

# **MiCollab Advanced Messaging Neverfail**

## **Integration & Administration Guide**

For version 6.1 and above

## Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

## Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at [legal@mitel.com](mailto:legal@mitel.com) for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2016, Mitel Networks Corporation

All rights reserved

# Contents

<b>Preface</b>	<b>5</b>
References	5
Documentation	5
Documentation Updates	6
Help	6
Document Conventions	6
Frequently Used Terms	7
Purchasing Neverfail for MiCollab AM	7
<b>Overview</b>	<b>9</b>
Neverfail Heartbeat	9
Neverfail Replicator	10
Neverfail TCP/IP Packet Filtering	10
Critical Application Considerations	10
<b>MiCollab AM with Neverfail Architecture</b>	<b>12</b>
<b>The Neverfail Telephony Server Plug-In</b>	<b>18</b>
<b>Neverfail SCOPE</b>	<b>19</b>
<b>Before You Begin</b>	<b>20</b>
<b>Critical Application Considerations</b>	<b>23</b>
<b>Planning the LAN Connections for Neverfail</b>	<b>24</b>
<b>Preparing for the Neverfail Installation</b>	<b>27</b>
<b>Installing Neverfail Software on a Physical or Hyper-V Windows Server 2008 / 2012</b>	<b>30</b>
<b>Installing Neverfail Software on a VMware Virtual Windows Server 2008 / 2012</b>	<b>32</b>
<b>Creating a Static IP Address with Neverfail</b>	<b>34</b>
<b>Customizing and Testing the Neverfail Installation</b>	<b>37</b>
<b>Maintaining the Neverfail Cluster</b>	<b>38</b>
Administering MiCollab AM System Servers in a Neverfail Environment	38
Maintaining Passive Neverfail Servers	39

<b>Patching MiCollab AM Software in a Neverfail Cluster</b>	<b>40</b>
<b>Installing MiCollab AM Software Updates and Upgrading MiCollab AM from a Previous Version</b>	<b>44</b>
<b>Upgrading Neverfail Heartbeat from V6.5.2 to V6.7.7</b>	<b>48</b>
Uninstalling Previous Versions of Neverfail SCOPE	48
Installing SCOPE version 5.3.0	48
Upgrading to Neverfail Heartbeat version 6.7.7	49
Installing the Telephony Server Plug in for MiCollab AM version 6.1	51
Completing the Neverfail and MiCollab AM Upgrade Process	53
<b>Adding a Tertiary Server</b>	<b>54</b>
<b>Split-Brain Avoidance</b>	<b>55</b>
<b>Appendix A – Replacing a Server</b>	<b>56</b>
<b>Appendix B – Tuning</b>	<b>60</b>

# Preface

This document is written for Mitel certified MiCollab Advanced Messaging (MiCollab AM) technicians and administrators who are experienced with MiCollab AM and are familiar with its procedures and terminology. This book assumes you are familiar with MiCollab AM and the Microsoft Windows® operating system, and have a working knowledge of TCP/IP protocols, as well as a working knowledge of domain administration in a Windows Server environment, including Active Directory.

This installation guide applies to the MiCollab AM version 6.1 and above, the Neverfail Heartbeat and Replicator software version 6.7.7, and the Neverfail Telephony Server Plug-in 201.8.7.1. It consists of the following parts:

- An introduction to Neverfail Replicator and its features
- An introduction to Neverfail Heartbeat and its features
- Information on the interaction between MiCollab AM and Neverfail
- An introduction to Neverfail SCOPE
- Information on planning a Neverfail installation with MiCollab AM
- Tips and Instructions on how to install the Neverfail Heartbeat and Replication software
- Tips and Instructions on how to install the Neverfail Telephony Server Plug-In for MiCollab AM
- Information on how to configure Neverfail Heartbeat for MiCollab AM
- Tips and Instructions on how to maintain a MiCollab AM System Server in a Neverfail cluster
- Instructions on how to upgrade or update MiCollab AM in a Neverfail environment
- Instructions on how to upgrade from Neverfail v6.5.2 to v6.7.7

## References

A catalog of technical documentation is included on the MiCollab AM Installation Media. If you are installing any advanced applications, such as Networking and Fax Server applications, you should refer to the appropriate technical documentation for application and installation information.

## Documentation

The technical documentation is produced in the PDF format and requires the PDF reader to view it. The documentation set for this MiCollab AM includes the following documents and resources:

- **Developer Resources.** Contains programming guides and API references for developers for integrating the server clients and web applications with MiCollab AM.
- **Integration Technical Notes (ITN).** Contains a set of guides that describe the integration methods and instructions for a variety of phone systems to work with MiCollab AM. The ITNs are generally used by resellers or administrators who are experienced with MiCollab AM and familiar with the integration procedures and terminology.

- **Quick Reference Card (QRC).** Contains shortcuts and quick instructions telling subscribers how to access and use the messaging system.
- **Server Documentation.** Available as a PDF only. Contains administrative guides for administrators about installing, configuring, and administering the messaging system, and user guides for subscribers about accessing the messaging system and checking and sending messages.
- **Spare Parts Documentation.** Contains a set of guides that describe the instructions for installing and configuring hardware parts to work with MiCollab AM. These documents are written for Mitel certified MiCollab AM technicians who are experienced with MiCollab AM and familiar with the procedures and terminology.
- **Software Release Notice (SRN).** This notice introduces the new features, capabilities, and hardware/software requirements for the corresponding MiCollab AM version.

## Documentation Updates

Documentation updates may be available from the following sources:

- Mitel certified technicians can view or download documents and program files from our partner web site: [connect.mitel.com/connect](http://connect.mitel.com/connect)

## Help

The primary source of information about MiCollab AM is the online help available within any of its administrative utilities. You can access **Help** as follows:

- Click the **Help** button in the dialog box or window in which you are working
- Press the **F1** key at any time.

## Document Conventions

The following conventions are used in this document:

- **Key Names.** Names of keys on the keyboard are shown in a box.

Example: **Enter**

When two keys must be pressed simultaneously, they are joined by a + sign.

Example: **Alt** + **Tab**

- **Reference to Document.** *Italics* fonts can also signify the titles of other documents.

Example: Refer to *System Installation Guide*.

- **UI Element Names.** Names of UI elements such as dialog windows, screens, menu items, tabs, buttons, icons, etc. are shown in bold.

Example: On the **Startup** screen, click the **Start** icon.

- **User Input.** Information required to be typed is shown in italics.  
| **Example:** Type the password *voicemail*.
- **Warning, Caution, Important, and Notes.** Text for the contents that require attention are shown as follows:

**WARNING** A warning paragraph advises you of circumstances that can result in the loss of data, harm to the system server platform, or personal harm.

**CAUTION** Failure to follow these recommendations can result in unauthorized access to the system and consequent loss of data.

**IMPORTANT** An important paragraph gives decision-making information or informs you of the order in which tasks need to be completed.

**NOTE** A note gives additional information, provides an explanation, or indicates an exception to the information in the preceding text.

## Frequently Used Terms

Table 1. Frequently Used Terms

Terms	Description
System Server	<p>Term refers to an organization's computer platform(s) that have MiCollab AM software installed and handles the core system functions such as storing messages, database.</p> <p>It can also refer generically to the System Server platform, the Call Server platform, or both. The term is most often used to describe a software or hardware installation or configuration practice where the role of the server platform is not specifically expressed.</p>
Call Server	<p>Term refers to an organization's computer platforms that have MiCollab AM software installed and serve as the interface to the system (PBX). The Call Server(s) interface with the System Server for the purpose of accessing messages, and database.</p>

## Purchasing Neverfail for MiCollab AM

The Neverfail Heartbeat and Replicator version 6.7.7 software for MiCollab AM is purchased through Mitel. The Neverfail software is a MiCollab AM licensed key attribute of Mitel and the System Server running in a Neverfail cluster must have Neverfail enabled on the license key.

In addition, you must be an Mitel certified technician with certification on the Neverfail products to install Neverfail on a MiCollab AM system. If you are not certified, you must make arrangements with Mitel Professional Services to assist in the installation process. The system must be covered with an active Mitel Software Maintenance Program contract. For more information on Software Maintenance Program products contact your Mitel sales representative or send an email to [connect.mitel.com/connect](mailto:connect.mitel.com/connect).

Neverfail license and login account information to the Neverfail Extranet website are sent to Mitel Professional Services and the e-mail account of the Mitel dealer's designated individual managing the site installation.

**NOTE** Do not contact Neverfail Technical Support for assistance with a Neverfail installation, configuration, or for troubleshooting purposes. They cannot assist you. Please call Mitel Technical Support for assistance.

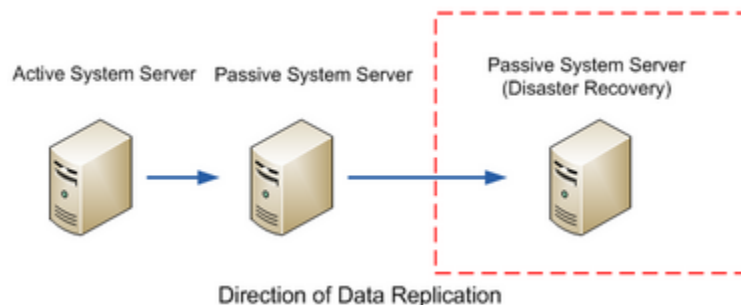


# Overview

The Neverfail Replicator and Heartbeat software runs on MiCollab AM System Servers to provide a High Availability and Disaster Recovery solution. System Servers are configured as a pair or a trio of servers that communicate with each other through network connections, referred to as Neverfail Heartbeat channels. MiCollab AM with Neverfail supports three types of Neverfail configurations.

- **High Availability** — the Primary and Secondary System Servers share the same IP address on the same LAN. In this configuration, the Secondary System Server performs an automatic switchover in the event the Primary System Server fails.
- **Disaster Recovery** — the Primary and Secondary System Servers do not share the same IP address. Making the Secondary server the active server is a manual procedure. The Secondary System Server is typically located on a WAN, at a remote disaster ready site.
- **High Availability and Disaster Recovery** — the Primary and Secondary System Servers share the same IP address on the same LAN. In this configuration, the Secondary System Server performs an automatic switchover in the event the Primary System Server fails. Making the Tertiary Disaster Recovery System Server the active server is a manual procedure. The Disaster Recovery System Server is typically located on a WAN, at a remote disaster ready site.

Each MiCollab AM System Server in a Neverfail cluster is assigned an identity of Primary, Secondary, or Tertiary. The identity of the server never changes, but the role of the server can change from Active to Passive. One server has the physical role of Active, the other servers remain in a Passive, yet ready state. The active server provides all System Server Services and applications to the MiCollab AM environment. It is also the replication source for all of the data to the passive server. The passive High Availability server is the replication source to the Disaster Recovery server, if installed.



## Neverfail Heartbeat

The Neverfail Heartbeat software monitors the Public LAN channel on the active server, the Neverfail LAN channels between the servers in the Neverfail cluster, and the protected programs running on the active server. When Neverfail detects a loss of communication with the active server, or the failure of a protected program on the active server, an automatic switchover to the passive server executes. This automatically swaps server roles; the once active server becomes the passive server and the once passive server becomes the active server. MiCollab AM automatically shuts down on the former, active server, and

automatically starts on the former passive, now active server. Once the problem is determined and corrected, the administrator can return the server roles to their original state, if desired.

**IMPORTANT** Switchover between the High Availability active and passive High Availability pair is automatic. Making the Disaster Recovery server the active server is a manual procedure.

## Neverfail Replicator

The Neverfail Replicator Service provides real time replication of all MiCollab AM application data, database changes, and registry changes from the active server to the passive servers in a daisy-chain fashion. This real time replication keeps the passive servers in a constant state of readiness to assume the active server role.

Call Servers are unaware that the System Server has changed platforms due to a managed, transparent automatic switchover through the Neverfail software. Once the System Server switches from the Primary to the Secondary server, the Call Servers begin replicating with the System Server on the server platform now playing the active role.

## Neverfail TCP/IP Packet Filtering

Neverfail installs a proprietary TCP/IP packet filter driver on all of the servers in the cluster during the installation process. The packet filter is applied to the Public network connection of each passive server and is used to mask the primary or Public TCP/IP address of the server. When a passive server becomes active, the packet filter is reset to a pass-through mode and the server now playing the active role becomes visible on the network with the TCP/IP address of the Primary server.

**IMPORTANT** The Neverfail packet filter always hides the identity of the passive servers from the Public network.

## Critical Application Considerations

- All MiCollab AM services that the site intends to protect *must* be **Running** or **set for "Automatic" startup** at the time the plugin is installed; otherwise they will not be protected. This is by design of the Neverfail Heartbeat application.

**IMPORTANT** This includes any MiCollab AM application services installed on the same machine (some may not be directly under MiCollab AM server) such as:

- MiCollab AM Digital Networking
- MiCollab AM UConnect
- MiCollab AM SIP Routing Manager
- MiCollab AM Integration Client Access

To accomplish this, configure the system with it in the state at which it should be protected with all services running that are to be protected and then install the plugin.

