SteelEye Protection Suite for Windows

Microsoft Internet Information Services Recovery Kit

v8.1.0

Administration Guide

May 2014

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 © 2014
By SIOS Technology Corp.
San Mateo, CA U.S.A.
All rights reserved

Table of Contents

Chapter 1: Introduction **1**

IIS Overview **1**

Chapter 2: IIS Installation **2**

Hardware and Software Requirements **2**

Kit Installation **3**

Kit Removal **3**

Configuration Definitions and Restrictions **4**

Active/Active Configuration 4

IIS Configuration Considerations **4**

Default Web Site or New Web Site 5

Primary and Backup Designations 5

Naming Restrictions 5

Identical Primary/Backup Web Sites 5

Configuring Secure Servers 5

IIS Configuration 6

Document Content Location 6

Shared and Replicated Content Storage 6

Non-Shared Storage 6

Use Different Volume for Multiple IIS Sites 6

Installing and Configuring IIS with LifeKeeper **7**

Installation Checklist 7

Install SteelEye DataKeeper and Create Mirrors 7

Install and Configure SteelEye Protection Suite and Recovery Kits **7**

Install and Configure Microsoft IIS on All Servers **8**

Install and Configure Microsoft IIS Web or FTP Site 9

Install and Configure SMTP Virtual Server 10

Chapter 3: IIS Configuration Definitions and Restrictions 11

IIS Required Roles and Role Services and Features 11

IIS Active Active 11

Primary and Backup Designations 12

Naming Restrictions 12

Identical Primary Backup Web Sites 13

Configuring Secure Servers 13

IIS Configuration 13

Document Content Location 13

Shared and Replicated Content Storage 13

Non-Shared Storage 14

Use Different Volume for Multiple IIS Sites 14

Chapter 4: IIS Resource Configuration Tasks 15

Create an IIS Resource Hierarchy 15

Extend an IIS Resource Hierarchy 15

Delete an IIS Resource Hierarchy 16

Unextend Your IIS Hierarchy 16

Chapter 5: Testing Your IIS Resource Hierarchy 18

Performing a Manual Switchover from the GUI 18

Recovery Operations 18

Chapter 6: IIS Hierarchy Administration 19

Modifying Quick Check Interval, Deep Check Interval and Local Recovery 19

Manual Switchover 19

IIS Failover 19

Protecting FTP Sites with Non-Anonymous Login 20

Using an FTP Login Script 20

Disabling the FTP Deep Check Process 20

Changing LifeKeeper Microsoft IIS Recovery Kit Configuration 20

Removing Microsoft IIS 21

Changing the Network Interface Card (NIC) **21**

Chapter 7: IIS Troubleshooting **22**

Symptoms and Solutions **22**

Chapter 1: Introduction

The SteelEye Protection Suite Microsoft IIS Recovery Kit extends your SteelEye Protection Suite product by adding specific protection to Internet servers. The SteelEye Protection Suite Microsoft IIS Recovery Kit continuously monitors the health of your Internet servers, and if a problem arises, provides automatic failover of the affected sites to a standby system. The Recovery Kit protects Web, FTP and SMTP sites. When multiple IIS resources are configured, Web, FTP or SMTP sites can be stopped/started independently.

IIS Overview

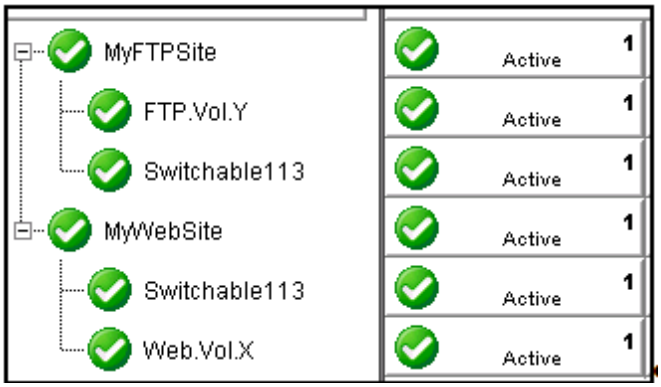
The SteelEye Protection Suite Microsoft IIS Recovery Kit protects Internet servers from the following problems:

- System failure or server shutdown
- Network Interface Card (NIC) failures
- Communication failures (Web server is running but stops responding)
- Startup failures (Web server aborts on startup)

The SteelEye Protection Suite Microsoft IIS Recovery Kit has two recovery procedures. For system or NIC failures, the Recovery Kit transfers the affected web server's IP address to a standby system, and then starts up the standby web server. If there is a communication or startup failure, and local recovery is enabled, the SteelEye Protection Suite Microsoft IIS Recovery Kit will first stop and restart the affected web server locally to see if that corrects the problem. If the restart is unsuccessful, then the Recovery Kit transfers service to the backup web server.

The SteelEye Protection Suite Microsoft IIS Recovery Kit manages the dependencies between the IIS application, IP and volume resources. First, you create the IP and volume resources to be used by your web servers. Then, when you create the IIS resource, the SteelEye Protection Suite Microsoft IIS Recovery Kit reads the Microsoft IIS configuration and automatically creates the required dependencies between the IIS resource and the IP and volume resources.

The following is a sample IIS hierarchy as shown in the LifeKeeper GUI. The Web site has dependencies on both the IP address "Switchable113", and on the volume "WEB.Vol.X", where the home directory containing the Web site's content resides. Both the IP and volume resources were created prior to the web site creation.



Chapter 2: IIS Installation

The topics in this section will assist in installing the LifeKeeper Microsoft IIS Recovery Kit.

