LifeKeeper for Windows

Microsoft Exchange Server 2003 Recovery Kit

Administration Guide

January 2012

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 2003

The Microsoft Exchange 2003 Protection Suite provides high availability for Microsoft Exchange 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.

Microsoft Exchange 2003 Server Services

LifeKeeper protects the following Microsoft Exchange Server services.

Core Services	Optional Services
Routing Engine	IMAP4
System Attendant	POP3
Information Store	Message Transfer Agent (MTA Stacks)
Simple Mail Transfer Protocol (SMTP)	Microsoft Search
World Wide Web Publishing Service	Connectivity Controller
	Connector for Lotus Notes cc:Mail
	Connector for Lotus Notes
	Router for Novell: Group Wise
	Connector for Novell: Group Wise
	Chat

Optional Exchange 2003 Server services that you wish to run should be protected by LifeKeeper. All optional services should be configured and tested prior to protecting under LifeKeeper. Any optional services that are NOT protected by LifeKeeper can interfere with LifeKeeper's operation and should be set to MANUAL startup.

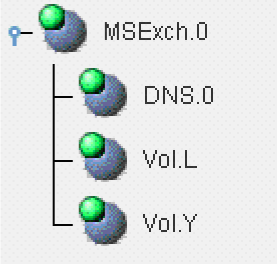
Resource Hierarchy for Microsoft Exchange 2003 Server

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.



Recovery Kit Requirements

Before installing and configuring the LifeKeeper Microsoft Exchange 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 Standard, Enterprise, Data Center, Web Editions
- Windows Server 2003 R2 Editions
- Windows Server 2008 Standard, Enterprise, Datacenter Editions (32- and 64-bit versions)

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

- Exchange Server 2003 (standard edition)
- Exchange Server 2003 Enterprise

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.

Chapter 2: LifeKeeper Microsoft Exchange 2003 Server Recovery Kit Installation

The LifeKeeper Microsoft Exchange Server Recovery Kit is available via ftp download. InstallShield provides a standard installation interface.

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.

Upgrading Recovery Kit From Previous Version

You may upgrade from the previous version of the LifeKeeper Microsoft Exchange Server Recovery Kit v4.x and v5.x software while preserving your resource hierarchies.

Upgrading from LifeKeeper Microsoft Exchange Server Recovery Kit v4.1.x is not supported. For information about upgrading your LifeKeeper environment, contact SIOS Technology Corp. support at support@us.sios.com or call:

1-877-457-5113 (toll-free in North America)

+1-803-808-4870 (International)

Starting and Stopping Exchange Services (Large Stores)

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

```
HKEY_LOCAL_MACHINE\SOFTWARE\SteelEye\LifeKeeper\RK\msexch
```

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 timeframe, 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 Server Recovery Kit software, choose **LifeKeeper Microsoft Exchange Server Recovery Kit v6** in the **Add/Remove Programs** applet in the control panel.

CAUTION: When removing the LifeKeeper Microsoft Exchange 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.

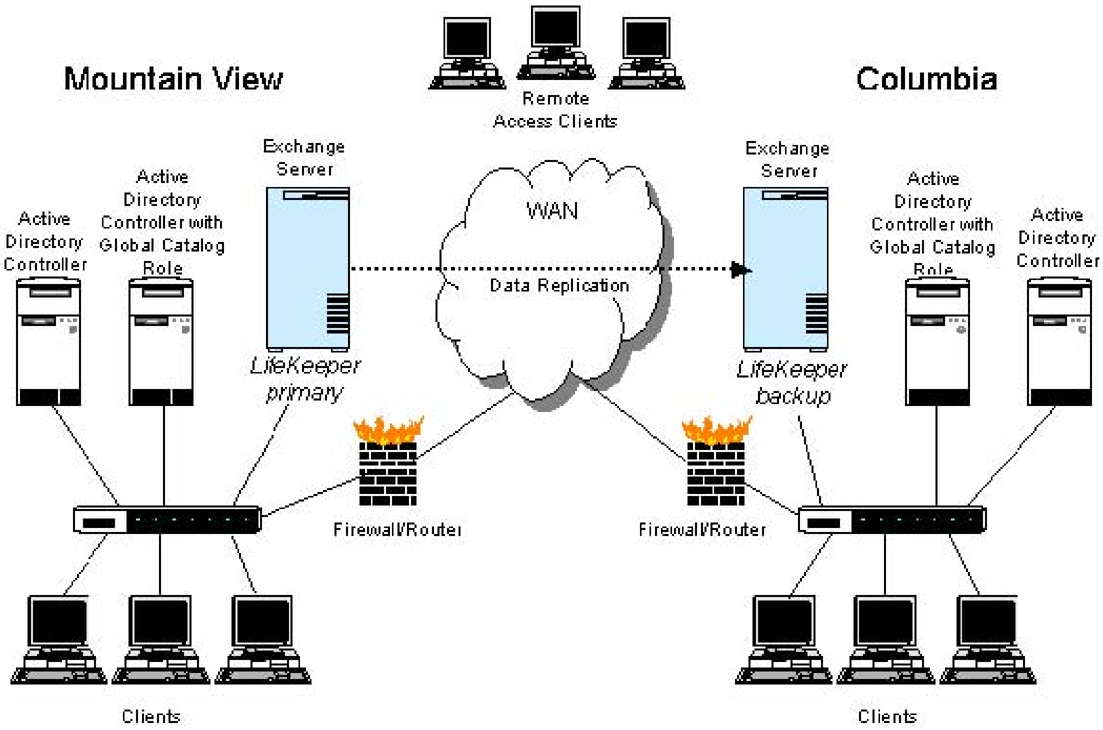
Optional Microsoft Exchange Server Services

Optional Exchange Server services that you wish to run should be protected by LifeKeeper. All optional services should be configured and tested prior to protecting under LifeKeeper. Any optional services that are NOT protected by LifeKeeper can interfere with LifeKeeper's operation and should be set to MANUAL startup.

Configuration Examples

Environment View

The following diagram depicts a WAN environment where LifeKeeper is protecting Microsoft Exchange Server. The primary and backup Exchange servers are in different geographic locations, and the Exchange data and transaction stores are replicated across the WAN using SteelEye DataKeeper.

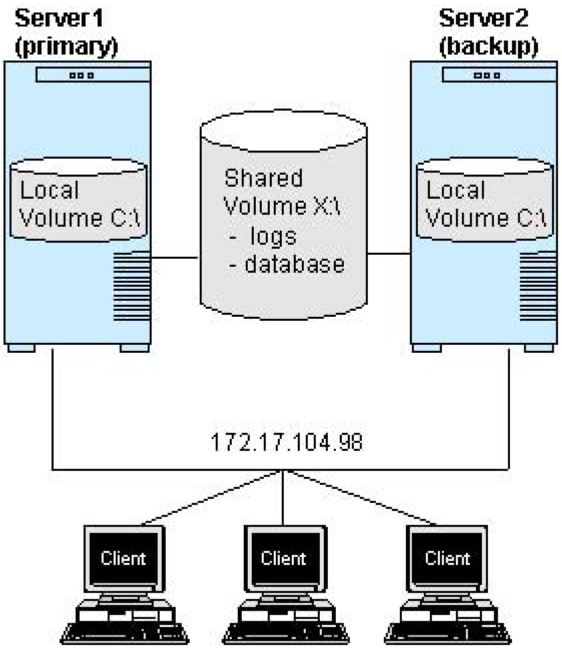


The following examples illustrate the different cluster configurations supported by the LifeKeeper Microsoft Exchange Server Recovery Kit.

Two-Node Cluster Using Shared Storage

This configuration consists of primary Exchange server and one backup server. Microsoft Exchange Server is started on the backup server only in the event of a failover or manual switchover from the primary server.

Configuration Notes:



Configuration Notes:

1. Server1 (primary) - Microsoft Exchange Server binaries are installed onto local volume C.
2. Server2 (backup) - Microsoft Exchange Server binaries are installed onto local volume C.
3. Transaction logs and Microsoft Exchange database files are located on shared volume D.
4. The IP address 172.17.104.98 will also switch between Server1 and Server2.

Cascading Exchange Cluster With More Than Two Nodes

Using the LifeKeeper Microsoft Exchange Server Recovery Kit, you can set up a cluster with more than two nodes in a cascading failover environment. This type of configuration allows more than one server to be a backup of a single primary Exchange server.

If Server1 fails, then Server2, which is next in the priority, takes over the responsibility of the Exchange server running on Server1. If the Server2 fails while Server1 is still down, then LifeKeeper on Server3 will perform the switchover and start Exchange on the server.