- Sites using Exchange 2010 or greater, must configure email profiles *before* installing the plugin in order to allow Mitel configuration and setup of the EWS service to run under MiCollab AM.
- Sites using Lync Presence Profiles must configure them, and meet the installation requirements noted in the *Availability Administration Guide*, before the plugin is installed for MiCollab AM UCMA service to run and be protected under MiCollab AM.

**NOTE** Adding any Exchange Email Server or Lync/Skype profiles after the plugin is installed will require that the plugin be removed and re-installed for Neverfail to protect these dependent profiles.

# MiCollab AM with Neverfail Architecture

MiCollab AM system administration is performed on the System Server. The System Server contains the system database and distributes a replicated database to the Call Servers through the network. Call Servers work independently from each other and do not require the System Server to carry on with basic call processing. Call Servers, configured as redundant to each other, or as unique Call Servers that serve particular groups of telephone systems, departments or facilities provide for high availability and flexibility within the system. Redundant Call Servers may be actively taking calls or they may be idle in a warm stand-by mode. In either case, they are synchronized and replicating with the active System Server at all times. In a warm stand-by mode the Call Servers require a Call Server license only. They do not require Line licenses until they are active, online, and taking calls.

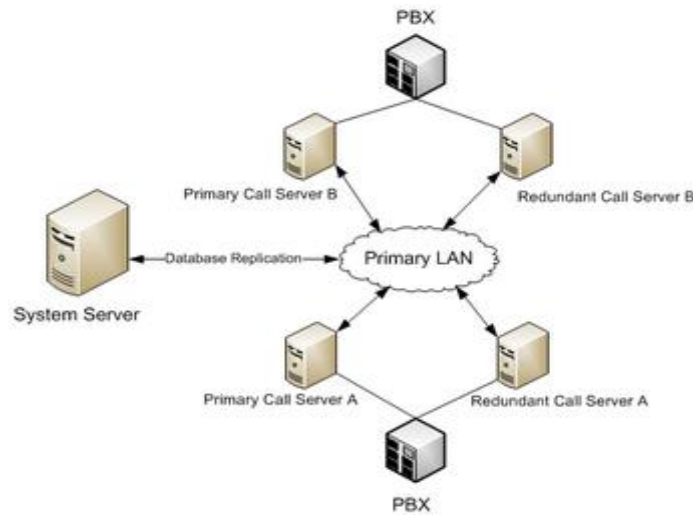


Figure 1. Multi-box configuration without Neverfail

When Neverfail is deployed in High Availability configuration, the System Server also becomes redundant, providing high availability to the System Servers.

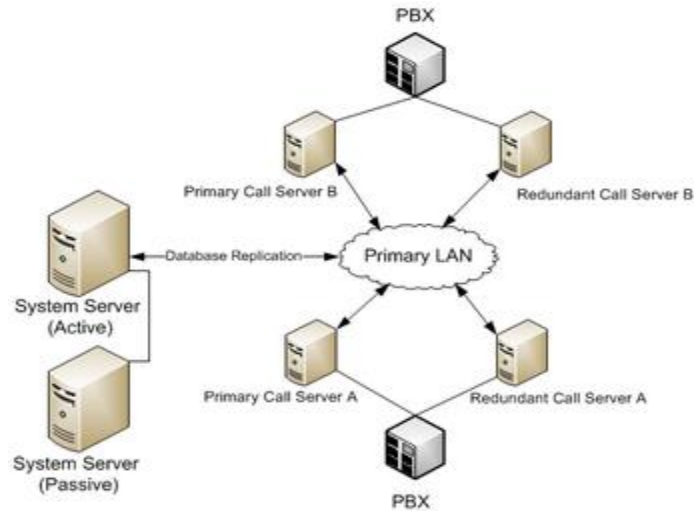


Figure 2. Multi-box configuration with Neverfail High Availability

When Neverfail is deployed in a Disaster Recovery configuration, the System Server is prepared for disaster recovery.

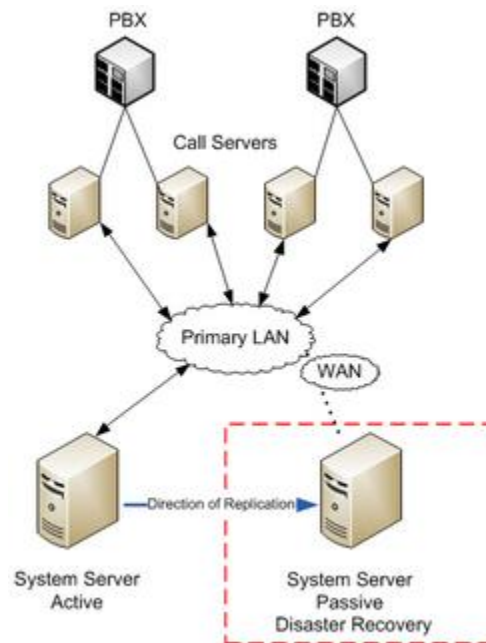


Figure 3. Disaster Recovery Cluster Configuration

When Neverfail is deployed in a High Availability and Disaster Recovery configuration, the System Server is redundant, providing high availability and disaster recovery to the System Servers.

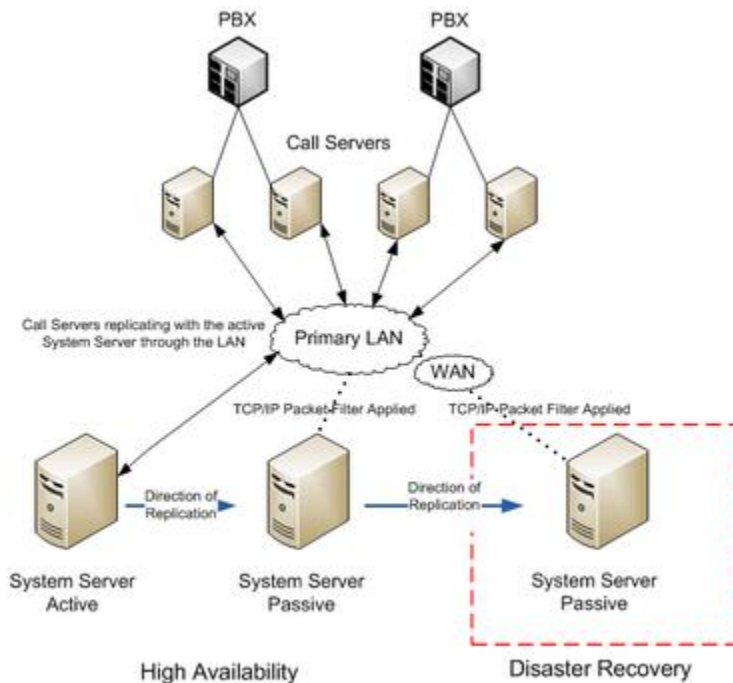


Figure 4. High Availability and Disaster Recovery Cluster Configuration

A set of redundant Call Servers connected to the Tertiary System Server at the disaster recovery site provide total system redundancy in the event of a major disaster to the enterprise. These Call Servers may be actively taking calls or they may be idle until the Tertiary server is made the active server. In either case, they are synchronized and replicating with the active System Server at all times.

Call Servers require both Call Services and Line licenses when they are actively processing calls. When idle, in a warm stand-by mode replicating with the System Server, they require only a Call Services license. If a disaster occurs, the Call Servers at the main site are down, and Line licenses are available for use with the System Server at the disaster recovery site.

**NOTE** Call Servers that are replicating with the System Server but have no line licenses available display a line status of *Not Licensed*.

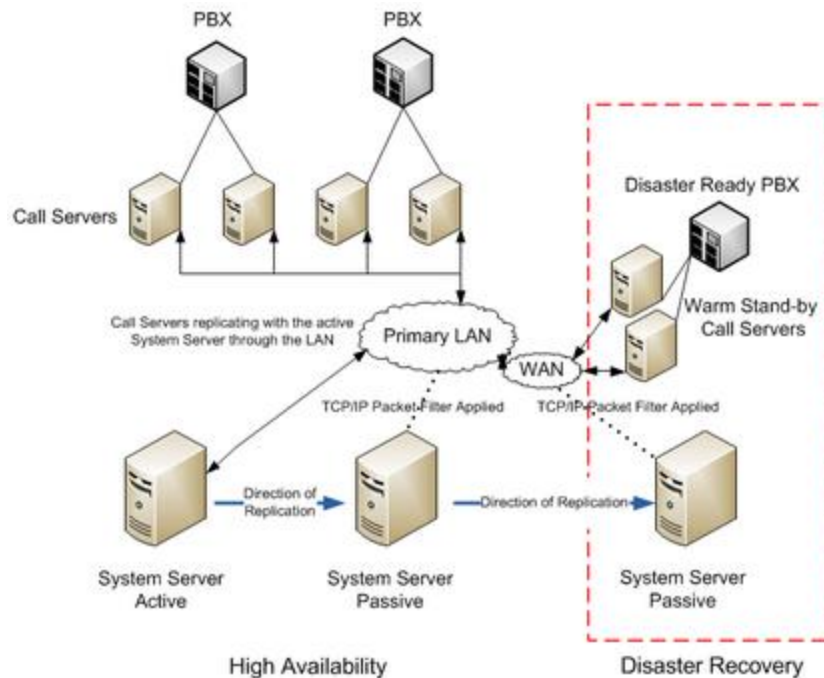


Figure 5. Disaster Recovery

Call Services or Line licenses are not required if Call Servers are installed at the disaster recovery site but not synchronized with the System Server. These Call Servers may be connected to a disaster ready telephone system but are not processing any calls or communicating with the System Server. In the event of a total site disaster, the Call Servers connect to the Tertiary System Server using the available licenses of the active (Tertiary) System Server. These Call Servers require human intervention to become synchronized and to begin replicating with the Tertiary System Server.

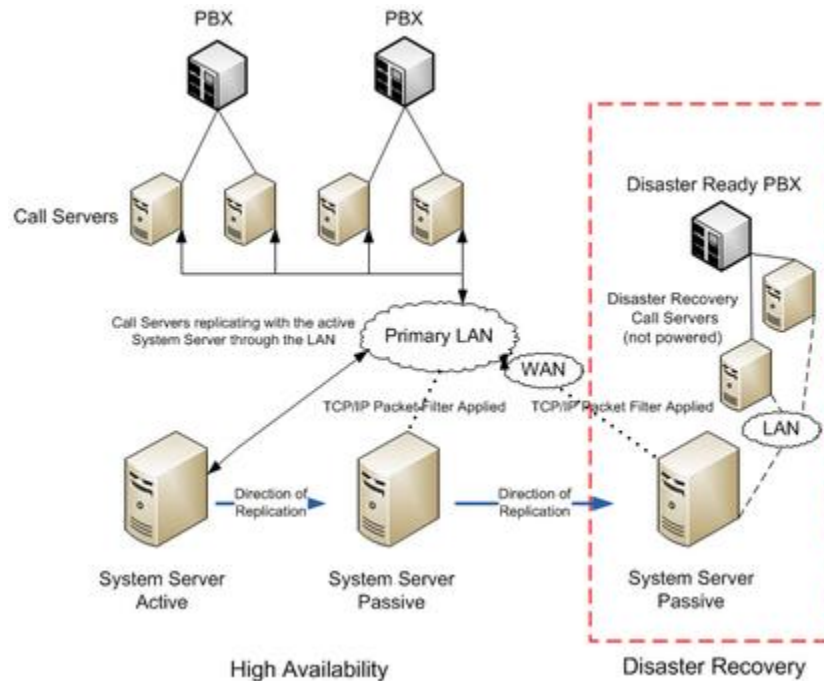


Figure 6. Disaster Recovery

The following illustration provides an overview of a full MiCollab AM system architecture with Neverfail High Availability and Disaster Recovery cluster deployed.

