LifeKeeper for Windows

Microsoft Exchange Server 2007 Recovery Kit

Administration Guide

January 2012

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

Table of Contents

Chapter 1: Introduction

LifeKeeper Microsoft Exchange Server 2007

The LifeKeeper Microsoft Exchange 2007 Server Recovery Kit provides for the installation and operation of Microsoft Exchange Server in a shared disk or replicated environment. The Microsoft Exchange Server resource hierarchy is created on one server and then extended to a backup server in the cluster. The resource is active on only one server at a given time. It may be brought into service on a backup server manually (for example, to perform maintenance on the primary server), or in the case of a server or resource failure, LifeKeeper will perform a failover automatically.

Exchange 2007 Services

LifeKeeper protects the following Microsoft Exchange Server services:

Core Services	Optional Services
Microsoft Exchange Active Directory Topology Service	Microsoft Exchange Monitoring
Microsoft Exchange System Attendant	Microsoft Exchange Anti-spam Update
Microsoft Exchange Information Store	Microsoft Exchange IMAP4*
Microsoft Exchange Service Host	Microsoft Exchange POP3*
Microsoft Exchange Mailbox Assistants	Microsoft Exchange EdgeSync
Microsoft Exchange Mail Submission	Microsoft Exchange Transport Log Search
Microsoft Search (Exchange)	
Microsoft Exchange Search Indexer	
Microsoft Exchange File Distribution*	
Microsoft Exchange Transport	
*Only if Client Access Role is installed.	*Only if Client Access Role is installed.

Resource Hierarchy for Microsoft Exchange 2007 Server

The typical Microsoft Exchange Server hierarchy consists of the following resources:

- Microsoft Exchange Server

- IP address (optional)

- DNS resource (optional)

- Volume(s)

The LifeKeeper GUI display shown below depicts a Microsoft Exchange Server hierarchy including two volume resources.
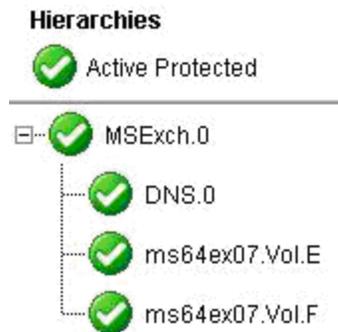
The Microsoft Exchange Server resource (MSExch.0) is the upper most (parent) resource in the above hierarchy tree. It is responsible for starting and stopping its dependent resources. The DNS resource (DNS.0) and two volume resources (E: and F:) are dependent resources under the Microsoft Exchange Server resource.

Chapter 2: Exchange Server Installation

When using LifeKeeper to protect Exchange, both the primary and backup Exchange servers should be in the same domain and in the same Administrative Group. If this is a multi-domain configuration, the Exchange servers should be members of the root domain of the Active Directory forest. It is not recommended to install Exchange on domain controllers.

IMPORTANT: LifeKeeper will not support Exchange 2007 if the Exchange binaries are installed on a replicated volume.

The Exchange kit supports Exchange Server 2007 installed in two different configurations as follows:

1. Standard installation **with** Client Access: Exchange Server installed with following roles.

   - Mailbox Server

   - Client Access Server

   - Hub Transport Server

2. Standard installation **without** Client Access: Exchange Server installed with following roles.

      - Mailbox Server

      - Hub Transport Server

Recovery Kit Requirements

The SteelEye LifeKeeper Microsoft Exchange 2007 Server Recovery Kit provides high availability for Microsoft Exchange 2007 Server environments running under LifeKeeper protection. LifeKeeper constantly monitors the health of both the physical server on which Exchange is active, the individual Exchange processes, and database status. On detection of any problem, LifeKeeper will initiate a recovery action to ensure that Exchange is always available.

Before installing and configuring the LifeKeeper Microsoft Exchange 2007 Server Recovery Kit, be sure that your configuration meets the following requirements:

Operating System software. LifeKeeper supports the following versions of Windows operating systems:

- Windows Server 2003 x64 Standard, Enterprise, Data Center Editions

- Windows Server 2003 R2 x64 Standard, Enterprise, Data Center Editions

- Windows Server 2008 Standard, Enterprise, Data Center Editions (32 and 64-bit versions)

Exchange Server software. LifeKeeper supports the following versions of Microsoft Exchange:

- Exchange Server 2007 (standard edition) with Service Pack 1

- Exchange Server 2007 Enterprise with Service Pack 1

Storage. The Exchange Storage Group must be accessible by all systems in the Exchange cluster so that recovery actions can take place. LifeKeeper for Microsoft Exchange Server can operate in two different storage configurations:

- Using a shared SCSI or Fiber Channel device between the primary and backup Exchange server with the Exchange Storage Group placed on this shared device. This configuration has the advantage that writes of Exchange data only occur once during processing.

- Using SteelEye DataKeeper to replicate the Exchange Storage Group between local volumes on the servers within the cluster. This configuration removes the requirement for a shared storage device which supports the building of a lower cost cluster configuration or of a wide area disaster recovery configuration.

Recovery Kit Installation

The LifeKeeper Microsoft Exchange 2007 Server Recovery Kit is available via ftp download. InstallShield provides a standard installation interface. For complete instructions on installing or removing LifeKeeper, refer to the Installation topic.

Important: Do not install LifeKeeper, this Recovery Kit or SteelEye DataKeeper until you have read and followed the detailed configuration procedures outlined in Configuring Microsoft Exchange Server with LifeKeeper.

