

MiCollab Advanced Messaging Neverfail Integration Guide

For version 9.1 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 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 2020, Mitel Networks Corporation

All rights reserved

Contents

Preface	5
References	5
Documentation	5
Documentation Updates	6
Help	6
Document Conventions	6
Frequently Used Terms	7
Purchasing Neverfail for MiCollab AM	7
Overview	9
Neverfail Engine	9
Neverfail TCP/IP Packet Filtering	10
Critical Application Considerations	10
MiCollab AM with Neverfail Architecture	12
The Neverfail Telephony Server Plug-in	18
Neverfail SCOPE	19
Before You Begin	20
Critical Application Considerations	23
Planning the LAN Connections for Neverfail	24
Preparing for the Neverfail Installation	27
Installing Neverfail Continuity Engine	29
Deploying Neverfail Continuity Engine	29
Deploying Management IP Addressing	31
Creating a Static IP Address with Neverfail	33
Customizing and Testing the Neverfail Installation	36
Maintaining the Neverfail Cluster	37
Administering MiCollab AM System Servers in a Neverfail Environment	37
Maintaining Passive Neverfail Servers	38

Patching MiCollab AM Software in a Neverfail Cluster	39
Installing MiCollab AM Software Updates and Upgrading MiCollab AM from a Previous Version	43
Recloning Secondary or Tertiary Server to Install Software Updates and Patches	47
Upgrading Neverfail Heartbeat from V6.7.7 to V8.5	50
Upgrading MiCollab AM to 9.1	50
Installing the Telephony Server Plug-in for MiCollab AM version 9.1	51
Adding a Tertiary Server	53
Split-Brain Avoidance	54
Appendix A – Replacing a Server	55
Appendix B – Tuning	60

Preface

This guide describes how to install and configure the Neverfail Continuity Engine software.

This guide is written for Mitel-certified MiCollab Advanced Messaging (MiCollab AM) administrators and technicians who are familiar with MiCollab AM procedures and terminology, the **MiCollab AM Configuration** utility 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 9.1 and above, the Neverfail Continuity Engine software version 8.5, and the Neverfail Telephony Server Plug-in 201.20.4.0.

Before implementing any procedures in this guide, ensure that MiCollab AM software is installed and running successfully.

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 MiCollab AM Documentation Library includes the following documents and resources:

- **Administration Documentation.** Available as a PDF only. Contains the following:
 - **Administration Guides.** Available as a PDF only. Contains administrative guides for administrators about how to manage and configure the messaging system.
 - **Quick Reference Cards (QRC).** Contains shortcuts and quick instructions telling subscribers how to access and use the messaging system.
 - **User Guides.** Available as a PDF only. Contains user guides for subscribers about accessing the messaging system and checking and sending messages.
- **Server Documentation.** Available as a PDF only. Contains the following:
 - **Developer Resources.** Contains programming guides and API references for developers for integrating the server clients and web applications with MiCollab AM.
 - **Installation and Configuration.** Available as a PDF only. Contains installation and configuration guides for server administrators about how to install and configure the messaging system.
 - **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.

- **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: www.mitel.com

Help

The primary source of information about MiCollab AM is the online help available within any of its administrative utilities. You can access **Help** by clicking the **Help** button in the dialog box or window in which you are working.

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** Titles of other documents are shown in italics.

Example: See the *System Installation and Configuration Guide*.

- **User Interface (UI) Element Names.** Names of UI elements such as dialog boxes, windows, screens, menu items, tabs, buttons, and icons 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 MiCollab AM 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 Continuity Engine version 8.5 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.

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.

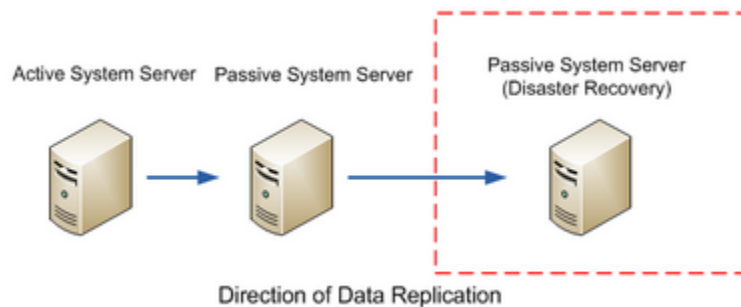
NOTE Do not contact Neverfail Technical Support for assistance with a Neverfail installation, configuration, or for troubleshooting purposes. They cannot assist you. Please call Mitel Technical Support for assistance.

Overview

The Neverfail Continuity Engine 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 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 Engine

The Neverfail Engine 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.

The Neverfail Engine also 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 Continuity Engine now uses a proprietary filtering system that works with the native Windows Filter Platform instead of the Neverfail Packet Filter Driver used with the previous versions. 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. Therefore, it is recommended that an additional network interface card be added as a management interface for when the server is in the passive role.

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 plug-in is installed; otherwise they will not be protected. This is by design of the Neverfail Engine 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 UCConnect
- 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 plug-in.

- Sites using Exchange 2010 or greater, must configure email profiles *before* installing the plug-in 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 plug-in 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 plug-in is installed will require that the plug-in 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.

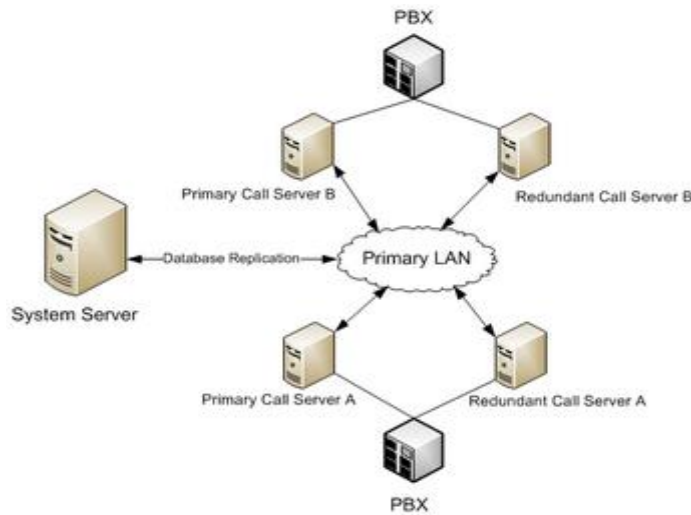


Figure 1. Multi-Box Configuration without Neverfail

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

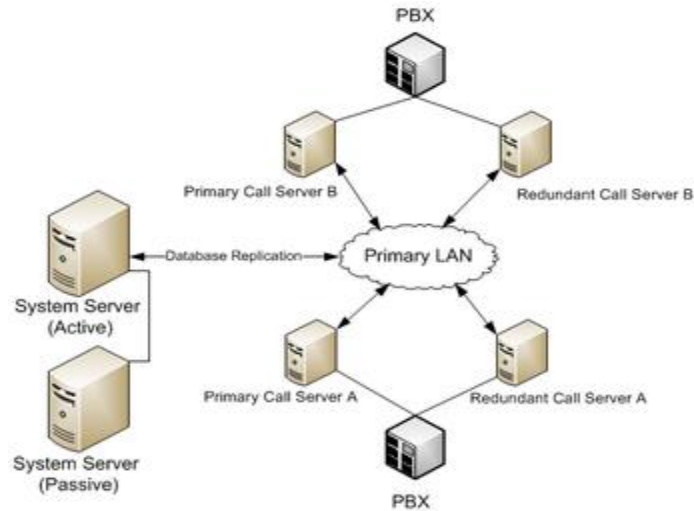


Figure 2. Multi-Box Configuration with Neverfail High Availability

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

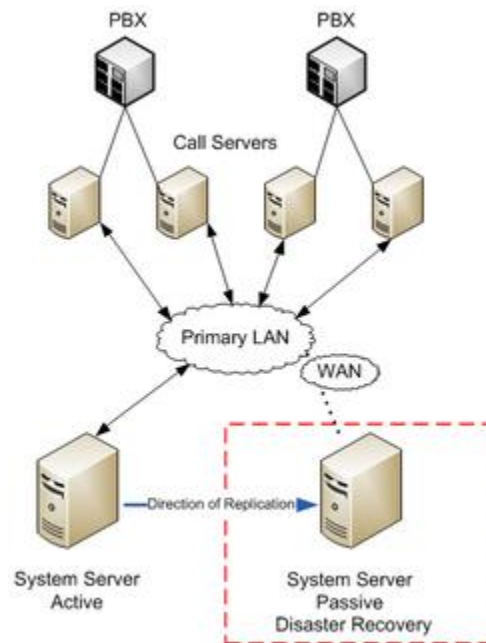


Figure 3. Disaster Recovery Cluster Configuration

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.