Hardware and Software Requirements

Before attempting to install or remove the SteelEye Protection Suite Microsoft IIS Recovery Kit, be sure that your configuration meets the following requirements:

- **Operating System software**. SteelEye Protection Suite supports the following versions of Windows operating systems:
  - Windows Server 2008 R2 and 2012 Standard, Enterprise, Data Center, Web Editions
- **SteelEye Protection Suite software**. You must install the same version of SteelEye Protection Suite software and any patches on each server. Please refer to the *Release Notes* for specific requirements.
- **SteelEye DataKeeper software (optional)**. If you plan to use IIS with replicated volumes rather than shared storage, you should install the SteelEye DataKeeper for Windows software on each server.
- **SteelEye Protection Suite IP Recovery Kit**. You must have the SteelEye Protection Suite IP Recovery Kit installed on each server. All TCP/IP configuration requirements for the IP Recovery Kit also apply to the SteelEye Protection Suite Microsoft IIS Recovery Kit.
- **IP network interface**. Each server requires at least one Ethernet TCP/IP-supported network interface. In order for IP switchover to work properly, user systems connected to the local network should conform to standard TCP/IP specifications. **Note**: Even though each server requires only a single network interface, you should use multiple interfaces for a number of reasons: throughput requirements, elimination of single points of failure,network segmentation, and so forth.
- **TCP/IP protocol**. Each server requires TCP/IP to be installed and configured properly.
  - The two servers must be on the same LAN segment (that is, no routers between the two systems).
  - Free IP addresses to create SteelEye Protection Suite hierarchies:
    - For each active Microsoft IIS site, you will need one switchable IP address to be shared between the active and standby IIS site.
    - If you plan to protect multiple Microsoft IIS sites, you will need additional IP addresses for each protected IIS resource.
  - **IIS Software.** The IIS Recovery Kit supports Microsoft Internet Information Services (IIS), Release 5.0, Release 6.0, Release 7.0, and Release 7.5. For systems running the IIS Kit and Microsoft FTP Service 7.5, Windows 2008 R2 is required. Microsoft FTP 7.5 service ships as a feature (Identified as “FTP Service”) in Windows 7 and Windows Server 2008 R2.

    Note: The IIS Recovery Kit does not support Microsoft FTP Service 7.5 if installed manually out-of-band on Windows 2008 R1.

    Microsoft IIS software, IIS server roles, FTP feature or SMTP feature must be installed and configured prior to configuring SteelEye Protection Suite and the SteelEye Protection Suite Microsoft IIS Recovery Kit. The same version

should be installed on each server. Please refer to IIS Required Roles and Role Services and Features for requirements that must be installed on each server.

Kit Installation

The SteelEye Protection Suite Microsoft IIS Recovery Kit is included with the SteelEye Protection Suite for Windows core product which is available on CD-ROM or via ftp download.

Kit Removal

CAUTION: Be sure to remove all SteelEye Protection Suite IIS resources from service and delete them prior to removing the recovery kit. Once the kit is removed these resources will be unusable.

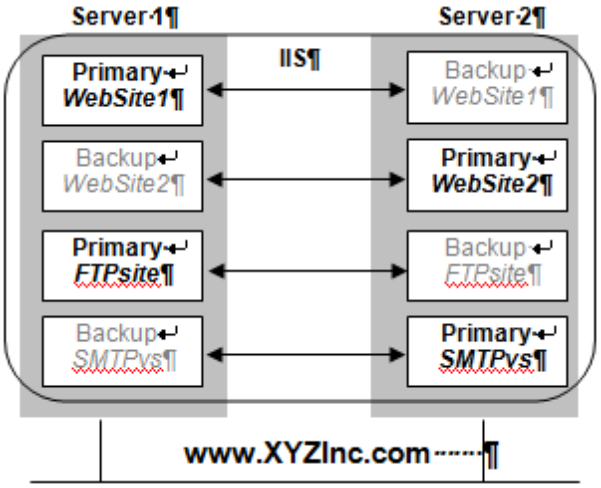
The SteelEye Protection Suite Microsoft IIS Recovery Kit is included with the SteelEye Protection Suite for Windows core product and will be uninstalled when removing the core product.

Configuration Definitions and Restrictions

Active/Active Configuration

IIS allows multiple Web and FTP sites and SMTP virtual servers to run on each server in a cluster. Only a single instance of the IIS software is allowed (or required) on a given system. The Web sites, FTP sites and SMTP virtual servers can be protected and managed individually by LifeKeeper. Subsequent descriptions may use the term “site” to refer generically to a Website, FTP site or SMTP virtual server.

The figure below illustrates a typical configuration of web servers.



In this configuration, each server has two Web sites: one primary and one backup Web site. Server 1 has the primary instance of *WebSite1* and the backup instance of *WebSite2*. Server 2 has the reciprocal configuration: a primary instance of *WebSite2* and a backup instance of *WebSite1*. Only the primary instances of the Web sites actually service incoming user requests on any given server.

In addition, Server 1 has the primary instance of an FTP site named *FTPsite* and the backup instance of the SMTP virtual server named *SMTPvs*, while Server2 has the backup instance of the FTP site and the primary instance of the SMTP virtual server.

If a primary Web site stops servicing user requests, LifeKeeper activates the backup instance on the backup server to resume service there. Thus, if *WebSite1* on Server 1 fails, then LifeKeeper activates the backup instance of *WebSite1* on Server 2. After the switchover, there will be two active instances running on Server 2. Once the problem with the failed web server is corrected,you may switch service back to Server 1. The LifeKeeper Microsoft IIS Recovery Kit allows you to manually switch service back or take advantage of the LifeKeeper automatic switchback feature.

IIS Configuration Considerations

LifeKeeper places certain restraints on your Internet server configurations. These restrictions will ensure that the standby web server/site can successfully and completely replace the active web server/site.

Default Web Site or New Web Site

The Default Web Site created by the IIS installation process may be protected by LifeKeeper with one minor configuration change. The Default WebSite must be reconfigured to use a LifeKeeper protected IP address for the site.

LifeKeeper can also protect new Web Sites that have been configured to use a LifeKeeper protected IP address for the site.

Primary and Backup Designations

The server where the active site is created will be the primary LifeKeeper server for this Web site. The server where the standby site is created will be the backup server for this site. Keep in mind that the designations “primary”and “backup” server change for each site you are configuring.

