LifeKeeper for Windows

LifeKeeper Microsoft Exchange Server Recovery Kit Administration Guide

July 2005

The product described in this book is a licensed product of SteelEye™ Technology, Inc.

It is the policy of SteelEye Technology, Inc. to improve products as new technology, components, software, and firmware become available. SteelEye Technology, Inc., therefore, reserves the right to change specifications without prior notice.

To maintain the quality of our publications, we need your comments on the accuracy, clarity, organization, and value of this book.

Address correspondence to:

ip@steeleye.com

Table of Contents

LifeKeeper Microsoft Exchange Server Recovery Kit Administration Guide

The SteelEye LifeKeeper Microsoft Exchange Server Recovery Kit provides high availability for Microsoft Exchange Server 2000 and 2003 environments running under LifeKeeper protection. LifeKeeper constantly monitors the health of both the physical server on which Exchange is active and the individual Exchange processes, client connections, and data volumes. On detection of any problem, LifeKeeper will initiate a recovery action to ensure that Exchange is always available.

Document Contents

This guide includes the following topics to help you successfully deploy and administer your Microsoft Exchange Server within a LifeKeeper environment.

- **LifeKeeper Microsoft Exchange Server Recovery Kit Overview**. Provides a general overview of Microsoft Exchange Server in a LifeKeeper environment.
- **Configuration Requirements**. Describes configuration requirements of Microsoft Exchange Server in a LifeKeeper environment.
- **Configuring Microsoft Exchange Server with LifeKeeper**. Provides configuration examples and describes the configuration tasks required prior to protecting Exchange with LifeKeeper. You will also find a worksheet to record your configuration, and instructions for installing/configuring Microsoft Exchange Server with LifeKeeper.
- **Resource Configuration Tasks**. Explains the various functions you may perform on your LifeKeeper-protected Exchange system including creating, extending, deleting and unextending Exchange resource hierarchies.
- **Microsoft Exchange Server Hierarchy Administration**. Provides important recommendations for ongoing administration of Microsoft Exchange resource hierarchies.
- **Troubleshooting**. Provides suggestions and insights into occurrences that are not specifically related to LifeKeeper, but which may be observed during operation.

LifeKeeper Documentation

The following documentation is associated with the LifeKeeper Core product:

- *Release Notes*
- *Online Product Manual*
- *Planning and Installation Guide*

This documentation, along with documentation associated with LifeKeeper Recovery Kits, is available online at www.steeleye.com/support/documentation

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 2000 Server Standard, Advanced, Data Center Editions
- Windows Server 2003 Standard, Enterprise, Data Center, Web Editions

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

- Exchange 2000 Server (standard edition)
- Exchange 2000 Server Enterprise
- 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 LifeKeeper Data Replication to replicate the Exchange Storage Group between local volumes on the servers within the cluster. This configuration has the advantage of removing the requirement for a shared storage device which supports the building of either a lower cost cluster configuration or of a wide area disaster recovery configuration.
-

Recovery Kit Installation

The LifeKeeper Microsoft Exchange Server Recovery Kit is distributed on CD-ROM or via ftp download. InstallShield provides a standard installation interface. For complete instructions on installing or removing LifeKeeper, refer to the *LifeKeeper for Windows Planning and Installation Guide*.

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

Upgrading Recovery Kit From v4.x

You may upgrade from the previous version of the LifeKeeper Microsoft Exchange Server Recovery Kit v5.0 software while preserving your resource hierarchies. Refer to the *Planning and Installation Guide* for the upgrade procedure.

Upgrading Recovery Kit from v4.1.x

You must delete any previously existing LifeKeeper Microsoft Exchange Server resource created using the LifeKeeper Microsoft Exchange Server Recovery Kit v4.1.x before upgrading to this version of the LifeKeeper Microsoft Exchange Server Recovery Kit. To do this, you may first delete the dependencies for the switchable IP (if used) and the volume(s) which exist in the LifeKeeper hierarchy.

Any previous version of the LifeKeeper Microsoft Exchange Server Recovery Kit v4.1.x must be uninstalled prior to installing LifeKeeper Microsoft Exchange Server Recovery Kit v5.0.

Note: The Microsoft Exchange Server software must be reinstalled on the backup server as part of the upgrade procedure per instructions in this document. Do **not** use Add/Remove Programs to uninstall the Microsoft Exchange Server software on the backup server, as this will modify Active Directory entries for the primary Exchange server. For additional information about upgrading your LifeKeeper environment, contact SteelEye support at support@steeleye.com, or call:

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

+1-803-461-3970 (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 v5.0" 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.