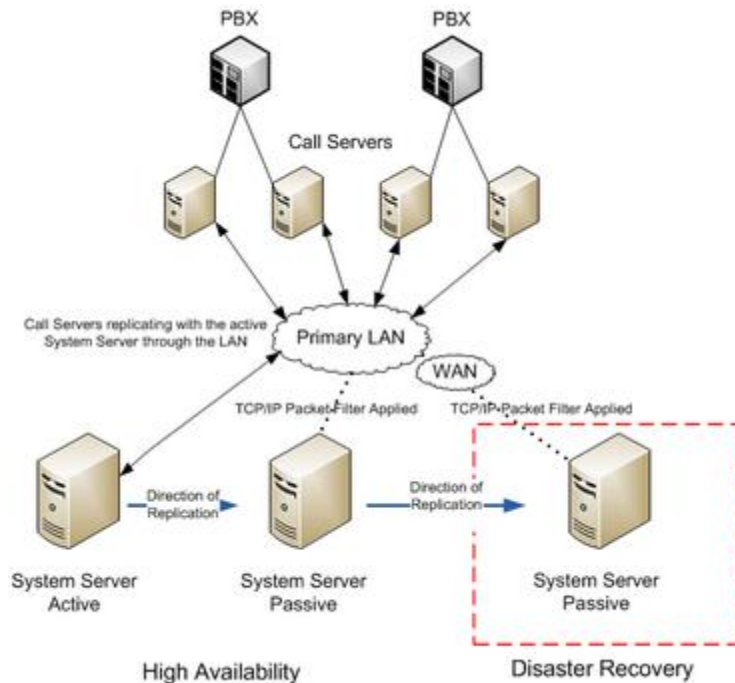


Figure 4. High Availability and Disaster Recovery Cluster Configuration

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*.

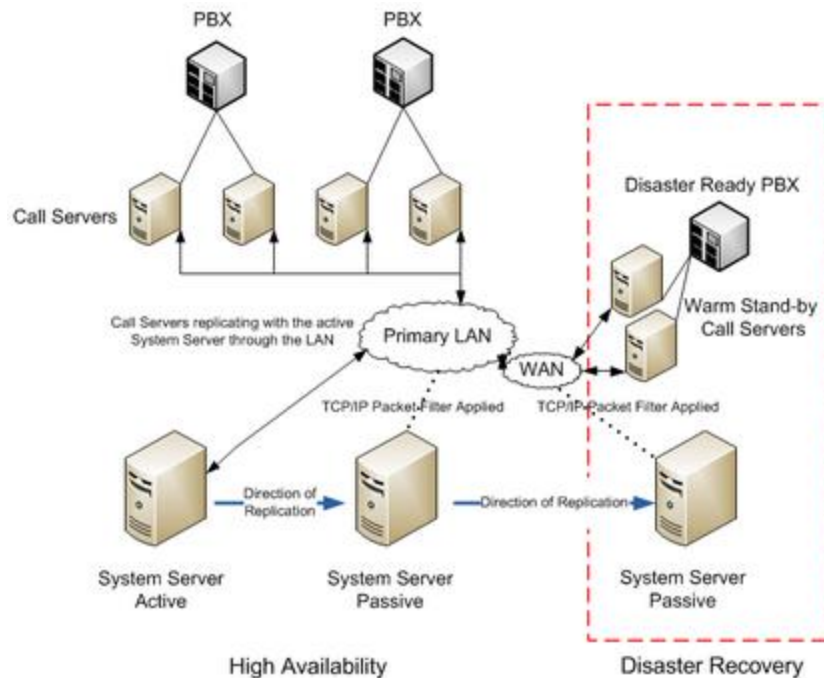


Figure 5. Disaster Recovery

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.

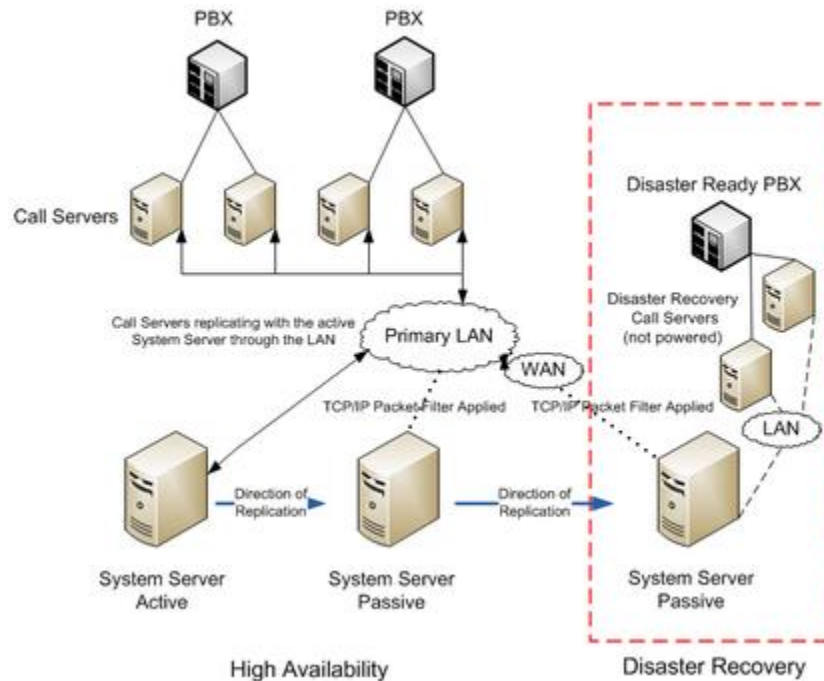


Figure 6. Disaster Recovery

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

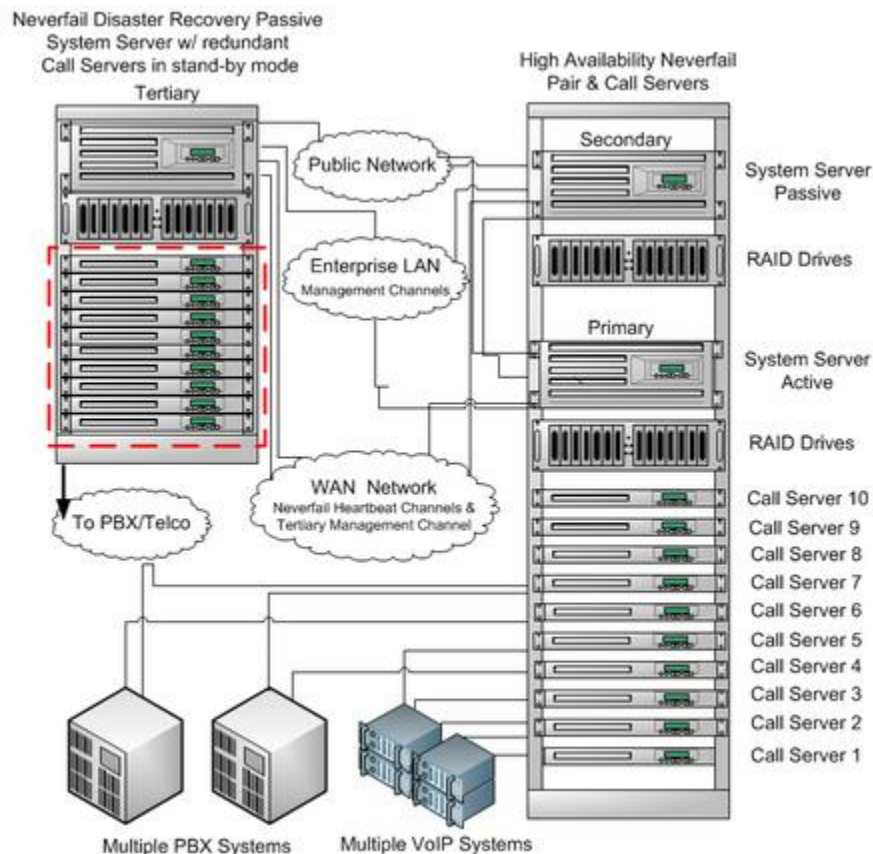


Figure 7. Neverfail Disaster Recovery

With 9.1, 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.