Naming Restrictions

In order to receive LifeKeeper protection, you should adhere to the following rules for site name (which is entered in the Description field of the IIS console):

- Use only alphanumeric characters and dashes (should NOT contain spaces).
- If you need to change the name (description) of a protected Web Site, first delete the LifeKeeper IIS resource, then change the description, and recreate the resource.

Identical Primary/Backup Web Sites

For each primary IIS site, you must create an identical backup IIS site on the other server. These two servers must be connected by a LifeKeeper heartbeat. In order for the primary and backup sites to be identical, the following criteria must be met:

- The site names entered in the *Description* field of the Properties form must be identical, including using the same case.
- The switchable IP addresses, port, and header assigned to the sites in the Properties form must be identical.
- If using a shared or replicated volume for your web or FTP content, the drive letter and folder of the volume you assign in the *Home Directory Path* must be identical.
- If you configure multiple backup sites for a particular Web site, then you must configure the other Web sites with the same identities; that is, the primary and backup Web sites must contain the same IP addresses, ports, and headers.
- If you configure one Web site as a secure Web site, then you must configure the other Web site as a secure Web site. Additional limitations apply to secure Web sites. See the following section for details.

Configuring Secure Servers

A secure server is a web server that uses Secure Socket Layers (SSL) for communication. Security is improved because the data sent and received are encrypted, and because the web client and the web server can identify one another. Secure servers use *https*: rather than *http*: in their URL. The default port number for a secure server is 443.

With regards to the LifeKeeper Microsoft IIS Recovery Kit and LifeKeeper,there is no difference in running a secure IIS Web site. In fact, IIS allows the same Web site to have both a TCP port and SSL port. There is no change in the startup or operational procedures. Therefore, after a key is generated and a corresponding digital certificate is installed in IIS, you may configure and run with SSL ports.

IIS Configuration

The following configuration rules must be followed to ensure LifeKeeper protection:

- IIS sites that do not have IP addresses specified in the "IPAddress" field of the Properties or Bindings form cannot be protected.
- If using a shared or replicated volume for your web content, the Home Directory should be specified as “A directory located on this computer”. LifeKeeper will not be able to protect the Home Directory if specified as either of the following:
    - a share located on another computer
    - a redirection to a URL
    - a volume that is not protected by LifeKeeper

Document Content Location

Shared and Replicated Content Storage

If the content volume is on a shared or replicated volume, both Web sites must point to the same shared or replicated volume and folder. The primary and backup servers must contain the same content files for the active and standby web servers/sites to be identical. However, if the content volume is not shared or replicated, the content may come from any location on either system.

To ensure data availability on a failover we suggest that you configure the Home Directory on the primary server as a folder on a shared or replicated disk and configure the Home Directory on the backup server identical to the primary server. You then have only one copy of the content files to maintain.

Non-Shared Storage

If your configuration does not utilize shared storage, then the content must be synchronized between local volumes on each server. While the LifeKeeper Microsoft IIS Recovery Kit does not contain any specific features to synchronize the content between two servers, the following are a few suggestions:

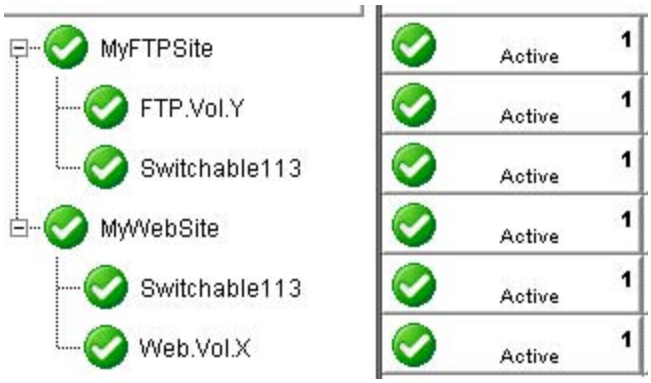
- Use SteelEye DataKeeper to automatically replicate the data volumes on each active server to the standby server(s).
- Use a content replication tool such as Microsoft Site Server 3.0. You can also use the utility *Robocopy* as a content replication tool. Microsoft Site Server is the preferred solution.
- If you have a tape backup system, make a tape backup of the files on the primary server, and then restore them to the backup server, as needed.

Use Different Volume for Multiple IIS Sites

When the LifeKeeper Microsoft IIS Recovery Kit creates an IIS resource hierarchy, it creates dependencies associated with the IP address and content volume using the home directory path designated in the IIS configuration. Were commend that if you protect

multiple sites, then you should designate DIFFERENT IP addresses and volumes for each site.

For example, the hierarchy shown below shows both *MyFTPSite* and *MyWebSite* utilizing the same IP address and different volume resources. Any maintenance done on one site will affect the other site since these have common IP resource dependency.



Bringing *MyFTPSite* In Service on the backup server will also move its dependencies to the backup server. This causes *MyWebSite* to be taken out of service on the primary server. You would then need to manually bring *MyWebSite* In Service on the backup server.

Assigning DIFFERENT IP addresses and volumes to each protected IIS site will give you more flexibility in managing your resources by NOT tying their recovery actions together. However, you may prefer to have them grouped as shown above.

Installing and Configuring IIS with LifeKeeper

Before proceeding, you should have already configured your storage and networking according to the recommendations in the previous chapters of this guide.

Installation Checklist

The installation and setup sequence should be performed in the following order (more detailed instructions for each of these steps are provided in other topics):

1. If using replicated volumes, install SteelEye DataKeeper software on each server and create your mirrors.
2. Install and configure the LifeKeeper Core, which includes the LifeKeeper IP Recovery Kit and LifeKeeper Microsoft IIS Recovery Kit, on each server.
3. Install and configure Microsoft IIS on all servers.

Install SteelEye DataKeeper and Create Mirrors

If you will be using replicated volumes, you should now install the SteelEye DataKeeper for Windows software and create your mirrors. Refer to the SteelEye Protection Suite Installation Guide for more details.