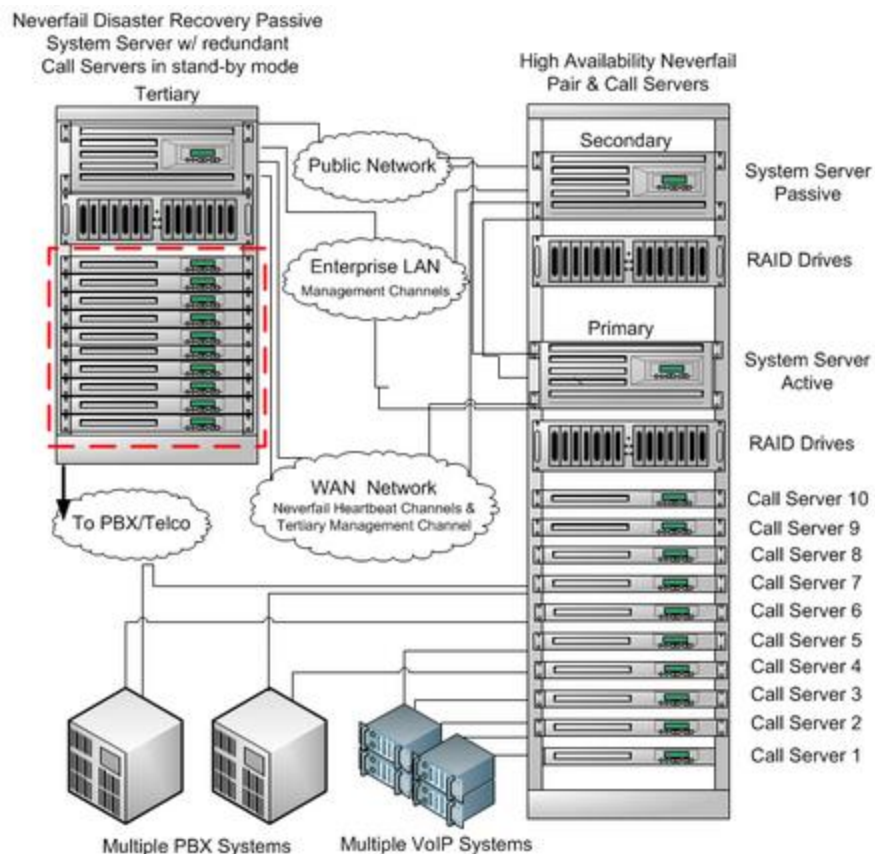


Figure 7. Neverfail Disaster Recovery

With 6.1 SU1, the System Server can now provide Call Services in a Stand-Alone configuration. Neverfail can be deployed in either High Availability, Disaster Recovery or both configurations.

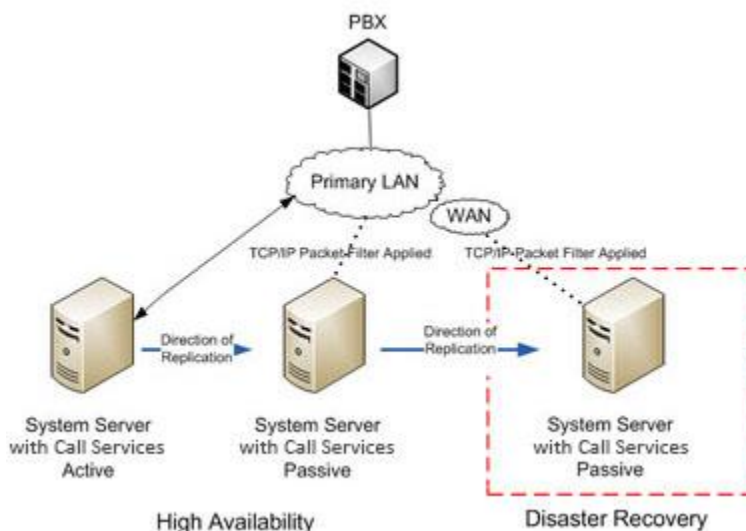


Figure 8. Stand-Alone System Server with Call Services



When Call Services are added to the System Servers, only IP Integrations where MiCollab AM registers with the PBX or where the PBX supports multiple End Points are supported. The Switch, Switch Section and Integration must be configured identically on all System Servers with Call Services.

When using a Disaster Recovery (Tertiary) server, the IP address of the Tertiary server is typically not the same as that of the High Availability servers. In order for the Call Services to continue to function when the Tertiary server is the Active server, it's important to use a SIP parser qualifier string in the Integration Options that is not the local IP address. For example, if your hunt number is 5000 then use "5000@" as your SIP parser qualifier string.

# The Neverfail Telephony Server Plug-In

The Neverfail Group created a Plug-in software module designed specifically for MiCollab AM. The Plug-in enhances the ability of Neverfail to monitor the availability, file, replication, and performance of the active System Server.

**NOTE** Please refer to the Neverfail knowledge base for complete information on the Telephony Server Plug-in at: [extranet.neverfailgroup.com/aspnet/pages/kb/Kb.aspx?id=1627](http://extranet.neverfailgroup.com/aspnet/pages/kb/Kb.aspx?id=1627)

The Telephony Server Plug-in monitors the MySQLBackup and MySQLCore Services and performs pre-configured actions when these processes fail. These actions are configured from the Application tab of the Neverfail Heartbeat Management Client.

Once installed, the Telephony Server Plug-in determines the location of the Primary and Secondary server's application, database, and log files. These files are referred to as protected; their contents are synchronized, and subsequent updates to the database are replicated to the passive servers.

In addition to the inherent features of Neverfail, the Telephony Server Plug-in performs the following tasks related to MiCollab AM:

- Automatic file filter discovery and protection
- Automatic protected Services discovery
- Automatic registry filter discovery and registry key protection
- Automatic switchover and database file protection

When an automatic switchover occurs, all running Services on the active server are stopped and updates to the MySQL Server databases are terminated. Once the passive server becomes the active server and assumes the role as the active server, all instances of MySQL Server are started and all Services including MiCollab AM are started.

**IMPORTANT** The Neverfail software and Telephony Server Plug-in do not replicate MiCollab AM software or MiCollab AM software updates to the passive servers. Software installation and updates must be performed at each individual server. To install or update MiCollab AM software the Neverfail Heartbeat must first be stopped.

# Neverfail SCOPE

Neverfail SCOPE is a software tool that provides a comprehensive analysis of the existing servers prior to the Neverfail High Availability and Disaster Recovery installation and can monitor the server performance while the Neverfail Heartbeat is running. Neverfail SCOPE diagnoses the health and reliability of the server environment and measures the available network bandwidth between the servers.

Neverfail Group recommends that the Neverfail SCOPE diagnostic tool run on the Primary, Secondary and Tertiary servers for a 24-hour period. The data collected during this analysis is gathered into a .cab file that must be uploaded to the Neverfail Extranet website for analysis. The report generated from the uploaded file determines the suitability of the server environment for a successful implementation of Neverfail.

Once the file analysis is uploaded to the Extranet website, the analysis completes, and you have the required SCOPE files, contact Mitel Professional Services or Technical Support. Technical Support contacts Neverfail with the information, and Neverfail generates the license key for the installation which is e-mailed to you for the site installation. The license key is required during the Neverfail installation process.

**NOTE** Please refer to the Neverfail document, *Getting Started with Neverfail SCOPE v5.3.0* for more information on installing and using the SCOPE Data Collector Service. This online book is found on the Neverfail Extranet website or the MiCollab AM Installation Media.

# Before You Begin

When using physical servers in the Neverfail cluster, they must be installed and the required network connections must be configured and active on each server in the cluster before you begin the Neverfail software installation. The server platforms must meet or exceed both the Mitel and Neverfail hardware requirements.

When using virtual servers in the Neverfail cluster, the Secondary/Tertiary servers will be clones created from the Primary virtual server. Each virtual machine used in the Virtual to Virtual pair must be on a separate ESX host to guard against failure at the host level.

Mitel recommends that the hardware platforms serving as Primary, Secondary and Tertiary servers be the same make and model type. For more information refer to the *Neverfail Heartbeat and Neverfail Replicator Windows Server 2008 Installation - Physical Server v6.7.0*, *Neverfail Heartbeat and Neverfail Replicator Windows Server 2008 Installation - Virtual Server v6.7.0*, *Neverfail Heartbeat and Neverfail Replicator Windows Server 2012 Installation - Physical Server v6.7.0*, or *Neverfail Heartbeat and Neverfail Replicator Windows Server 2012 Installation - Virtual Server v6.7.0*.

For information on the Neverfail hardware requirements, refer to the *Software Release Notice* for Mitel hardware requirements and platform recommendations.

## Secondary Server

The Secondary server in a P2P architecture must meet specific hardware and software requirements to ensure adequate performance when the server assumes the active role.

## Hardware

The Secondary server in a P2P architecture must meet the following hardware requirements:

- Hardware must be equivalent to the Primary server:
  - Similar CPU (must have same multi-processor configuration as the Primary)
  - Similar memory
- OR:
  - Hardware meets minimum CPU (must have same multi-processor configuration as the Primary) and memory requirements for the MiCollab AM system size

Note on the CPU:

*The CPU multi-server configuration must be the same as for the Primary server: If Primary server has a single CPU, the Secondary must have a single CPU; if the Primary server has more than one CPU, the Secondary must have more than one CPU.*

*For the multiple CPU case, the number of CPUs does not have to be equal between the Primary and Secondary servers.*

- An identical number of NICs to the Primary server
  - Minimum two NICs if no Tertiary server exists
  - Minimum three NICs if Tertiary server exists
- Drive letters must match the Primary server
- The amount of available disk space on each partition should be equal to or greater than that on the equivalent partition on the Primary server
- ACPI compliance must match the Primary server

## Software

The Secondary server in a P2P architecture must meet the following software requirements:

- The OS version and Service Pack version must match the Primary server
- The OS Updates installed must match the Primary Server
- The OS must be installed to same drive letter and directory as on the Primary server
- The machine name must be different from the Primary server prior to installing Neverfail Heartbeat
- Set up in a Workgroup prior to installing Neverfail Heartbeat
- The System Date, Time, and Time Zone must be consistent with Primary server

## Tertiary Server

The Tertiary server in a P2P architecture must meet specific hardware and software requirements to ensure adequate performance when the server assumes the active role.

## Hardware

The Tertiary server in a P2P architecture must meet the following hardware requirements:

- Hardware must be equivalent to the Primary server:
  - Similar CPU
  - Similar memory

OR:

- Hardware meets minimum CPU and memory requirements for the MiCollab AM system size
- A minimum of three NICs
- Drive letters must match the Primary server
- The amount of available disk space on each partition should be equal to or greater than that on the equivalent partition on the Primary server
- ACPI compliance must match the Primary server

## Software

The Tertiary server in P2P architecture must meet the following software requirements:

- The OS version and Service Pack version must match the Primary server
- The OS Updates installed must match the Primary Server
- The OS must be installed to same drive letter and directory as on the Primary server
- The Machine name must be different from the Primary and Secondary server prior to installing Neverfail Heartbeat
- Set up in a Workgroup prior to installing Neverfail Heartbeat
- System Date / Time and Time Zone must be consistent with Primary server

# Critical Application Considerations

Known limitations or conditions that affect the Neverfail installation or upgrade are listed here. General recommendations are provided when ways to avoid these limitations exist.

- During the Neverfail Heartbeat software installation, Neverfail Setup changes the registry key `HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange` to a value of 1.

This change prevents the system from forcing a password change at the default interval (30 days). However, if the domain administrator has applied Microsoft's Best Practices and secured the domain, the "Maximum Machine Account Password Age" policy is enabled. This Active Directory Domain policy overrides the Neverfail Setup registry change of the local computer policy and resets the registry key value to "0."

To resolve this issue, create a separate OU (Organizational Unit) for the Neverfail servers. Follow Microsoft's Best Practices to create the location of the OU. Once the OU is created, create a GPO (Group Policy Object) to configure the "Maximum Machine Account Password Age" policy as disabled. For more information, refer to the Neverfail Knowledge Base article, *Configuring the Maximum Machine Account Password Age*.

- Cloning or Restoring to Secondary and Tertiary servers may require re-activation of the Windows Server 2008 R2 with Service Pack 1 or Windows Server 2012 R2 license during the installation of the Neverfail Heartbeat if the Primary server hardware differs from that of the Secondary or Tertiary server hardware. The differences may be minor and include:
  - The amount of RAM
  - NIC cards or other PCI/PCIe devices in different slots
  - The number of previous hardware changes the server has had
  - Differing physical system disk serial numbers and assignments
  - Differing MAC addresses of network interface hardware

You must perform the activation process while the server is in the "Active" role during acceptance testing, or by telephone with Microsoft. For more information, refer to the Neverfail Knowledge Base article #78, *Restoring to Secondary or Tertiary may Require Reactivation of Windows License*.

# Planning the LAN Connections for Neverfail

Each server in the Neverfail cluster must have a minimum of two Ethernet network interface cards (NIC) in a High Availability pair configuration and three NIC interfaces in a Tertiary disaster recovery configuration. A NIC that supports multiple virtual interfaces is permissible, provided the card is supported by the operating system. When using virtual servers in the Neverfail cluster, each virtual NIC must use a separate virtual switch. Configure each server to include:

- A Public network LAN connection
  - Assign an IP Address for the Management IP Address. This is the first IP Address on the Public LAN connection. On Windows Server 2008 R2 with Service Pack 1 or 2012 R2, the Management IP Address must be a lower number than the Public IP Address. This associates the default gateway with the Management IP Address.
  - Assign a second IP Address to this Public network LAN connection for MiCollab AM. MiCollab AM uses the Public IP Address of the Public LAN connection for all communications to other Call Servers, ancillary servers such as Web PhoneManager, E-mail servers, and subscribers.
  - Assign the default gateway to the Public LAN network connection.

**NOTE** If assigning two IP Addresses to the Public NIC for use of a Management interface, do not register this Public NIC with DNS. A static IP Address will need to be created. For more information on having Neverfail create the static IP Address in DNS, please see section "Creating a Static IP Address with Neverfail."