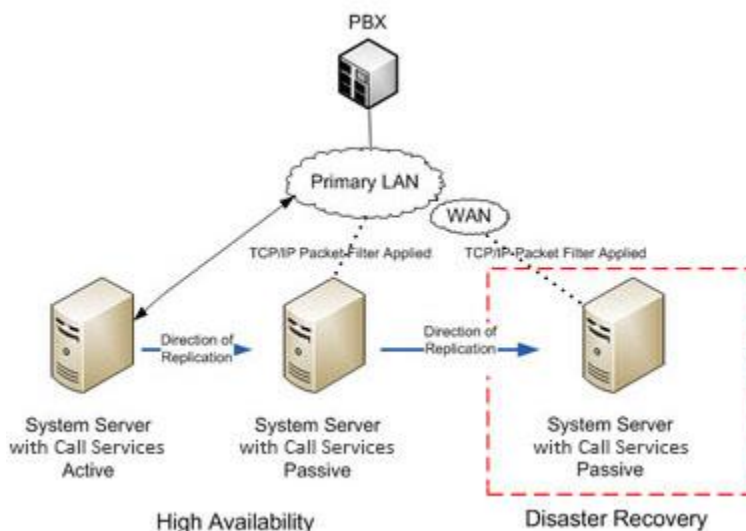


Figure 8. Stand-Alone System Server with Call Services

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.

IMPORTANT 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 manually update the "Network Join Local Address" on the Server tab, update the "Local IP Address to bind on" in the Integration Options and to also 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

Mitel 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.

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 Advanced 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 Engine must first be stopped.

Plug-in Management

Neverfail also includes a collection of default plug-ins. Some plug-ins are beneficial to the operation of the system while others could interfere with the Telephony Server Plug-in. It is recommended that you uninstall the following default plug-ins:

- MySqlNFPlugin.dll
- SqlServerNFPlugin.dll

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 Engine 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 Appendix C in the Neverfail document, *Neverfail Continuity Engine v8.5 Administrator's Guide* 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 should 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 Continuity Engine v8.5 Administrator's Guide* and the *Neverfail Continuity Engine v8.5 Installation Guide*.

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 driver letter and directory as on the Primary server
- The machine name must be different from the Primary server prior to installing Neverfail Engine
- Set up in a Workgroup prior to installing Neverfail Engine
- 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 Engine
- Set up in a Workgroup prior to installing Neverfail Engine
- 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 Engine 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 2012 R2, Windows Server 2016 (Server with Desktop Experience), or Windows Server 2019 (Server with Desktop Experience) license during the installation of the Neverfail Engine 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
- Multi-Tenant systems do not support TeamQ, Digital Networking. If you are planning to add additional tenants to a Neverfail system that previously protected these applications, then the following services must be stopped and the Neverfail Plug-In will need to be removed and re-added so it will not attempt to start these services.
 - Digital Networking
 - IVR Application Service

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

It is recommended that each server in the Neverfail cluster 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 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 Do not register the 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."

- A Management network LAN connection
 - Assign a secondary IP address to the Public LAN to be used as the Management IP Address. This will allow access to the server when the server is in the passive role. If you configure the Management network in this fashion then you will need to specify a SkipAsSource policy for Management IP addresses to ensure that they are not used for public traffic. SkipAsSource prevents an IP address from being selected by the operating system as a source IP address for out-going network connections. For more information on SkipAsSource, refer to the Management IP Addressing section in the *Neverfail Continuity Engine v8.5 Administrator's Guide*.
 - Otherwise assign an IP Address to a dedicated Management LAN for the Management IP Address. This will allow access to the server when the server is in the passive role. The Management IP address is a static IP address in a different subnet than the Public IP address or Neverfail Channel IP address and is always available for administrators to access the server.

NOTE When the Management IP is on a separate LAN, it will be necessary to create Static Routes for the Management IP Address in order to access the server remotely, perform Windows updates or other maintenance tasks when the server is in the passive role.

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

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

The Neverfail 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

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	10.16.6.992	06	F2	
Channel 1	192.168.1.101	01	F3	NF Secondary Ch1
Channel 2	192.168.2.101	02	F4	NF Tertiary Ch1
NF Secondary Server	IP Address	VLAN	Switch Port	Notes
Primary (Public)	10.16.7.101	07	F5	w/ packet filter enabled
Management	10.16.6.991	06	F6	
Channel 1	192.168.1.102	01	F7	NF Primary Ch1
Channel 2	192.168.3.102	03	F8	NF Tertiary Ch2
NF Tertiary Server	IP Address	VLAN	Switch Port	Notes
Primary (Public)	10.12.17.103	17	WR1	w/ packet filter enabled
Management	10.12.16.99	16	WR2	

Channel 1	192.168.2.103	02	WR3	NF Primary Ch2
Channel 2	192.168.3.103	03	WR4	NF Secondary Ch2

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

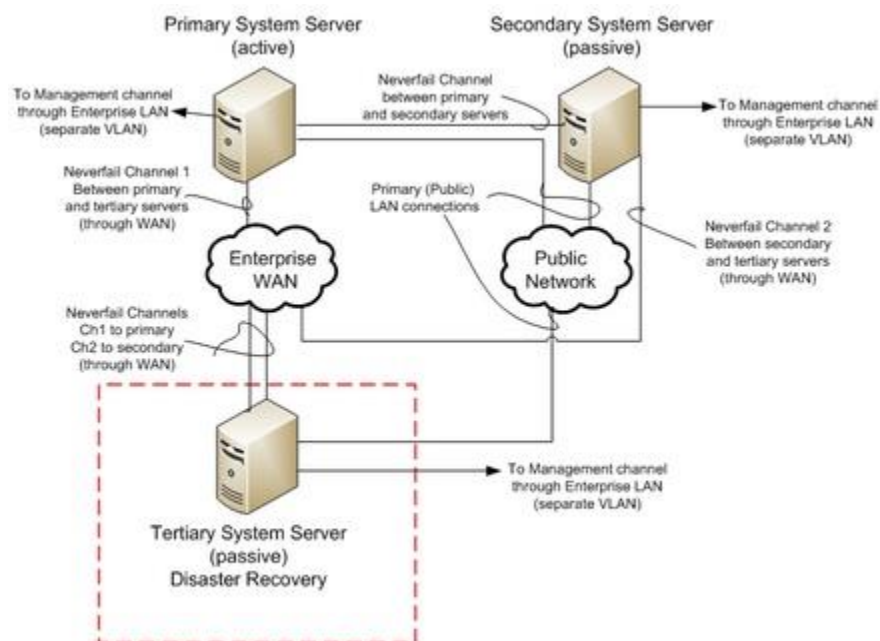


Figure 9. Tertiary System Server

Preparing for the Neverfail Installation

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

- Review the *Neverfail Continuity Engine Installation Guide*.
- Review the *Neverfail Continuity Engine Administrator's Guide* and *Appendix C: Neverfail SCOPE Data Collector Service Overview*.
- 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 2012 R2, Windows Server 2016 (Server with Desktop Experience), or Windows Server 2019 (Server with Desktop Experience) 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.

- On a Physical or Virtual server cluster, install the Primary System Server 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.
- 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.
- 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 and Configuration 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, it is recommended that you integrate the Neverfail Continuity Engine with VMware vCenter Server to automate the creation of the stand-by VMs (Secondary and Tertiary servers). Review the *Minimal VMware Permissions Requirements* in the *Neverfail Continuity Engine Installation Guide*.

IMPORTANT Physical server clusters require using Neverfail Continuity Engine's manual cloning during the installation process.

- Review the *Pre-Install Requirements* in the *Neverfail Continuity Engine Installation Guide*.
- On a Physical or Hyper-V server cluster, 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 2012 R2, Windows Server 2016 (Server with Desktop Experience), or Windows Server 2019 (Server with Desktop Experience) 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 Telephony Server Plug-in version 201.20.4.0 to the Primary server in the Neverfail cluster. The Telephony Server Plug-in is located on your Server DVD media under the **\\3rd Party Application\Neverfail\Continuity Engine 8.5** folder.

IMPORTANT The Telephony Server Plug-in should be on a local drive of the Primary server to be installed.

Installing Neverfail Continuity Engine

Follow the procedures in Chapter 3 of the *Neverfail Continuity Engine Installation Guide* to install the Neverfail software on all of the System Servers in the Neverfail cluster. The software must be installed using the steps provided in the installation guide.

IMPORTANT It is recommended that you install the Neverfail Continuity Engine at the default installation location (C drive).

NOTE The following procedures reference sections in chapter 3 of the *Neverfail Continuity Engine Installation Guide*. These procedures provide additional information to guide you through the installation process.