Install and Configure SteelEye Protection Suite and Recovery Kits

The next step is to install the SteelEye Protection Suite Core, which includes the IP Recovery Kit and Microsoft IIS Recovery Kit, on

all servers. See the SteelEye Protection Suite Installation topics for details on installing SteelEye Protection Suite. You must have the same version of SteelEye Protection Suite on all servers.

After you have installed LifeKeeper, you will need to reboot all the servers. After rebooting, make sure LifeKeeper is up and running on all servers.

You can now configure LifeKeeper. The LifeKeeper setup tasks are given in the proper sequence below. For detailed instructions on the LifeKeeper configuration tasks, use the **Help** button or refer to LifeKeeper Configuration.

1. For increased availability, you may set the LifeKeeper Shutdown Strategy to *Switchover Resources*. This task can be done by editing the Server Properties on each server in the cluster. The *Switchover* shutdown strategy allows LifeKeeper to move the all LifeKeeper-protected resources to the other server should the server be shut down gracefully. You will need to set the Shutdown Strategy on all servers.
2. Set up your LifeKeeper communication paths. For the most reliable communication path configuration, we recommend creating two separate TCP/IP comm paths, and if possible, a third comm path. For TCP/IP comm paths, the best results are obtained when you use a private network between the two servers.
3. Create switchable IP addresses for each web server/site pair as required. On the **Edit** menu, select **Server**, then **Create Resource Hierarchy**. From the drop down list, select **IP Address**, and then fill in the information required by the **Protected Application Wizard**. Repeat for each switchable IP address needed.

   When creating LifeKeeper switchable IP addresses, consider the following:

   a. The primary server is the one that normally runs the active Webserver/site. It should be set to priority 1 so that the IP resource matches the IIS resource to be created later.

   b. If desired, change the Switchback Strategy from *Intelligent* (the default) to *Automatic**.

   c. If you have two NICs on the same subnet, you can set the IP Local Recovery* option to have LifeKeeper transfer service of the switchable IP address between the two cards for increased availability.

   *See related topics for additional information on Switchback Strategy and IP Local Recovery.
4. Test your switchable IP addresses for switchover and response.

   a. To test switchover, open the LifeKeeper GUI. Your switchable IP resources should display as green (Active) on the primary server and blue(Standby) on the backup. Right click on the IP instance in the hierarchy tree.From the pop-up menu, select In Service, and select the backup server from the list box. This switchable IP resource will turn from blue to green on the backup server. Repeat this test on any remaining switchable IP addresses. When you are finished testing all the switchable IP addresses, bring them back In Service on their primary servers.

   b. To test response, open an MS-DOS window and use the ping command on each switchable IP address. Your switchable IP addresses should return a response time and packet loss value for each ping.

   c. Do not proceed until your switchable IP addresses pass both the switchover and ping tests successfully.
5. Create your Volume resource(s) which will contain the home directories for your Web/FTP/SMTP services. Perform Volume resource switchovers to ensure that that your volume(s) can be placed in service on primary and backup servers. Also make sure that the priorities you assign to protected IP and Volume resources match on each server.

Install and Configure Microsoft IIS on All Servers

The next step is to configure Microsoft IIS on all the servers in your cluster.

Install and Configure Microsoft IIS Web or FTP Site

To create a Web site or FTP site pair, you need to add a new site on each server and configure the pair to be identical, or you can choose to protect the Default Web and FTP sites:

1. Use the LifeKeeper GUI to bring the switchable IP address and protected Volume resource, if any, in-service on the primary server.
2. Launch the Internet Information Services (IIS) Manager (from Administrative Tools in the Program menu). You will use this interface to create the primary and backup sites.
3. Launch the New Web Site Wizard and enter the Site Name or Description, remembering that the name must be identical on both primary and backup servers.
4. **Web site only**: Enter the TCP port and Host Header fields. They will need to be identical on primary and backup servers.
5. Select or enter the Switchable IP Address for the Web site Note that a protected switchable IP address may not appear in the drop-down list if it is out-of-service, but you can type it in. The IP address for the web site must be identical on primary and backup servers.
6. Web site only: If you plan on configuring your Web sites with multiple identities, enter the switchable IP address in the IP Address field for each multiple identity.
7. The Home Directory or Physical Path for the site can be local (not protected by LifeKeeper) or LifeKeeper shared or replicated storage may be used. If using shared or replicated storage, the volume must be in-service and this directory must already exist.
8. **Web site only**: Select your Web Site Access Permissions.
9. Ensure the Microsoft IIS site is started, and then test it to ensure it is accessible and working properly before proceeding with web site setup on the backup server.
10. Use the LifeKeeper GUI to bring the switchable IP address(es) and protected volume(s), if any, in-service on the backup server.
11. Repeat steps 2-10 to create the site on the backup server. Remember that the Web or FTP site pairs must be identical on the primary and backup servers.

Once you have created and configured all your IIS sites, do the following:

1. Use the LifeKeeper GUI to bring the switchable IP address and protected volume, if any, in-service on their primary server(s).
2. Use the Internet Information Services (IIS) Manager to start the primary site(s) on their primary server(s), and stop the backup sites on the backup servers.

Note: The Microsoft Management Console IIS screen may show all available IP addresses for a site even if the LifeKeeper-protected IP address is NOT in service on that server. This is a bug in the Microsoft Management Console snap-in. It does NOT affect operations.

If your protected FTP site will not permit anonymous logins, the LifeKeeper deep check process must be configured to perform non-anonymous logins. See Protecting FTP Sites with Non-Anonymous Login for more information.

If you wish to create an SMTP Virtual Server, then proceed to Install and Configure SMTP Virtual Server. Otherwise, you are ready to add LifeKeeper protection to the Internet servers by configuring one or more IIS resource hierarchies.

Install and Configure SMTP Virtual Server

Follow the steps below to create an SMTP Virtual Server. You need to add a new virtual server on each system and configure the pair to be identical.