Configuration Notes:

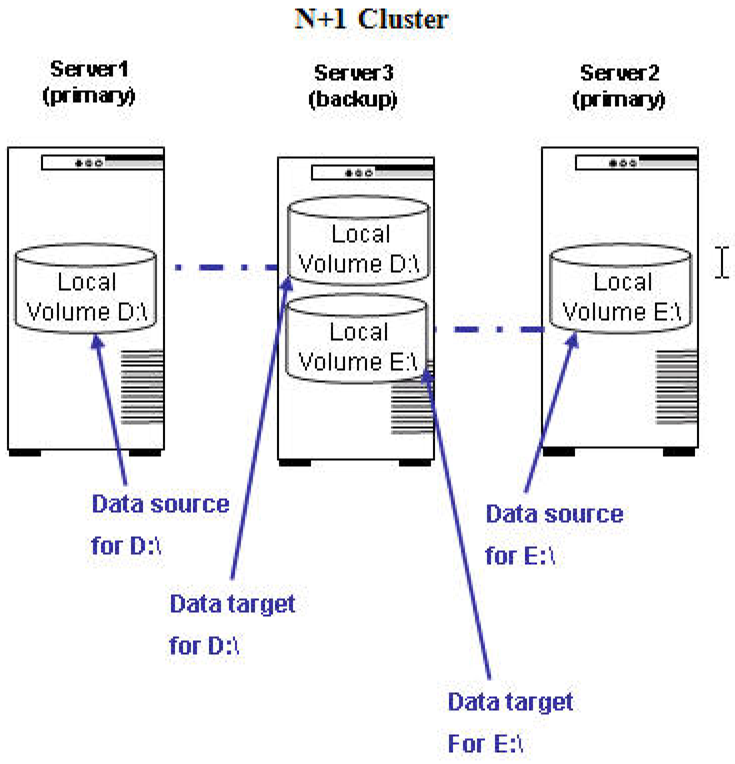
1. Server1 (primary) - Microsoft Exchange Server binaries are installed onto a local volume.
2. Server2 (backup) - Microsoft Exchange Server binaries are installed onto a local volume.
3. Server3 (backup) - Microsoft Exchange Server binaries are installed onto a local volume.

4. Transaction logs and Microsoft Exchange database files are located on shared or replicated volume(s).

N+1 Cluster

In this configuration, you can set up three or more Exchange servers with one server acting as a stand-by server for all other primary servers. All the *N* primary servers will fail over over to a single +1 server. The +1 server will allow only one Exchange server to be failed over at a time. The +1 node will not allow failover of any other primary Exchange server while it is serving clients of the first primary Exchange server.

N+1 Cluster



In above diagram, Server3 serves as a backup of two primary Exchange servers, Server1 and Server2. When Server1 fails, LifeKeeper on Server3 will initiate a failover and start Exchange on Server3. However, Server3 will not be able to do failover for Server2 while still running Exchange for failed server Server1.

Configuration Notes:

1. Server1 (primary) - Microsoft Exchange Server binaries are installed onto local volume C.
2. Server2 (primary) - Microsoft Exchange Server binaries are installed onto local volume C.
3. Server3 (backup) - Microsoft Exchange Server binaries are installed onto local volume C.
4. Transaction logs and Microsoft Exchange database files for Server1 are located on replicated volume D.
5. Transaction logs and Microsoft Exchange database files for Server2 are located on replicated volume E.

SteelEye DataKeeper Configuration

This configuration consists of two servers using replicated volumes on each local server in place of shared storage. SteelEye DataKeeper software provides the replicating capability over a LAN or WAN in conjunction with LifeKeeper's failover protection.

Configuration Notes:

- Server1 (primary) Microsoft Exchange Server binaries are installed onto local volume C.
- Server2 (backup) Microsoft Exchange Server binaries are installed onto local volume C.
- Transaction logs and Microsoft Exchange database files are located on replicated volume D.
- The IP address 172.17.104.98 can switch between Server1 and Server2.

  Note: In a WAN implementation, multiple options exist for client re-direction. Some examples are Route update, Layer 4 Switching,and DNS update.
- The primary and backup servers are not required to be in the same geographic location.

Configuring Microsoft Exchange Server with LifeKeeper

The following configuration method is a result of rigorous design and testing by SIOS Technology Corp.

The procedures for configuring Microsoft Exchange Server with LifeKeeper fall into three major steps. Details of each of these three steps follow.

1. Prepare the Servers and Network
2. Install Microsoft Exchange Server
3. Install and Configure LifeKeeper

Note: These instructions apply to both shared storage and replicated configurations. Any steps that apply to only shared storage or only replicated volumes will be noted.

Prepare the Servers and Network

The following checklist specifies the requirements to be met before installing LifeKeeper and/or SteelEye DataKeeper.

1. Ensure that your servers meet the following criteria:

    - Both servers should be running in a Windows Active Directory domain.
    - DNS should be configured properly.

    - All mail clients should be working with the Exchange server.

2. Plan and record your configuration. Use the Configuration Examples and Configuration Worksheet provided to determine your configuration.

3. Check installation of Windows service packs (depending on the version of Microsoft Exchange Server to be installed).

Configuration Worksheet

Complete the following worksheet when setting up a primary server for Microsoft Exchange Server. Keep a copy of this for your future reference.

Information	Description
Microsoft Exchange Server Organization Name: __________________________	The new or existing Microsoft Exchange Server Organization name.
Microsoft Exchange Server Administrator Account: __________________________	This is a special domain account that is used for installation of Microsoft Exchange Server.
Switchable IP Address (optional): __________________________	This is the IP address that switches between the primary and backup LifeKeeper servers.
Exchange Server Installation: Volume:* ____	The drive letter for the location of the Microsoft Exchange Server files.
Private Information Store: Transaction Logs Volume:* ____ Database Volume :* ____	The drive letter for the location of the Exchange Private Information Store.
Public Information Store: Transaction Logs Volume:* ____ Database Volume :* ____	The drive letter for the location of the Exchange Public Information Store.
Additional Information Stores (optional): Transaction Logs Volume:* ____ Database Volume :* ____	The drive letter for the location of any additional Exchange Information Store(s).

Transaction Logs Volume:* ____ Database Volume :* ____	
Optional services to protect: ______________________________ ______________________________ ______________________________ ______________________________ ______________________________ ______________________________ ______________________________ ______________________________	Note all of the optional Microsoft Exchange Server services that LifeKeeper will protect. It is important that these services are installed on the backup server and configured correctly.

* For replicated volumes, this should be a local NTFS volume that is not a system volume.

Otherwise, it should be an NTFS volume on a shared disk.

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 (ForestPrep)
- Schema Admins (ForestPrep)
- Domain Admins (DomainPrep)
- Domain Users

On the Primary Server

1. Log in to the primary server using the domain account created above. Insert the Microsoft Exchange Server CD and run the **Exchange Setup utility** with the **/ForestPrep** option using

the following command:

```
d:\SETUP\i386\Setup.exe /ForestPrep
```

where d: is the drive letter for the CDROM.

2. Run the **Exchange Setup utility** with the **/DomainPrep** option using the following command:

   ```
   d:\SETUP\i386\Setup.exe /DomainPrep
   ```

   where d: is the drive letter for the CDROM. Be sure to select the same drive for installation as you did in ForestPrep.

3. From a command prompt, install the **Microsoft Exchange Server software** to a local, non-replicated volume using the following command:

   ```
   d:\SETUP\i386\Setup.exe
   ```

   where d: is the drive letter for the CDROM.

   Note: A Typical Microsoft Exchange Server installation includes the MTA, IMAP4, POP3 and Event services. Choose **Custom** if you wish to install and protect additional optional services, remembering that you should install only those optional services that you plan to protect with LifeKeeper.

4. Install Exchange Service Pack(s) at this time.

5. 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 System Manager 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 System Manager 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” and “Exchange streaming database” to point to the LifeKeeper-protected shared or replicated volume(s).

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

7. 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.

1. Log in to the backup server using the Exchange Administrator account. From a command prompt, install the Microsoft Exchange Server software to a local, non-replicated volume using the following command:

   ```
   d:\SETUP\i386\Setup.exe
   ```

   where d: is the drive letter for the CDROM.

2. During the setup program, you will be prompted to select Microsoft Exchange components. Install the same Microsoft Exchange components that were installed on the primary server. The following Microsoft Exchange components were installed if you performed a default installation on the primary server:

- Microsoft Exchange
- Microsoft Exchange Messaging and Collaboration Services
- Microsoft Exchange System Management Tools

3. Install Exchange Service Pack(s) at this time.

4. For N+ 1 configuration, delete the public folder store on the backup using Exchange System Manager. This step is not applicable for two-node and cascading environments.

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 Installation section of the SteelEye DataKeeper for Windows Documentation.
2. Install the LifeKeeper Core software, including the license key.
3. Install the LifeKeeper Microsoft Exchange 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 Server Recovery Kit to the backup server.