LifeKeeper Microsoft Exchange Server Recovery Kit Overview

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

LifeKeeper protects the following Microsoft Exchange Server services:

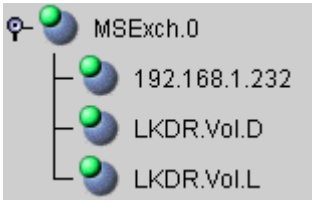
Core Services	**Optional Services**
Routing Engine	IMAP4
System Attendant	POP3
Information Store	Event
Simple Mail Transfer Protocol (SMTP)	Message Transfer Agent (MTA Stacks)
World Wide Web Publishing Service	Microsoft Search
	Connectivity Controller
	Connector for Lotus Notes cc:Mail
	Connector for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

Resource Hierarchy for Microsoft Exchange Server

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

- Microsoft Exchange Server
- IP address (optional)
- Volume(s)

The LifeKeeper GUI display shown below depicts a Microsoft Exchange Server hierarchy including two volume resources.



The Microsoft Exchange Server resource (*MSExch.0*) is the uppermost (parent) resource in the above hierarchy tree. It is responsible for starting and stopping its dependent resources. The IP resource (*192.168.1.232*) and two volume resources (D: and *L:*) are dependent resources under the Microsoft Exchange Server resource.

Configuration Requirements

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

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 Microsoft.com at:

http://support.microsoft.com/default.aspx?scid=%2Fservicedesks%2Fwebcasts%2Fen%2Ftranscripts%2Fwct090903.asp

Our 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, 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 failover one of the *N* primary servers at a time.

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.

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.

LifeKeeper Communications Path Considerations

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

In this type of configuration, LifeKeeper cannot protect an IP address for the Microsoft Exchange Server. However, transparent client connectivity can be achieved through DNS entries for the servers. When the primary server running Microsoft Exchange Server fails, the DNS entry for the primary server must be manually updated to be the static IP of the backup Exchange Server. The mail client of Microsoft Exchange Server will experience a temporary interruption in the connection and in most cases the mail client application will need to be restarted.

Client Connection after Switchover/Failover

During switchover of the Microsoft Exchange Server resource from one server to another, clients connected to the Exchanger 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, a URL that maps to this IP address or the static IP address of the server where Exchange is running 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

Public folder access in N+1 type cluster

In a *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 e-mail to a public folder is different than sending an e-mail to a user mailbox. As per Microsoft documentation, when an e-mail 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

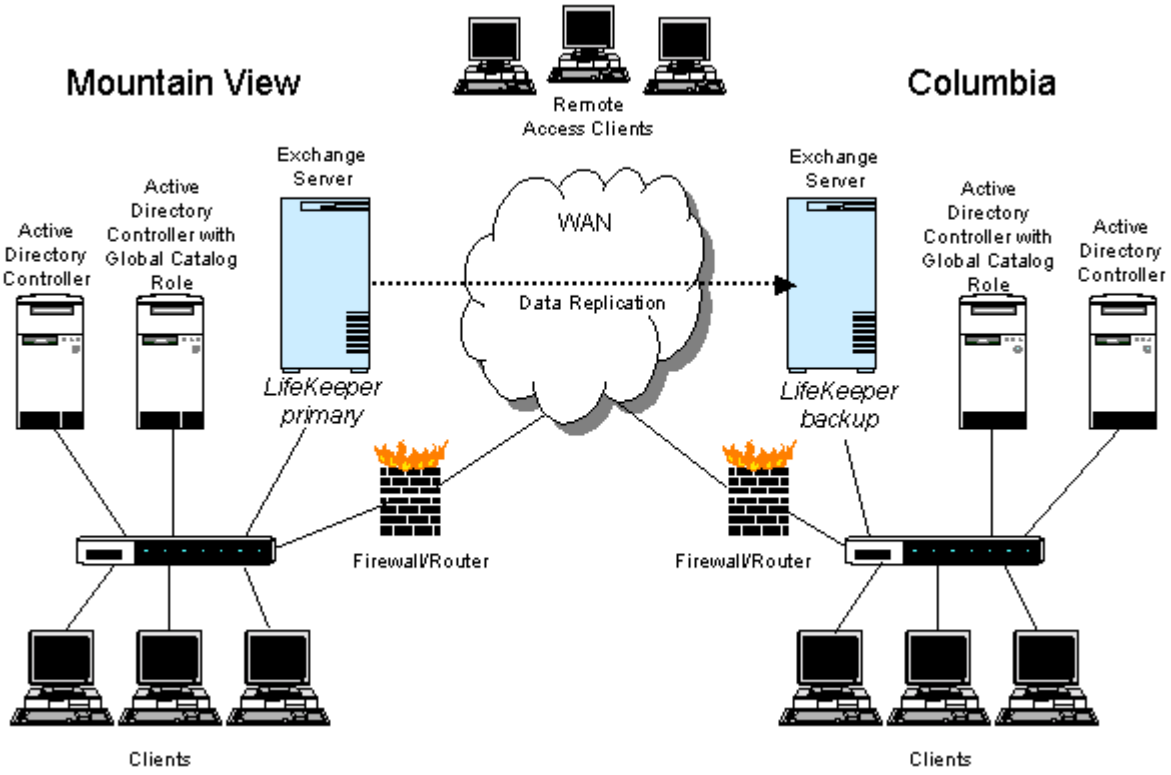
folder object (CN=Public Folders,CN=Folder Hierarchies,CN=<Your Administrative Group>,CN=Administrative Groups,CN=<Your Organization>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<YourDomain>,DC=com/local) in Active Directory. The Exchange server sends the e-mail to the first server in this list. If this e-mail server is down, then the e-mail is not delivered to the public folder. This behavior has implications in a *N+1* type configuration.