1. Use the LifeKeeper GUI to bring the switchable IP address and protected volume, if any, in-service on the primary server.
2. Launch the Internet Information Services (IIS) Manager for SMTP sites(from Administrative Tools in the Program menu). You will use this interface to create the primary and backup SMTP Virtual Server.
3. Launch the New Web Site Wizard by selecting the server name, then on the Action menu, select New, and then SMTP Virtual Server.
4. Enter the site description, remembering that the description should be identical on both primary and backup servers.
5. Select the switchable IP address for the SMTP Virtual Server when prompted to “Select the IP address to be used for this Web site.” It must be the same on primary and backup servers.
6. When prompted for the home directory path, choose a file share or volume on your shared or replicated storage device.
7. Enter the default domain for this virtual server.
8. Ensure the SMTP virtual server is started, and then test it to ensure it's accessible and working properly before proceeding to setup on the backup server.
9. Use the LifeKeeper GUI to bring the switchable IP address and protected volume, if any, in-service on the backup server.
10. Repeat steps 2-9 to create the site on the backup server. Remember that site pairs must be identical on the primary and backup servers.

Once you have created and configured all your SMTP virtual servers, start the primary sites and stop the backup Web sites as follows:

1. Use the LifeKeeper GUI to bring the switchable IP address and protected volume, if any, in- service on the primary server(s).
2. Use the Internet Information Services (IIS) Manager to start the primary SMTP site on the primary server.

Now you are ready to add LifeKeeper protection to the Internet servers by creating one or more IIS resource hierarchies.

Chapter 3: IIS Configuration Definitions and Restrictions

The topics in this section will assist in configuring the SteelEye Protection Suite Microsoft Internet Information Services Recovery Kit.

IIS Required Roles and Role Services and Features

LifeKeeper interfaces to IIS require the following roles, role services and features to be installed on the server:

Roles:

- Web Server (IIS)

Role Services:

- IIS Management Console
- IIS6 Management Compatibility
- IIS6 WMI Compatibility
- IIS6 Metabase Compatibility
- IIS6 Management Console
- FTP Server (If protecting FTP Sites):
- FTP Service

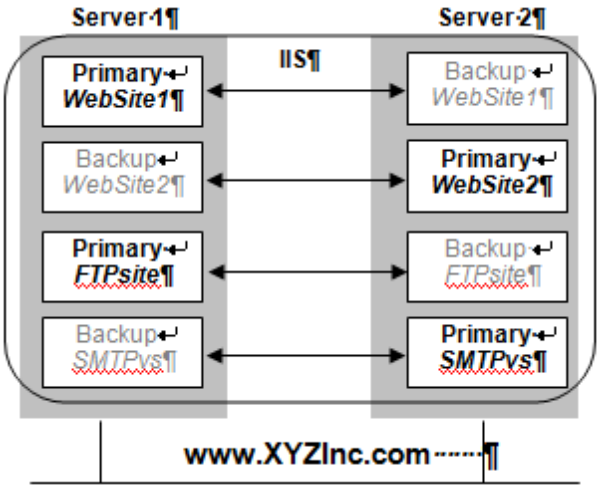
Features:

- SMTP Server (If protecting SMTP sites)

IIS Active Active

IIS allows multiple Web and FTP sites and SMTP virtual servers to run on each server in a cluster. Only a single instance of the IIS software is allowed (or required) on a given system. The Web sites, FTP sites and SMTP virtual servers can be protected and managed individually by LifeKeeper.Subsequent descriptions may use the term “site” to refer generically to a Website, FTP site or SMTP virtual server.

The figure below illustrates a typical configuration of web servers.



In this configuration, each server has two Web sites: one primary and one backup Web site. Server 1 has the primary instance of *WebSite1* and the backup instance of *WebSite2*. Server 2 has the reciprocal configuration:a primary instance of *WebSite2* and a backup instance of *WebSite1*. Only the primary instances of the Web sites actually service incoming user requests on any given server.

In addition, Server 1 has the primary instance of an FTP site named FTP site and the backup instance of the SMTP virtual server named *SMTPvs*, while Server2 has the backup instance of the FTP site and the primary instance of the SMTP virtual server.

If a primary Web site stops servicing user requests, LifeKeeper activates the backup instance on the backup server to resume service there. Thus, if *WebSite1* on Server 1 fails, then LifeKeeper activates the backup instance of *WebSite1* on Server 2. After the switchover, there will be two active instances running on Server 2. Once the problem with the failed web server is corrected, you may switch service back to Server 1. The LifeKeeper Microsoft IIS Recovery Kit allows you to manually switch service back or take advantage of the LifeKeeper automatic switchback feature.

Primary and Backup Designations

The server where the active site is created will be the primary LifeKeeper server for this Web site. The server where the standby site is created will be the backup server for this site. Keep in mind that the designations “primary” and “backup” server change for each site you are configuring.

Naming Restrictions

In order to receive LifeKeeper protection, you should adhere to the following rules for site name (which is entered in the Description field of the IIS console):

- Use only alphanumeric characters and dashes.
- If you need to change the name (description) of a protected Web Site, first delete the LifeKeeper IIS resource, then change the description, and recreate the resource.

Identical Primary Backup Web Sites

For each primary IIS site, you must create an identical backup IIS site on the other server. These two servers must be connected by a LifeKeeper heartbeat. In order for the primary and backup sites to be identical, the following criteria must be met:

- The site names entered in the **Description** field of the **Properties** form must be identical, including using the same case.
- The switchable IP addresses, port and header assigned to the sites in the **Properties** form must be identical.
- If using a shared or replicated volume for your web or FTP content, the drive letter and folder of the volume you assign in the **Home Directory Path** must be identical.
- If you configure multiple backup sites for a particular Web site, you must configure the other Web sites with the same identities; that is, the primary and backup Web sites must contain the same IP addresses, ports and headers.
- If you configure one Web site as a secure Web site, then you must configure the other Web site as a secure Web site. Additional limitations apply to secure Web sites. See Configuring Secure Servers for details.

Configuring Secure Servers

A secure server is a web server that uses Secure Socket Layers (SSL) for communication. Security is improved because the data sent and received are encrypted and because the web client and the web server can identify one another. Secure servers use https: rather than http: in their URL. The default port number for a secure server is 443.