- At least one Neverfail Heartbeat LAN channel for each connection between servers in the Neverfail Cluster.

**NOTE** Redundant Neverfail Heartbeat channels are optional between the System Servers. If you want to use redundant Neverfail Heartbeat channels, you must have a separate NIC for each redundant channel, in each server of the cluster.

The Neverfail Heartbeat channels between the Primary, Secondary, and Tertiary servers must reside on separate VLANs or subnets than the Public network. The network connections between the Primary and Secondary servers may be a simple crossover cable. The Neverfail network channels through the enterprise WAN for the Tertiary server must also be on a separate VLAN or subnet.

**NOTE** For more information on configuring the IP Addresses for Neverfail servers, refer to the Microsoft TechNet article on Multi-homed Windows Computers:

[blogs.technet.com/b/networking/archive/2009/04/25/source-ip-address-selection-on-a-multi-homed-windows-computer.aspx](http://blogs.technet.com/b/networking/archive/2009/04/25/source-ip-address-selection-on-a-multi-homed-windows-computer.aspx)



The following sample reference for LAN connections and IP addresses provides an example of a Neverfail High Availability and Disaster Recovery trio LAN assignment. If the Neverfail installation is configured as a High Availability pair only, the Tertiary server and IP address assignments are not required.

**NOTE** Mitel recommends that you carefully plan the LAN connections and associated IP addresses and then write them down so you can refer to them throughout the installation process, as well as for future reference when maintaining and troubleshooting the site.

Table 2. IP Address scheme for Neverfail trio

NF Primary Server	IP Address	VLAN	Switch Port	Notes
Primary (Public)	10.16.7.101	07	F1	
Management	10.16.7.992	07	F1	
Heartbeat Ch1	192.168.1.101		crossover	NF Secondary Ch1
Heartbeat Ch2	10.16.8.101	08	H6	NF Tertiary Ch1
NF Secondary Server	IP Address	VLAN	Switch Port	Notes
Primary (Public)	10.16.7.102	07	F5	<b>See note 1</b>
	10.16.7.101			w/ packet filter enabled
Management	10.16.7.982	7	F5	
Heartbeat Ch1	192.168.1.102		crossover	NF Primary Ch1
Heartbeat Ch2	10.16.10.102	10	J4	NF Tertiary Ch2
NF Tertiary Server	IP Address	VLAN	Switch Port	Notes
Primary (Public)	10.12.17.103	17	WR4	
Management	10.12.17.99	17	WR4	<b>See note 2</b>
Heartbeat Ch1	10.16.8.103	08	WH7	NF Primary Ch2
Heartbeat Ch2	10.16.10.103	10	WJ2	NF Secondary Ch2

**NOTE 1:** The Neverfail Secondary server is initially configured, and joined to the network with a unique TCP/IP address. During the Neverfail installation, the packet filter is applied to the Public network connection of each server in the cluster. At this time the IP address of the Secondary server in a High Availability configuration is changed to the same Public IP address as that of the Primary server's IP address during the Neverfail installation.

**NOTE 2:** On Windows Server 2008 R2 with Service Pack 1/2012 R2 servers, the Management IP Address must be a lower number than the Primary IP Address. The default gateway is associated with this IP Address.

The following illustration provides a network example of a Neverfail cluster configured as a pair for High Availability or as a Disaster Recovery trio.

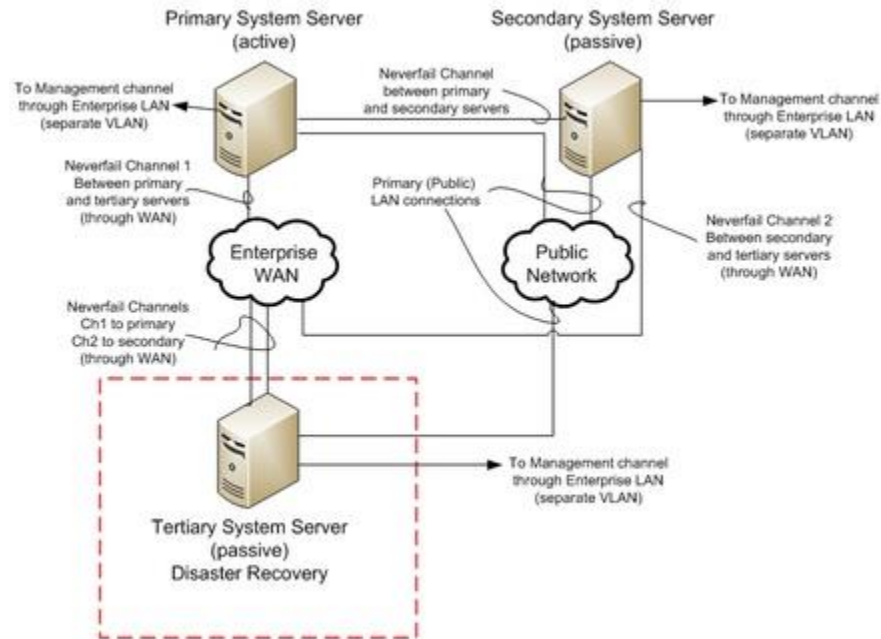


Figure 9. Tertiary System Server

# Preparing for the Neverfail Installation

This section lists the requirements and tasks necessary prior to installing Neverfail Heartbeat and Replication software on a pair or trio of Neverfail servers.

- Review the Neverfail Heartbeat and Neverfail Replicator Windows Server 2008 or 2012 Installation guides.
- Review the Neverfail SCOPE Installation Guide.
- Review the Neverfail Heartbeat Administrators Guide.
- Review the installation requirements from both Mitel and Neverfail Group. The platforms must meet or exceed the hardware requirements.
- Obtain domain administrator rights for the installation or coordinate with the IT department to participate in the installation.

**IMPORTANT** Installing Neverfail on Windows Server 2008 R2 with Service Pack 1/2012 R2 as a domain administrator simplifies the installation process. If you install Neverfail as a local administrator, you must right-click each object you want to run or install, and then select **Run as an Administrator**.

In addition, administering Neverfail with only local Administrator rights requires you to right-click each object you want to run, and then select **Run as an Administrator** to start a Neverfail utility or application.

- Write down all IP, subnet, and gateway addresses for reference during the install.

**IMPORTANT** The default gateway IP Address is associated with the Public NIC only.

- Configure the network connections for all servers in the Neverfail cluster.
- Name the network connections for identification purposes during the installation.
- On a Physical or Virtual server cluster, install the Primary with the desired OS, service packs, and software updates.
- On a Physical or Hyper-V server cluster, install the Secondary and Tertiary System Servers — all servers must be identical in OS, service packs, software updates, and they should be identical in hardware.
- On a Physical or Hyper-V server cluster, install the Windows Server Backup and Command Line Tools (For Windows Server 2008 R2 with Service Pack 1 only). To install the backup and restore utilities navigate to **Server Manager > Features**, and then click **Add Features**. Select the Windows Server Backup Features, **Windows Server Backup** and **Command Line Tools** (For Windows Server 2008 R2 with Service Pack 1 only).
- Ping all network connections to verify the network integrity before you begin the Neverfail software installation.

**IMPORTANT** Prior to installing MiCollab AM on the Primary server, refer to the *Licensing the Messaging System* section in the *System Installation Guide* to properly register/license the Primary server.

- Install MiCollab AM and any applications on the Primary server only, and then start MiCollab AM and all services.
- Install the Call Servers and verify the Call Servers are replicating with the System Server.
- On a VMware virtual server cluster only, clone the Primary VM server using the VMware vCenter to create the Secondary/Tertiary cloned VM server(s). The clone must be 100% with no changes to the Name, SID or domain membership. Perform the following steps:
  - Once the cloned image has been created, and before powering on the cloned image, edit the virtual machine settings using vCenter. Select the Public and Channel virtual network adapters and clear the *Connected* and *Connect at power on* check boxes.
  - Power on the Secondary or Tertiary (previously cloned) server image and once started, open Network Connections and make the following changes to all the Neverfail Channel network adaptors.
  - Right-click the Neverfail Channel network adaptor and select Properties. Select Internet Protocol (TCP/IP) and click Properties.
  - Configure the appropriate Neverfail Channel IP address and Subnet mask. Default gateway and DNS addresses should remain blank. Click Advanced.
  - Select the DNS tab, clear the *Register this connection's addresses in DNS* check box.
  - Select the WINS tab, select *Disable NetBIOS over TCP/IP*, then click OK twice and close the Neverfail Channel network adaptor.
  - Select the Principal (Public) network adaptor, right-click and select Properties. Select Internet Protocol (TCP/IP) and click Properties. Set the appropriate Management IP address (this must be different than the Primary server), Subnet Mask, Default Gateway and DNS, then click Advanced.
  - In Network Connections Advanced TCP/IP Settings, verify that the Principal (Public) NIC IP address is listed second in the Bind Order, and click OK.
  - Once all network adaptors have been properly configured, edit the virtual machine settings for the Secondary or Tertiary (cloned) server image using vCenter.
  - Select the Neverfail Channel virtual network adapter(s) and select the *Connected* and *Connect at power on* check boxes. At this point, you have IP communications with the Secondary or Tertiary server via the Neverfail Channel. The Public network adaptor will be reconnected after Neverfail has been installed on the Secondary/Tertiary servers.
- Install SCOPE on all of the servers in the Neverfail cluster. Run the program for twenty-four hours on existing systems, and for a minimum of fifteen minutes on newly installed systems.
- Collect and send the SCOPE .cab file results to Mitel Technical Support. (The configuration of your SCOPE software determines the location of the .cab files.) Technical Support contacts Neverfail with the information, and Neverfail generates the license key for the installation, which is e-mailed to you for the site installation.

**NOTE** Create a text file of the license number and save it to a folder that all of the Neverfail servers can access throughout the installation process.

- Map a drive\folder on the Secondary server as the destination for the NTBackup. During the Neverfail installation of the Primary server you can point the destination of the NTBackup to the mapped drive. When you install the Secondary and Tertiary servers you can perform the NTRestore by pointing to this mapped drive as the source. All servers in the Neverfail cluster can access this folder during the NTBackup and NTRestore process.

**IMPORTANT** On Windows Server 2008 R2 with Service Pack 1/2012 R2 installations you cannot point to a mapped drive and there is no Browse button to locate the correct path/folder. You must type the full UNC path. For example, \\secondaryserver\neverfail\backup.

- Copy the Neverfail software version 6.7.7 and Telephony Server Plug-in version 201.8.7.1 to each server in the Neverfail cluster.

**IMPORTANT** The Neverfail software and Telephony Server Plug-in must be on a local drive of each server to run the installation.

- Once the software is copied to the correct location for the installation, run setup to begin the installation process.

**NOTE** On Windows 2008 R2 with Service Pack 1/2012 R2 systems, right-click the setup file, and then select **Run as Administrator**.

# Installing Neverfail Software on a Physical or Hyper-V Windows Server 2008 / 2012

Follow the procedures in Chapter 3 (Installing Neverfail Heartbeat) of the *Neverfail Heartbeat and Neverfail Replicator Windows Server 2008 Installation - Physical Server v6.7.0* or *Neverfail Heartbeat and Neverfail Replicator Windows Server 2012 Installation - Physical Server v6.7.0*. to install the Neverfail software and the Telephony Server Plug-in on all of the Windows Server 2008 R2 with Service Pack 1/2012 R2 servers in the Neverfail cluster. The software must be installed using the steps provided in the installation guide. The following installation notes reference the steps in chapter 3 of the Neverfail Installation Guide. For example, Section 3-2 Step 7 refers to Chapter 3, Section 2, and procedural step 7. The notes provide additional information to guide you through the installation process.

## To install the Neverfail software and Telephony Server Plug-in on the Primary server:

- Section 3-2 Step 10: Determines the final topology of your Neverfail system. Select the topology for the site you are installing to continue the installation. Select the Neverfail cluster topology for the site.
- Section 3-2 Step 21: This is the step in which you install the Telephony Server Plug-in. Type the UNC path or click **Browse** to locate the source folder on the local drive, and then select the Plug-in software to continue.
- Section 3-2 Step 32-34: These are the steps in which you select the backup location and choose to include protected data during the pre-synchronization process. You must select **Include protected data in Pre-synchronization data**. Type the UNC path to the backup folder. The domain user ID and password are required to access the location.

**IMPORTANT** The protected data contains all of MiCollab AM. This data must be included in the backup. During the restore process, MiCollab AM is "restored" to the Secondary and Tertiary servers during the Secondary and Tertiary software installation.

- Section 3-2 Step 36: **Do not** start the Heartbeat in this step. Leave the checkbox cleared.

## To install the Neverfail software on the Secondary/Tertiary server:

**IMPORTANT** On Windows Server 2008 R2 with Service Pack 1/2012 R2 servers the backup you made on the Primary server has the following affects when you use it to create the Secondary server.

The IP Addresses and VLAN settings for the network interface cards (NIC) match the Primary server. You **must** change these settings to match those of the Secondary server after the Neverfail software installation is complete.