Configure LifeKeeper

1. Change the location of the SMTP system queues to a shared or replicated volume(s) by running the utility *SetSMTPQueuePath.vbs*, which is located in *%LKROOT%/Admin/Kit/msexch/bin*. At the command line, change to *%LKROOT%/Admin/Kit/msexch/bin* directory and execute the utility as follows:

   ```
   cscript /nologo SetSMTPQueuePath.vbs <Exchange Server Name><x>
   ```

2. Login to the LifeKeeper GUI.

3. Create the communication paths between the primary and backup servers.

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

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

5. On the primary server, modify the replication properties of each public folder in your organization as follows.

   a. Using **Exchange System Manager**, expand **<Your Administrative Group>under Administrative Groups**.

   b. Expand the public folder tree Folders.

   c. Right-click the top-level public folder in your organization and click **Properties**. Select the **Replication** tab and add the backup Exchange server's public folder store name for a cluster protecting only one primary exchange server. For N+1 configurations, add names of the other primary servers to the list of replicas.

      For a two-node Exchange configuration, set the **Public folder replication interval:** to **Never Run** and **Replication message priority:** to **Not Urgent**. These changes do not apply to N+1 configurations.

      Click **Apply** and then click **OK** to save changes and exit.

   d. Right-click the same top-level public folder, select **All Tasks**, and then select **Propagate Settings…** from the list. **Note**: If the public folder does not have sub folders, the Propagate Settings… will be disabled. From the **Propagate Folder Settings dialog**, select **Replicas**, **Replication message priority**, and **Replication schedule** and click **OK**. Wait for the replica setting to propagate to all subfolders in the tree.

      If Microsoft Exchange 2003 SP2 is installed, select **All Tasks**, and then select **Manage Settings.** This will start the **Manage Public Folders Settings wizard**. Click on **Next**. From the **Specify Action** dialog, select **Overwrite Settings** and then click on **Next**. From the **Overwrite Settings dialog**, select **Replicas**, **Replication message priority**, and **Replication schedule** and click **Next** and then **Finish**. Wait for the replica setting to propagate to all subfolders in the tree.

   e. Set the replica settings for each top-level folder tree under Folders.

      Note: These changes only apply to public folders that are being replicated between the primary and backup Exchange servers. For any future public folders created after creating your Exchange resource, these same changes for replication should be applied so that both the Exchange servers appear in the list.

6. On the primary server, modify the replication properties of the Offline Address Book (OAB) folders. Public Folder stores of both the Exchange servers should be listed for replication. Change the replication setting as follows.

   a. Using **Exchange System Manager**, expand **<Your Administrative Group>** under **Administrative Groups**.

   b. Expand **Folders**, right-click **Public Folders**, and then click **View System Folders**.

   c. Expand **Public Folders**, expand **OFFLINE ADDRESS BOOK**, and then select the container that contains the offline Address Book. For example select **/o=<Your Organization>/cn=addrlists/cn=oabs/cn=Default Offline AddressList**

   d. Right-click the folder and then click **Properties**.

   e. Select the **Replication** tab and add the backup Exchange server to the list for a cluster protecting only one primary Exchange server. For N+1 configurations, add names of the other primary servers to the list of replicas.

   a. Using **Exchange System Manager**, expand **<Your Administrative Group>** under **Administrative Groups**.

   b. Expand **Folders**, right-click **Public Folders**, and then click **View System Folders**.

   c. Expand **Public Folders**, expand **OFFLINE ADDRESS BOOK**, and then select the container that contains the offline Address Book. For example select **/o=<Your Organization>/cn=addrlists/cn=oabs/cn=Default Offline AddressList**

   d. Right-click the folder and then click **Properties**.

   e. Select the **Replication** tab and add the backup Exchange server to the list for a cluster protecting only one primary Exchange server. For N+1 configurations, add names of the other primary servers to the list of replicas.

      Click **Apply**, and then click **OK** to save changes and exit.

   f. Right-click the same folder **(o=<YourOrganization>/cn=addrlists/cn=oabs/cn=Default Offline Address List)**, select **All Tasks**, and select **Propagation Settings…** from the list. From the **Propagate Folder Settings** dialog box, select **Replicas** and click **OK**. Wait for the replica setting to propagate to all sub folders in the tree.

      If Microsoft Exchange 2003 SP2 is installed, select **All Tasks**, and then select **Manage Settings**. This will start the **Manage Public Folders Settings** wizard. Click on **Next**. From the **Specify Action** dialog, select **Overwrite Settings** and then click on **Next**. From the **Overwrite**

Settings dialog, select **Replicas** and click **Next** and then **Finish**. Wait for the replica setting to propagate to all subfolders in the tree.

g. Set the replica settings for other top level OAB folders under **OFFLINE ADDRESS BOOK** if they contain offline address books.

7. On the primary server, modify the replication properties of the Schedule+Free Busy folders. Public Folder stores of both the Exchange server should be listed for replication. Change the replication setting as follows.

   a. Using **Exchange System Manager**, expand **<Your Administrative Group>** under **Administrative Groups**.

   b. Expand **Folders**, right-click **Public Folders**, and then click **View System Folders**.

   c. Expand **Public Folders**, expand **SCHEDULE+ FREE BUSY**, and then select the container that contains the Schedule+ Free Busy.

   d. Right-click the folder and then click **Properties**.

   e. Select the **Replication** tab and add the backup Exchange server to the list for a cluster protecting only one primary Exchange server. For N+1 configurations, add names of other primary servers to the list of replicas.

   a. Using **Exchange System Manager**, expand **<Your Administrative Group>** under **Administrative Groups**.

   b. Expand **Folders**, right-click **Public Folders**, and then click **View System Folders**.

   c. Expand **Public Folders**, expand **SCHEDULE+ FREE BUSY**, and then select the container that contains the Schedule+ Free Busy.

   d. Right-click the folder and then click **Properties**.

   e. Select the **Replication** tab and add the backup Exchange server to the list for a cluster protecting only one primary Exchange server. For N+1 configurations, add names of other primary servers to the list of replicas.

   Click **Apply**, and then click **OK** to save changes and exit.

8. 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: Steps 5, 6 and 7 described above are required to access the public folders and system public folders from the backup server after the failover. However, doing this affects the replication of folder contents to any Exchange servers you have outside the LifeKeeper cluster. At present, the kit updates the list of replica servers for MAPI public folders on Exchange Server 2003 ONLY because of lack of interface from Microsoft for system public folders and on Exchange 2000 Server. The replica list update feature is disabled by default because it is a time-consuming process and does not help in all Exchange environments. Depending upon your Exchange environment, it may be necessary to update the list of replica servers by removing the name of the failed server from the list using **Exchange System Manager** (ESM) to resolve replication issues.

9. 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.

10. If your Exchange server is configured with routing group and connectors to work with other Exchange server or messaging system, 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 configuration. For example, if your primary Exchange server is configured as a local bridgehead server, then you will need to add the backup Exchange server's default SMTP virtual server name to the list of Local Bridgehead servers for your SMTP connector. You typically select **<YourOrganization> -> Routing Group -> <Your Routing Group>->Connectors -> <Your SMTP Connector>** and add name in **General** tab of **Properties** of the connector.

11. If using a switchable IP address for 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:

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

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

    f. 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.

Example - Setting up Exchange in a Single Subnet Environment (virtual IP)

Refer to the following example when you set up Exchange in a single Subnet Environment using a virtual IP.

IP Address Settings Before You Start:

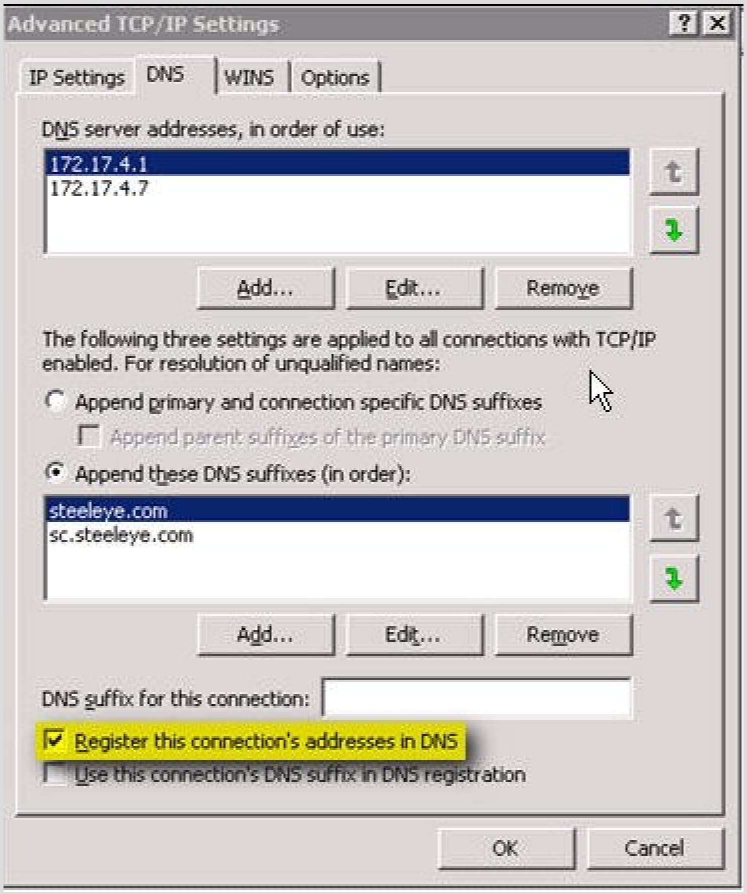
Exchange Server(s)	**Static IP Addresses**
PRI_EXCH	172.17.6.1
BKUP_EXCH	172.17.6.2