With regards to the LifeKeeper Microsoft IIS Recovery Kit and LifeKeeper, there is no difference in running a secure IIS Web site. In fact, IIS allows the same Web site to have both a TCP port and SSL port. There is no change in the startup or operational procedures. Therefore, after a key is generated and a corresponding digital certificate is installed in IIS, you may configure and run with SSL ports.

IIS Configuration

The following configuration rules must be followed to ensure LifeKeeper protection:

- IIS sites that do not have IP addresses specified in the "IPAddress" field of the **Properties** or **Bindings** form cannot be protected.
- If using a shared or replicated volume for your web content, the **Home Directory** should be specified as "**A directory located on this computer**". LifeKeeper will not be able to protect the **Home Directory** if specified as any of the following:
  - a share located on another computer
  - redirection to a URL
  - volume that is not protected by LifeKeeper

Document Content Location

Shared and Replicated Content Storage

If the content volume is on a shared or replicated volume, both Web sites must point to the same shared or replicated volume and folder. The primary and backup servers must contain the same content files for the active and standby web servers/sites to be identical. However, if the content volume is not shared or replicated, the content may come from any location on either system.

To ensure data availability on a failover we suggest that you configure the **Home Directory** on the primary server as a folder on a shared or replicated disk and configure the **Home Directory** on the backup server identical to the primary server. You then have only one copy of the content files to maintain.

Non-Shared Storage

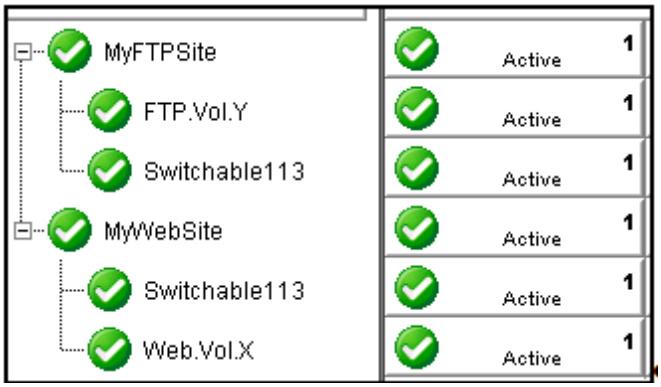
If your configuration does not utilize shared storage, then the content must be synchronized between local volumes on each server. While the LifeKeeper Microsoft IIS Recovery Kit does not contain any specific features to synchronize the content between two servers, the following are a few suggestions:

- Use SteelEye DataKeeper to automatically replicate the data volumes on each active server to the standby server(s).
- Use a content replication tool such as Microsoft Site Server 3.0. You can also use the utility **Robocopy** as a content replication tool. Microsoft Site Server is the preferred solution.
- If you have a tape backup system, make a tape backup of the files on the primary server and then restore them to the backup server, as needed.

Use Different Volume for Multiple IIS Sites

When the LifeKeeper Microsoft IIS Recovery Kit creates an IIS resource hierarchy, it creates dependencies associated with the IP address and content volume using the home directory path designated in the IIS configuration. We recommend that if you protect multiple sites, then you should designate DIFFERENT IP addresses and volumes for each site.

The hierarchy shown below shows both MyFTPSite and MyWebSite utilizing the same IP address and different volume resources. Any maintenance done on one site will affect the other site since these have common IP resource dependency.



Bringing *MyFTPSite* In Service on the backup server will also move its dependencies to the backup server. This causes *MyWebSite* to be taken out of service on the primary server. You would then need to manually bring *MyWebSite* In Service on the backup server.

Assigning DIFFERENT IP addresses and volumes to each protected IIS site will give you more flexibility in managing your resources by NOT tying their recovery actions together. However, you may prefer to have them grouped as shown above.

Chapter 4: IIS Resource Configuration Tasks

The topics in this section describe the tasks involved in configuring resources.

Create an IIS Resource Hierarchy

Before creating your IIS hierarchy, be sure you have created the associated IP and volume (if needed) resource hierarchies first.

To create a resource instance from the primary server, you should complete the following steps:

1. From the LifeKeeper GUI menu, select **Edit**, then **Server**. From the drop down menu, select **Create Resource Hierarchy**. Click **Next** after selecting the serves for your protected application.

   A dialog box will appear with a drop down list box with all the recognized applications you can protect within the cluster.

   Note: When the **Back** button is active in any of the dialog boxes, you can go back to the previous dialog box. This is especially helpful should you encounter an error that might require you to correct previously entered information. If you click **Cancel** at any time during the sequence of creating your hierarchy, LifeKeeper will cancel the entire creation process.

2. The **Create Protected Application** window will appear. Select **IIS** from the drop down list for **Application to Protect** and click **NEXT**.

3. Select the Service Type (**WEBeb**, **FTP** or **SMTP**) and click **NEXT**.

4. Accept the Site Name listed or select enter a new one from the drop down list and click **NEXT**. LifeKeeper generates this list from the IIS configuration information.

5. Accept the Site Tag offered by LifeKeeper that is the same as the Site Name or enter a new **Site Tag** and click **NEXT** to create the IIS resource.

LifeKeeper will validate that you have provided valid data to create your resource hierarchy. If LifeKeeper detects a problem, an error message will appear in the information box. If the validation is successful, your resource will be created.

Extend an IIS Resource Hierarchy

This operation can be started from the **Edit** menu or initiated automatically upon completing the **Create IIS Resource Hierarchy** option, in which case you should refer to Step 2 below.

1. On the **Edit** menu, select **Resource** then **Extend Resource Hierarchy**. The **Pre-Extend Wizard** appears.

2. The **Pre-Extend Wizard** will prompt you to enter the following information.

   Note: The first two fields appear only if you initiated the **Extend** from the **Edit** menu.

Field	Tips
Primary Server	Enter the server where your IIS resource is currently in service.

Field	Tips
Resource Hierarchy to Extend	Select the IIS resource hierarchy to be extended.
Backup Server	Select a server from the list of connected servers for which you have Administrator permission to be the backup server for the IIS resource.

