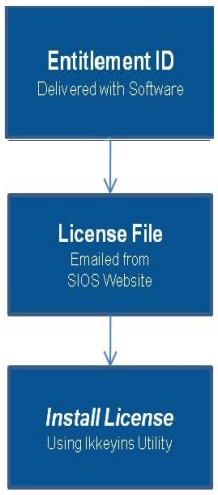
SPS for Linux requires a unique license for each server. The license is a run-time license, which means that you can install SPS without it, but the license must be installed before you can successfully start and run the product.

Note: If using newer hardware with RHEL 6.1, please see the IP Licensing Known Issues in the SPS for Linux Troubleshooting Section.

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 SIOS Protection Suite 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.

Starting with release 8.2.0 any new 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. Existing users that obtained their licenses prior to 8.2.0 should see the License Rehost for Existing Users section below. The Entitlement ID (Authorization Code) which was provided with your SIOS Protection Suite Software, is used to obtain the permanent license required to run the SIOS Protection Suite 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 SPS 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.

Obtaining an Internet HOST ID

Use lmutil to obtain your machine's Internet Host ID. The Internet Host ID is normally the primary IP address of the primary network interface in the system. Internet Host IDs can be used as an alternative to Ethernet (or MAC) Host IDs and may be preferable in virtual environments where MAC addresses can change due to VM cloning.

1. Type the following command:

    ```
    # /opt/LifeKeeper/bin/lmutil lmhostid -internet -n
    ```

2. Record the ID returned by the program.

Example:

/opt/LifeKeeper/bin/lmutil lmhostid -internet -n

"INTERNET=172.17.100.161"

Note: This info must match the information contained in the permanent license key obtained from SIOS Technology Corp.

Verifying SPS Installation

You can verify that the SPS 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.

Upgrading SPS

SPS for Linux may be upgraded to future releases while preserving existing resource hierarchies. Review this information carefully to ensure that you minimize application downtime.

Note: LifeKeeper can be upgraded to the current version from up to two versions back. If upgrading from a version previous to that, the older version will need to be uninstalled, and SIOS Protection Suite for Linux will have to be reinstalled. An alternative to uninstalling the older version would be to upgrade from the older version to one of the two acceptable versions, then perform the upgrade to the current version.

Note: If using `lkbackup` during your upgrade, see the lkbackup Known Issue for further information.

Note: Beginning with Version 8.1.1, SPS uses PAM for GUI user authentication. Due to this change, an attempt will be made to add any entries from the old */opt/LifeKeeper/website/passwd* to the new group membership mechanism. If the users do not get re-created, they will not be assigned to the corresponding LifeKeeper groups and will have to be added manually. To avoid confusion and maintain consistency if leveraging more complex PAM configurations such as LDAP, NIS and AD, it is recommended that all user and LifeKeeper group accounts exist prior to upgrading SPS.

1. While upgrading a cluster, switch all applications away from the server to be upgraded now. Do this manually or by setting the LifeKeeper shutdown strategy to **"Switchover"** which causes the applications to be switched when LifeKeeper is stopped or the server is shut down.
2. If necessary, upgrade the Linux operating system before upgrading SPS. It is recommended that you unextend all resources from a server that is to be upgraded prior to performing the operating system upgrade.
3. Upgrade SPS using the SPS Installation Image File. Mount the SPS Installation Image 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
4. Change to the `sps.img` mounted directory and type the following:

   ```
   ./setup
   ```

   You will see informational messages confirming that the packages are being upgraded.
5. A list of all available SPS Recovery Kits will appear. You will see a "**u**" next to each currently installed recovery kit indicating that this kit will be upgraded. If you would like to install any additional kits, select the kits by highlighting and pressing the "space" bar. This will place an "**i**" next to each kit that will be installed.

   Note: Previous to SPS for Linux Version 8.1, recovery kits would need to be upgraded from their individual image files once the core packages finished upgrading. Now, once the packages have been upgraded, you are presented with a list indicating which kits are currently installed and will be

automatically upgraded, and you're also given the option to select any other kits you would like installed.

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

```
./setup -k
```

Note: Because following packages won't be upgraded by the setup script, update each with the "rpm -U" command.

- steeleye-lkQWK
- steeleye-lkECC
- steeleye-lkROUTE53
- steeleye-lkOPENSWAN

6. Execute the following command by a user with root authorization if the NFS Recovery Kit is being used on RHEL7, CentOS7, OEL7 or SLES12 (systemd environments).

```
systemctl stop var-lib-nfs-rpc_pipefs.mount
 systemctl disable var-lib-nfs-rpc_pipefs.mount
```

7. Switch all applications back to the upgraded server.
8. Repeat this procedure for each server in the SPS cluster to be upgraded.

CAUTION: The same version and release of SPS must be installed on all systems in a cluster. In general, different versions and/or releases of SPS are not compatible. For situations other than rolling upgrades, LifeKeeper should not be started when a different version or release is resident and running on another system in the cluster.

Notes for OS upgrades

When upgrading the OS, make sure the currently installed version of LifeKeeper supports the upgraded version of the OS. If it is not supported, LifeKeeper will need to be upgraded as well provided a version of LifeKeeper has been released that supports the new OS version. If no version of LifeKeeper has been released that supports the new OS version you may not be able to upgrade the OS. Refer to the Supported Operating Systems.

Before upgrading the OS, it is recommended that the LifeKeeper configuration be backed up via the lkbackup command.

Notes: When to use lkbackup, refer to the known issues of lkbackup.

1. When upgrading the cluster, all the resource hierarchies and thus the applications they protect, must be switched from the server to be upgraded to a standby node in the cluster. This can be done manually, or, be setting the LifeKeeper Sshutdown Strategy to "Switchover". By setting the Shutdown Strategy to “Switchover”, the resource hierarchies are switched over to a standby node when LifeKeeper stops or the servers are shutdown.
2. Stop LifeKeeper.
3. Perform only one of the following steps if the current OS version matches:
   - If the current OS version is RHEL 6.0 and an upgrade is being performed to RHEL 6.1 or later, then executer the following command to remove the HADR package:

     ```
     # rpm -e HADR-RHAS
     ```

   - If the current OS version is RHEL 7.0, 7.1 or 7.2 and an upgrade is being performed to RHEL 7.3, then execute the following command to remove the HADR package:

     ```
     # rpm -e HADR-RHAS
     ```

   - If the current OS version is Oracle Linux 7.0, 7.1 or 7.2 and an upgrade is being performed to Oracle Linux 7.3, then execute the following command to remove the HADR package:

     ```
     # rpm -e HADR-OEL
     ```

   - For any other OS version the removal of the HADR package is not required.
4. Upgrade and reboot the OS.
5. Upgrade LifeKeeper when required.
   To upgrade LifeKeeper, refer to Upgrading LifeKeeper.
6. Start up LifeKeeper.
7. Switch all the resource hierarchies to the upgraded server.
8. Execute these steps for all the nodes in the SPS cluster.

Notes: All nodes in the cluster must be running the same version of the OS and the same version of LifeKeeper to be considered supported. Only during the upgrade process can the nodes differ in OS and LIfeKeeper versions as this would be considered a temporary condition.