Deploying Neverfail Continuity Engine

To install the Neverfail Continuity Engine Management Service:

- The Neverfail Continuity Engine Management Service must first be installed on a separate Server or Workstation that will be used to manage the Neverfail Protected Servers. The Neverfail Continuity Engine Management Service can be used to manage multiple Neverfail Protected Servers.
- The Neverfail Continuity Engine software is located on your Server DVD media under the **\\3rd Party Application\Neverfail\Continuity Engine 8.5** folder.
- Follow the steps listed in *Installing Neverfail Continuity Engine*.
- The Neverfail Continuity Engine Management Service is accessed through a web interface using the following URL on the Server or Workstation where it was installed:
 - <https://localhost:9727/engine-ui/index.html>
- After the Neverfail Continuity Engine Management Service has been installed and you can login, if you plan to use a virtual server cluster, now is when you should configure the connection to VMware vCenter Server. Click **vCenter** and complete the configuration. For more information, refer to *Configure Connection to VMware vCenter Server*.

To deploy the Neverfail Engine on the Primary Server:

- Regardless of whether the Primary server is Physical or Virtual, follow the steps listed in *Deploying Neverfail Engine on the Primary Server*.
- Scope will be installed as part of the Neverfail Engine installation. This will only be needed in a manual license key generation process.

To deploy the Secondary/Tertiary server:

Depending on whether you are going to use the automated deployment using VMware vCenter or the semi-automatic deployment of the Secondary/Tertiary server, follow the steps listed in either section:

- For VMware vCenter automated cloning, follow the steps in *Automated Deployment of Stand-by Servers with Automatic Cloning*.
- For Manual cloning, follow the steps in *Semi-Automatic Deployment of Stand-by Servers Leveraging Manual Cloning*.
- Proceed to deploy the Secondary/Tertiary server(s).

IMPORTANT On Windows Server 2012 R2, Windows Server 2016 (Server with Desktop Experience), or Windows Server 2019 (Server with Desktop Experience) 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.

To deploy MiCollab AM Software Based Licensing:

IMPORTANT Prior to installing MiCollab AM on the Primary server, refer to the *Licensing the Messaging System* section in the *System Installation and Configuration 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.
- Deploy the Neverfail Continuity Engine Management Service on a separate Server or Workstation that will be used to manage the Neverfail Protected Servers.
- Deploy the Neverfail Engine on the Primary server but **Do Not** install the Telephony Server Plug-in at this time.
- Deploy the Secondary/Tertiary server(s).
- Once all Neverfail servers have been deployed, make each server active and run the MiCollab AM License Management Utility to register the Secondary and Tertiary servers.
- Make the Primary server active and then shutdown Neverfail.
- Start MiCollab AM and all services.
- Start Neverfail and install the Telephony Server Plug-in.

NOTE If you already have an active Neverfail system running and wish to convert MiCollab AM to Software Based Licensing, uninstall the Telephony Server Plug-in, shut down MiCollab AM, make each server active, and run the MiCollab AM License Management Utility to register each server. Once all servers have been registered, you can restart MiCollab AM and all services and reinstall the Telephony Server Plug-in.

To deploy the Telephony Server Plug-in:

- Launch the Neverfail Advanced Management Client on the Primary Server and navigate to the **Applications: Plug-ins page**. If this is the first time that you are launching the Neverfail Advanced Management Client, you will need to first add a connection.
- Click **Install**.
- 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 201.20.4.0 for MiCollab AM is located on the MiCollab AM Server DVD media in the **\3rd Party Application\Neverfail\Continuity Engine 8.5** folder. It is recommended that you copy the plug-in locally before installing. The filename is TelephonyServerNFPlugin.dll.

- Click **OK**.

To license the Neverfail System:

- Follow the steps in *License* to apply a license from your Neverfail account for the Neverfail Continuity Engine.
- If there is no Internet connection from the Neverfail Continuity Engine Management Service, allow Scope to run 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 to be applied, which is e-mailed to you.
- Once you receive your license key, follow the steps in *License* to manually enter a license key.

Deploying Management IP Addressing

To deploy a Management IP address to the Public network LAN connection:

- With the Neverfail Engine stopped, navigate to **Start > All Programs > Neverfail Engine > Configure Server Wizard** to launch the *Configure Server Wizard*.
- Select the **Management** tab.

- Provide the information for **Management Name**, **Management IP** and **Name Servers**. For more information, refer to the *Management IP Addressing* section in the *Neverfail Continuity Engine v8.5 Administrator's Guide*.
- The **DNS Test** button allows you to test the adding/checking/removing of DNS entries to the DNS server if a Name Server was provided.
- Specify the **Skip when Active and Public Subnet** SkipAsSource Policy for Management IP address to ensure that they are not used for public traffic.
- Complete this process on the Primary, Secondary/Tertiary servers.

To deploy a dedicated Management network LAN connection:

- Once the Secondary/Tertiary server(s) has been created, log on to the console of the machine and open the Network Connections.
- Right-click the Management network adaptor and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**.
- Configure the appropriate Management IP address and Subnet mask. Default gateway and DNS addresses should remain blank.

NOTE It will be necessary to create Static Routes for the Management IP Address in order to access the server remotely, perform Windows updates or other maintenance tasks when the server is in the passive role.

Creating a Static IP Address with Neverfail

This section describes how to use the Neverfail Advanced Management Client 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:

- 1 Launch the Neverfail Advanced Management Client.
- 2 Click the **Application** button.
- 3 Select the **Tasks** tab.
- 4 Click 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 through 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 click **Close**.

NOTE A DNSUpdate task for Primary, Secondary and/or Tertiary should already exist. If not, then continue with steps 8 through 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:

- 1 Launch the Neverfail Advanced Management Client.
- 2 Click the **Application** button.
- 3 Select the **Tasks** tab.
- 4 Click 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 through 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 click **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 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 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 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 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 through 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, the Neverfail Engine should now be running on the Primary server. Refer to the *Neverfail Continuity Engine v8.5 Administrator's Guide* for configuring, testing, maintaining, and troubleshooting of the Neverfail cluster.

NOTE Mitel recommends you familiarize yourself with the terms and procedures in the Neverfail Administrator's Guide, the Neverfail Continuity Engine Management Service, the Neverfail Advanced Management Client, and the Neverfail System Tray Application. Desktop icons were created for these programs during the Neverfail installation. The System Tray Application icon appears on the Windows tray of the task bar. This icon provides the server designation and current role on each Neverfail server; right-click the icon to open the tool.

- Test the switchover of server roles. Use either the Neverfail Continuity Engine Management Service or the Neverfail Advanced Management Client 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 Chapters 3 and 4 to customize the Neverfail settings for your site. It provides information on configuring the Engine settings, pings, ping targets, switchover, and response times. These parameters allow you to customize how the Neverfail cluster responds for automatic switchover.
- Refer to Chapters 3 and 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 Engine is running. You must stop the Neverfail Engine 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 Engine is running. In addition, the current **Neverfail Status** appears on the bottom area of the **Main** tab of each server in the Neverfail cluster.

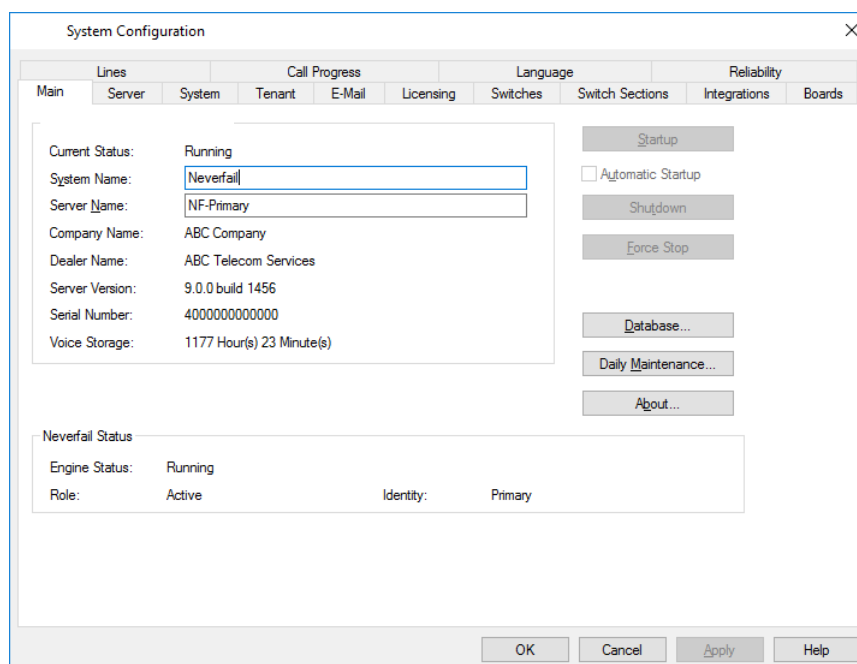


Figure 10. Main Tab

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 Engine to administer MiCollab AM unless MiCollab AM has to be shut down.
- If you must shutdown MiCollab AM, you must first stop the Neverfail Engine.