Starting and Stopping Exchange Services (Large Stores)

The LifeKeeper Microsoft Exchange 2007 Server Recovery Kit installation creates a registry entry, MAXWAIT, which is stored in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SteelEye\LifeKeeper\RK\ms64ex07
```

MAXWAIT is an integer value that specifies the number of seconds that LifeKeeper will wait for a single Microsoft Exchange Server service to start or stop. If the service has not started within the specified time frame, LifeKeeper will assume there is a failure.

The default value for MAXWAIT is 900 seconds (15 minutes); however, it is possible that for extremely large stores, 900 seconds might not be enough time for the related services to reach the STARTED or STOPPED state. If this is the case, you should change the registry entry to a more appropriate value for your environment.

Kit Removal

To remove the LifeKeeper Microsoft Exchange 2007 Server Recovery Kit software, choose **LifeKeeper Microsoft Exchange 2007 Server Recovery Kit v7** in the **Add/Remove programs** applet in the control panel.

CAUTION: When removing the LifeKeeper Microsoft Exchange 2007 Server Recovery Kit, be sure there are no Microsoft Exchange instances or resources in use. Once the kit is removed, these resources will be unusable.

Exchange Server Installation

When using LifeKeeper to protect Exchange, both the primary and backup Exchange servers should be in the same domain and in the same Administrative Group. If this is a multi-domain configuration, the Exchange servers should be members of the root domain of the Active Directory forest. It is not recommended to install Exchange on domain controllers.

Install Microsoft Exchange Server
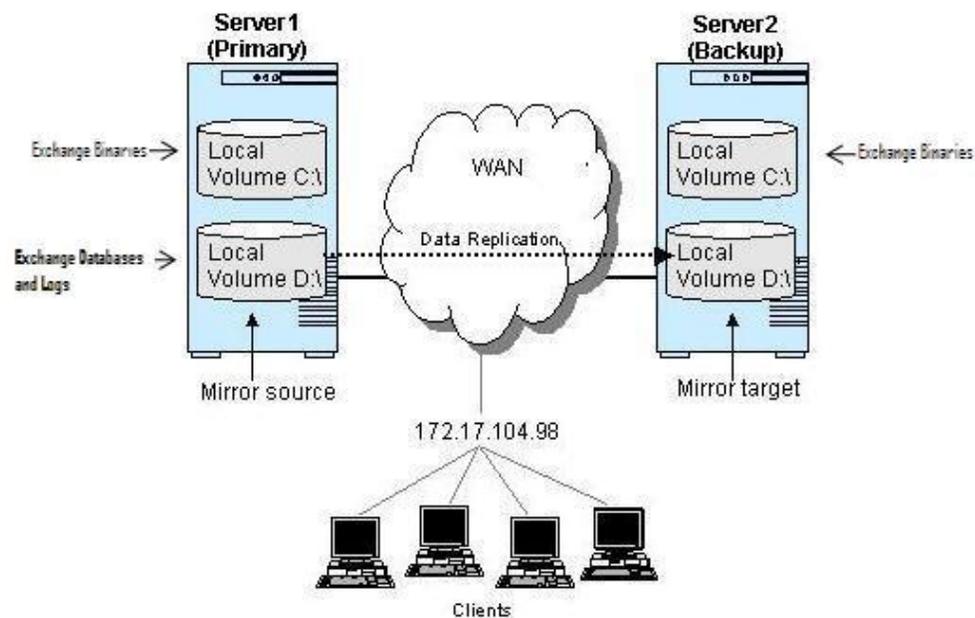
Use the following steps to install Microsoft Exchange Server on both your primary and backup servers. Be sure to read the Microsoft Exchange Server installation documentation and the Release Notes provided on the Microsoft Exchange Server CD carefully before beginning the installation. It is not recommended that Exchange be installed on domain controllers.

Note: If Microsoft Exchange Server is already installed on the system that will become your primary server, skip to the section On the Backup Server, which provides the steps needed to install Microsoft Exchange Server on your backup server.

On the Domain Controller in Active Directory Site

On the Domain Controller in the Active Directory site, create an Exchange Administrator account to use for the installation. Use the Active Directory Users and Computers snap-in to create an Exchange Administrator account that is a domain account, and make it a member of following groups:

- Enterprise Admins

- Schema Admins

- Domain Admins

- Domain Users

On the Primary Server

1. Install Exchange Server 2007 SP1 using steps described in How to Perform a Typical Installation Using Exchange Server 2007 Setup at http://technet.microsoft.com/en-us/library/bb123694(EXCHG.140).aspx

2. Install any additional Exchange Service Pack(s) at this time.

3. Perform the following steps to make the required changes in the location of the Microsoft Exchange transaction logs and database files to the shared or replicated volume(s) to be protected by LifeKeeper. Microsoft Exchange server must be running in order to perform the following steps.

   a. Use Exchange Management Console to move the Microsoft Exchange log files to the shared or replicated volume(s). Open properties of all storage groups and change the "Transaction log location" and "System path location" to the LifeKeeper protected shared or replicated volume(s). This will unmount, move,and remount the databases files and log files in the new location.

   b. Use Exchange Management Console to move the Microsoft Exchange database files to the shared or replicated volume(s). Open the properties of all private mailbox stores and public folders and select the "Database" page. Change the value of "Exchange database" to point to the LifeKeeper-protected shared or replicated volume(s).

4. Change the location of the queue database and queue database transaction logs to a shared or replicated volume(s) using the method described in the article "How to Change the Location of the Queue Database" at *http://technet.microsoft.com/en-us/library/bb125177.aspx*

5. Configure your clients to connect to the Exchange server.

6. Test that messages can be sent externally and internally to other mail recipients on the Exchange server using all clients you plan to support (i.e.,MAPI, POP3, OWA etc.). See Client and Other Microsoft Exchange Server Access for additional information.

On the Backup Server

Perform the following steps on the backup server.

Using the same method described above, install Exchange Server 2007 SP1 on the backup server. Ensure that roles installed are same as the primary server.

- Install any additional Exchange Service Pack(s) at this time.

Install LifeKeeper

After you have installed and tested Microsoft Exchange Server, perform the following tasks to install

LifeKeeper on both servers.

On the Primary Server

1. If you plan to use replicated volumes rather than shared storage, install the SteelEye DataKeeper software and license key on the primary server. Refer to the SteelEye DataKeeper Technical Documentation.

2. Install the LifeKeeper Core software, including the license key.

3. Install the LifeKeeper Microsoft Exchange 2007 Server Recovery Kit, including the recovery kit license key.

4. Reboot the server.

On the Backup Server

Repeat steps 1-4 above to install SteelEye DataKeeper (if applicable), LifeKeeper, and LifeKeeper Microsoft Exchange 2007 Server Recovery Kit to the backup server.

Chapter 3: Exchange Server 2007 Configuration Considerations

Some of the basic configuration requirements for Microsoft Exchange Server in a LifeKeeper environment are described below. These considerations should be reviewed carefully prior to configuring Microsoft Exchange Server in your LifeKeeper environment. A hyperlink has been provided if this configuration information is also applicable to Exchange 2003 configurations.

- Active/Active and Active/Standby Configurations
- Active/Standby N+1 Configuration
- Public Folder Access in N+1 Type Cluster
- LifeKeeper Communication Path Considerations
- Consistent Network Name Resolution