The Registry of the Primary server is cloned to the Secondary server, including the MAC addresses. These MAC addresses override the physical MAC addresses of the network adapters in the Secondary server. You **must** remove the MAC addresses that are populated in the "Locally Administered Address" field of the network adapter properties of each NIC card after the Neverfail software installation is complete.

- Section 3-3 Step 4: Select **Secondary or Tertiary** in this step.
- Section 3-3 Step 5: This is the step in which you select the backup that you created during the Neverfail installation on the Primary server. Type the UNC path to the drive and folder of the backup.

**IMPORTANT** On Windows Server 2008 R2 with Service Pack 1/2012 R2 servers, the backup you made on the Primary server has the following affects when you use it to create the Tertiary server.

The IP Addresses and VLAN settings for the network interface cards (NIC) match the Primary server. You **must** change these settings to match those of the Tertiary server after the Neverfail software installation is complete.

The Registry of the Primary server is cloned to the Tertiary server, including the MAC addresses. These MAC addresses override the physical MAC addresses of the network adapters in the Tertiary server. You **must** remove the MAC addresses that are populated in the "Locally Administered Address" field of the network adapter properties of each NIC card after the Neverfail software installation is complete.

- Section 3-3 Step 21: **Do not** start the Heartbeat in this step. Leave the checkbox cleared.

**IMPORTANT** Prior to starting the Neverfail Heartbeat, if you are using Software Based Licensing, make sure to register the Secondary and Tertiary servers.

# Installing Neverfail Software on a VMware Virtual Windows Server 2008 / 2012

Follow the procedures in Chapter 3 (Installing Neverfail Heartbeat) of the *Neverfail Heartbeat and Neverfail Replicator Windows Server 2008 Installation – Virtual Server v6.7.0* or *Neverfail Heartbeat and Neverfail Replicator Windows Server 2012 Installation – Virtual Server v6.7.0*. to install the Neverfail software and the Telephony Server Plug-in on all of the Windows Server 2008 R2 with Service Pack 1/2012 R2 servers in the Neverfail cluster. The software must be installed using the steps provided in the installation guide. The following installation notes reference the steps in chapter 3 of the Neverfail Installation Guide. For example, Section 3-2 Step 7 refers to Chapter 3, Section 2, and procedural step 7. The notes provide additional information to guide you through the installation process.

**IMPORTANT** Before proceeding, ensure that you have properly cloned the Primary VM server and reviewed the requirements in the “Preparing for the Neverfail Installation” section relating to Virtual clusters.

## To install the Neverfail software and Telephony Server Plug-in on the Primary server:

- Section 3-2 Step 11: Determines the final topology of your Neverfail system. Select the topology for the site you are installing to continue the installation. Select the Neverfail cluster topology for the site.
- Section 3-2 Step 22: This is the step in which you install the Telephony Server Plug-in. Type the UNC path or click **Browse** to locate the source folder on the local drive, and then select the Plug-in software to continue.
- Section 3-2 Step 23: This is the step in which you select the location to place the backup files. Type the UNC path to the backup folder. The domain user ID and password are required to access the location.

**NOTE** It is recommended that you create a Backup folder on the Secondary VM server on the D: partition and share out the folder. Connect to the Backup folder from the Primary using the IP address of the Heartbeat channel of the Secondary VM server.

- Section 3-2 Step 34: **Do not** start the Heartbeat in this step. Leave the checkbox cleared.



## To install the Neverfail software on the Secondary/Tertiary server:

- Section 3-3 Step 2 or 3: If you have successfully completed the requirements in the "Preparing for the Neverfail Installation" section relating to Virtual clusters, then these steps should not be necessary.
- Section 3-3 Step 6: Select **Secondary or Tertiary** in this step.
- Section 3-3 Step 7: This is the step in which you select the backup that you created during the Neverfail installation on the Primary server. Type the UNC path to the drive and shared backup folder. Connect using the IP address of the Heartbeat channel of the Secondary VM server.
- Section 3-3 Step 15: After the Packet Filter has been successfully installed on the Public NIC, the Public NIC must be reconnected at this time through VMware vCenter.
- Section 3-3 Step 18: **Do not** start the Heartbeat in this step. Leave the checkbox cleared.

**IMPORTANT** Prior to starting the Neverfail Heartbeat, if you are using Software Based Licensing, make sure to register the Secondary and Tertiary servers.

# Creating a Static IP Address with Neverfail

This section describes how to use the Neverfail Heartbeat DNSUpdate tool to automate the changing of the IP address. The utility removes the A and PTR records for the protected server and replaces them with the records for the new IP addresses after a switchover has occurred.

Using this method to update the DNS record is useful when adding a secondary IP address to the Public NIC for use as a Management interface. When using this method do not register the Public NIC with DNS.

**IMPORTANT** While Neverfail does not support IPv6 at this time, you may experience issues with the DNSUpdate tool if your DNS contains IPv6 Reverse Lookup Zones. If you do experience issues, then proceed to using the NFDNSCMD instead.

To create a DNSUpdate task manually, follow these steps:

- 1 Launch the Neverfail Heartbeat Management Client.
- 2 Click on the **Application** button.
- 3 Select the **Tasks** tab.
- 4 Click on the **User Accounts** button.

**NOTE** Verify that a User Account already exists that has access to update the domains DNS server(s). If not, then continue with steps 5 – 7 to add an account.

- 5 Click the **Add** button.
- 6 Enter the credentials for an account with rights to update the DNS (a member of the Administrators or Server Operators group on the target server).
- 7 Click **Ok**, and then **Close**.

**NOTE** A DNSUpdate task for Primary, Secondary and/or Tertiary should already exist. If not, then continue with steps 8 – 11 to add a new task.

- 8 Click the **Add** button to add a new task.
- 9 Provide a descriptive name for the 'Task' (i.e. DNSUpdate).
- 10 Select 'Network Configuration' for Task type.
- 11 Select either Primary or Secondary for the server the task should run on as appropriate.

**NOTE** If a DNSUpdate task for Primary, Secondary and/or Tertiary already exists, then select the appropriate task and click **Edit**.

- 12 In the Command field, enter the "dnscmd" with appropriate flags as shown below in the example.
- 13 In the 'Run As' field select the user appropriate user account from the drop down and then click Ok.

**NOTE** The DNSUpdate tool will detect if it's being run on Primary, Secondary and/or Tertiary servers by checking the registry as described previously.

The following example can be used for all three tasks for the Primary, Secondary and/or Tertiary servers.

Example: "DNSUpdate.exe -pri {primary public IP address} -sec {secondary public IP address} -ter {tertiary public IP address} -ns {Specify the IP Addresses of the DNS's that are to be updated}"

### To create a NFDNSCMD task manually, follow these steps:

- 1 Launch the Neverfail Heartbeat Management Client.
- 2 Click on the **Application** button.
- 3 Select the **Tasks** tab.
- 4 Click on the **User Accounts** button.

**NOTE** Verify that a User Account already exists that has access to update the domains DNS server(s). If not, then continue with steps 5 – 7 to add an account.

- 5 Click the **Add** button.
- 6 Enter the credentials for an account with rights to update the DNS (a member of the Administrators or Server Operators group on the target server).
- 7 Click **Ok**, and then **Close**.
- 8 At this time, you will need to create a Batch script file that contains the necessary NFDNSCMD commands to execute.

Example Batch file:

```
REM First you want to delete the ex-active IPs
REM "NFDndCmd.exe {DNS Server} /RecordDelete {Zone} {Server Name} {Record Type} {IP Address} /f"
NFDnsCmd.exe 172.16.1.22 /RecordDelete blvu.company.com PRIMARY_SRV A 172.16.17.250 /f
REM If you have more DNS servers you can add more lines here:
REM NFDnsCmd.exe 172.16.1.26 /RecordDelete blvu.company.com PRIMARY_SRV A 172.16.17.250 /f
```

```
REM Second you want to add the new active IPs
REM "NFDndCmd.exe {DNS Server} /RecordAdd {Zone} {Server Name} {TTL} {Type} {IP Address}"
NFDnsCmd.exe 172.16.1.22 /RecordAdd blvu.company.com PRIMARY_SRV 60 A 172.16.4.40
REM If you have more DNS servers you can add more lines here:
REM NFDnsCmd.exe 172.16.1.26 /RecordAdd blvu.company.com PRIMARY_SRV 60 A 172.16.4.40
```

- 9 Once the Batch file has been created, copy the file(s) to where Neverfail was installed, typically "\Program Files\Neverfail\R2\Bin" directory.

**NOTE** A DNSUpdate task for Primary, Secondary and/or Tertiary should already exist. If not, then continue with steps 10 – 13 to add a new task.

- 10 Click the **Add** button to add a new task.
- 11 Provide a descriptive name for the 'Task' (i.e. DNSUpdate).
- 12 Select 'Network Configuration' for Task type.
- 13 Select either Primary or Secondary for the server the task should run on as appropriate.

**NOTE** If a DNSUpdate task for Primary, Secondary and/or Tertiary already exists, then select the appropriate task and click **Edit**.

- 14 In the Command field, click Browse and navigate to the location of the Batch script created as shown in the example above.
- 15 In the 'Run As' field select the user appropriate user account from the drop down and then click Ok.

**NOTE** The DNSUpdate tool will detect if it's being run on Primary, Secondary and/or Tertiary servers by checking the registry as described previously.

# Customizing and Testing the Neverfail Installation

Once you have completed the software installation start the Neverfail Heartbeat on the Primary server. Refer to the *Neverfail Heartbeat Administrator's Guide v6.7.0* for configuring, testing, maintaining, and troubleshooting of the Neverfail cluster.

**NOTE** Mitel recommends you familiarize yourself with the terms and procedures in the Neverfail Administration Guide, the Neverfail Heartbeat Management Client, the Neverfail Server Configuration application, and the Neverfail Heartbeat Interactive Tool. Desktop icons were created for these programs during the Neverfail installation. The Interactive tool's icon displays on the Windows tray of the task bar. This icon provides the server designation and current role on each Neverfail server; right-click on the icon to open the tool.

- Test the switchover of server roles. Use the Neverfail Management Heartbeat Client utilities program to perform a managed switchover to the passive servers, and then switch back to the active server. Once the passive server has become active, verify that MiCollab AM is running and that the Call Servers are replicating with the System Server.
- Refer to Chapter 4 to customize the Neverfail settings for your site. It provides information on configuring the Heartbeat settings, pings, ping targets, switchover, and response times. These parameters allow you to customize how the Neverfail cluster responds for automatic switchover.
- Refer to Chapter 4 for information on common administrative tasks such as starting replication, managing switchover, and recovering from a failure.

# Maintaining the Neverfail Cluster

MiCollab AM runs in a protected environment once Neverfail is running on the System Server. You cannot stop any protected Service or application, including MiCollab AM, while the Neverfail Heartbeat is running. You must stop the Neverfail Heartbeat before you can proceed with shutting down MiCollab AM.

The Startup and Shutdown buttons on the Main tab of MiCollab AM Configuration are grayed out while the Neverfail Heartbeat is running. In addition, the current Neverfail status displays on the bottom area of the Main tab of each server in the Neverfail cluster.

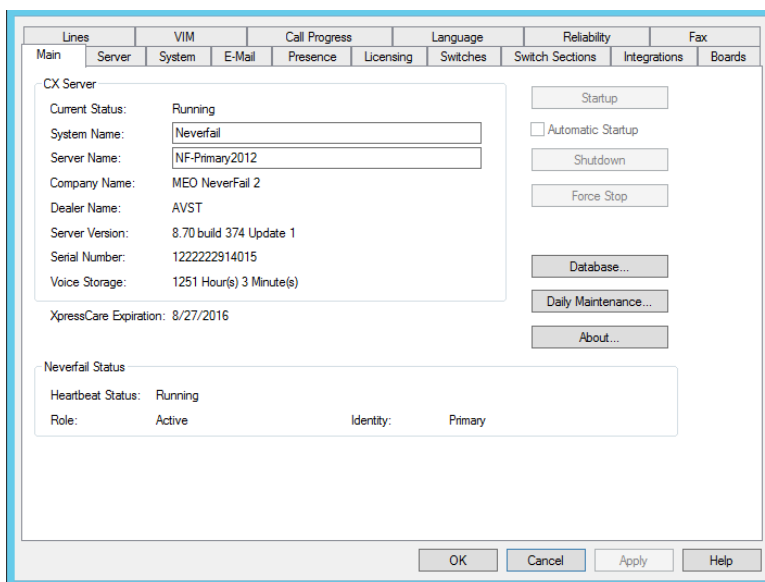


Figure 10. Main Tab

## Administering MiCollab AM System Servers in a Neverfail Environment

The Neverfail Replication Service replicates the MiCollab AM database and registry keys in real time from the active server to the passive servers in a daisy chain fashion. Always administer MiCollab AM and run its client utilities on the active server only.