- 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 Engine 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 Engine without first stopping the Engine.

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.

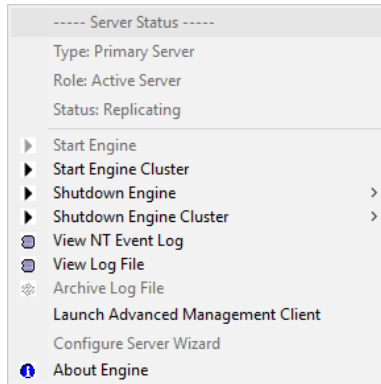
This process can be completed by either following the procedure in this section to install MiCollab AM Software Patches in a Neverfail environment or by using the Recloning procedure found in the *Recloning Secondary or Tertiary Server to Install Software Updates and Patches* section when using a virtual 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 Engine 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 Engine Cluster/Start Engine Cluster feature of the Neverfail Tray Tool to shut down and start the Engine 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 Engine 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:

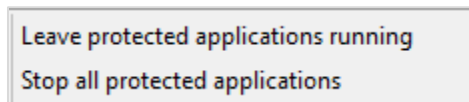
- 1 On the active server, right-click the **Neverfail Tool** icon  on the task bar tray. The Neverfail Server Status and Management Tool appears.



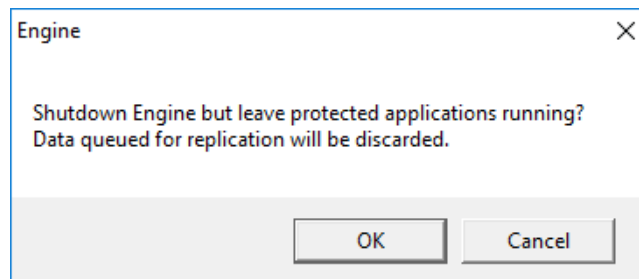
- 2 Click **Shutdown Engine Cluster**. The following pop-up appears.

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

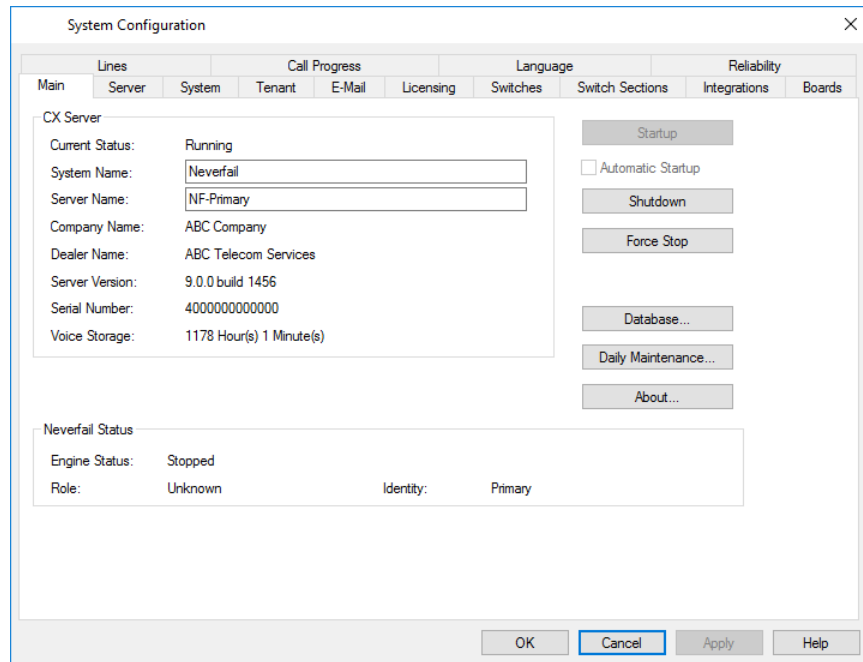
If you select **Shutdown Engine**, you must shutdown the Engine on each individual passive server.



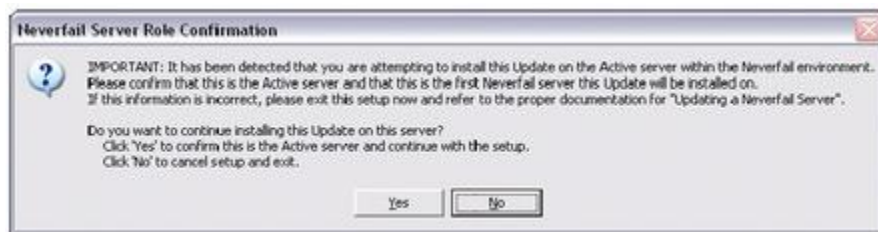
- 3 Select **Leave protected applications running**. The Neverfail Engine stops in an orderly shutdown. A pop-up confirmation appears.



- 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 appears.



- 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 appears.



- 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 appears.




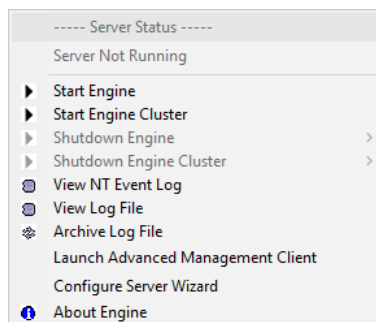
- 10 Click **Yes** to continue updating on the passive server. Allow each server to restart and complete the installation process before you continue.

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 appears.



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 appears.



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

NOTE Restarting the Neverfail Engine 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 Engine 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.

This process can be completed by either following the procedure in this section to install MiCollab AM Software Updates and to upgrade your system to new software version in a Neverfail environment or by using the Recloning procedure found in the [Recloning Secondary or Tertiary Server to Install Software Updates and Patches](#) section when using a virtual environment.

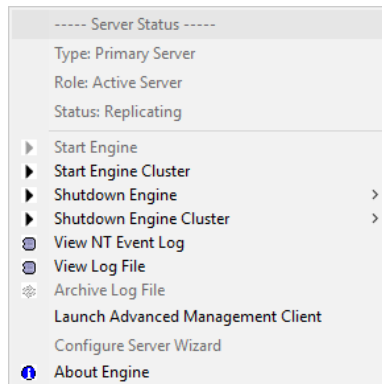
IMPORTANT The Neverfail replication Service does not replicate program files, Software Updates or Upgrades. Any time MiCollab AM software is installed on one System Server, you must install it on all of the Neverfail servers in the cluster.

- Always stop the Neverfail Engine 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 Engine Cluster/Start Engine Cluster** feature of the Neverfail Tray Tool to shut down and start the Engine on all Neverfail servers in the cluster.
- Once the Neverfail Engine 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 Engine on all of the servers in the cluster, perform the same Software Updates or Upgrades to each Call Server in the system.

IMPORTANT It is recommended that you install the Neverfail Continuity Engine at the default installation location (C drive). If you have previously installed the Neverfail Heartbeat 6.7.7 on a drive that is not the default location, then you cannot upgrade to the current version of the Neverfail Continuity Engine. Refer to [Upgrading Neverfail Heartbeat from V6.7.7 to V8.5](#) for more information.

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 appears.



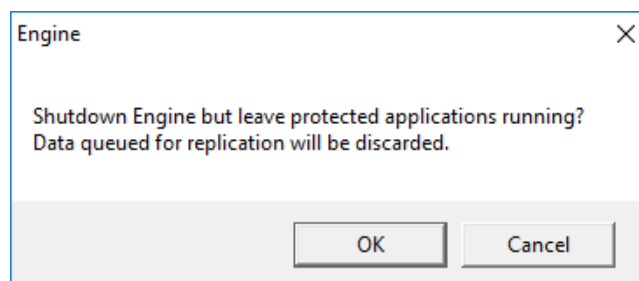
- 2 Click **Shutdown Engine Cluster**. The following pop-up appears.

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

If you select **Shutdown Engine**, you must shutdown the Engine on each individual passive server.