LifeKeeper Virtual IP	Static IP Address
EXCH_ALIAS	172.17.6.99

DNS – “A records”	Static IP Addresses
PRI_EXCH	172.17.6.1
BKUP_EXCH	172.17.6.2

Procedure:

1. Uncheck **Register this connection’s address in DNS** in the **Advanced TCP/IP Settings** dialog box depicted below:



Advanced TCP/IP Settings

DNS server addresses, in order of use:

172.17.4.1
172.17.4.7

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

○ Append primary and connection specific DNS suffixes

□ Append parent suffixes of the primary DNS suffix

● Append these DNS suffixes (in order):

steeleye.com
sc.steeleye.com

DNS suffix for this connection:

☑ Register this connection's addresses in DNS

□ Use this connection's DNS suffix in DNS registration

2. Change the “A Record” of the primary Exchange Server in DNS to point to the virtual IP address.

DNS Setting Before Step 2	
DNS – “A records”	Static IP Addresses
PRI_EXCH	172.17.6.1
BKUP_EXCH	172.17.6.2

DNS Setting After Step 2	
DNS – “A records”	Static IP Addresses
PRI_EXCH	172.17.6.99
BKUP_EXCH	172.17.6.2

3. Verify that the HOSTS files are updated properly for the GUI Connection.

HOSTS file settings After Step 3	
HOSTS file on PRI_EXCH	HOSTS file on BKUP_EXCH
BKUP_EXCH 172.17.6.2	PRI_EXCH 172.17.6.1

12. 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.

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

    a. Perform a manual switchover.

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

    c. Verify that SMTP Queue directories have been created on the shared or replicated volume.

Installing Software Updates in a LifeKeeper Environment

Exchange Software Update Procedure

Microsoft Exchange software updates should be applied where the Microsoft Exchange Server resource is active. Use the following procedure to install Microsoft Exchange software updates:

On the Primary:

1. Change directory to the *$LKROOT\bin* directory on the primary server and, from a command prompt, run the command `lkstop.exe -f`. This will stop the LifeKeeper service on the primary server but leave LifeKeeper protected resources active on the primary server.

2. If using replicated volume(s), pause the mirror(s) using the LifeKeeper GUI or the SteelEye DataKeeper GUI.

3. Install Microsoft Exchange software updates on the primary server where Microsoft Exchange Server is active.
   Note: Microsoft Exchange services may be stopped during the installation of some Microsoft Exchange software updates.

4. Verify that the primary server switchback type is "**Do Not Switchover Resources**". Reboot

the primary server, if required. If reboot is not required, manually restart the LifeKeeper services on the primary server using the Services MMC snap-in.

5. Once the Microsoft Exchange Server resource is active on the primary server, verify Exchange is working correctly before applying the updates to the backup server.

6. If using replicated volume(s), continue the mirror(s) using the LifeKeeper GUI or the SteelEye DataKeeper GUI. A partial resync will occur to the backup server. Wait until the replicated volume(s) is in the “**Mirroring**” state before applying the updates to the backup server.
   Note: It is recommended that you perform a backup of your Exchange data before upgrading the backup server.

7. Shutdown the primary server.

On the Backup:

1. Perform a manual in-service of the Exchange resource on the backup server.
   Note: If using LifeKeeper with SteelEye DataKeeper (DATAKEEPER), mirror(s) must be in the “Mirroring” state prior to performing the manual in-service.

2. Once Microsoft Exchange resource is active on the backup server, change directory to the *$LKROOT\bin* directory on the backup server and, from a command prompt, run the command `lkstop.exe -f`. This will stop the LifeKeeper service on the backup server, but leave LifeKeeper protected resources active on the backup server.

3. If using replicated volume(s), pause the mirror(s) using the LifeKeeper GUI or the SteelEye DataKeeper GUI.

4. Install Microsoft Exchange software updates on the backup server where Microsoft Exchange Server is active.
   Note: Microsoft Exchange services may be stopped during the installation of some Microsoft Exchange software updates.

5. Verify that the backup server switchback type is "**Do Not Switchover Resources**". Reboot the backup server, if required. If reboot is not required, manually restart the LifeKeeper services on the backup server using the Services MMC snap-in.

6. Once the Microsoft Exchange Server resource is active on the backup server, verify Exchange is working correctly before restarting the primary server.

7. Restart the primary server.

8. If using replicated volume(s), continue the mirror(s) using the LifeKeeper GUI or the SteelEye DataKeeper GUI. A partial resync will occur to the primary server. Wait until the replicated volume(s) is in the “Mirroring” state before bringing the Exchange resource in-service on the primary server.

9. The Microsoft Exchange resource can be brought back in-service on the original primary at some scheduled time by performing a manual in-service.
   Note: If using LifeKeeper with SteelEye DataKeeper (DATAKEEPER), the mirror(s) must be in the “**Mirroring**” state prior to performing a manual in-service.

Chapter 3: Configuration Considerations

Some of the basic configuration requirements for Microsoft Exchange Server in a LifeKeeper environment are described in the following topics. These considerations should be reviewed carefully prior to configuring Microsoft Exchange Server in your LifeKeeper environment.

Active-Active and Active-Standby Configurations

While the vast majority of LifeKeeper configurations support Active/Active clusters, LifeKeeper for Microsoft Exchange supports only Active/Standby clusters. This is due to Microsoft's recommendation that Exchange not be run in Active/Active cluster configurations. You can read more about the performance and memory fragmentation reasons for this configuration limitation on the Microsoft web site at:

http://technet.microsoft.com/en-us/library/aa997507(EXCHG.65).aspx

SIOS's experience has shown that Active/Active Exchange clusters do not provide the level of protection expected from a high availability solution; therefore, we have limited LifeKeeper's functionality for Exchange environments to Active/Standby.

This does not mean, however, that you must have one physical standby server for every active Exchange server. Using machine virtualization technology, such as VMware ESX Server, you can run Exchange within a virtual machine on a physical server while having a separate virtual machine on that same server available as a failover target for a separate Exchange instance. This allows you to run two copies of Exchange on the same physical server while ensuring that each has its own dedicated set of system resources.

You can also place a number of standby Exchange systems onto a single physical server thereby gaining the benefits of a many-to-one cluster configuration within the limitations imposed by Microsoft Exchange. You must, of course, ensure that the physical server hosting the Exchange standby virtual systems has sufficient CPU cycles, RAM and network connectivity to handle the workload which may be placed upon it in the event of a failure of multiple of the active Exchange servers.

Active/Standby N+1 Configuration

You can use the LifeKeeper Microsoft Exchange Server Recovery Kit to protect two or more active Exchange servers with one backup server in a N+1 type configuration. In this configuration, you can create a cluster of >2 Exchange servers with +1 node providing failover support for the entire N Exchange servers. The +1 node can fail over one of the N primary servers at a time.

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

Public Folder Access in an N+1 Type Cluster

In an N+1 type configuration, the backup server does not have a public folder store. So when a primary Exchange Server (one out of total N) fails over to the backup server, the LifeKeeper Microsoft Exchange Server Recovery Kit sets the "**Default public store**" for all the private mailboxes on the backup server to other primary Exchange server in the cluster. Hence, the users on that Exchange server continue to access the public folders through the other primary Exchange servers running in the cluster.

Sending an email to a public folder is different than sending an email to a user mailbox. As per Microsoft documentation, when an email is sent to a public folder from an Exchange server without public folder store, the Exchange server uses the list of replicas where the public folder hierarchy is replicated. This list is stored in the "*msExchOwningPFTreeBL*" attribute of public folder object (CN=Public Folders,CN=Folder Hierarchies,CN=<YourAdministrative Group>,CN=Administrative Groups,CN=<YourOrganization>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<YourDomain>,DC=com/local) in Active Directory. The Exchange makes selection based on following algorithm.