- Client and Other Microsoft Exchange Server Access

Clients connect to the Microsoft Exchange Server system using the computer name as the home server for their mailbox. Since LifeKeeper supports TCP/IP and NetBIOS protocols, at least one of these protocols must be installed and configured on the client systems.

- Usage of Protected IP Address in Exchange Server Hierarchy

  A LifeKeeper protected IP address (switchable IP address) provides transparent connectivity to mail clients of the protected Exchange resource after failover occurs. However, in a WAN environment, depending upon subnet configuration, it may not be possible to protect an IP address. Use the following guidelines to help you determine whether to use a switchable IP address in the Exchange Server hierarchy.

- All LifeKeeper Servers in One IP Subnet

  When LifeKeeper servers are running in the same IP subnet, a switchable IP address provides for client connectivity after the failover. This means that the client application/system does not have to be reconfigured to access the Exchange Server. For this environment, it is best to use the switchable IP address through a static entry in DNS.

- LifeKeeper Servers in Different IP Subnets

  LifeKeeper cannot protect an IP address for the Microsoft Exchange Server if the LifeKeeper servers are in different IP subnets. However, transparent client connectivity can be achieved through necessary updates in DNS entries for the servers, which can be accomplished using a LifeKeeper DNS resource. The DNS Recovery Kit, included

with the LifeKeeper for Windows core product, allows you to create a DNS resource protecting A record and PTR record (if exists) of the primary server or an alias name. For further information see Creating a DNS Resource Hierarchy.

Depending on the type of clients being used, the Exchange resource hierarchy requires one or two LifeKeeper DNS resources. A DNS resource protecting the primary server name is required for the Outlook MAPI client. A DNS resource protecting an alias name is required for OWA clients.

The example below describes how the DNS update works for the different mail client protocols after a failover.

Primary server   ExchSrvr1(172.17.10.24/255.255.255.0)

Backup Server   ExchSrvr2(172.16.10.25/255.255.255.0)

Zone: mydomain.com

DNS Configuration - Before failover:

A Record ExchSrvr1 - > 172.17.10.24

   ExchSrvr2 - > 172.16.10.25

   ExchSrvr1Alias-> 172.17.10.24

DNS Configuration - After failover:

A Record ExchSrvr1 - > 172.16.10.25

   ExchSrvr2 - > 172.16.10.25

   ExchSrvr1Alias-> 172.16.10.25

Outlook MAPI clients connect using **ExchSrvr1.mydomain.com**

OWA clients connect using **ExchSrvr1Alias.mydomain.com**

Configuring LifeKeeper

1. Login to the LifeKeeper GUI.

2. Create the communication paths between the primary and backup servers. See creating communication paths for details.

   Note: If using SteelEye DataKeeper, be sure that a TCP/IP communications path is established over the replicating network.

3. In LifeKeeper, create (optional) IP resource or (optional) DNS resource and extend them to the backup server. The volume resources for the volumes storing the Exchange database, log files and the queue database and queue transaction logs will be automatically created during the create of the Exchange resource in Step 8.

4. Create the Microsoft Exchange Server resource hierarchy and extend it to the backup server. See Creating a Microsoft Exchange Server Hierarchy for details. The creation will create the

necessary dependencies on the volume and IP resources created in previous steps. If you are having a problem extending your Exchange resource hierarchy, see Extend of Exchange Resource Problems under the Troubleshooting section for help.

If you are protecting more than one Exchange server with a single backup Exchange server in an N+1 configuration in Active/Standby mode, you will need to create the hierarchy on all the primary servers and extend it to the common "+1" backup server. This will leave one Exchange hierarchy on each of the primary servers and N numbers of hierarchies on the backup server.

5. If your Exchange server is configured with routing group and Send connectors to work with other Exchange servers or messaging systems, you may need to configure on the backup Exchange server. Based on your setting and network configuration you may have to add the backup Exchange server to your routing or Send connector configuration.

   To add your backup server as Source Server in Send Connectors, open the Exchange Management Console and navigate to Organization Configuration >Hub Transport > Send Connectors. Select all Send Connectors and add backup server name through Properties -> Source Server page.

6. If using a switchable IP address for 6 client connections, configure a static entry in DNS for the primary Exchange Server.

   On the primary Exchange Server, change the DNS registration default as follows:

   a. Right-click **My Network Places**, and then click **Properties**.

   b. Right-click the connection that you want to configure, and then click **Properties**. Click **Internet Protocol (TCP/IP)**, click **Properties**, click **Advanced**, and then click the **DNS** tab.

   c. By default, "**Register this connection's address in DNS**" is selected. De-select this option.

   On the DNS server, create a static entry for the Microsoft Exchange Server name that is mapped to the switchable IP address as follows:

   a. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **DNS**.

   b. Under **DNS**, expand the applicable DNS server, expand **Forward Lookup Zones** and then click the applicable zone.

   c. Assign the switchable IP address to the A record of the primary server.

   Note: No changes are required in DNS for the backup Exchange Server.

7. To avoid LifeKeeper GUI connection problems caused by the above DNS change, add an entry of each LifeKeeper server mapping to its static IP address in the `%WINDIR%\system32\drivers\etc\hosts` file.

   For example, LifeKeeper server *Server1*'s hosts file should be modified to map *Server2* and its static IP address, and LifeKeeper server *Server2*'s hosts file should be modified to map

Server1 and its static IP address. Use the *NetBIOS* name of the computer and not the fully qualified domain name when entering name in the hosts file.