Leave protected applications running
Stop all protected applications

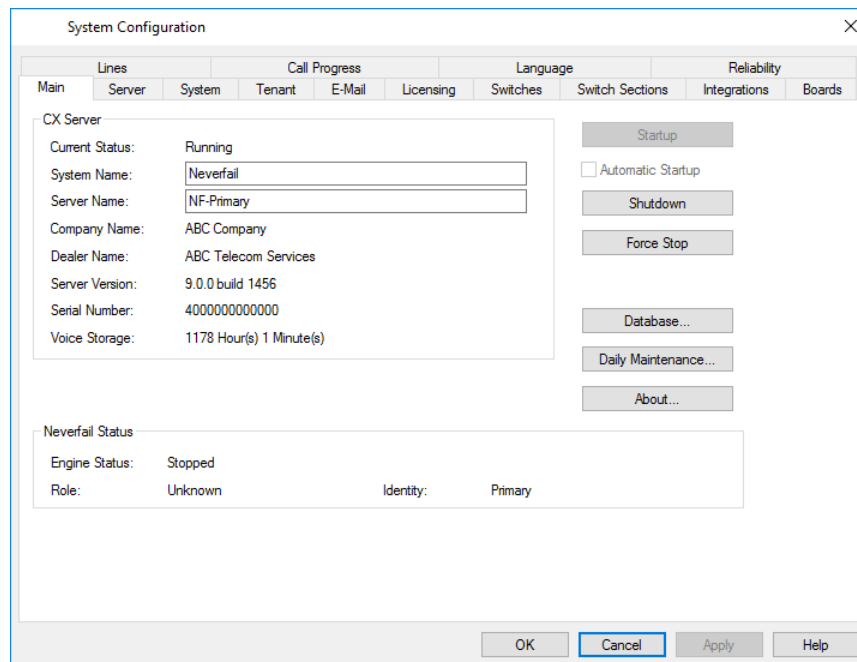
- 3 Select **Leave protected applications running**. The Neverfail Engine stops in an orderly shutdown. A pop-up confirmation appears.




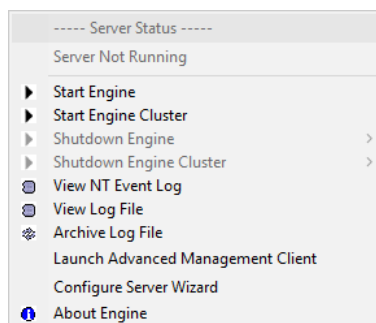
- 4 Click **OK** to continue.

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 appears.



- 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 appears.



- 10 Click **Start Engine Cluster**. The Engine starts on all Neverfail servers.

NOTE Restarting the Neverfail Engine 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 Engine starts and the replication process is complete, you can continue with updating/upgrading the Call Servers.

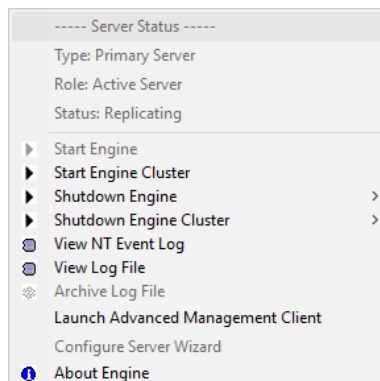
Recloning Secondary or Tertiary Server to Install Software Updates and Patches

Mitel and Microsoft release Software Patches and Updates to maintain current releases of software and to provide new features. Installing Software Patches and Updates and upgrading 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 on all of the Call Servers in the system.

If you are using a virtual environment, you can use the new Recloning feature to perform a reclone of the Secondary or Tertiary as a means to deploy software patches or upgrades. For more information on Recloning, refer to the *Recloning Secondary or Tertiary Server* section in the *Neverfail Continuity Engine v8.5 Administrator's Guide*.

To reclone the Secondary or Tertiary server:

- 1 With the Primary server active, right-click the **Neverfail Tool** icon  on the task bar tray. The Neverfail Server Status and Management Tool appears.



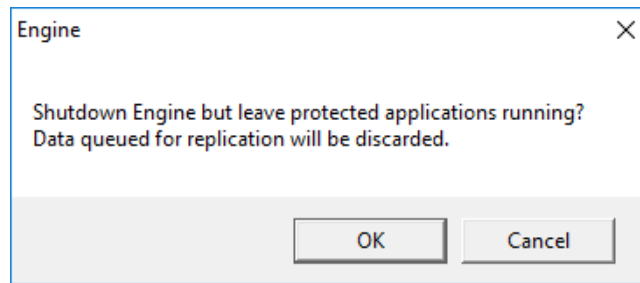
- 2 Click **Shutdown Engine Cluster**. The following pop-up appears.

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

If you select **Shutdown Engine**, you must shut down the Engine on each individual passive server.

Leave protected applications running
Stop all protected applications

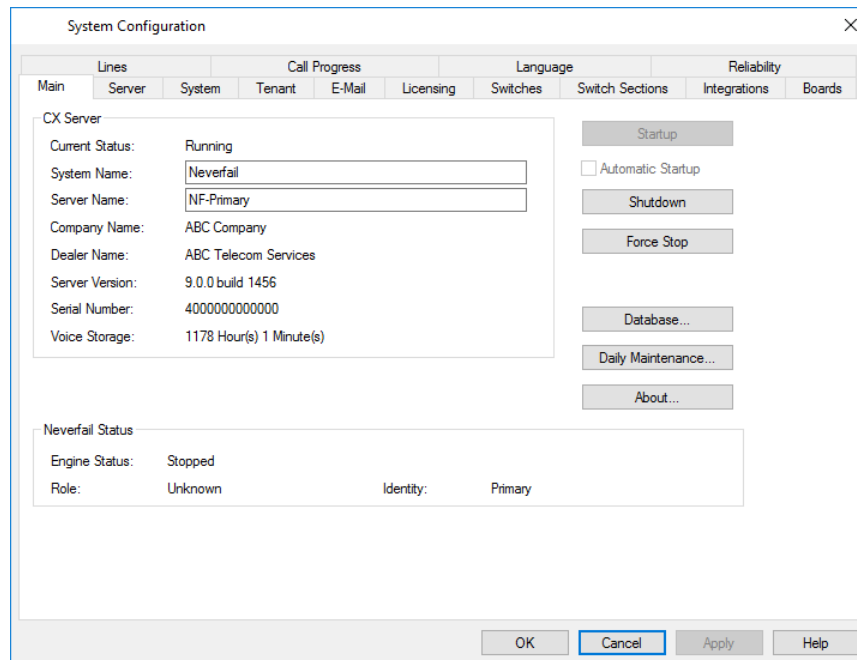
- 3 Select **Leave protected applications running**. The Neverfail Engine stops in an orderly shutdown. A pop-up confirmation appears.




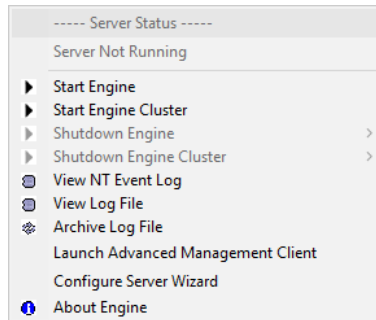
- 4 Click **OK** to continue.

NOTE The MiCollab AM 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 **MiCollab AM Configuration**. The MiCollab AM System Configuration utility appears.



- 6 Click **Shutdown**. MiCollab AM shuts down. Other dependent service will continue to run, such as the MySQLCore service.
- 7 Install the MiCollab AM or Microsoft software patch or upgrade on the Primary active System Server. Allow the server to restart if necessary and complete the installation process before you continue.
- 8 On the Primary active server, right-click the **Neverfail Tool** icon  on the task bar tray. The Neverfail Server Status and Management Tool appears.



- 9 Click **Start Engine**. The Engine starts only on the Primary server.

NOTE Restarting the Neverfail Engine on the Primary active server will also start MiCollab AM.

- 10 Once the Neverfail Engine starts, login to the Neverfail Continuity Engine Management Service UI and select the Management drop-down. Select **Deploy > Reclone Secondary or Tertiary server**.
- 11 Follow the steps in *Automated Recloning* in the *Neverfail Continuity Engine v8.5 Administrator's Guide*.
- 12 You may need to reregister the Secondary/Tertiary server if you are using Software Based Licensing.