1. Local Server (if it has public folder store) in the msExchOwningPFTreeBL.
2. First in the List of Exchange servers in the same RG in the msExchOwningPFTreeBL Attribute.
3. First in the List of E2K3 Servers in the same AG in the msExchOwningPFTreeBL Attribute.
4. First E2K3 Server in the msExchOwningPFTreeBL Attribute. This server will be the most recent add Exchange server.

This behavior has implications in an N+1 type configuration.

LifeKeeper Communication Paths Considerations

All clustered systems in an Exchange Server hierarchy must be interconnected by at least one LifeKeeper TCP/IP type communication path.

Consistent Network Name Resolution

It is crucial that DNS, WINs (if configured) and Active Directory resolve correctly and consistently for the servers and clients to work.

Client Connection After Switchover and Failover

During switchover of the Microsoft Exchange Server resource from one server to another, clients connected to the Exchange server or attempting to open a public folder, shared calendar or global address book will get an error saying that the server is not available. After Microsoft Exchange Server has been restored on the backup server, clients attempting to open a message may get an error message (varying by client type) which indicates that the operation failed. The user may then retry the operation or may exit and restart the mail client to access items on the Exchange server.

Other client-side considerations:

- In a WAN configuration where DNS is changed after the failover, the client machine's DNS cache should be purged using the command "`ipconfig/flushdns`". This will allow the Exchange client to connect with the Exchange server instantly without delay when restarted.
- Microsoft Outlook MAPI clients (such as Outlook 2000 and 2003) must be closed and restarted after a failover in order to connect to the recovered server.
- Microsoft Outlook Web Access (OWA) clients must use the LifeKeeper protected (switchable) IP address or a DNS alias name. OWA clients can use a URL that maps to the switchable IP address, the static IP address of the server where Exchange is running or the DNS alias name to connect.

Another method would be to create an additional static entry in DNS for the LifeKeeper protected (switchable) IP address and then create an Alias name for the static entry. For example, create a static entry in the DNS mapping your primary Exchange server, "MailServer", to the LifeKeeper protected IP address,"172.17.100.35". Now create another unique static entry, "MailServer1", mapping it to the same IP address, "172.17.100.35". Then create an Alias (CNAME) entry, "WebMail" for MailServer1. All OWA clients can use "WebMail" in their browser to access the Exchange server for mail.

Name	Type	Data
MailServer	Host (A)	172.17.100.35
MailServer1	Host (A)	172.17.100.35
WebMail	Alias (CNAME)	MailServer1

When a primary Exchange server, which is the first server in the list of replica servers in the Active Directory, fails over to the backup node, the email sent from the +1 backup server to the public folders will not be delivered and an NDR is generated. The user continues to access the public folder from the other primary Exchange server in the administrative group and can drag-n-drop email using MAPI Outlook client. However, e-mail (SMTP email) sent to the public folder is not delivered and a Non-Delivery Report (NDR) is sent to the user.

Chapter 4: Resource Configuration

Task Overview

Once you have completed the setup tasks described in the Planning and Installation Guide, you are ready to create and extend your Microsoft Exchange Server resource hierarchies.

Following are the four main tasks required to configuring your Microsoft Exchange Server resources for LifeKeeper protection.

- Create a Resource Hierarchy - Creates an application resource hierarchy in your LifeKeeper cluster.
- Extend a Resource Hierarchy - Extends a resource hierarchy from the primary server to a backup server.
- Unextend a Resource Hierarchy - Unextends (removes) a resource hierarchy from a single server in the LifeKeeper cluster.
- Delete a Resource Hierarchy - Deletes a resource hierarchy from all servers in your LifeKeeper cluster.

If necessary, refer to the following tasks for additional information as you complete these configuration procedures.

- Create a Resource Dependency - Creates a parent/child dependency between an existing resource and another resource instance and propagates the dependency changes to all applicable servers in the cluster.
- Delete a Resource Dependency - Deletes a resource dependency and propagates the dependency changes to all applicable servers in the cluster.
- In Service - Brings a resource hierarchy into service on a specific server.
- Out of Service - Takes a resource hierarchy out of service on a specific server.
- View/Edit Properties - Allows viewing or editing of the properties of a resource hierarchy on a specific server.

Note: Throughout this help project, configuration tasks are performed using the **Edit** menu. You can also perform most of these tasks:

- from the toolbar
- by right clicking on a global resource in the left pane of the status display
- by right clicking on a resource instance in the right pane of the status display

Using the right-click method allows you to avoid entering information that is required when using the **Edit** menu.

Creating a Microsoft Exchange Server Hierarchy

After you have completed the necessary setup tasks including creation of the Volume resource, perform the following steps to define the Microsoft Exchange Server hierarchy to protect your database(s). 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**.

   The **Create Protected Application** dialog box will appear with a drop-down list box displaying all recognized Recovery Kits installed within the cluster.

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

3. 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
Server	Select the server on which you want to create the hierarchy.
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**: Optional Exchange Server services (i.e. Microsoft Event service) should be configured and running on the Exchange Server prior to protecting under LifeKeeper. **Note**: Any services that you do not select will not be able to run. Thus, any service you wish to run must be protected by LifeKeeper.
Microsoft Exchange Administrative User Name	Enter the Exchange 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 log in 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.
Microsoft Exchange Server Administrative Password	Enter the password for the Exchange Server 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 assigns the highest priority, by default 1, to the resource. Then when you extend the resource hierarchy to the backup server, 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 a resource hierarchy from the primary server as this would designate the backup server the primary role.

Extending a Micrsosoft Exchange 2003 Server Resource Hierarchy

This operation can be started from the **Edit** menu or initiated automatically upon completing the Create 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. If you are unfamiliar with the Extend operation, click **Next**.

Field	Tips
Primary Server	Select the server where your Microsoft Exchange Server resource is currently in service.
Resource Hierarchy to Extend	Select the Microsoft Exchange Resource
Backup Server	Select the server you want to function as the backup server

2. After receiving the message that the pre-extend checks were successful, click **Next**.

3. Depending upon the hierarchy being extended, LifeKeeper will display a series of information boxes showing the Resource Tags to be extended, some of which cannot be edited. If an IP address is part of the hierarchy, you will be able to edit the **Subnet Mask**, **Network Connection** and **Target Local Recovery** fields. If a DNS resource is part of the hierarchy, select the IP address of this server. The IP address of the *A record* associated with the protected primary server or alias name will be updated with this IP address when the DNS resource is brought in service on this server.

Field	Tips
Is this an N+1 Cluster?	An N+1 cluster has two or more primary servers (N) being protected by a single backup server (+1). In an N+1 configuration, the backup server cannot have Public Folders.

4. The **Extend Wizard** will make configuration checks. The names of the Microsoft Exchange storage groups and mailbox stores should be the same on both the primary and backup servers. The **Extend Wizard** compares the database configuration of Exchange running on the primary and backup servers. It will display all the changes that are needed to match the configuration and will invoke a utility to make the required changes in the Exchange configuration on the backup server. If no changes are needed, the window will be empty. Click **Next** to continue. If changes are needed, click **Cancel** to make the changes yourself.

Field	Tips
Backup Priority	This number determines the failover priority when your application is protected by more than one backup server.

5. Enter any unused priority value from 1 to 999. A lower number gives it a higher priority. The default backup priority is 10.

6. At this point, all checks have been completed. Press **Extend** to extend the resource hierarchy. If it is open, command output will be displayed in this window. Any errors that occur will also be logged in both the LifeKeeper log and the GUI log on the designated server.

7. After receiving the message, "**Hierarchy extend operations completed**", click **Finish**.

Unextending a Microsoft Exchange 2003 Server Hierarchy

We recommend that the Microsoft Exchange Server resource hierarchy be unextended from the backup server where Microsoft Exchange Server is not in service.

WARNING: Do not unextend the resource hierarchy from the primary server while the Exchange resource is in service on the backup server.

1. On the **Edit** menu, select **Resource**, then **Unextend Resource Hierarchy**.

2. Select the Target Server where you want to unextend the Microsoft Exchange Server resource. It cannot be the server where the resource is currently in service. (This dialog box will not appear if you selected the Unextend task by right-clicking on a resource instance in the right pane.) Click **Next**.