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 e-mail sent from the *+1* backup server to the public folders will not be delivered and a 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 e-mail using MAPI Outlook client. However, e-mail (SMTP e-mail) sent to the public folder is not delivered and a Non-Delivery Report (NDR) is sent to the user.

Configuration Examples

Environment View

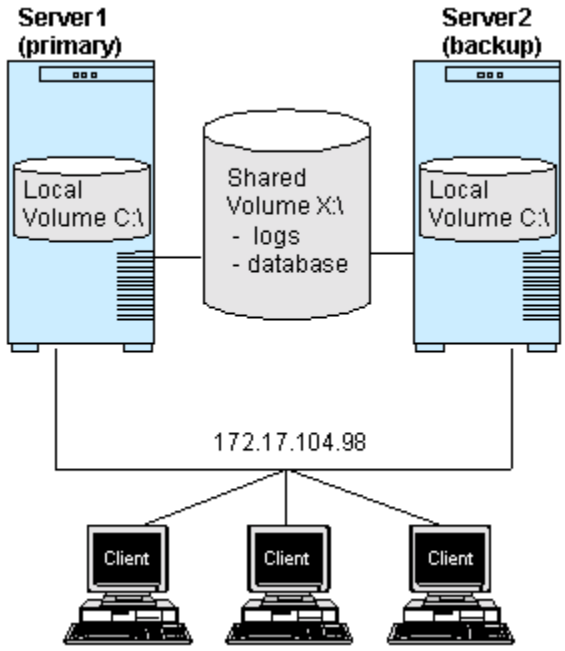
The following diagram depicts a WAN environment where LifeKeeper is protecting Microsoft Exchange Server. The primary and backup Exchange servers are in different geographic locations, and the Exchange data and transaction stores are replicated across the WAN using LifeKeeper Data Replication.



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:

- 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 shared volume D.
- The IP address 192.168.1.232 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 setup 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 Server1fails, 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.

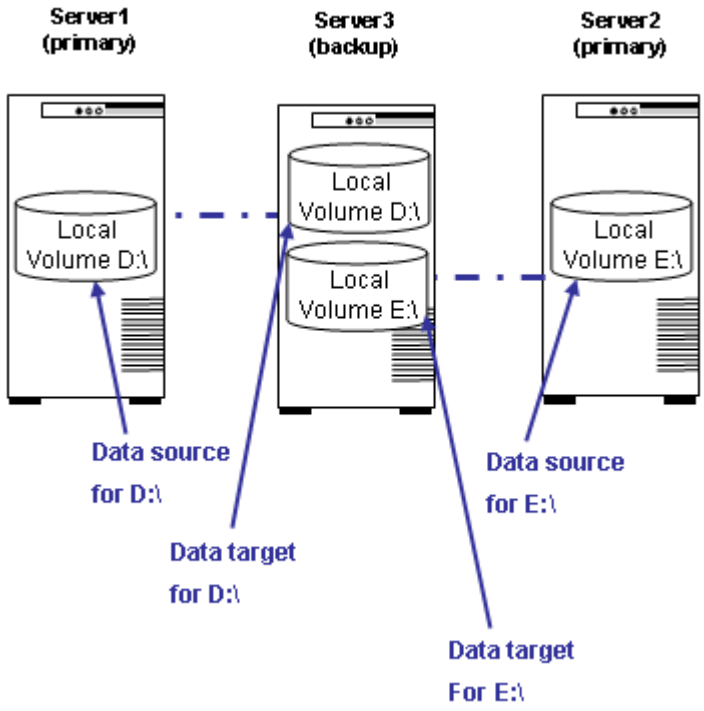
Configuration Notes:

- Server1 (primary) - Microsoft Exchange Server binaries are installed onto a local volume.
- Server2 (backup) - Microsoft Exchange Server binaries are installed onto a local volume.
- Server3 (backup) - Microsoft Exchange Server binaries are installed onto a local volume.
- Transaction logs and Microsoft Exchange database files are located on a shared volume.

N+1 Cluster

In this configuration you can setup 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 failover 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



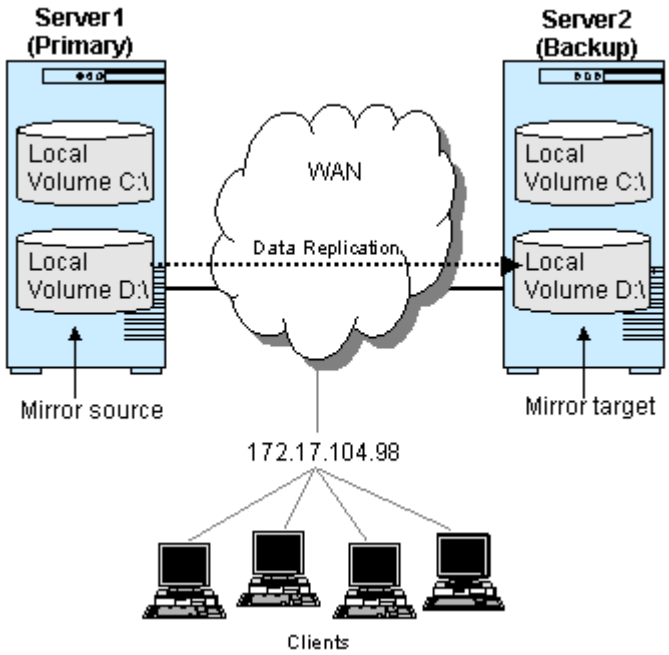
In above diagram, Server3 serves as a backup of two primary Exchange servers, Server1 and Server2. When Server1 fails, LifeKeeper on Server3 will initiate a failover and start Exchange on Server3. However, Server3 will not be able to do failover for Server2 while still running Exchange for failed server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

Configuration Notes:

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

LifeKeeper Data Replication Configuration

This configuration consists of two servers using replicated volumes on each local server in place of shared storage. SteelEye's LKDR 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 SteelEye Technology, Inc.

The procedures for configuring Microsoft Exchange Server with LifeKeeper fall into three major steps. Each of these three steps link to detailed tasks that 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 LifeKeeper Data Replication.

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).
4. For Windows 2000, you should modify the default replication interval by making the following registry changes on all Domain Controllers that are in the domain and in the same Active Directory site of the LifeKeeper protected Exchange Server. This procedure is provided by the Microsoft Knowledge Base article #214678: “How to Modify the Default Intra-Site Domain Controller Replication Interval”.

   On each Domain Controller, set the "Replicator notify pause after modify (secs)" DWORD value to 60 (seconds) and "Replicator notify pause between DSAs (secs)" DWORD value to 15 (seconds) in the following registry key:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters

   Then reboot all the Domain Controllers where these changes have been made.

   This change is not applicable to Windows 2003.

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 :* ____ Transaction Logs Volume:* ____ Database Volume :* ____	The drive letter for the location of any additional Exchange Information Store(s).
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 a 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.

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 necessary changes in the configuration of Exchange database and SMTP. Also change 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. On the **primary** Exchange server, use the Exchange System Manager to rename the default **private** mailbox store and **public** store to remove the server name. For example, rename "Mailbox Store (Server1)" to "Mailbox Store".

   If running Exchange Enterprise Edition, we recommend using the Exchange System Manager to add any additional storage groups and mailbox stores to the configuration before installing Exchange on the backup server. Unused mailbox stores can be set up with the option "Do not mount this store at start-up".