- You do not have to stop the Neverfail Heartbeat to administer MiCollab AM unless MiCollab AM has to be shut down.
- If you must shutdown MiCollab AM, you must first stop the Neverfail Heartbeat.
- The Neverfail Replicator Service replicates only the MiCollab AM database and registry data, it does not replicate anti-virus software updates, or Windows software updates. You must install the same software on each System Server in the Neverfail cluster.

- Always shut down the Neverfail Heartbeat prior to installing Windows updates, service packs, software patches, anti-virus software updates, or other software on a Neverfail server. Use the Management IP LAN connection to administer passive servers.

## Maintaining Passive Neverfail Servers

The Neverfail packet filter prevents TCP/IP packets through the Public IP LAN connection of the passive servers. You can administer the passive servers through the Management IP LAN connection using a terminal Service such as Remote Desktop. However, you cannot stop or restart any Service or application protected by the Neverfail Heartbeat without first stopping the Heartbeat.


# Patching MiCollab AM Software in a Neverfail Cluster

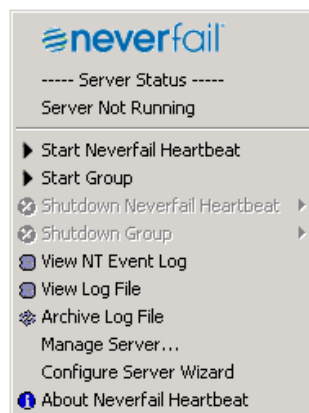
Mitel releases software patches to support and maintain current releases of MiCollab AM software. You can find a current list of software patches on the Mitel Mitel Connect website. Installing software patches to maintain current software versions is a common administrative task that you must perform on each System Server in the Neverfail cluster, as well as all of the Call Servers in the system. Follow the procedures in this section to install MiCollab AM software patches in a Neverfail environment.

**IMPORTANT** The Neverfail replication Service does not replicate software patches. Any time MiCollab AM software is installed on one System Server, you must install it on all of the System Servers in the Neverfail cluster.

- Always stop the Neverfail Heartbeat before you shut down MiCollab AM or restart the server.
- Always apply software patches to the active server in the Neverfail cluster first.
- Use the Shutdown Group/Start Group feature of the Neverfail Tray Tool to shut down and start the Heartbeat on all Neverfail servers in the cluster.
- For information that is more current, read the Technical Bulletin provided with the software patch to complete the update process.
- Once you have updated the System Servers in the Neverfail cluster, brought the active server online, and restarted the Heartbeat on all of the servers in the cluster, apply the same software patch to each Call Server in the system.

## To install MiCollab AM software patches in a Neverfail cluster:

- 1 On the active server, right-click the Neverfail Tool icon  on the task bar tray. The Neverfail Server Status and Management Tool displays.





- 2 Click **Shutdown Group**. The following pop-up displays.

**IMPORTANT** To shut down the group, use the Shutdown Group feature of the Neverfail Server Status and Management Tool to stop the Heartbeat on all of the servers in the cluster. If you use the Shutdown Group feature, you do not have to stop the Heartbeat on each individual server.

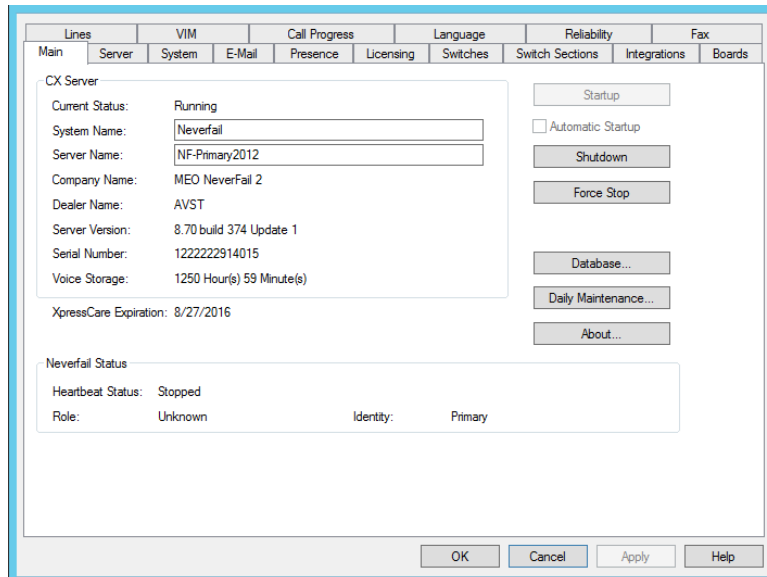
If you select Shutdown Neverfail Heartbeat, you must shutdown the Heartbeat on each individual passive server.



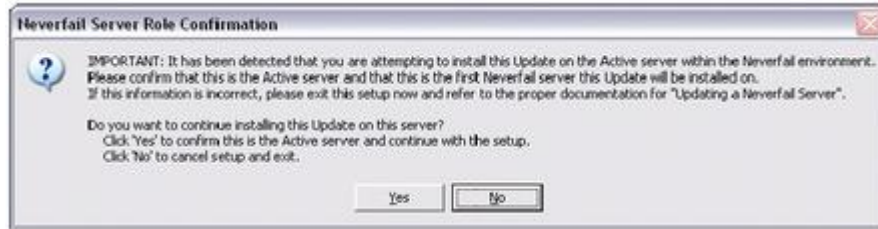
- 3 Select **Leave protected applications running**. The Neverfail Heartbeat stops in an orderly shutdown. A pop-up confirmation displays.



- 4 Click **OK** to continue.
- 5 Select **Start > All Programs > MiCollab AM Desktop**, and then click **MiCollab AM Configuration**. The MiCollab AM System Configuration utility displays.



- 6 Click **Shutdown**. MiCollab AM shuts down. Other dependent service will continue to run, such as the MySQLCore service.
- 7 Install the MiCollab AM software patch on the active System Server. The Neverfail Server Role Confirmation dialog box displays.



- 8 Click **Yes** to continue updating on the active server. Allow the server to restart and complete the installation process before you continue.
- 9 Install the MiCollab AM software patch on each passive System Server in the Neverfail cluster. The Neverfail Server Role Confirmation dialog box displays.




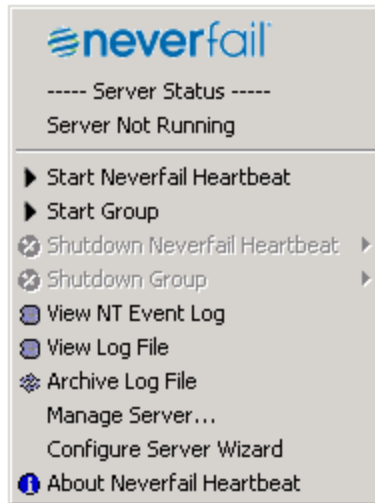
- 10 Click **Yes** to continue updating on the passive server. Allow each server to restart and complete the installation process before you continue.

**NOTE** If you did not follow all of the steps to prepare the server for software installation before you attempt to begin the software installation process, the following error message displays.



Review steps 1 through 6 to put the server in a state in which it can be updated.

- 11 Allow each server to restart and finish the installation and configuration process before continuing.
- 12 On the active server, right-click the **Neverfail Tool** icon  on the task bar tray. The Neverfail Server Status and Management Tool displays.



- 13 Click **Start Neverfail Group**. The Heartbeat starts on all of the System Servers in the Neverfail cluster.

**NOTE** Restarting the Neverfail Heartbeat on the Active server starts MiCollab AM and stops any MiCollab AM Services on the passive servers that may have been restarted due to the update.

- 14 Once the Neverfail Heartbeat starts and the replication process completes, you can continue with updating the Call Servers.


# Installing MiCollab AM Software Updates and Upgrading MiCollab AM from a Previous Version

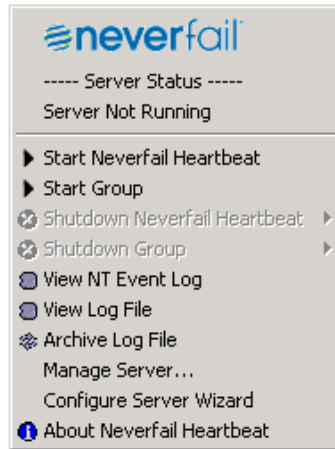
Mitel releases Software Updates to maintain current releases of MiCollab AM software and to provide new features. In addition, Mitel releases new versions of MiCollab AM software to enhance the MiCollab AM product, provide new features, and maintain its presence in the marketplace. Installing Software Updates and upgrading MiCollab AM to a new software version is a common administrative task that you must perform on each System Server in the Neverfail cluster, as well as all of the Call Servers in the system. Follow the procedures in this section to install MiCollab AM Software Updates and to upgrade your system to new software version in a Neverfail environment.

**IMPORTANT** The Neverfail replication Service does not replicate program files, Software Updates or Upgrades. Any time MiCollab AM software is installed on one System Server, you must install it on all of the Neverfail servers in the cluster.

- Always stop the Neverfail Heartbeat before you shut down MiCollab AM or restart the server.
- Always install Software Updates and Software Upgrades on the active server in the Neverfail cluster first.
- Use the Shutdown Group/Start Group feature of the Neverfail Tray Tool to shut down and start the Heartbeat on all Neverfail servers in the cluster.
- Once the Neverfail Heartbeat stops, maintain MiCollab AM using the procedures and principles found in the Mitel documentation and in the online help. All servers in the Neverfail cluster must receive the same Software Update or Upgrades.
- Once you have updated the System Servers in the Neverfail cluster, brought the active server online, and restarted the Heartbeat on all of the servers in the cluster, perform the same Software Updates or Upgrades to each Call Server in the system.

## To install MiCollab AM Software Updates or perform Software Upgrades:

- 1 On the active server, right-click the Neverfail Tool icon  on the task bar tray. The Neverfail Server Status and Management Tool displays.



- 2 Click **Shutdown Group**. The following pop-up displays.

**IMPORTANT** Use the Shutdown Group feature of the Neverfail Server Status and Management Tool to stop the Heartbeat on all of the servers in the cluster. If you use the Shutdown Group feature, you do not have to stop the Heartbeat on each individual server.

If you select Shutdown Neverfail Heartbeat, you must shutdown the Heartbeat on each individual passive server.



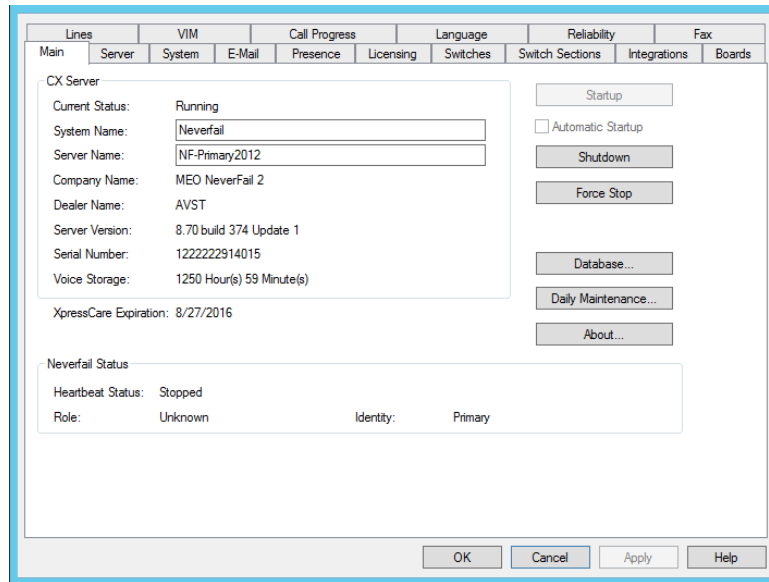
- 3 Select **Leave protected applications running**. The Neverfail Heartbeat stops in an orderly shutdown. A pop-up confirmation displays.




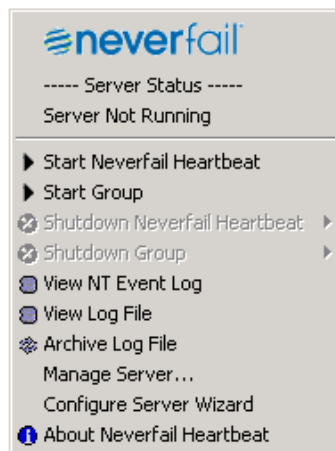
- 4 Click **OK** to continue.

**NOTE** The InstallShield Wizard changes the Services to Manual start and restores them to Automatic start when the installation is complete.

- 5 Select Start > All Programs > MiCollab AM Desktop, and then click Configuration. The MiCollab AM System Configuration utility displays.



- 6 Click **Shutdown**. MiCollab AM shuts down. Other dependent services will continue to run, such as the MySQLCore service.
- 7 Install the MiCollab AM Software Update or perform the Software Upgrade on the active System Server. Allow the server to restart and complete the installation process before you continue.
- 8 Install the MiCollab AM Software Update or perform the Software Upgrade on each passive System Server in the Neverfail cluster. Allow each server to restart and complete the installation process before you continue.
- 9 On the active server, right-click the **Neverfail Tool** icon  on the task bar tray. The Neverfail Server Status and Management Tool display.