3. After receiving the message that the pre-extend checks were successful, click **Next**.
4. Depending upon the hierarchy being extended, LifeKeeper will display a series of information boxes showing the **Resource Tags** to be extended which cannot be edited. Click **Next** to extend each of the dependencies.
5. Select a priority for the IIS resource on the backup server. Click **Extend** to extend the IIS resource to the backup server.
6. Click **Finish** to complete the extend process.

Delete an IIS Resource Hierarchy

To delete a resource hierarchy from all the servers in your LifeKeeper environment, complete the following steps:

1. From the LifeKeeper GUI menu, select **Edit** then **Resource**. From the drop down menu, select **Delete Resource Hierarchy**.
2. Select the **Target Server** where you will be deleting your IIS resource hierarchy. Click **Next** to proceed to the next dialog box. **Note**: This dialog will not appear if you selected the **Delete Resource** task by right-clicking on an individual resource instance in the right pane or on a global resource in the left pane where the resource is on only one server.
3. Select the hierarchy to delete. Remember that the list box displays every hierarchy on the target server (i.e. in-service and out-of-server). If you want to stop the IIS instance and remove the resource hierarchy from LifeKeeper protection, you must make sure that the hierarchy you choose is out of service before deleting it. **Note**: This dialog will not appear if you selected the **Delete Resource** task by right-clicking on a global resource in the left pane or an individual resource instance in the right pane.
4. Click **Next** to proceed to the next dialog box.
5. An information box appears confirming your selection of the target server and the hierarchy you have selected to delete. Click **Delete** to remove the IIS resource from LifeKeeper protection. The IIS resource and all its dependencies will be deleted form LifeKeeper protection. Another information box appears confirming that the IIS resource was deleted successfully.
6. Click **Done** to exit the **Delete Resource Hierarchy** menu selection.

Unextend Your IIS Hierarchy

To unextend your IIS hierarchy from a system:

1. From the LifeKeeper GUI menu, select **Edit** then **Resource**. From the drop down menu, select **Unextend Resource Hierarchy**.
2. Select the Target Server where you want to unextend the IIS resource. It cannot be the server where the IIS resource is currently in service.

   Note: The dialog to select the target server will not appear if you selected the **Unextend** task by right-clicking from the right pane on an individual resource instance.

3. Click **Next** to proceed to the next dialog box.
4. Select the IIS resource hierarchy to unextend. Click **Next** to proceed to the next dialog box.

   Note: This dialog will not appear if you selected the **Unextend** task by right-clicking on a global resource in the left pane or an individual resource instance in the right pane.
5. An information box appears confirming the target server and the IIS resource hierarchy you have chosen to unextend. Click **Unextend**.
6. Another information box appears confirming that the IIS resource was unextended successfully. Click **Done** to exit.

Chapter 5: Testing Your IIS Resource Hierarchy

The topics in this section assist in testing your IIS resource hierarchy.

Performing a Manual Switchover from the GUI

You can initiate a manual switchover from the LifeKeeper GUI by selecting **Edit**, then **Resource**, then **In Service**. For example, an In Service request executed on a backup server causes the application hierarchy to be taken out of service on the primary server and placed in service on the backup server. At this point, the original backup server is now the primary server and original primary server has now become the backup server.

If you execute the **Out of Service** request, the application is taken out of service without bringing it in service on the other server.

Recovery Operations

When the primary server fails, the LifeKeeper Microsoft IIS Recovery Kit software performs the following tasks:

- Brings the IIS resource hierarchy into service on the backup server by bringing In Service the IP address(s) on one of that server's physical network interfaces
- Unlocks the shared or replicated volume - if one is being used - for the backup server and locks it for the primary server
- Starts the IIS Web site on the backup server

After recovery, web server users may reconnect by clicking on the **Reload/Refresh** button of their browsers.

Chapter 6: IIS Hierarchy Administration

The topics in this section assist in the administration of IIS hierarchies.

Modifying Quick Check Interval, Deep Check Interval and Local Recovery

The default values for the quick check interval, deep check interval and local recovery may be modified after the resource has been placed under LifeKeeper protection by using the LifeKeeper GUI. To change the default values, right-click on the resource and select the entry from the menu list you wish to modify. After changing the value, click **Modify**. Results from the modify operation will be displayed in a dialog box. Click **Done** to complete the process.

Default values are as follows:

- Quick Check Interval is **180 seconds** (3 minutes)
- Deep Check Interval is **300 seconds** (5 minutes)
- Local Recovery is "**Enabled**"

Manual Switchover

Manual switchover can be performed from the LifeKeeper GUI using the **In Service** option. LifeKeeper will move the switchable IP addresses, volume and the IIS Web/FTP/SMTP site to the other server. You may wish to do this, for example, after a failover and you have fixed the primary and you want the primary to take over again.

IIS Failover

A failover occurs in two situations:

- The first situation is when the hardware or operating system has suffered a major failure and the server is no longer functioning. The LifeKeeper core on the backup server detects this when its heartbeat messages fail. At that time, the LifeKeeper core invokes the kit's recovery script. The recovery script ensures that the Internet server(s) is brought In Service on the backup server.
- The second situation is when the Recovery Kit's **Deepcheck** and **Quickcheck** scripts detect failures of the application. These scripts respond to the LifeKeeper core with code(s) indicating failure. The LifeKeeper core starts the failover process and invokes the kit's recovery scripts. The LifeKeeper core first stops the local server (if it is not stopped) and deactivates the switchable IP address and LifeKeeper volumes. It then continues the failover to the backup server.

When the primary server is repaired, the Internet server automatically returns to the primary server if switchback type is **Automatic**. You must perform a manual switchover if switchback type is **Intelligent**.

A relatively small number of web clients will experience a problem whenever a switchover or failover occurs. First, the process of moving the IP addresses and volumes to the backup system and starting the backup server there takes approximately 45 seconds (depending on the number of IP addresses and volumes), and users cannot connect to the server during that time. Second, the active server is stopped during the switchover, and users with open connections to the active server will be disconnected. In any case, if the

IIS client retries the request, the request should succeed. Of course, once the switchable IP addresses and volumes have moved to the backup system and the backup site is running, service will be normal again.