   IMPORTANT: It is required that the names of the Microsoft Exchange storage groups and mailbox stores be the same on both the primary and backup servers. This is also true for *N+1* configurations. All the *N* primary servers storage group names and associated mailbox store names should be the same. If they are not configured with the same name and location, client failover will **not** work correctly and extension of the Exchange hierarchy between primary and backup servers will fail.

b. 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.

c. 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).

d. Change the location of the SMTP system queues to the shared or replicated volume(s) that was specified above 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>

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. Perform the following step to make the necessary changes in the configuration of Exchange on the **backup**. Microsoft Exchange server must be running in order to perform the following steps.
   a. On the **backup** Exchange server, use the Exchange System Manager to rename the default **private** mailbox store and **public** store to remove the server name. For example, rename "Mailbox Store (Server2)" to "Mailbox Store".

      Using Exchange System Manager set up any additional storage groups and mailbox stores to the configuration that were created on the **primary** Exchange server. Unused mailbox stores can be set up with the option "Do not mount this store at start-up".

      IMPORTANT: It is required that the names of the Microsoft Exchange storage groups and mailbox stores be the same on both the primary and backup servers. This is also true for *N+1* configurations. All the *N* primary servers storage group names and associated mailbox store names should be the same. If they are not configured with the same name and location, client failover will **not** work correctly and extension of the Exchange hierarchy between primary and backup servers will fail.
5. 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 LifeKeeper Data Replication software and license key on the primary server. Refer to the *LifeKeeper Data Replication Administration Guide* for details.
2. Install the LifeKeeper Core software, including the license key. Refer to the *LifeKeeper Planning and Installation Guid*e for details.
3. Install the LifeKeeper Microsoft Exchange Server Recovery Kit.
4. Reboot the server.

On the Backup Server

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

Configure LifeKeeper

1. Login to the LifeKeeper GUI.
2. Create the communications paths between the primary and backup servers. See the *Online Product Manual* for details on creating communications paths.

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

3. If using LifeKeeper Data Replication, open the LifeKeeper Data Replication Administrative Window and create your mirror(s) now. **IMPORTANT: Mirrors must be created using IP address rather than computer name.**
4. In LifeKeeper, create your volume and (optional) IP resources and extend them to the backup server. Refer to the *LifeKeeper Online Product Manual* for details on creating these resources.
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.
   e. From the **Propagate Folder Settings** dialog box, select **Replicas**, **Replication message priority**, and **Replication schedule** and click **OK**. Wait for the replica setting to propagate to all subfolders in the tree.
   f. 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 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 **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 Address List**

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=<Your Organization>/cn=addrlists/cn=oabs/cn=Default Offline Address List**), select **All Tasks,** and select **Propagation Settings…** from the list.

g. 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.

h. Set the replica settings for other top level OAB folders under **OFFLINE ADDRESS BOOK** if they contains offline address book.

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.

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

f. Right-click the same folder, select **All Tasks,** and select **Propagation Settings…** from the list.

g. 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.

8. 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 servers 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.

Note: If using virus protection software, see Virus Protection Software in the Troubleshooting section.

9. If your Exchange server is configured with routing group and connectors to work with other Exchange servers or messaging systems, you may need to configure on the backup Exchange server. Based on your setting and network configuration you may have to add the backup Exchange server to your routing 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 **<Your Organization> -> Routing Group -> <Your Routing Group> ->Connectors -> <Your SMTP Connector>** and add name in **General** tab of **Properties** of the connector.
10. 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:
    a. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **DNS**.
    b. Under DNS, expand the applicable DNS server, expand Forward Lookup Zones and then click the applicable zone.
    c. Assign the switchable IP address to the 'A' record of the **primary** server.

    Note: No changes are required in DNS for the backup Exchange Server.
11. 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.
12. Test your Microsoft Exchange Server resources by doing the following:
    a. Perform a manual switchover. See Testing Your Resource Hierarchy for details.
    b. After the switchover, test that messages can be sent externally and internally to other mail recipients.
    c. Verify that SMTP Queue directories have been created on the shared or replicated volume.

Resource Configuration Tasks

Once you have completed the setup tasks as described in the previous section, you are ready to create and extend your Microsoft Exchange Server resource hierarchies.

The following four tasks are described in this guide, as they are unique to a Microsoft Exchange Server resource instance and different for each Recovery Kit.

- 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.

The following tasks are described in the GUI Administrative Tasks section within the *LifeKeeper Online Product Manual*, because they are common tasks with steps that are identical across all Recovery Kits.

- **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.** View or edit the properties of a resource hierarchy on a specific server.