- 10 Click **Start Neverfail Group**. The Heartbeat starts on all Neverfail servers.

**NOTE** Restarting the Neverfail Heartbeat on the Active server starts MiCollab AM and also stops any MiCollab AM Services on the passive servers that may have been restarted due to the update.

- 11 Once the Neverfail Heartbeat starts and the replication process is complete, you can continue with updating/upgrading the Call Servers.

# Upgrading Neverfail Heartbeat from V6.5.2 to V6.7.7

This section provides systematic procedures to upgrade MiCollab AM 5.0 SP3 to MiCollab AM 6.1 as well as the Neverfail Heartbeat version 6.5.2 to Neverfail Heartbeat version 6.7.7. Upgrading from a Neverfail Pair (two servers) to a Neverfail Trio (three servers) is not a supported procedure. However, instructions are provided for adding a Tertiary server after the upgrade is complete.

## Uninstalling Previous Versions of Neverfail SCOPE

Before you begin the upgrade, you must first uninstall the previous version of Neverfail SCOPE. Follow the procedures in the next section to install SCOPE version 5.3.0

To remove the previous version of SCOPE:

- 1 Select **Start > Control Panel > Add or Remove Programs > Neverfail SCOPE Data Collector Service**, and then click Remove to uninstall the program.
- 2 Once the program is removed, close the Control Panel windows.

## Installing SCOPE version 5.3.0

Once the previous version of SCOPE is uninstalled, you can install SCOPE version 5.3.0. This software is located on the Mitel MiCollab AM Installation Media version 6.1 in the \3rd Party Application\Neverfail\Scope\_5.3.0 folder and on the Neverfail Extranet website in the Products/Downloads/Neverfail SCOPE area.

**NOTE** The SCOPE software is available from the Neverfail Extranet as a zip file, the SCOPE software on the Mitel MiCollab AM Installation Media version 6.1 is not packaged as a .zip file.

To install SCOPE version 5.3.0:

- 1 Download the Neverfail SCOPE version 5.3.0 from the Neverfail extranet website by navigating to Products/Downloads/Neverfail SCOPE, or insert the MiCollab AM Installation Media into the appropriate drive in the servers.



If...	Then...
You download SCOPE from the Neverfail Extranet	Save the .Zip file to an appropriate location on the server, and then go to Step 2.
You are installing SCOPE from the MiCollab AM Installation Media version 6.1	Navigate to the media to the appropriate 32-bit or 64-bit \3rd Party Application\Neverfail\Scope_5.3.0 folder, and then skip to Step 3.

- 2 Double-click the .ZIP file and extract the SCOPE Data Collector Service.msi file.
- 3 Double-click the **SCOPE Data Collector Service.msi** file to start the installation wizard.
- 4 Follow the instructions within the SCOPE Data Collector Service InstallShield Wizard to complete the installation.

## Upgrading to Neverfail Heartbeat version 6.7.7

Follow the steps in this section to preserve your current Neverfail configuration settings while upgrading from previous version of Neverfail Heartbeat to Neverfail Heartbeat version 6.7.7.

**NOTE** You are required to obtain a new license key during the upgrade process.

### To prepare the Neverfail cluster for the Neverfail version 6.7.7 installation:

- 1 Upload the Neverfail SCOPE .Cab data file to the Neverfail Extranet and obtain a new Neverfail license key based on HBSig.
- 2 Obtain Heartbeat version 6.7.7 from the MiCollab AM Installation Media version 6.1 and copy the contents to an appropriate location on both Primary and Secondary servers.
- 3 On the Primary/active server, stop the **Neverfail Heartbeat**. You can leave the protected applications running.
- 4 Select **Start > Administrative Tools > Services > Neverfail Server R2 Service**.
- 5 Right click the **Neverfail Server R2 Service**, select **Properties**, and then change the startup type to **Manual**.
- 6 On the Secondary/passive server, stop the **Neverfail Heartbeat**. You can leave the protected applications running.
- 7 Select **Start > Administrative Tools > Services > Neverfail Server R2 Service**.
- 8 Right click the **Neverfail Server R2 Service**, select **Properties**, and then change the startup type to **Manual**.
- 9 On the Secondary/passive server, disconnect the network cable on the Primary (Public) network connection.

## To install Neverfail version 6.7.7 software on the Primary server:

- 1 Double-click the Neverfail version 6.7.7 **Setup.exe** file, and then select **Install Service Pack** from the Setup Type area.
- 2 Follow the Neverfail InstallShield instructions to install the ServicePack.nfs script.
  - a Click **Add** from the Service Pack Configuration area, locate the **ServicePack.nfs** script in the local folder you copied from the MiCollab AM Installation Media, and then click **Next**.
  - b Click **Next** at the Install Summary window.
  - c Click **Next** at the Stop Neverfail Heartbeat window.
  - d Click **Next** at the Close Programs window.
  - e Click **Next** at the Pre-Install Checks window.
  - f Click **Next** at the Install window.
  - g Click **Finish**.
- 3 When prompted, restart the server.
- 4 After the Server restarts a Software Installation window displays. Click **Continue Anyway**.
- 5 A Hardware Installation window displays for each Network interface card. Click **Continue Anyway**. This action re-installs the Neverfail TCP/IP Packet Filter on the Primary (Public) Network interface card.

## To install Neverfail version 6.7.7 software on the Secondary server:

- 1 Double-click the Neverfail version 6.7.7 **Setup.exe** file, and then select **Install Service Pack** from the Setup Type area.
- 2 Follow the Neverfail InstallShield instructions to install the ServicePack.nfs script.
  - a Click **Add** from the Service Pack Configuration area, locate the **ServicePack.nfs** script in the local folder you copied from the MiCollab AM Installation Media, and then click **Next**.
  - b Click **Next** at the Install Summary window.
  - c Click **Next** at the Stop Neverfail Heartbeat window.
  - d Click **Next** at the Close Programs window.
  - e Click **Next** at the Pre-Install Checks window.
  - f Click **Next** at the Install window.
  - g Click **Finish**.
- 3 When prompted, restart the server.
- 4 After the Server restarts a Software Installation window displays. Click **Continue Anyway**.
- 5 A Hardware Installation window displays for each Network interface card. Click **Continue Anyway**. This action re-installs the Neverfail TCP/IP Packet Filter on the Primary (Public) Network interface card.

## To complete the Neverfail version 6.7.7 software installation:

- 1 On both the Primary/active server and the Secondary/passive servers, verify the Network Interface card configurations. The Neverfail TCP/IP Packet Filter must be selected on the Principal (Public) network connection of both servers, and remain cleared on all Neverfail Heartbeat Channel network connections and the Management LAN connection.
- 2 On the Primary/active server, start the **Neverfail Server Configuration** wizard.
- 3 Click on the **License** tab, and then enter the Neverfail Heartbeat V6.7.7 license key you downloaded from the Neverfail Extranet website.
- 4 Click on the **Public** tab, enter a valid Public IP Address, and then click **Finish**.
- 5 On the Primary/active server, start the **Neverfail Heartbeat**.
- 6 Select **Start > Administrative Tools > Services > Neverfail Server R2 Service**.
- 7 Right click the **Neverfail Server R2 Service**, select **Properties**, and then change the startup type to **Automatic**.
- 8 On the Secondary/passive server, start the **Neverfail Heartbeat**, and then reconnect the network cable to the Principal (Public) NIC.
- 9 Select **Start > Administrative Tools > Services > Neverfail Server R2 Service**.
- 10 Right click the **Neverfail Server R2 Service**, select **Properties**, and then change the startup type to **Automatic**.

## Installing the Telephony Server Plug in for MiCollab AM version 6.1

MiCollab AM version 6.1 ships with the Telephony Server Plug-In version 201.8.7.1. The following procedures guide you through the process of uninstalling previous versions of the Plug-in for MiCollab AM and the installation of the Telephony Server Plug-in version 201.8.7.1 for MiCollab AM.

### Uninstalling previous versions of the Neverfail Plug-in for MiCollab AM:

**NOTE** Neverfail recommends that you uninstall previous Plug-ins using the Neverfail Heartbeat Management Client application. This procedure ensures that all components of the Plug-in are properly removed and allows for the re-installation of the new Plug-in.

- 1 Select **Start > All Programs > Neverfail > Manage Server**.
- 2 Select **Application**, and then select **Plug-ins**.
- 3 Select the Telephony Server Plug-in.
- 4 Click on the **Uninstall** button.

## Installing the Telephony Server Plug-in version 201.8.7.1:

**NOTE** When you install the new Telephony Server Plug-In, leave MiCollab AM Services running. Neverfail looks for the running MiCollab AM Services, and then adds them to its list of Services to monitor. Neverfail recommends installing Plug-ins using the Neverfail Heartbeat Management Client application. This procedure ensures that all components of the Plug-in are properly installed.

- 1 Select **Start > All Programs > Neverfail > Manage Server**.
- 2 Select **Application**, and then select **Plug-ins**.
- 3 Click the **Install** button.
- 4 Type the path to the TelephonyServerNFPlugin.dll Plug-in location, or click **Browse** to navigate to the Plug-in (recommended).

**NOTE** The Telephony Server Plug-In version 201.8.7.1 for MiCollab AM is located on the MiCollab AM Installation Media in the \3rd Party Application\ Neverfail\Heartbeat\_6.7.7 folder. Select the correct folder for your operating system, 32-bit or 64-bit. The filename is TelephonyServerNFPlugin.dll.

- 5 Click **OK** to install the Plug-in.

## Manually Adding Additional MiCollab AM Services:

There are two MiCollab AM Services that are not included in the Telephony Server Plug-In. These services are only needed if MiCollab AM is connected with an Exchange server or with a Unified Communications Managed API server.

- MiCollab AM Exchange Web Services
- MiCollab AM UCMA Server

- 1 Select **Start > All Programs > Neverfail > Manage Server**.
- 2 Select **Application**, and then select **Services**.
- 3 Click on the **Add** button.
- 4 Select the appropriate MiCollab AM Service that you want to add by clicking the **Name** dropdown list:
  - CXEWSSERVICE – MiCollab AM Exchange Web Services
  - CXUCMASERVICE – MiCollab AM UCMA Server
- 5 Leave remaining setting on the Add Service page as default.
- 6 Click **OK** to add the service.

## Completing the Neverfail and MiCollab AM Upgrade Process

Once the upgrade to Neverfail version 6.7.7 is complete and MiCollab AM is running properly in the new Neverfail environment, you can proceed with upgrading MiCollab AM to version 6.1. Refer to the section, "Installing MiCollab AM Software Updates and Upgrading MiCollab AM from a Previous Version" for specific information on upgrading MiCollab AM in a Neverfail environment.

# Adding a Tertiary Server

Currently, upgrading from a Neverfail Cluster Pair environment to a Neverfail Cluster Tertiary environment requires that the Neverfail software be uninstalled, and then reinstalled in a Tertiary configuration. Unfortunately, there is no simpler method in which to perform this task at this time. In addition, Neverfail currently does not provide any documentation or KB articles defining this procedure. However, the Neverfail Support Team does have full working knowledge on how to perform the procedure, and can help you at any time.

Therefore, your best course of action at this time is to uninstall Neverfail on both servers in the Neverfail cluster, and then to re-install the software following the procedures in both this document and the Neverfail Heartbeat and Neverfail Replicator Windows Server 2008 Installation - Physical Server v6.7.0, Neverfail Heartbeat and Neverfail Replicator Windows Server 2008 Installation - Virtual Server v6.7.0, Neverfail Heartbeat and Neverfail Replicator Windows Server 2012 Installation - Physical Server v6.7.0, or Neverfail Heartbeat and Neverfail Replicator Windows Server 2012 Installation - Virtual Server v6.7.0 to install Neverfail version 6.7.0 in a Tertiary configuration. During setup, you can make the selection that the Secondary server is a pre-clone. The Tertiary server can be a pre-clone or not, depending on how you want to setup of the Tertiary node.

# Split-Brain Avoidance

Split-Brain is a condition in which more than one server in a Neverfail cluster is operating in the active mode and attempting to service MiCollab AM clients. A split-brain condition occurs when the Heartbeat channel between the active and passive servers fails and the passive server fails to receive a Heartbeat reply from the active server. The passive server performs a switchover and becomes active as well, unaware that the active server is still operational and communicating through the Public LAN channel.

A Split-Brain condition results in independent database updates to multiple System Servers. Split-Brain is a serious condition because MiCollab AM cannot reconcile the database between the two servers and the Call Servers no longer know the correct System Server with which to replicate the database. If a Split-Brain condition exists, immediately stop the Neverfail Heartbeat and all instances of MiCollab AM.

Once you stop all of the Services, correct the problem, and then determine which server in the cluster is to be the active server. Restart the Heartbeat, and then once MiCollab AM is running again on the System Server you must stop all of the Call Servers and re-synchronize each Call Server to the System Server. Re-synchronize the Call Server from the Database dialog box of the Main tab on the MiCollab AM Configuration utility. For more information on re-synchronizing the Call Server, press F1 or click Help from the Database dialog box.