Protecting FTP Sites with Non-Anonymous Login

The default procedure used to monitor protected FTP sites is to connect to the site and use an anonymous login. This feature is performed by the LifeKeeper deep check process assigned to monitor each FTP site. If your site does not permit an anonymous login, the default deep check operation will fail. Where anonymous logins are not permitted, you may either provide LifeKeeper with a small login script, or disable the deep check process for the LifeKeeper resource by setting the associated deep check interval to 0 seconds.

Using an FTP Login Script

The Microsoft FTP command provides the ability to use scripted FTP logins. LifeKeeper will create an empty login script file for each protected FTP site and the file names will match the FTP site names. The empty scripts are not used by LifeKeeper until written with FTP commands. They are created in the following folder:

```
<LifeKeeper Root Install Folder>\admin\kit\webapp
```

For instance, an empty login script for the “Default FTP Site” would be located at:

```
<LifeKeeper Root Install Folder>\admin\kit\webapp\Default FTPSite.txt
```

Spaces are permitted in the file name so it can match the FTP site name exactly with a .txt extension. The content of the script should include only 4 lines containing the FTP open command, the login ID, the login password, and the FTP bye command. For example, a login script might contain the following 4 lines:

```
open 192.168.1.10
 mytestloginID
 mytestloginPW
 bye
```

LifeKeeper will use a search mechanism for each response from the FTP client utility. A response starting with “230” indicates a successful login. A login failure will fail the deep check process. Other commands can be added to the script but they will be ignored by LifeKeeper.

Disabling the FTP Deep Check Process

If the protected FTP site does not permit anonymous logins and you prefer not to use a login script as described above, you may disable the deep check process for a particular LifeKeeper protected resource. Change directory to the LifeKeeper "bin" folder and use the following LifeKeeper command to disable deep check for the resource.

```
cd <LifeKeeper Root Install Folder>\bin
ins_setchkint -t <LifeKeeper Resource Tag Name> -c d -v 0
```

Changing LifeKeeper Microsoft IIS Recovery Kit Configuration

Any configuration change that affects the port number, IP address, hardware virtual servers or secure/non-secure setting, will affect the LifeKeeper configuration. As there is no direct linkage between the server and this kit, you should follow this procedure to synchronize the configuration.

1. Remove protection of the IIS resource by taking the hierarchy out of service and then deleting the hierarchy.
2. On the primary server, run the IIS Console as appropriate and apply the changes to the server.
3. On the backup server, run the IIS Console and apply the changes to the server.
4. Add LifeKeeper protection to the IIS resource by creating the IIS resource hierarchy and extending it to the backup server.

Removing Microsoft IIS

Remove LifeKeeper protection for the IIS Web/FTP/SMTP site before removing either the site itself or the entire software package. This is important so that LifeKeeper will not try to protect something that does not exist.

Note: This release of the kit was tested with Microsoft IIS 5.0 and Microsoft IIS 6.0. It will not necessarily be compatible with later releases, mainly because of dependencies on the location and content of certain registry keys and configuration files.

Changing the Network Interface Card (NIC)

The procedure for changing the Network Interface Card (NIC) depends upon whether the replacement NIC is the same type of card as the original. If the NIC is exactly the same model, you only need to power down the system, replace the card, and then restart the system; no software reconfiguration is necessary. Because you can switch to the backup server during this procedure, there is no need for a service interruption for your web service.

In contrast to the simple procedure above, the procedure for changing to a different type of NIC is long and will interrupt the web service. The basic reason for this is that the LifeKeeper IP hierarchy data includes the NIC model number. That piece of data cannot easily be changed, so the procedure is to remove and reinstall the Switchable IP addresses by doing the following:

1. Use the LifeKeeper GUI to remove protection from all IIS resources by taking them out of service, then deleting the hierarchies.
2. Stop all IIS services, including those on the backup server(s). All IIS services are now out of service.
3. Delete all IP hierarchies (be sure to save the configuration data in a notebook).
4. Shut down the server, replace the NIC, and then reboot the server.
5. Create all IP hierarchies again.
6. Bring the IP hierarchies In Service on each Web site's primary server.
7. On the primary server, start the IIS services again. The Web sites are now in-service again.
8. On each web server’s primary server, use the LifeKeeper GUI to re-create the IIS resource hierarchy.

Note1: A quick way to identify the type of NIC currently installed is to run the ipconfig command from a DOS prompt. The type of NIC is displayed in the output (for example, "Ethernet adapter: DC21X41" describes an Ethernet NIC named DC21X41.

Note2: Changing the primary NIC could potentially affect LifeKeeper licensing. Refer to the Planning and Installation Guide for additional information on licensing.

Chapter 7: IIS Troubleshooting

This section is intended to provide suggestions and insights into occurrences that are not specifically related to the LifeKeeper software, but have a relationship with the total environment.

Symptoms and Solutions

SYMPTOM: Identical sites are created on both the primary and the secondary servers, but the sites are not displayed in the **Site Name list** in the **Create Resource Wizard.**

SOLUTION:

- Check that the same optional parameters are specified and their values are also the same (even the same letter case) on both systems.
- Also ensure that all sites have a valid description for LifeKeeper (alphanumeric characters and dashes only). If you need to change the name (description) of a protected Web Site, first delete the IIS resource, then change the description and recreate the resource.

SYMPTOM: When attempting to access the FTP site, the following error message is received:

```
"User x cannot login, home directory inaccessible".
```

SOLUTION: To allow users to log on to an FTP site as *ANONYMOUS*, the Internet Guest Account user `IUSR_{machine name}` must be given the right to logon on locally.

SYMPTOM: When configuring your IIS Web/FTP/SMTP in the Internet Information Services (IIS) Manager and you attempt to select the IP address from the drop-down list, your switchable IP address is not displayed.

SOLUTION: Manually enter the switchable IP address.