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

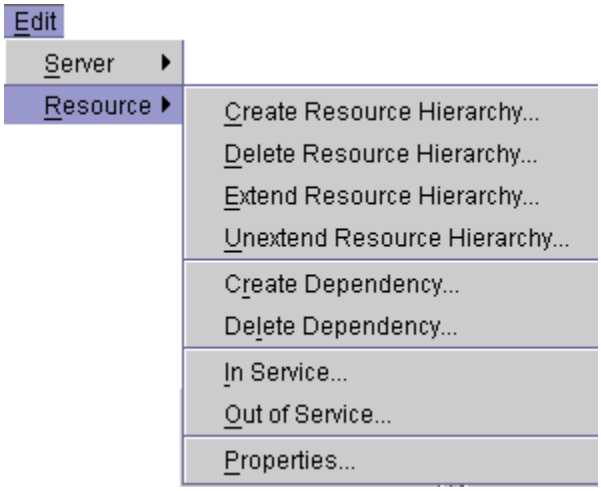
- from the toolbar
- by right clicking on a global resource in the left pane of the status display
- by right clicking on a resource instance in the right pane of the status display

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).

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



The *Create Resource Wizard* 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**
Switchback Type	Choose either *intelligent* or *automatic*. This dictates how the Exchange resource will be switched back to this server when the server comes back up after a failover. If using data replication, choose *intelligent* as the switchback type. **Note:** The switchback type must match that of the dependent resources (IP and volume resources) used by the Exchange resource, or else the create will fail.
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 services 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. Format is: **<username>@<fully qualified domain name>** **Note: This user should be a member of the root domain.**
Enter Microsoft Exchange Server Administrative Password	Enter the password for the Exchange Server Administrator account.
IP Address	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.
Quick Check Interval	Enter the interval (in minutes) between basic checks of the resource's availability. Different values can be specified for each system. The default value is 3 minutes. Value can be between 0 to 10080. Setting interval value to 0 will disable the quick check.
Deep Check Interval	Enter the interval (in minutes) between extensive checks of the resource's availability. This program utilizes Quickcheck for its Deepcheck implementation. Different values can be specified for each system. The default value is 5 minutes. Value can be between 0 to 10080. Setting interval value to 0 will disable the Deep Check.
Local Recovery	Select **Yes** to enable Local Recovery for this resource. Local recovery for a Microsoft Exchange Server resource means that if any of the protected services fail, LifeKeeper will attempt to restart the affected service. If the restart is unsuccessful, then LifeKeeper will failover the Microsoft Exchange Server hierarchy to the backup server.

Extending a Microsoft Exchange Server Hierarchy

This operation can be started from the **Edit** menu, or initiated automatically upon completing the **Create Resource Hierarch**y 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**. If you are familiar with the LifeKeeper **Extend Resource Hierarchy** defaults and want to bypass the prompts for input/confirmation, click **Accept Defaults**.
2. The *Pre-Extend Wizard* will prompt you to enter the following information.
   Note: The first two fields appear only if you initiated the Extend from the **Edit** menu.

Field	Tips
Template Server	Select the server where your Microsoft Exchange Server resource is currently in service.
Tag to Extend	Select the Microsoft Exchange Server resource you wish to extend.
Target Server	Enter or select the server you are extending *to*.
Switchback Type	This dictates how the Microsoft Exchange Server instance will be switched back to this server when it comes back into service after a failover to the backup server. You can choose either intelligent or automatic. The switchback type can be changed later, if desired, from the General tab of the Resource Properties dialog box. **Note:** Remember that the switchback strategy must match that of the dependent resources to be used by the Microsoft Exchange Server resource.
Template Priority	(This field appears only if you did NOT extend directly from the Create function.) Enter a number between 1 and 999 to specify the template server's priority in the cascading failover sequence for this resource. A lower number means a higher priority. LifeKeeper assigns the number “1” to the server on which the hierarchy was created. No two servers can have the same priority for a given resource.
Target Priority	Enter a number between 1 and 999 to specify the target server's priority in the cascading failover sequence for this resource. A lower number means a higher priority. LifeKeeper offers a default of 10 for the first server to which a hierarchy is extended.

3. After receiving the message that the pre-extend checks were successful, click **Next**.
4. Depending upon the hierarchy being extended, LifeKeeper will display a series of information boxes showing the Resource Tags to be extended, 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.

5. Select **Yes** to enable Local Recovery for the Microsoft Exchange Server resource on the target server; otherwise choose **No**.
6. After receiving the message "Hierarchy extend operations completed" click **Finish**.
7. After receiving the message "Hierarchy Verification Finished", click **Done**.