8. Test your Microsoft Exchange Server resources by doing the following:

    a. Perform a manual switchover. See Testing Your Resource Hierarchy for details.

    b. After the switchover, test that messages can be sent externally and internally to other mail recipients.

Exchange 2007 Overview

Refer to the following topics for instructions for creating and extending your Microsoft Exchange Server resource hierarchies.

- Creating a Microsoft Exchange Server Hierarchy

- Extending a Microsoft Exchange Server Resource Hierarchy

- Unextending a Microsoft Exchange Server Hierarchy

- Updating Resource Configuration

- Deleting a Microsoft Exchange Server Hierarchy

- Using Microsoft Exchange Server After Removing LifeKeeper Protection

Creating a Microsoft Exchange Server 2007 Hierarchy

After you have completed the necessary setup tasks, perform the following steps to define the Microsoft Exchange Server hierarchy to protect your Exchange Server. You need to create the hierarchy on the primary server.

1. From the LifeKeeper GUI menu, select **Edit**, then **Server**. From the menu, select **Create Resource Hierarchy**.

2. The **Create Protected Application** dialog will display. Select the **Primary** and **Backup** Servers from the pull-down list. Select **Next** to continue.

3. Select **MS Exchange Server** and click **Next**.

4. You will be prompted to enter the following information. When the **Back** button is active in any of the dialog boxes, you can go back to the previous dialog box. This is helpful should you encounter an error requiring you to correct previously entered information. You may click **Cancel** at any time to cancel the entire creation process.

Field	Tips
Microsoft Exchange Server Resource Tag	Enter a unique tag name, or you can accept the default tag name offered by LifeKeeper.
Select Optional Services	LifeKeeper will display all optional Exchange Server services that are installed. Select the optional services that you wish to protect under LifeKeeper. Note: Any Exchange services that you do not select will be set to manual. These services should not be started unless they are protected by LifeKeeper. Thus any Exchange services you wish to run must be protected by LifeKeeper
Domain Administrator User Name	Enter the Domain Administrator account that was used to install Microsoft Exchange Server. The format is: `<username>@<fully qualified domain name>` Note: This user should be a member of the root domain. It is also required that the user has the right to login locally on the server. It is also recommended that you login using that user on the server so that its profile is created. You may get an error from WMI object in the LifeKeeper GUI if the user does not have this correct. On Windows Server 2003, this user account should be a member of the Domain Administrators group. However on Windows Server 2008 systems, the user must be the Domain Administrator.
Microsoft Domain Administrative Password	Enter the password for the Domain Administrator account.
IP Address (optional)	Select the switchable IP address (if used) to protect with this resource. The drop-down list will show all available IP addresses. Select None if you do not plan to use a switchable IP address.
DNS Resource (optional)	Select the DNS resource (if used) to protect with this resource. Multiple DNS resources may be selected if needed. Select None if you do not plan to use a DNS resource.

WARNING: When the Exchange resource hierarchy is created on the primary Exchange server, LifeKeeper by default assigns the highest priority, by default 1, to the resource. Then when you extend the resource hierarchy to the backup server (see instruction below), LifeKeeper assigns lower priority (higher in numerical value) , by default 10, to the resource. The Exchange kit treats the Exchange server as the primary Exchange server where the resource hierarchy is the highest, by default 1. It is not recommended that you swap the priority of Exchange resource because doing this would make the backup Exchange server the primary for the kit and failover/switchover would fail. You should also not unextend resource hierarchy from the primary server as this would designate the backup server the primary role.

Manage User

During the creation of a LifeKeeper Microsoft Exchange Server resource, the administrator must enter an Domain administrator username and password which allows LifeKeeper to perform necessary changes in the Active Directory during failover. Should the password of this username change after creation of the Exchange resource in LifeKeeper, the MS Exchange resource must be updated on all systems in the cluster with this new password. Failure to do so will leave the MS Exchange resource and the information in the Active Directory security database out of sync and will prevent the MS Exchange resource from coming in and out of service properly.

Select **Action**:

- Show Current User - Display the current user name used by the protected resource hierarchy.

- Change Password - Update the user password for the current user associated with the protected resource hierarchy.

- Change User and Password - Update both the user and password to be used during LifeKeeper operations to edit Active Directory.

Field	Tips
Domain Administrative User Name	Enter the Domain administrative user name. This user account must have enough permission to modify Active Directory. On Windows Server 2003, this user account should be a member of the Domain Administrators group. However on Windows Server 2008 systems, the user must be the Domain Administrator.
Domain Administrator Password	Enter the Domain administrative password for the user account being updated.

Using Microsoft Exchange Server 2007 After Removing LifeKeeper Protection

Deleting a Microsoft Exchange Server hierarchy removes it from both servers in the cluster. Microsoft Exchange will not start after deleting the hierarchy. If you wish to continue using Microsoft Exchange Server on the primary server without LifeKeeper protection, you will need to do the following:

1. Run the following utility to set the appropriate Microsoft Exchange services to **Automatic startup mode**. (The **SetSvcMode.vbs** utility is located in the `<%LKROOT%>\admin\kit\msexch\bin` folder, where *%LKROOT* is the root of the LifeKeeper installation path.)