Upgrading Neverfail Heartbeat from V6.7.7 to V8.5

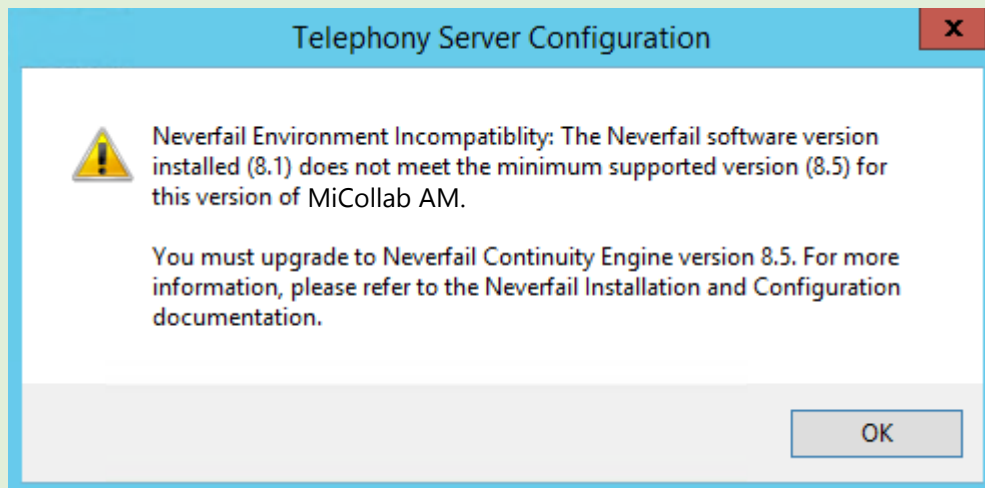
This section provides systematic procedures to upgrade MiCollab AM 6.1 to MiCollab AM 9.1 as well as the Neverfail Heartbeat version 6.7.7 to Neverfail Continuity Engine version 8.5. Upgrading from a Neverfail Pair (two servers) to a Neverfail Trio (three servers) is not a supported procedure. However, instructions are provided for adding a Tertiary server after the upgrade is complete.

IMPORTANT Neverfail does not support upgrades of the Neverfail Continuity Engine 8.5 if the previous version was installed outside of the default installation location (C drive). If you have previously installed Neverfail Heartbeat 6.7.7 on a drive that is not the default location, then you cannot upgrade to Neverfail Continuity Engine 8.5. Neverfail Heartbeat 6.7.7 will have to be uninstalled and Neverfail 8.5 will need to be deployed as a new installation.

Upgrading MiCollab AM to 9.1

Before you upgrade to Neverfail version 8.5, it is recommended that you upgrade MiCollab AM to version 9.1. 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.

IMPORTANT If you upgrade MiCollab AM from a previous version and then open the MiCollab AM control panel before you upgrade Neverfail Heartbeat version 6.7.7 to Neverfail Continuity Engine version 8.5, you will receive a warning message stating that the minimum supported version of Neverfail (8.5) is not installed.



When you start MiCollab AM, an error is logged in the Event Viewer. You will not be blocked from installing MiCollab AM, but please be advised that you must upgrade to Neverfail Continuity Engine 8.5 in order to successfully run MiCollab AM.

Follow the steps in this section to preserve your current Neverfail configuration settings while upgrading from a previous version of Neverfail Heartbeat to Neverfail Continuity Engine version 8.5.

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

To prepare the Neverfail cluster for the Neverfail version 8.5 installation:

- 1 Upload the Neverfail SCOPE .cab data file to the Neverfail Extranet and obtain a new Neverfail license key based on HBSig.
- 2 Before the upgrade can begin, the old Neverfail Plug-in for MiCollab AM will need to be uninstalled from the Primary server. Follow the steps in *Uninstalling previous versions of the Neverfail Plug-in for MiCollab AM* in this document.
- 3 Obtain the Continuity Engine version 8.5 from the MiCollab AM Server DVD media version 9.1 and install the Continuity Engine on a separate Server or Workstation that will be used to manage the Neverfail Protected Servers. Follow the steps listed in *Installing Neverfail Continuity Engine* in Chapter 3 of the *Neverfail Continuity Engine Installation Guide*.
- 4 Launch the Neverfail Continuity Engine Management Service and log in.
- 5 Select **Management > Manage > Add a protected server...** to add the existing Neverfail cluster.
- 6 Select the newly added protected servers and then select **Management > Deploy > Upgrade the selected server...** to begin the upgrade process.
- 7 Provide the local built-in administrator account and password.
- 8 Select the **I confirm that no users are logged on to the Primary, Secondary (or Tertiary) Servers** option.
- 9 Select the **Upgrade all server nodes in cluster (recommended)** option. Click **Next**.

NOTE Single node upgrades should only be used in the event the upgrade of the whole cluster has failed. If you select to upgrade only a specific server in the cluster, you must configure a Management IP address on the target server prior to attempting the upgrade. A new instance will then be added in the Protected Servers list represented by the management IP.

- 10 Once validation is complete, click **Next**.
- 11 Review the information and click **Finish** to begin the upgrade process.
- 12 Once the upgrade process has completed, the new Neverfail Plug-in for MiCollab AM will need to be installed on the Primary server. Follow the steps in *Installing the Telephony Server Plug-in version 201.20.4.0* in this document.

Installing the Telephony Server Plug-in for MiCollab AM version 9.1

MiCollab AM version 9.1 ships with the updated Telephony Server Plug-in version 201.20.4.0 to support the Neverfail Continuity Engine version 8.5. 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 201.20.4.0 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 Advanced Management Client application on the Primary server. 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 > Neverfail > Advanced Management Client** or **Neverfail Heartbeat Management Client**.
- 2 Select **Application**, and then select **Plug-ins**.
- 3 Select the Telephony Server Plug-in.
- 4 Click the **Uninstall** button.

Installing the Telephony Server Plug-in version 201.20.4.0:

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 Advanced Management Client application on the Primary server. This procedure ensures that all components of the plug-in are properly installed.

- 1 Select **Start > Neverfail > Advanced Management Client**.
- 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 201.20.4.0 for MiCollab AM is located on the MiCollab AM Server DVD media in the **\3rd Party Application\Neverfail\Continuity Engine 8.5** folder. It is recommended that you copy the plug-in locally before installing. The filename is TelephonyServerNFPlugin.dll.

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

Adding a Tertiary Server

With Neverfail version 8.5, it is now possible to add a stand-by (Tertiary) server for disaster recovery to an existing high availability pair environment. Follow the procedures in Chapter 3 of the *Neverfail Continuity Engine Installation Guide* to install the stand-by (Tertiary) server.

To deploy the Stand-by Tertiary server:

- The Neverfail Continuity Engine Management Service must first be installed on a separate Server or Workstation that will be used to manage the Neverfail Protected Servers.

NOTE The Neverfail Continuity Engine software is located on your Server DVD media under the **\\3rd Party Application\Neverfail\Continuity Engine 8.5** folder.

- Follow the steps listed in *Add a Stand-by Server for Disaster Recovery* section of the *Neverfail Continuity Engine Installation Guide*.

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 Neverfail Channel between the active and passive servers fails and the passive server fails to receive a Channel 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 Engine 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 Engine, 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 Channels between the active and passive servers to increase the reliability of Engine communications.

Appendix A – Replacing a Server

On the Primary server or the server to be backed up:

- 1 Shutdown Neverfail Engine.
- 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 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.

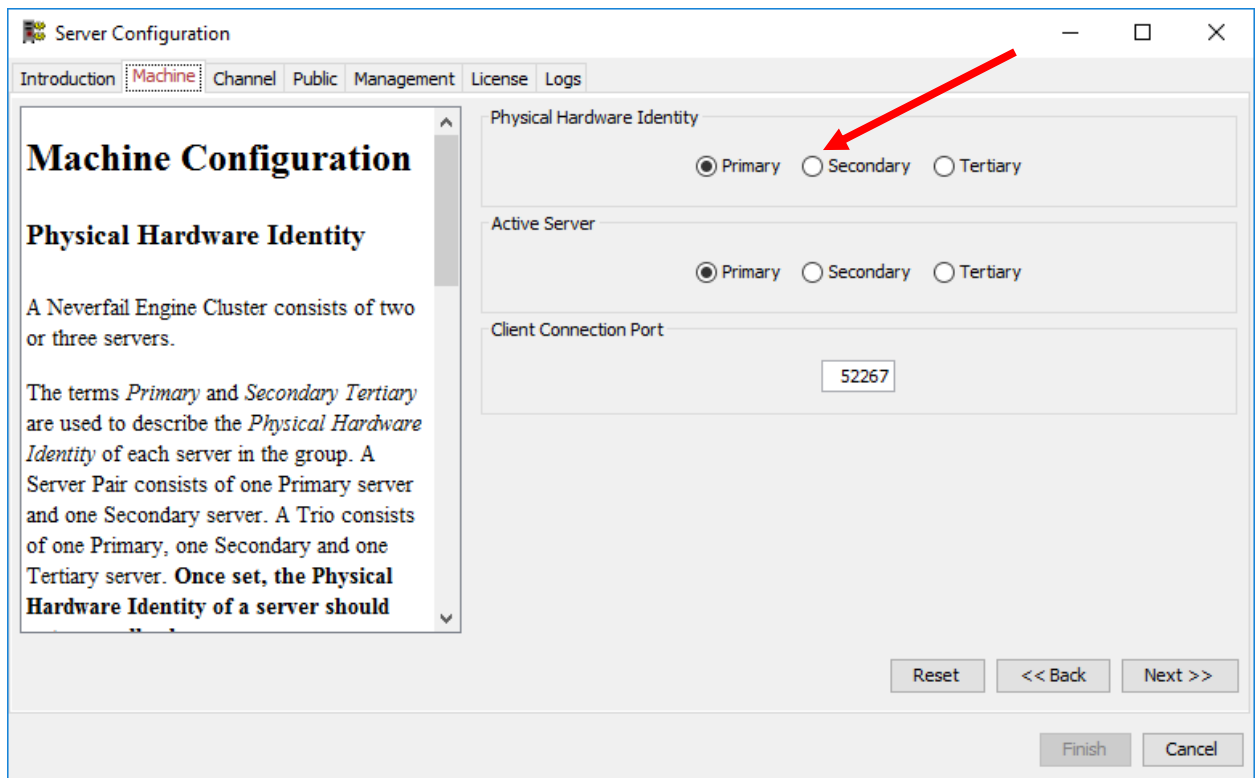


Figure 11. Configure Server Wizard – Machine Tab

- 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.