Unextending a Microsoft Exchange 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.

- To remove a resource hierarchy from a single server in the LifeKeeper cluster, do the following:
  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.

Deleting a Microsoft Exchange Server Hierarchy

We recommend that the Microsoft Exchange Server resource hierarchy be in service on the primary before deleting the Microsoft Exchange Server resource hierarchy.

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 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 Exchanger server using the actual computer name (rather than the switchable IP address).

Testing Your Resource 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.

Selecting **Edit**, then **Resource**, then **In Service**. For example, an *In Service* request executed on a backup server causes the application hierarchy to be taken out of service on the primary server and placed in service on the backup server. At this point, the 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.

Microsoft Exchange Server Administration

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

Microsoft Exchange Server Administration Guidelines

You can reduce the number of errors you encounter when administering your Microsoft Exchange Server resource hierarchy if you follow these administrative guidelines:

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 whichever server is currently running the Exchange instance.

Reserve Volumes for Exclusive Use by Microsoft Exchange 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 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.

Automatic LifeKeeper Restore 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 is not reliable, it is highly recommended that you disable automatic failover. This eliminates possibilities of false failover of Microsoft Exchange Server.

The **SetExchRestore** utility displays the current recovery setting on that system, and allows the administrator to change the setting to ENABLED or DISABLED. The **SetExchRestore** utility is located in the *<%LKROOT%>\admin\kit\msexch\bin* folder, where *%LKROOT%* is the root of the LifeKeeper installation path. To run the **SetExchRestore** utility, enter the following from a command prompt:

cscript /nologo SetExchRestore.vbs <TagName>

The <*TagName*> input argument is the LifeKeeper tag name associated with the Microsoft Exchange Server resource. A pop-up dialog is provided. After displaying the current recovery setting, it will permit the administrator to immediately exit, or change the setting.

To invoke the **SetExchRestore** utility without generating pop-up dialogs, use the following options:

cscript /nologo SetExchRestore.vbs <TagName> [-e | -d]

The **-e** option enables automatic recovery of the Microsoft Exchange Server resource on the local server. The **-d** option disables automatic recovery of the Microsoft Exchange Server resource on the local server. When either the **-e** or **-d** options are used, pop-up dialogs are not generated.

Disabling Automatic LifeKeeper Restore

To disable LifeKeeper recovery for the Microsoft Exchange Server resource, go to the server where recovery is to be disabled and use the LifeKeeper supplied **SetExchRestore** utility to change the recovery capability for the server and run the following from a command prompt:

cscript /nologo SetExchRestore.vbs <TagName> -d

Enabling Automatic LifeKeeper Restore

To re-enable LifeKeeper recovery for the Microsoft Exchange Server resource, go to the server where recovery was disabled and use the LifeKeeper supplied **SetExchRestore** utility to change the recovery capability for the server and run the following the following from a command prompt:

cscript /nologo SetExchRestore.vbs <TagName> -e

Special Considerations

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

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.

Running Third-party Software with Exchange

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 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.

Troubleshooting

Microsoft Exchange Server

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.

Extend Of Exchange Resource Problems

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

```
Error - Database configuration on Microsoft Exchange Servers
<primary server> and <backup server> does not match. It is
required that the names of the Exchange storage groups and
mailbox stores be the same on both the servers. The location
of the transaction and system logs, log file prefix, and
location of exchange databases must also be the same on both
the Exchange servers.
```

Using Microsoft Exchange System Manager, verify that the Storage Groups, Mailbox Stores, and Public Stores have exactly the same names on both the primary and backup Exchange servers. Correct any inconsistencies and retry the Extend operation.

The LifeKeeper Microsoft Exchange Recovery Kit installs a command line utility **ValidateExDBConfig.exe**, which can be used to validate the configuration on the primary and backup Exchange servers before extending the hierarchy. This utility is installed to $LKROOT/bin, where $LKROOT is the LifeKeeper installation path (C:/LK by default).

If you are having a problem extending the LifeKeeper Exchange hierarchy, run this utility on the backup server where the Exchange hierarchy is being extended. From a command prompt change to the $LKROOT/bin directory and run the following command:

ValidateExDBConfig.exe <UserName@FQDN> <Password> <Primary Exchange Server Name> <Local Exchange Server Name>

Note: <UserName@FQDN> should be the fully qualified domain Exchange administrator account used to install Microsoft Exchange Server.