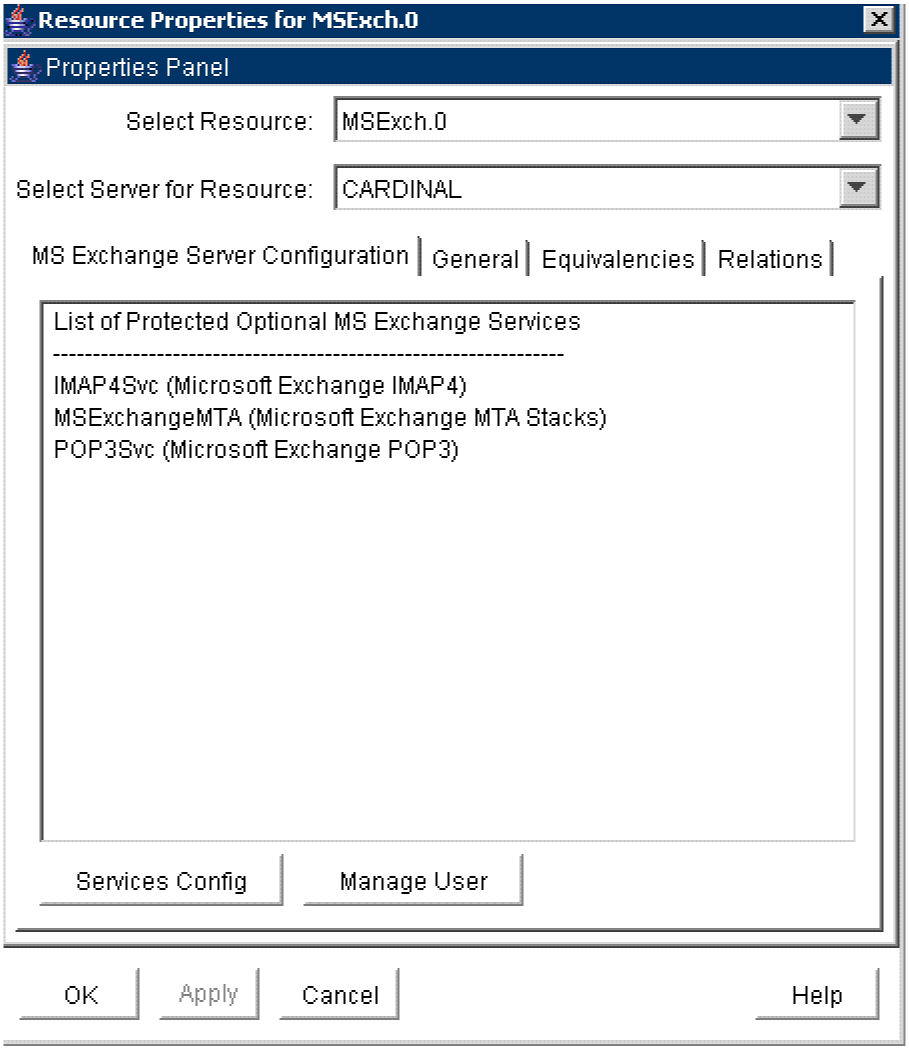
3. Select the Microsoft Exchange Server hierarchy to unextend and click **Next**. (This dialog will not appear if you selected the **Unextend** task by right-clicking on a resource instance in either pane).

4. An information box appears confirming the target server and the Microsoft Exchange Server resource hierarchy you have chosen to unextend. Click **Unextend**.

5. Another information box appears confirming that the Microsoft Exchange Server resource was unextended successfully. Click **Done** to exit the **Unextend Resource Hierarchy** menu selection.

Updating an Exchange Resource Configuration

To administer a protected Microsoft Exchange Server resource from the LifeKeeper GUI, right-click on the MS Exchange resource (on the right-hand side of the LifeKeeper GUI) and select **properties**, then select the **MS Exchange Server Configuration** tab. Use the **MS Exchange Server Configuration page** to view or change information about your MS Exchange resource.



Select Resource: MSExch.0

Select Server for Resource: CARDINAL

List of Protected Optional MS Exchange Services

```
------------------------------------------------------------
IMAP4Svc (Microsoft Exchange IMAP4)
MSExchangeMTA (Microsoft Exchange MTA Stacks)
POP3Svc (Microsoft Exchange POP3)
```

Services Config

This menu allows users to modify the list of optional Exchange services that are protected under the resource hierarchy.

Select **Action**:

- **Add Service** - Add an additional service to the protected configuration. LifeKeeper will start monitoring the added MS Exchange service. You can add any service that belongs to third party software like Anti-Virus or Anti-SPAM that has a dependency on MS Exchange services. The services should be entered in their start order. The only restriction is that the service name must not have spaces.

  Important: It is essential that you test the services configuration before making changes in the hierarchy on a production server. You should verify that the service can be started and stopped.

- **Delete Service** - Remove a service from the protected configuration.

Field	Tips
Service Name	Select an optional service to Add or Delete from the protected configuration. You may also enter a service name not listed. Do not enter the display name of the service. **Example**: If you are using GFI Anti-Spam software and would like to protect the "**GFI Mail Essentials Enterprise Transfer Service**" service, then you would enter the service name **GFIMETRXSVC**.
Update All Systems	Select **Yes** to update all systems in this cluster. Otherwise, select **No** to only update the current system. If you choose **No**, you must manually add the service to the backup servers.

Microsoft Exchange 2003 Server - Services Config

This menu allows users to modify the list of optional Exchange services that are protected under the resource hierarchy.

Select **Action**:

- **Add Service** - Add an additional service to the protected configuration. LifeKeeper will start monitoring the added MS Exchange service. You can add any service that belongs to third party software like Anti-Virus or Anti-SPAM that has a dependency on MS Exchange services. The services should be entered in their start order. The only restriction is that the service name must not have spaces.

  Important: It is essential that you test the services configuration before making changes in the hierarchy on a production server. You should verify that the service can be started and stopped.

- **Delete Service** - Remove a service from the protected configuration.

Field	Tips
Service Name	Enter the name of a service, not the display name, to Add or Delete from the protected configuration. **Example**: If you are using GFI Anti-Spam software and would like to protect the "**GFI Mail Essentials Enterprise Transfer Service**" service, then you would enter the service name **GFIMETRXSVC**.
Update All Systems	Select **Yes** to update all systems in this cluster. Otherwise, select **No** to only update the current system. If you choose **No**, you must manually add the service to the backup servers.

Microsoft Exchange 2003 Server - Manage User

During the creation of a LifeKeeper Microsoft Exchange Server resource, the administrator must enter a domain administrative 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 permissions to edit Active Directory.
Domain Administrative Password	Enter the domain administrative password for the user account being updated.

Deleting a Microsoft Exchange 2003 Server Hierarchy

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**.
4. An information box appears confirming your selection of the target server and the hierarchy you have selected to delete. Click **Next**.
5. Another information box appears confirming that the Microsoft Exchange Server resource was

deleted successfully.

6. Click **Done** to exit.

Using Microsoft Exchange 2003 Server 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).

Testing Your Microsoft Exchange 2003 Hierarchy

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.

Select **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 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.

Chapter 5: Microsoft Exchange 2003 Server Administration Guidelines

You can reduce the number of errors you encounter when administering your Microsoft Exchange Server resource hierarchy if you follow the administrative guidelines in this section.

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 on LifeKeeper DNS Recovery Kit, refer to the LifeKeeper Online Help included with the LifeKeeper core product. 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