```
cscript /nologo SetSvcMode.vbs -a
```

where -a option indicates Automatic startup mode. As an alternative to the above utility, you can use the Services administrative tool to set the startup type to Automatic for the previously protected services.

2. For client connectivity, ensure that all mail clients connect to the Microsoft Exchange server using the actual computer name (rather than the switchable IP address).

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**"

Testing Your Microsoft Exchange Resource

After creating and extending your Microsoft Exchange Server resource hierarchy, you should test it by initiating a manual switchover. This will simulate a failover of a resource instance from the primary server to the backup server.

1. From the LifeKeeper GUI menu, select **Edit**, then **Resource** and then **In Service**.

   This will result in an *In Service* request being executed on a backup server, which 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 backup server is now the active Exchange 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.

2. After the switchover, test that messages can be sent externally and internally to other mail recipients.

3. Verify that the queue database directory has been created on the shared or replicated volume.

Chapter 4: Microsoft Exchange Server Administration

The following topics provide recommendations for performing various administration tasks related to your Microsoft Exchange Server systems.

Exchange Server 2007 Access via Switchable IP Address

LifeKeeper can only protect a switchable IP address that is in the same network as the LifeKeeper servers. The protected Microsoft Exchange Server instance is active on only one server at a time. To ensure that users are able to access the Exchange server, regardless of which physical system it is currently running on, all remote access should be done through the switchable IP address associated with the Exchange hierarchy. LifeKeeper will make the switchable IP address available on whichever server is currently running the Exchange instance.

Reserve Volumes for Exclusive Use by Exchange Server 2007

The shared or replicated volume(s) that house the Microsoft Exchange Server database and transaction logs should be reserved for use by Microsoft Exchange Server exclusively. They should not be shared for users to access via LAN Manager, and should not be accessed by any other applications or users (local or remote).

The operation that removes a volume resource from service can fail if a remote user is accessing one of the volumes over the network or if a local process has done an open for write access on the volume. Local processes that have read-only access to volumes will not prevent removal of a resource from service but may cause a restore to fail when you try to switch back. Examples include the Performance Monitor, which periodically polls each volume, any running process that is installed on the shared volume, the Exchange Administrator, or even the Event Viewer focused on an event related to a service whose executable resides on a shared volume. In particular, avoid accessing a Microsoft Exchange Server volume in Windows Explorer during switchover.

Running Third-Party Software With Exchange Server 2007

Third-party software applications that are installed to work with Exchange server (i.e. Backup Agent, Anti Virus, SPAM, PDA Connectors, etc.) must be configured to work with both the primary and backup Exchange servers. If the third-party applications can connect to the Exchange server using

an IP address, they should be configured to use the LifeKeeper protected IP address.

Creating Exchange Users on the Backup Exchange Server 2007

If a new user is added to the Exchange server while running on the backup server, the user's MAPI client will have a problem connecting once the Exchange server is running on the primary. To resolve this issue, the user's MAPI profile must be updated to connect to the primary Exchange server name once Exchange is running on the primary. This profile change will not be required for subsequent failovers.

Updating Routing Topology for Public Folder EMail Routing

Note: This section applies if you have active Exchange 2003 or Exchange 2000 servers in the same organization as your Exchange 2007 server.

The LifeKeeper Microsoft Exchange 2007 Server Recovery Kit updates the routing topology upon failover. The kit does this update only if the failed primary server is the first in the list and the backup server is in different routing groups. So it is required that primary server and backup server in the LifeKeeper cluster be placed in different routing groups. If the backup server is the only server in its routing group, there is no need to create any connectors to that routing group.