This utility will print the configurations of the all the storage groups and mail stores for both the primary and backup Exchange servers. It will also print the name of each storage group and/or mail store whose configuration does not match.

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.

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 failover

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 or a single user to 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 the users 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 all the domain controllers of that domain available. To run the **LKMoveEXUsers** utility, enter the following from a command prompt:

LKMoveExUsers.exe <UserName@FQDN> <Password> <Local Exchange Server Name> <Failed Exchange Server Name> <<-d <domain name> | -u <user 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 -d child.rootdomain.com

An example for moving one user (User1) 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 -u CN=User1,CN=Users,DC=Child,DC=rootdomain,DC=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.

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 DistingushedName format as it appears in the log file) to move all users or an individual user.

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
<system name>. 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.

Virus Protection Software

If you are running third party virus protection software, which has dependencies on Microsoft Exchange services, you must also protect the virus protection service as an optional service under LifeKeeper. Failure to do so will prevent the Microsoft Exchange Server resource from going out of service in the event of a manual switchover. This service dependency will prevent the Microsoft Exchange Server services from stopping, which prevents LifeKeeper from failing over the Microsoft Exchange Server resource.

Perform the following steps on the primary Microsoft Exchange server:

1. Stop the virus protection service which has dependencies on the Microsoft Exchange service.
2. Set the startup mode for the virus protection service to Manual.
3. After creating your Microsoft Exchange resource in LifeKeeper, edit the following registry key to add the virus protection service to the list of optional services to be protected by LifeKeeper:

   HKLM\SOFTWARE\SteelEye\LifeKeeper\RK\msexch\<Tag Name>

   Add the virus protection service name to the end of the list of "OptProServices" registry value.

   Note: **Service names cannot contain spaces.**
4. On the backup server, set the startup mode for the virus protection service to Manual.

5. After extending Microsoft Exchange Server resource to backup server, verify that the virus protection service name is in the list of protected optional services by looking at the registry key from step 3.

Example

If you are using McAfee Groupshield, add **AVEXch32Service** to the "OptProServices" registry value under the registry entry as follows:

```
HKLM\SOFTWARE\SteelEye\LifeKeeper\RK\msexch\MSEx2k.0
  OptProServices  REG_SZ MSExchangeMTA IMAP4Svc POP3Svc AVExch32Service
```

For additional information about running virus protection software in a LifeKeeper environment, contact SteelEye support at support@steeleye.com, or call:

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

+1-803-461-3970 (International)

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.

Appendix: Installing Software Updates in a LifeKeeper Environment

Windows Software Update Procedure

To install Windows software updates, use the following procedure to minimize downtime to your Microsoft Exchange Server:

1. If using LifeKeeper with LifeKeeper Data Replication (LKDR), pause the mirror(s) for all LifeKeeper protected volumes.
2. Install Windows software updates on the backup server.
3. Reboot the backup server, if required.
4. If using LifeKeeper with LKDR, after 3 - 4 minutes, "Continue" the mirror(s) (from the primary server) and wait for the mirror(s) to become “Mirroring”.
5. Make sure that on the primary server switchback type is "Do Not Switchover Resources".
6. Install software updates on the primary server.
7. Reboot the primary server, if required. LifeKeeper will automatically bring the Microsoft Exchange Server resource back in-service on the primary server.

Exchange Software Update Procedure

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

1. Install Microsoft Exchange software updates on the primary server where Microsoft Exchange Server is active.

2. Make sure that the primary server switchback type is "Do Not Switchover Resources". If using LifeKeeper with LifeKeeper Data Replication (LKDR), verify that the mirror(s) are in the “Mirroring” state.

3. Reboot the primary server, if required.

4. Once the Microsoft Exchange Server resource is active on the primary server, perform a manual switchover to the backup server. **Note:** If using LifeKeeper with LifeKeeper Data Replication (LKDR), mirror(s) must be in the “Mirroring” state prior to performing a manual switchover.

5. Once Microsoft Exchange resource is active on the backup server, install Microsoft Exchange software updates.

6. Make sure that the backup server switch back type is "Do Not Switchover Resources". If using LifeKeeper with LifeKeeper Data Replication (LKDR), verify that the mirror(s) are in the “Mirroring” state.

7. Reboot the backup server, if required.
8. The Microsoft Exchange resource can be brought back in-service on the original primary at some scheduled time by performing a manual switchover. **Note:** If using LifeKeeper with

LifeKeeper Data Replication (LKDR), the mirror(s) must be in the “Mirroring” state prior to performing a manual switchover.