               ExchSrvr1 Alias-> 172.16.10.25
```

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

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

Microsoft Exchange Server 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 which ever server is currently running the Exchange instance.

Reserve Volumes For Exclusive Use By Microsoft Exchange 2003 Server

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.

Microsoft Exchange 2003 Server Share Names

Microsoft Exchange Server creates the following file shares on the volume where the Microsoft Exchange Server software is installed:

1. Address
2. Resources$
3. $<Exchange Server Name>.log

These shares are removed and restored with the hierarchy during a failover or manual switchover.

Running Third-Party Software With Exchange 2003

Third-party software applications that are installed to work with Exchange server (i.e. Backup Agent, AntiVirus, 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 2003 Server

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 Exchange server is running on the primary. To resolve the 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.

Chapter 6: Special Considerations for Public Folders

Updating the Routing Topology for Public Folder E-Mail Routing

The LifeKeeper Microsoft Exchange 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.

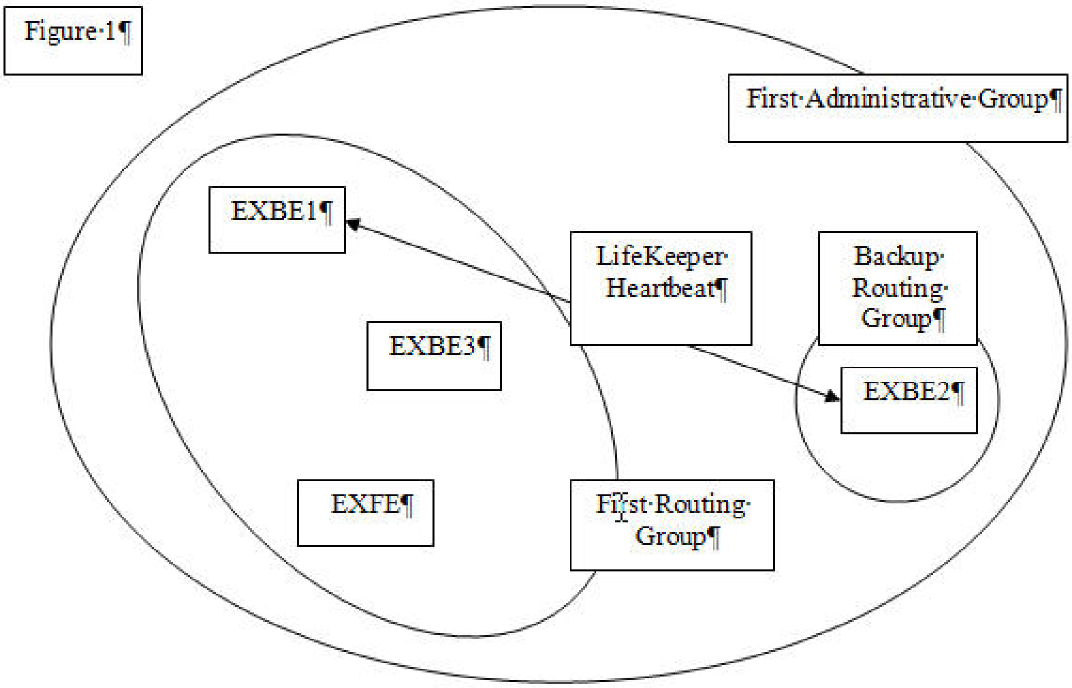
Note: To determine the order of the Exchange servers in the list, use the ExchDump tool available from Microsoft. Please refer to the KB article: http://support.microsoft.com/default.aspx?scid=kb;EN-US;839116

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.

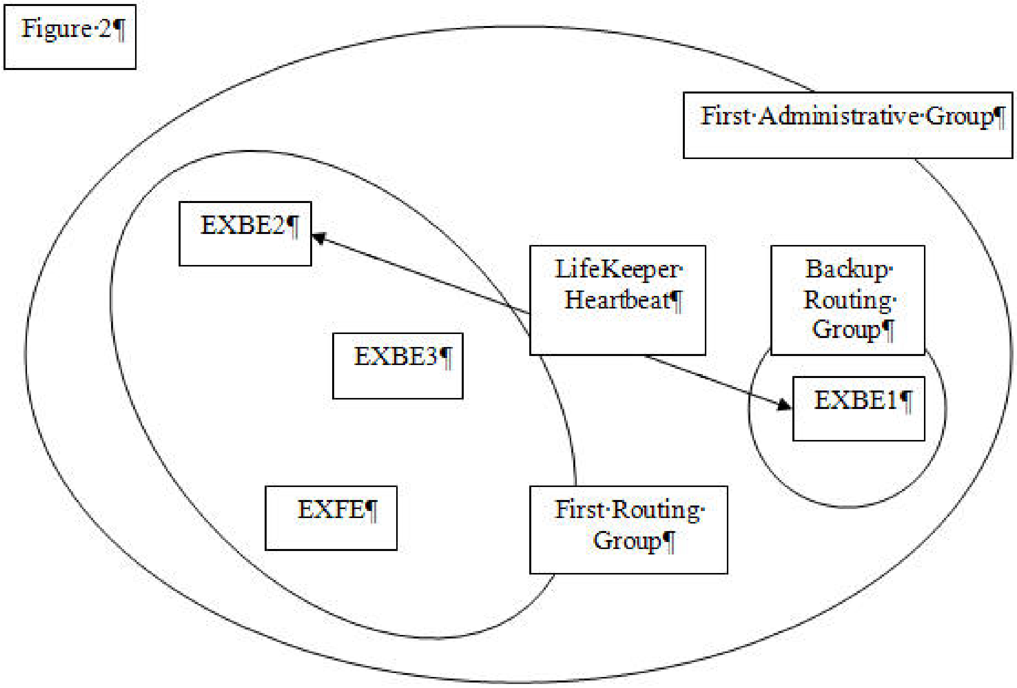
If the primary server EXBE1 fails, flow of public folder e-mail will be affected and front-end Exchange server EXFE will have problems delivering e-mail.

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¶

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

Note: EXFE in this example is a front-end server with no public folder store.


Figure·2¶

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 pick up the new server from the list pointed to by attribute *msExchOwningPFTreeBL* and maintain email flow. It is possible that while other e-mail 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 Server recovery kit does not update routing groups and connectors in an N+1 type configuration because the +1 node cannot have a public folder store.

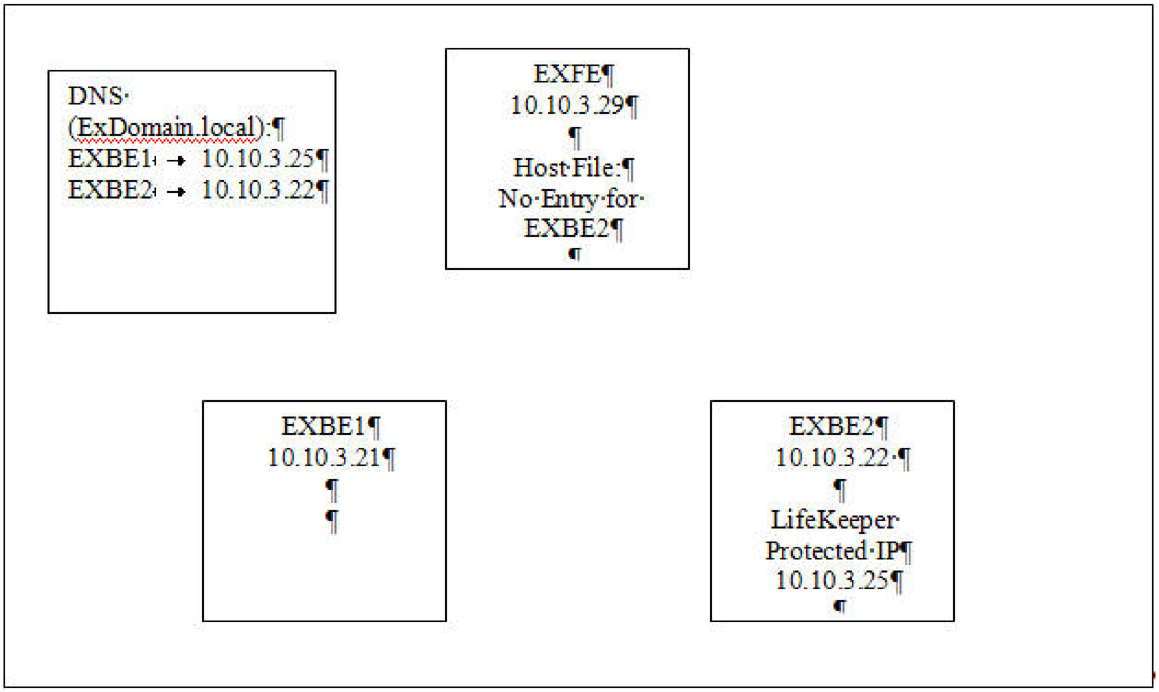
Mail Flow When Routing Topology is Changed

When the routing groups and connectors in the local Exchange administrative group are updated as described above, email bound to those affected users from a third Exchange server (outside the LifeKeeper cluster) may be affected. This is because the Exchange server that is sending email to a user on the primary server does not pickup the changes in the topology in a timely manner. In this scenario, the email bound to the primary exchange server will be queued in the wrong connector queue. However, we have found that Exchange re-categorizes the messages and sends them to the backup server over the correct connector.

Retrieving Email Queued During Exchange Fail Back

When LifeKeeper performs a fail back of an Exchange server from the backup server to the primary, it is possible that some email will get queued on other Exchange servers in your Exchange Organization. This happens because of latency in picking up changes in Active Directory and latency in DNS resolution.

Consider the following diagram which shows configuration details when Exchange server is running on the backup server EXBE2.



When a fail back occurs and LifeKeeper brings the Exchange resource hierarchy in-service on the primary server, some email will get queued in the SMTP queue for server EXBE2 on Exchange server EXFE. This is because Active Directory changes made by LifeKeeper during fail back are not picked up by Exchange running on EXFE. This email can be retrieved by adding an entry for EXBE2 in the Hosts file on Exchange server EXFE as per following procedure.

1. If LifeKeeper GUI is running on EXFE server, exit from it.

2. Edit the `%SystemRoot%\System32\drivers\etc\hosts` file and add an entry of the backup server assigning the LifeKeeper protected IP address to it. In our example it would be EXBE2.ExDomain.local 10.10.3.25

   Note: If you are in a WAN type environment and protecting a DNS resource instead of IP address, you need to assign the permanent IP address of the primary server to the backup server in the hosts file.

3. Run `ipconfig /flushdns` on server EXFE.

4. Start Exchange System Manager (ESM) and go to <Your Administrative Group> -> Servers -> <EXFE> -> Queues container.

5. Right click queue for “EXBE2.ExDomain.local” and select “Force Connection”.

6. Wait for Exchange to deliver queued messages.

7. Undo changes in **hosts** file by deleting or commenting out mapping for EXBE2.ExDomain.local.

8. Run `ipconfig /flushdns` on the server.

It is important to note that during failover from primary server EXBE1 to EXBE2, it is possible that some email would get queued on the Exchange server EXFE. However changes in hosts file are not required. Exchange on EXFE does detect, after some delay, that the primary server is reachable and delivers the email.

Public Folder Replica List Update (Exchange Server 2003 ONLY)

The LifeKeeper Microsoft Exchange Server recovery kit provides an option to 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 0 (zero), 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 would enable the update of public folder replica list.

If you are upgrading from a previous version of the LifeKeeper Microsoft Exchange Server Recovery Kit and you would like to use this feature, you must manually create value name UpdateReplicaList and set the value to 1 in the Registry.

IMPORTANT: It is recommended that you set the value of UpdateReplicaList to 0 if there is no public folder Exchange server outside the LifeKeeper cluster. If you are disabling the dynamic update of the replica list then you should add the Exchange servers in the LifeKeeper cluster in the replica list as described in the section **Configure LifeKeeper**. However, if any public folder server outside the cluster is listed in the replica list, then you can enable the feature by setting the value of UpdateReplicaList to 1.

Mail Flow When Replica List of Public Folders is Updated

When the replica list update feature is enabled, the LifeKeeper Exchange 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 email, sometimes the email is delivered to the folder, but the NDR is still generated. It is also possible that sometimes public folder re-mails are queued into the SMTP queue when the Exchange resource hierarchy is failed back, i.e. backup server to primary server. In this situation, email can be retrieved by updating the hosts file on the primary server and forcing the connection on the SMTP queue. For the detailed procedure on how to retrieve email, refer to the topic Retrieving Email Queued During Exchange Fail Back.

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 in-box.