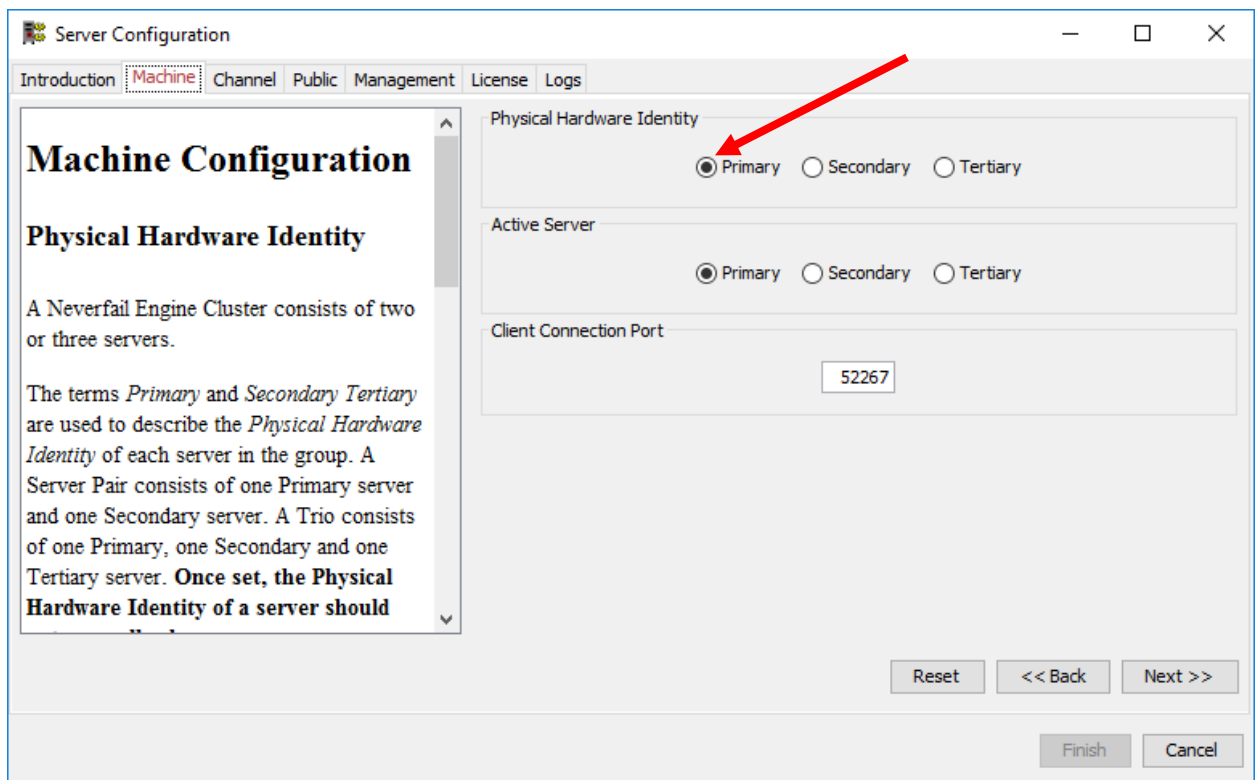


Figure 12. Configure Server Wizard – Machine Tab

- 18 Click **Finish**.
- 19 In the task bar, right click the Neverfail System Tray Application icon and select Start Engine.
- 20 Log into the Neverfail Advanced 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 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. through f. for any additional drives that must be restored.

- 12 Restore the System State.
 - a Perform steps a. through 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 then 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 Channel Packet Filter is enabled for the Public network connection and disabled for all channel connections (C:\Program Files\Neverfail\R2\bin nfpkftlfr.exe displayconfig). 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 Server Configuration wizard, verify that the Identity and Active Server are configured correctly.

19 On the **Public** tab of the Neverfail Server Configuration wizard, verify that the Public IP is correct.

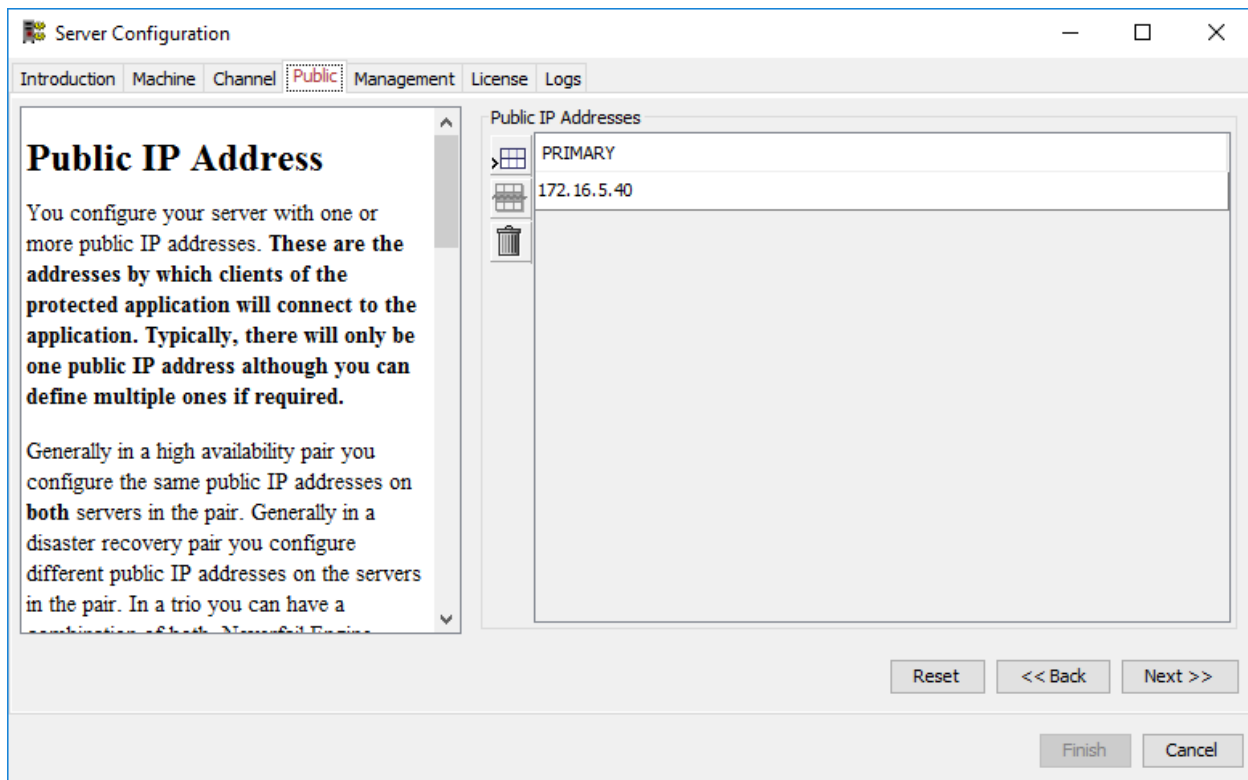


Figure 13. Configure Server Wizard – Public Tab

- 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 interface for testing.
- 22 Reconnect the Public and Channel interface cable.
- 23 In the task bar, right click the Neverfail System Tray Application icon and then select **Start Engine**.
- 24 Log into the Neverfail Advanced 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 > Neverfail > Advanced Management Client**.
- 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 > Neverfail > Advanced Management Client**.
- 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.