Use redundant Neverfail Heartbeat channels between the active and passive servers to increase the reliability of Heartbeat communications.

# Appendix A – Replacing a Server

On the Primary server or the server to be backed up, do the following:

- 1 Shutdown Neverfail Heartbeat.
- 2 Set the Neverfail Server R2 service to Manual using the Windows Service Control Manager.
- 3 Write down the identity of this server.
- 4 Open the Neverfail Heartbeat Configure Server wizard.
- 5 Select the **Machine** tab.
- 6 Change the Physical Hardware Identity of the server scheduled for replacement to the Secondary server or the server to be replaced.

**WARNING** Do not change the Server Identity in any situation other than this.

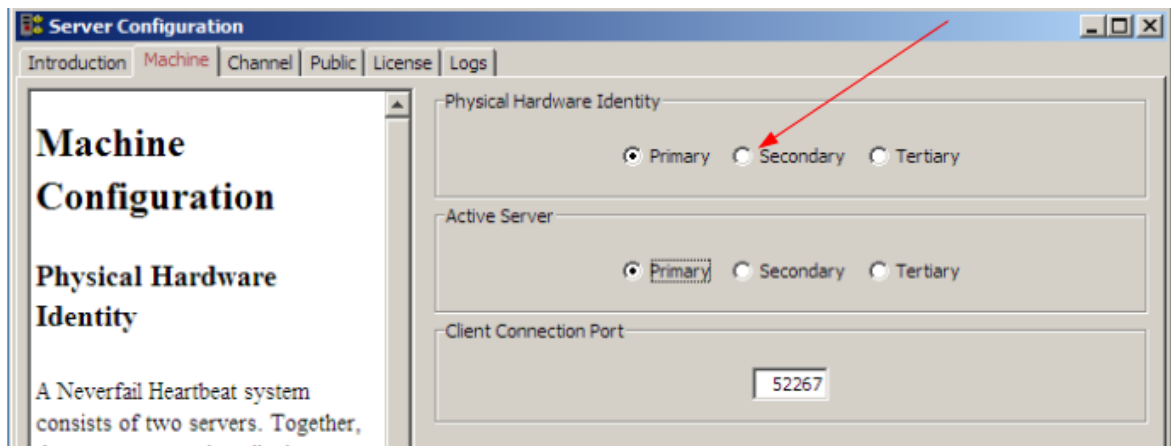


Figure 11. Configure Server Wizard – Machine Tab

- 7 Click **Finish**.
- 8 Launch the Windows Server Backup utility.
- 9 Start the Backup Once action
- 10 Select Different Options
- 11 In the next screen, select Custom and press **Next**.
- 12 Click **Add Items** and select **System State** and any other drives that contain protected application critical program files or any other application that is required to be present on the replacement server. Click **OK** and then click **Next**.



- 13 Select the destination of the backup using a local location or directly on the Secondary or on other server. If the destination is remote, a Share or Administrative Share location for that server must be provided.
- 14 Before starting the backup, you may want to exclude large files located on the drives selected (see step d, above) to reduce the size of the backup files
- 15 After the backup is complete, run the Neverfail Heartbeat Configure Server wizard again.
- 16 Select the **Machine** tab.
- 17 Change Physical Hardware Identity to the Primary server or the server to be backed up.

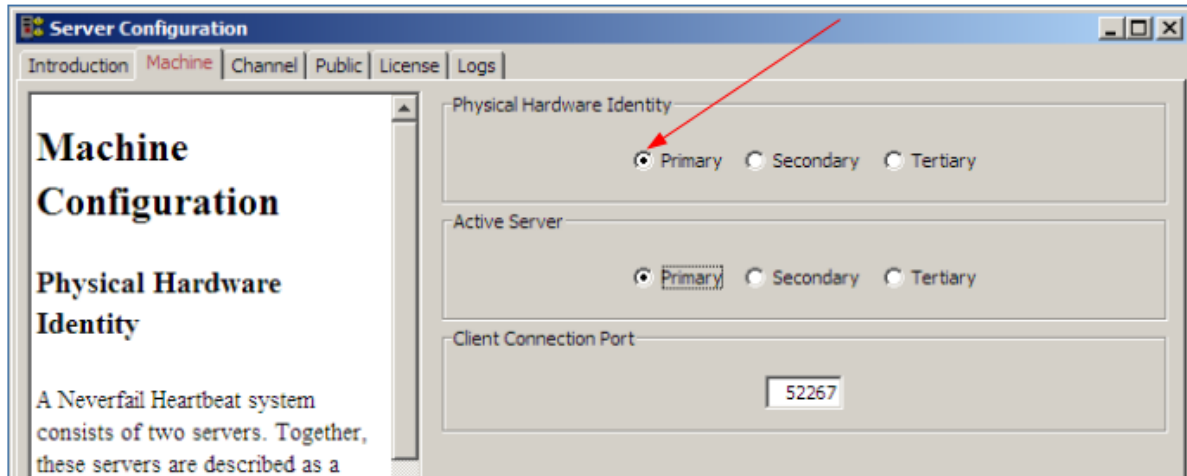


Figure 82. Configure Server Wizard – Machine Tab

- 18 Click **Finish**.
- 19 In the task bar, right click the Neverfail Heartbeat Server icon and select Start Neverfail Heartbeat.
- 20 Log into the Neverfail Heartbeat Management Client. Do not select the option to Stop replication. Leave the Protected Application running.
- 21 Set the Neverfail Server R2 service to Automatic using the Windows Windows Service Control Manager.

### To prevent the Secondary sever from becoming unbootable:

- 1 Run msinfo32.exe on both servers and expand the Components node and the Storage node.
- 2 Select the IDE and\or SCSI node depending on the type of disk controllers in use.
- 3 Make a note of the disk controllers' names (for example, viaide.sys, intelide.sys, pciide.sys, or cercsr6.sys).
- 4 On the Secondary (or Tertiary) server, navigate to Start - Run, enter Regedit.exe and click OK.
- 5 Navigate to HKLM\System\CurrentControlSet\Control\BackupRestore\KeysNotToRestore.
  - a Create a Multi-String Value and assign a name (for example, Disks Controllers).
  - b Add all of the Primary server's disk controller's information in the Secondary (or Tertiary) exclusion multi-string value created at step 5 using the following syntax:

CurrentControlSet\Services\{DriverNameWithoutExtension}\

- c** Enter each driver on a separate line as shown in the following example of the viaide.sys and intelide.sys drivers:

CurrentControlSet\Services\viaide\

CurrentControlSet\Services\intelide\

## On the New Server (the Replacement):

- 1** Move the USB drive to the Secondary server if the new server is not attached to the network
- 2** Recover the files and folders.
- 3** Start Windows Server Backup. Go to Action - Recover.
- 4** Select A backup stored on another location, click **Next**.
- 5** Select Remote shared folder, click **Next**.
- 6** Type the path for the backup (for example, \\localhost\D\$). Click **Next**.
- 7** Check that the correct backup is selected and click **Next**.
- 8** Select files and folders, click **Next**.
- 9** Select the first disk the needs to be recovered (for example, Local disk C:) and click **Next**.
- 10** Select another location and browse to the corresponding drive; select to overwrite the existing versions with the recovered versions; select Restore Access Control list (ACL) permissions to the file or folder being recovered and click **Next**.
- 11** Review the backup recovery items and click **Recover**.

**NOTE** Perform steps a. - f. For any additional drives that must be restored.

## **12** Restore the System State

- a** Perform steps a.- e. from Step 2.
- b** Select System State and click **Next**.
- c** Select Original location, click Next and acknowledge the warnings:

A window displays the message: "The specified backup is of a different server than the current one. We do not recommend performing a system state recovery with the backup to an alternate server because the server might become unusable. Are you sure you want to use this backup for recovering the current server?"

- d** Click **OK**. Another window displays the message:

If you perform a system state recovery from a backup on a remote shared folder, if there are network connection issues during the operation, the computer that you are recovering may become unusable. Instead, if possible, copy the backup to the local computer and then perform the recovery. Do you want to continue?"

- e** Click **OK** if the conditions are met. Then click **Next**.

- f** Clear the Automatically reboot the server check box and click **Recover**.
- 13** When prompted for a restart, unplug all network cables and restart the server.
- 14** Allow Plug and Play to continue and restart the server if prompted.
- 15** In the Properties window of each network card, verify that the IP address settings are correct for the Secondary server and that the Neverfail Heartbeat Packet Filter is enabled for the Public network connection and disabled for all channel connections (C:\Neverfail\R2\bin\nfpkftlfr.exe /getstate). It may be necessary to remove ghost NICs. If ghost NICs are found, open a command prompt and run the following commands:
- ```
set devmgr_show_nonpresent_devices=1  
devmgmt.msc
```
- 16** In the device manager snap-in click View- Show hidden devices.
- 17** Uninstall all ghost NICs without deleting driver software for those devices.
- 18** On the Machine tab of the Neverfail Heartbeat Configure Server wizard, verify that the Identity and Active Server are configured correctly.
- 19** On the Public tab of the Neverfail Heartbeat Configure Server wizard, verify that the Public IP is correct.

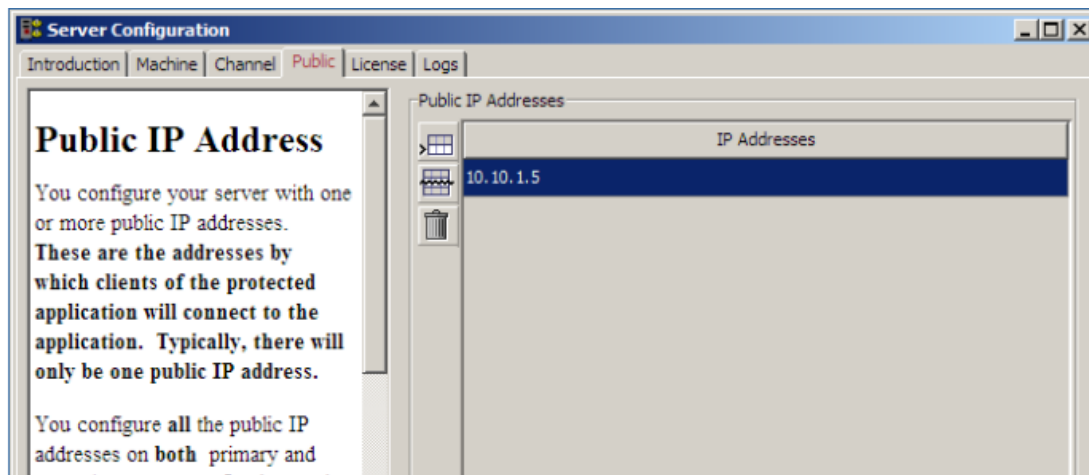


Figure 93. Configure Server Wizard – Public Tab

- 20** Use the route print command to check that a WAN routes are correctly configured.

**NOTE** It will be necessary to re-authenticate Windows.

- 21** Reconnect the Management Channel for testing.
- 22** Reconnect the Public and Heartbeat channel cable.
- 23** In the task bar, right click the Neverfail Heartbeat Server icon and select Start Neverfail Heartbeat.
- 24** Log into the Neverfail Heartbeat Management Client and start replication.
- 25** Set the Neverfail Server R2 service to Automatic using the Windows Service Control Manager.

# Appendix B – Tuning

Tuning system level rules may be necessary to reduce Neverfail warnings that may be triggered by system performance on larger systems. Listed are some of the more common rules that may need to be adjusted.

## Memory Pages Per Sec. rule:

A common rule to get triggered is the “Memory Pages Per Sec”. The default rule is to log a warning if this rule exceeds 10. We have observed values as high as 3000 without adverse impact on high performance systems, and values in the hundreds are common during nightly maintenance. We recommend increasing this value from 10 to 1000.

- 1 Select **Start > All Programs > Neverfail > Manage Server.**
- 2 Select **Application**, and then select **Rules.**
- 3 Select “Memory Pages Per Sec” found under System > Memory.
- 4 Click the **Edit** button.
- 5 Adjust the “Memory Pages / Sec” from 10 to 1000.
- 6 Click **OK** to save the changes

## Disk IO rule:

A common rule to get triggered is Disk IO. With multiple disks in a RAID array disk time can exceed 90% and disk queue can exceed 4 without hurting system performance. However, this rule has been triggered at customer sites where we did have a real disk performance issue. One customer had disk times at 300% and another customer peaked over 1000% due to lack of raid caching. We recommend leaving this alone, but are documenting that this rule could be triggered and give a false warning with high performance raid arrays, and it’s safe to increase the thresholds to avoid those false warnings.

- 1 Select **Start > All Programs > Neverfail > Manage Server.**
- 2 Select **Application**, and then select **Rules.**
- 3 Select “Disk IO” found under System > Disk.
- 4 Click the **Edit** button.
- 5 Adjust the “Disk Usage: Time” and “% or queue” as necessary.
- 6 Click **OK** to save the changes