```
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 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.

Chapter 7: Special Considerations When Using Replicated Volume(s)

If a replicated volume is being used with a Microsoft Exchange Server resource hierarchy, there are some situations that deserve special attention.

Replicated Volume - Failed Primary Server and Blocked Recovery on Backup Server

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.

Chapter 8: Microsoft Exchange Server 2003 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 2003 Resource

LifeKeeper Microsoft Exchange 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.

- If Exchange data (not program files) are on %SystemDrive%.
- Database (EDB) files of mailstore "Mailbox Store" of storage group "First Storage Group" are located on system drive (C:).
- Database (STM) files of mailstore "Mailbox Store" of storage group "First Storage Group" are located on system drive (C:). Relocate the files to LifeKeeper protected volume(s) using Exchange System Manager.
- SMTP Badmail directory is located on system drive (C:). Relocate the SMTP queue directories to a LifeKeeper protected volume using SetSMTPQueuePath.vbsscript located in C:\LK\Admin\kit\msexch\bin directory as follows:cscript /nologo SetSMTPQueuePath.vbs <Primary Exchange server><x>

  where <Primary Exchange server> is the name of the Exchange server where the hierarchy is being created.

  where <x> is the drive letter of a LifeKeeper protected volume.

These error messages indicate that Exchange server’s store files, transaction log files or SMTP queue directories are located on the *%SystemDrive%*, which is not eligible for protection by LifeKeeper. The administrator should relocate to a drive other than %SystemDrive%. These volumes should be protected by LifeKeeper before creating the Exchange resource hierarchy.

To relocate mail stores and transaction log files, use Exchange System Manager. To relocate SMTP queue directories, use SetSMTPQueuePath.vbsscript

- If Exchange data (not program files) are not on a LifeKeeper protected volume.

  ERROR:

```
A LifeKeeper resource protecting volume "L:\" is not created.
```

```
LifeKeeper resource(s) protecting volume(s) "W:\ L:\" needs to be
created and brought in-service before creating the MS Exchange
Server resource hierarchy. Also the LifeKeeper volume resource(s)
shouldn't be part of another LifeKeeper Hierarchy.
```

The Exchange kit has detected that some of the Exchange data (not program files) are on a volume that is not protected by LifeKeeper. Volume resources containing Exchange data should be created in LifeKeeper prior to creating the Exchange resource.

- When previously created Exchange resource hierarchy was deleted while last active on a backup server.

```
It appears that the previous LifeKeeper Exchange resource hierarchy
was deleted while it was active on a backup node. If you plan to
recreate the hierarchy with server <primary servername> as primary
Exchange server, run lkmsad_mu.exe utility from <%LKROOT%>\bin
directory as follows:
```

```
lkmsad_mu.exe <UserName@FQDN> <Password> <primaryservername>
<primary servername> -f <another servername>
```

This error message is displayed when a previously created Exchange resource is deleted in failover mode, i.e. the resource hierarchy was deleted while it was in-service or last active on the backup server (specified by -f <another servername>). This left certain attributes of Exchange server in a state not consistent which prevents making <primary servername> the primary server again.

To resolve this problem, run the LifeKeeper command utility `lkmsad_mu.exe` displayed in the error message. This utility will fail back all the users to the primary server.

Extend of Exchange 2003 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 does not match with the
configuration on the Exchange server . The following changes should
be made on the Exchange server :
```

```
- 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.

Warning Message During Restore of Exchance 2003 Resource

After upgrading from a previous version of the LifeKeeper Microsoft Exchange Server Recovery Kit, the following warning will be displayed in the LifeKeeper GUI the first time the Exchange resource in brought in-service:

```
WARNING*(No. 28540) Failed to get value from the Registry.
Skipping update of public folder replica list.
```

If you wish the public folder replica list to be automatically updated on failover of the Exchange resource, you must manually create the registry value `UpdateReplicaList`, described in section Public Folder Replica List Update (Exchange Server 2003 ONLY), and set `UpdateReplicaList` to 1.

Service Startup Problems

You may wish to reduce the MAXWAIT value in the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\SteelEye\LifeKeeper\RK\msexch` 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)

Client Connection Problems

- If client systems are slow in establishing a connection to the Microsoft Exchange Server system, check the binding order for both server and clients as described in the Microsoft Exchange Server documentation. Client access will be fastest if clients use TCP/IP and ‘ncacn_tp_tcp’ first in the binding order list. You may use the RPC Ping utilities located on the Microsoft Exchange Server installation CD to determine which bindings are supported in your environment.
- After the failover/switchover the Outlook MAPI clients must be exited and restarted. In some cases the Outlook MAPI client application does not exit completely. When the user tries to restart the client, the error 0x80040119 occurs. This is because the previous instance of MAPI Outlook is still running. To confirm, use Task Manager to check the client’s system for the “Outlook.exe” process. If found, end the hanging instance of “Outlook.exe” and restart the Outlook application.
- For Outlook Web Access (OWA) clients, use the protected switchable IP address or the static

IP address of the server where Exchange Server is running to connect to the Exchange server.

- For Windows 2003 and Windows XP, IMAP4, POP3, and OWA clients may require the fully qualified domain name in order to logon (i.e. user@domain.com or<domain NetBIOS name>\user).
- Using Active Directory Users and Computers MMC snap-in, verify that the location of the user’s mailbox is located on the server where Exchange Server is running.

Mail Remains in SMTP Queue on Smart Host Server After Failure

In an Exchange environment where Exchange Server is configured on the Smart Host server in addition to the LifeKeeper protected Exchange servers, incoming mail will remain in the SMTP queue on the Smart Host server after failover. The SMTP server on the Smart Host Server does a lookup of the user in Active Directory to find the location of the recipients’ mailboxes. This may cause a problem when the Active Directory lookup is done during the time the users are being moved to the backup Exchange Server as part of the LifeKeeper failover. The Active Directory lookup succeeds, but Exchange is running on the backup server after the failover. This may cause mail to remain undelivered in the SMTP’s delivery queue on the Smart Host Server. To resolve this issue, move the mail files from the SMTP Queue directory to the SMTP Pickup directory on the Smart Host Server forcing SMTP to do the Active Directory lookup again and send the mail to the backup Exchange Server, which now hosts the mailboxes of the recipients.

Manually Moving All Users of a Domain to an Active Exchange Server

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> <LocalExchange 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.

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.

Error During In-Service of Exchange Resource

If the Exchange resource is brought in and out of service on the same system, an error is logged to the **Application Event Log** indicating that moving users to the Exchange Server failed.

```
*ERROR* (No. 28523) Failure in moving users to exchange server
<systemname>. Please refer to the file C:/LK/out/FailedExUsers.log
for list of users.
```

This error may be ignored, as moving users is not required unless a switchover or failover occurs.

Slow Microsoft Exchange Server Startup After Multiple Failovers

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.

LifeKeeper GUI Does Not Connect After Failover

Verify that each LifeKeeper server has the appropriate entry of the other LifeKeeper server in its *%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.