Note: To determine the order of the Exchange servers in the list, use the **ExchDump** tool available from Microsoft. Please refer to the KB article:
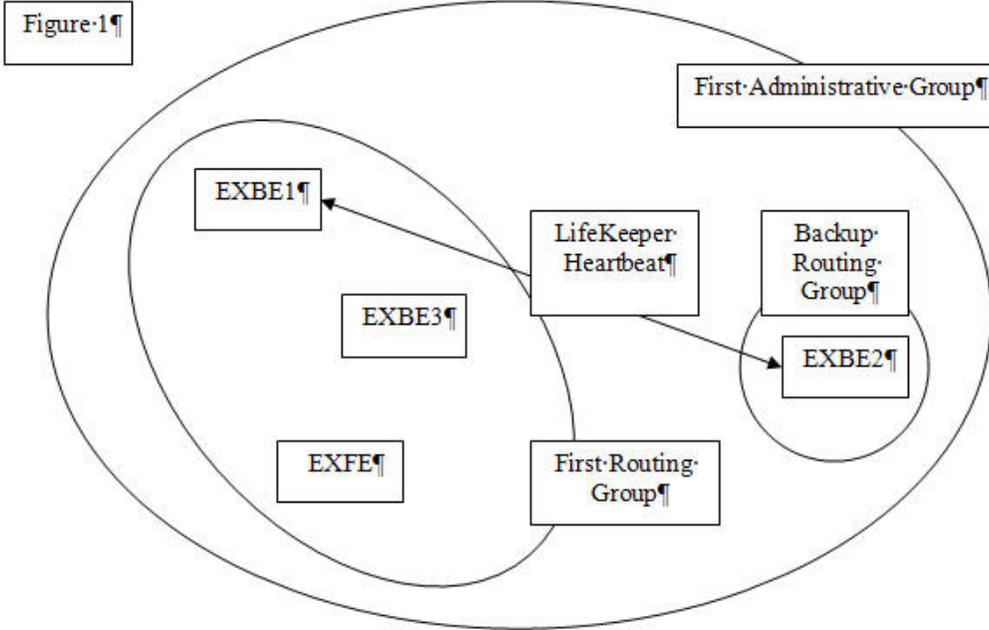http://support.microsoft.com/default.aspx?scid=kb;EN-US;839116

Consider following example where an Exchange environment with three back-end and one front-end Exchange servers - EXBE1, EXBE2, EXBE3 and EXFE (Exchange front-end server with no public folder store). All the Exchange servers are in the same routing group, i.e. "First Routing Group". LifeKeeper is protecting EXBE1 as the primary server and EXBE2 as the backup server. Exchange servers are listed in the following order in the list pointed by **msExchOwningPFTreeBL** attribute in Active Directory:

EXBE1, EXBE2 and EXBE3.

If the primary server EXBE1 fails, flow of public folder e-mail will be affected and front-end Exchange server EXFE will have problems delivering email.

Therefore, the user should create a new Routing group, i.e. "Backup Routing Group", and move the backup Exchange server EXBE2 to the newly created routing group. See Figure 1 below.

Figure·1¶

First·Administrative·Group¶

EXBE1¶

LifeKeeper Heartbeat¶

Backup· Routing· Group¶

EXBE3¶

EXBE2¶

EXFE¶

First·Routing· Group¶

When LifeKeeper performs a failover from EXBE1 to EXBE2, it swaps the servers between the two routing groups. The configuration would looks like Figure 2 after the failover.

Figure·2¶

First·Administrative·Group¶

EXBE2¶

LifeKeeper· Heartbeat¶

Backup· Routing· Group¶

EXBE3¶

EXBE1¶

EXFE¶

First·Routing· Group¶
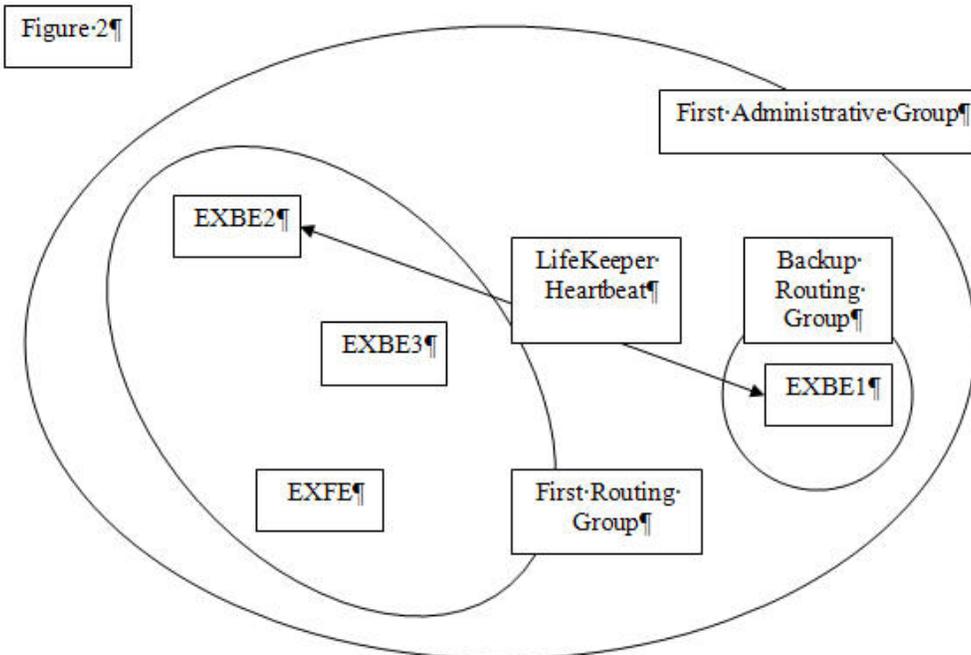
Note: EXFE in this example is a front-end server with no public folder store.

The kit also updates all affected routing group connectors in the local Exchange administrative group. This includes updating all "Routing Groups (RG)" and "SMTP" connectors.

The updates of Routing Groups allow Exchange on EXFE to pickup the new server from the list pointed to by attribute **msExchOwningPFTreeBL** and maintain email flow. It is possible that while other email servers pick up changes in routing topology, some of the email to public folders as well as private mailbox users may cause mail to be not delivered. During this transition, many messages may get stuck in the "`Queue: Messages with an unreachable destination`" SMTP Queue. These messages can be retrieved and put back in the queue if they are in the SMTP Virtual server's **Queue** folder by moving them to **Pickup** folder. Latencies in Active Directory lookup and picking up new configuration information along with DNS name resolution replication may result in looping messages, loss of messages, non-delivery reports or all of these problems.

Note: The LifeKeeper Microsoft Exchange 2007 Server Recovery Kit does not update routing groups and connectors in an N+1 type configuration because the +1 node can not have a public folder store.

Public Folder Replica List Update

The LifeKeeper Microsoft Exchange 2007 Server Recovery Kit automatically update the list of replica servers on affected public folders upon failover/switchover. The kit adds the name of the backup server and removes the name of the primary server (which has just failed) from the list of replica servers. These changes are performed on the backup server. While the update process is running, not all public folders are accessible. The folders become accessible as they are updated. This option should be enabled if you have more than two Exchange servers in your environment. An alternative would be to have a separate dedicated Exchange public folder server.

Depending on the number of public folders in your Exchange environment, the entire update process may take a long time to complete. While the replica list is being updated, private mailbox users are available. For this reason, the Exchange kit performs the update in a background process and allows the LifeKeeper Exchange resource to become active (Green) after failover.

This feature is configurable through the Registry. When an Exchange resource is created, a DWORD value name **UpdateReplicaList**, with default value 1 (one), is created under Registry key `HKEY_ LOCAL_MACHINE\SOFTWARE\SteelEye\LifeKeeper\RK\msexch\<TagName>`, where <TagName> is the name of the LifeKeeper Exchange Resource. Setting the value of **UpdateReplicaList** to 1 (one) would enable the update of public folder replica list.

If the user wants to disable the feature, set the value of **UpdateReplicaList** to 0 (zero). But then you need to add both, primary and secondary Exchange servers to replica list using method described in article Scripts for Managing Public Folders in the Exchange Management Shell at http://technet.microsoft.com/en-us/library/aa997966.aspx. You need to use same PowerShell script to update following system folders and their subfolders:

```
OFFLINE ADDRESS BOOK

SCHEDULE+FREE BUSY
```

If you have any organizational forms folders created under the ***EFORMS REGISTRY*** folder, you have to add a secondary system to the replica list for all such form folders.

IMPORTANT NOTE:

If you add any other public folders to Exchange after the LifeKeeper resource hierarchy is created and extended and you have disabled **UpdateReplicaList** in the registry, you will need to repeat the procedure above to update the replica list of the new public folder.

Mail Flow When Replica List of Public Folders is Updated

When the replica list update feature is enabled, the LifeKeeper Exchange Recovery Kit will update the replica list on all affected public folders. This is done after the Exchange services are started on the server. If a new email for a public folder is received by the server before the replica list is updated, it will be rejected and a NDR will be sent to the sender of the email. In our testing we have also found that, depending upon the time of arrival of the public folder e-mail, sometimes the email is delivered to the folder, but the NDR is still generated. It is also possible that sometimes public folder emails are queued into the queue database when the Exchange resource hierarchy is failed back, i.e. backup server to primary server.

The dynamic update of the public folder replica list sometimes causes Exchange to generate conflict messages from the public folder store. All owners of a public folder will receive the following type of message in their inbox.

```
From: <Public Folder Name>

Subject: Conflict Message

A folder design conflict has occurred in "<Public Folder Name>".
The design of this folder has been simultaneously modified on two
or more folder replicas. Only the set of changes made last have
been saved.
```

In our testing, we have not seen any impact on public folders and these messages can be ignored.

Disabling Automatic Failover of the Microsoft Exchange Server 2007 Resource

In the event that the primary server has attempted and failed local recovery, or failed completely, most server administrators will want LifeKeeper to automatically restore the Microsoft Exchange Server to a backup server. This is the default LifeKeeper behavior. However, some administrators may not want Microsoft Exchange Server to automatically go in-service at a recovery site. For example, if additional expenses are incurred when running Microsoft Exchange Server at a backup location, manual intervention may be the preferred operating procedure before restarting Microsoft Exchange Server on a backup server.

Note: If LifeKeeper is installed in a WAN environment where the network connection between the servers may not be reliable, it is highly recommended that you disable automatic failover. This eliminates the possibility of false failovers of Microsoft Exchange Server.

Refer to Disable Automatic Failover for more information about disabling automatic failover.

Replicated Volume - Failed Primary Server and Blocked Recovery on Backup

If the decision is made to completely abandon a recovery that was blocked on the backup server and

instead restart the primary server, then some special considerations are in order. When the primary server is restarted it will still be the replicated volume source. It will begin a full resynchronization of the replicated volume from the primary system to the backup system. Depending on the size of the replicated volume and the communication link speed connecting replicated volume source and replicated volume target, this resynchronization may take a significant amount of time to complete. During this resynchronization the recovery capability on the backup server should not be re-enabled. The backup server will not be capable of recovering from another Microsoft Exchange Server failure until this volume resynchronization is complete. After resynchronization has been completed, the automatic recovery capability on the backup server may be re-enabled, if this is desired.

Deleting A Microsoft Exchange Server 2007

The Microsoft Exchange Server resource hierarchy should be in service on the primary before deleting the Microsoft Exchange Server resource hierarchy.

WARNING: Do not delete the resource hierarchy while the Exchange resource is in-service on the backup server.

WARNING: Deleting the Microsoft Exchange Server hierarchy will delete all of its dependencies. Therefore, you should remove the volume/IP dependencies before deleting the Microsoft Exchange Server hierarchy if you wish to continue using these resources.

To delete the Microsoft Exchange Server resource hierarchy from both of the servers in your LifeKeeper environment, perform the following steps:

1. On the Edit menu, select Resource, then Delete Resource Hierarchy.
2. Select the Target Server where you will be deleting your Microsoft Exchange Server resource hierarchy and click Next. (This dialog will not appear if you selected the Delete Resource task by right clicking on a resource instance in either pane.)
3. Select the Hierarchy to Delete. (This dialog will not appear if you selected the Delete Resource task by right clicking on a resource instance in the left or right pane.) Click Next.

Command output will be displayed on the output panel if that is open, and on this dialog if the output panel is not open. Any errors that occur will also be logged in both the LifeKeeper log and the GUI log on that server.

Exchange Server 2007 Access via Switchable IP Address (LAN only)

LifeKeeper can only protect a switchable IP address that is in the same network as the LifeKeeper servers. The protected Microsoft Exchange Server instance is active on only one server at a time. To ensure that users are able to access the Exchange server, regardless of which physical system it is currently running on, all remote access should be done through the switchable IP address associated with the Exchange hierarchy. LifeKeeper will make the switchable IP address available on whichever server is currently running the Exchange instance.

Chapter 5: 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.

Error Creating Exchange Resource

LifeKeeper Microsoft Exchange 2007 Server Recovery Kit performs various checks related to Exchange configuration when you create a LifeKeeper Exchange resource. This topic describes what error messages you may see if a particular check fails and how to correct the problem.

Condition:

Exchange data (not program files) are on %SystemDrive%

Error Message:

```
Database (EDB) files of mailstore "Mailbox Store" of storage group
"First Storage Group" are located on system drive (C:).
```

Recommended Action:

Use Exchange Management Console to relocate mail stores and transaction log files to a LifeKeeper protected volume(s).

Note: The location of the queue database and queue database transaction logs is not checked during create of the Exchange Resource. It is recommended that the queue database and queue database transaction logs are relocated using the procedure outlined at http://technet.microsoft.com/en-us/library/bb125177.aspx.

Extend of Exchange Resource Problems

The Extend of an Exchange resource will fail with the following error if the primary and backup Exchange servers' database configurations are different.

Sample Error Message:

```
The database configuration on the server <backup server> does not
match with the configuration on the Exchange server <primary
server>.The following changes should be made on the Exchange server
<backupserver>:

- Rename MailStore DB <backup server>\MailboxDB -> Mailbox

- Rename Storage Group Second Storage Group -> SSG
```

Recommended Action:

Select **Next** for LifeKeeper to correct the problem(s). Or, select **Cancel** to make the changes manually.

Use the **Microsoft Exchange Management Console** to change the **Storage Groups**, **Mailbox Stores** and **Public Stores** to have the exact same names on both the primary and backup Exchange servers. Correct any inconsistencies and retry the **Extend** operation.

Note: In an N+1 configuration, the configuration on both primary Exchange servers must match with the configuration on the backup server. When extending the second Exchange primary server to the +1 backup server and a configuration mismatch is detected, you must manually make the changes on the second primary Exchange server using the **Microsoft Exchange Management Console**.

Exchange 2007 Service Startup Problems

You may wish to reduce the MAXWAIT value in the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SteelEye\LifeKeeper\RK\ms64ex07` while troubleshooting service startup/shutdown errors. This will reduce the time it takes for LifeKeeper to report that a service has failed to start or stop.

Note: By default, this value is 900 seconds (15 minutes).

Exchange 2007 Client Connection Problems

Refer to the topic Client Connection Problems in the Exchange 2003 documentation.

Moving All Users of a Domain to Active Exchange Servers

When LifeKeeper migrates the Exchange hierarchy to the backup server but some or all users within a domain are not migrated due to a failure condition, the LifeKeeper supplied **LKMoveExUsers** command line utility can be used to manually move all users of a domain to the backup server. You can see if any user migrations failed by viewing the LifeKeeper log file located under `%LKROOT%\out\FailedExUsers.log`.

The utility should be invoked from the backup Exchange server where the Exchange hierarchy has been brought in-service. The **LKMoveEXUsers** utility is located in the `<%LKROOT%>\bin` folder, where `%LKROOT%` is the root of the LifeKeeper installation path.

In a situation where all Domain Controllers of a child domain are not available during LifeKeeper failover, none of the users of that domain that have mailboxes on the failed Exchange server would be migrated. For this situation, the administrator should use the **LKMoveEXUsers** utility to move all users of the domain after making a domain controller of that domain available. To run the **LKMoveEXUsers** utility, enter the following from a command prompt:

```
LKMoveExUsers.exe  <UserName@FQDN> <Password> <Local Exchange
Server Name> <Failed Exchange Server Name> <<-d<domain name>>
```

An example for moving all users in a child domain *(child.rootdomain.com)* from the failed Exchange server (Server1) to the server where Exchange is running (Server2) is:

```
LKMoveExUsers.exe exadmin@rootdomain.com password Server2 Server1 -
dchild.rootdomain.com
```

The user,*exadmin@rootdomain.com*, must be the domain administrator of the root domain of the forest and should have privileges to modify Active Directory of the child domain.

To move a single user from the failed Exchange server to backup Exchange server, use the command line utility **LKExADUtil.exe** with the */MSU* option. The utility is located in *%LKROOT%/bin* directory.

```
LKExADUtil.exe /MSU /S:<Primary Exchange Server Name>/T:<Secondary
Exchange Server Name> /M:<User Principal Name>
```

Where the user name provided with the */MSU* option must be in the format **UserID@FQDN**.

The logged in user invoking this utility must have domain administrative privileges to make the changes to the user properties in Active Directory.

On **Windows Server 2003**, the logged on user account should be a member of the Domain Administrators group. However on Windows Server 2008 systems, the user must be the Domain Administrator.

The administrator can refer to the log file *%LKROOT%\out\FailedExUsers.log* to get the name of the failed domain or users. The administrator can use the name of the domain or of individual users (in Distinguished Name format as it appears in the log file) to move all users.

Slow Microsoft Exchange 2007 Server Startup After Multiple Failovers

Refer to this topic for details on how to resolve the redo of the log files and the slow startup of the Microsoft Exchange services.

When a failover to the standby system occurs, Microsoft Exchange Server rebuilds the log files during startup to recover from a "dirty shutdown". After multiple failovers, the redo of the log files and startup of the Microsoft Exchange services may take an extended period of time. This problem can be resolved by doing a Full or Incremental Backup of the Microsoft Exchange Server stores, since this flushes committed entries from the log files. To avoid the problem, do periodic backups of your Microsoft Exchange Server system as recommended in the Microsoft Exchange Server documentation.