

Command Line Installation

For
Neverfail Heartbeat v6.7



You can find the most up-to-date technical documentation on the Neverfail Extranet at:

<http://extranet.neverfailgroup.com>.

The Neverfail Extranet also provides the latest product updates. If you have comments about this documentation, submit your feedback to:

docfeedback@neverfailgroup.com

The Neverfail Group has taken all reasonable care to ensure the information in this document is accurate at the date of publication. In relation to any information on third party products or services, the Neverfail Group has relied on the best available information published by such parties. The Neverfail Group is continually developing its products and services, therefore the functionality and technical specifications of the Group's products can change at any time. For the latest information on the Neverfail Group's products and services, please contact us by email (info@neverfailgroup.com) or visit our Web site www.neverfailgroup.com).

Heartbeat is a product trade mark of the Neverfail Group Ltd. Neverfail products are protected, in whole or in part by U.S. and foreign patents, which include US. Patent No. 7,409,577 and 7,788,524 and European Patent No. 1,397,744.

All third party product names referred to in this document are acknowledged as the trade marks for their respective owner entities.

© 2002-2013 Neverfail Group Ltd. All rights reserved.

Contents

Preface: About This Book.....	v
Chapter 1: Introduction.....	7
Neverfail Heartbeat Concepts.....	7
Communications.....	8
Neverfail Heartbeat Switchover and Failover Processes.....	9
Chapter 2: Implementation.....	11
Implementation Overview.....	11
Common Requirements.....	11
Server Architecture Options.....	13
Virtual to Virtual (V2V).....	13
Physical to Virtual (P2V).....	13
Physical to Physical (P2P).....	13
Cloning Technology Options.....	15
Supported Pre-Clone Technologies.....	15
Supported Install Clone Technologies.....	15
Network Options.....	16
Local Area Network (LAN).....	16
Wide Area Network (WAN).....	16
Network Interface Card (NIC) Configuration.....	18
Chapter 3: Command Line Installation.....	21
Command Line Usage.....	21
Parameter File Elements.....	22
Command Line Installation of the Primary Server.....	24
Command Line Installation of a Virtual Secondary or Tertiary Server.....	25
Command Line Installation of a Physical Secondary or Tertiary Server.....	26
Command Line Installation of Neverfail Heartbeat Client Tools.....	26
Command Line Uninstall of Neverfail Heartbeat	27
Appendix A: Setup Error Messages.....	29
Appendix B: Installation Verification Testing.....	33
Testing a Neverfail Heartbeat Pair.....	33
Exercise 1 - Auto-switchover.....	33
Exercise 2 - Data Verification.....	35
Exercise 3 - Switchover.....	36
Testing a Neverfail Heartbeat Trio.....	36
Exercise 1 - Auto-switchover.....	37
Exercise 2 - Managed Switchover.....	38
Exercise 3 - Data Verification.....	40

Glossary.....43

About This Book

The Installation Guide provides information about installing Neverfail Heartbeat, including implementation in a Local Area Network (LAN) or Wide Area Network (WAN). This book provides an overview of installation procedures and guidance for configuration of Neverfail Heartbeat when using the Command Line installation method.

Intended Audience

This guide assumes the reader has a working knowledge of networks including the configuration of TCP/IP protocols and domain administration, notably in Active Directory and DNS.

Overview of Content

This guide is designed to give guidance on the installation and configuration of Neverfail Heartbeat, and is organized into the following sections:

- Preface — *About This Book* (this chapter) provides an overview of this guide and the conventions used throughout.
- Chapter 1 — *Introduction* presents an overview of Neverfail Heartbeat concepts including the Switchover and Failover processes.
- Chapter 2 — *Implementation* discusses environmental prerequisites and pre-install requirements for installation, options for server architecture, cloning technology, application components, and network configurations. It also gives guidance on anti-malware solutions, and provides a convenient summary of supported configurations as you perform the installation.
- Chapter 3 — *Command Line Installation* describes the installation process, guides you through installation on the Primary, Secondary, and Tertiary servers, and through post-installation configuration.
- Appendix A — *Setup Error Messages* lists error messages that may appear during setup and tests that will help you resolve the errors.
- Appendix B — *Installation Verification* provides a procedure to verify that Neverfail Heartbeat is properly installed and initially configured.

Document Feedback

Neverfail welcomes your suggestions for improving our documentation and invites you to send your feedback to docfeedback@neverfailgroup.com.

Abbreviations Used in Figures

Abbreviation	Description
Channel	Neverfail Channel
NIC	Network Interface Card
P2P	Physical to Physical
P2V	Physical to Virtual
V2V	Virtual to Virtual

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current version of this book and other books, go to <http://extranet.neverfailgroup.com> .

Online and Telephone Support

Use online support to view your product and contract information, and to submit technical support requests. Go to <http://extranet.neverfailgroup.com/support> .

Support Offerings

To find out how Neverfail Support offerings can help meet your business needs, go to <http://www.neverfailgroup.com/services/technical-support.html> .

Neverfail Professional Services

Neverfail Professional Services courses offer extensive hands-on labs, case study examples, and course materials designed for use as on-the-job reference tools. Courses are available on site, in the classroom, and live online. For the day-to-day operations of Neverfail Heartbeat, Neverfail Professional Services provides offerings to help you optimize and manage your Neverfail Heartbeat servers. To access information about education classes, certification programs, and consulting services, go to <http://www.neverfailgroup.com/services/professional-services.html> .

Chapter 1

Introduction

Neverfail Heartbeat is a Windows based service specifically designed to provide High Availability or Disaster Recovery for server configurations in one solution

Neverfail Heartbeat Concepts

Architecture

Neverfail Heartbeat software is installed on a *Primary* (production) server and a *Secondary* (ready-standby) server. These names refer to the Identity of the servers and never change throughout the life of the server.

***Note:** In this document, the term “Cluster” refers to a Neverfail Heartbeat Cluster. Refer to the [Glossary](#) for more information about Neverfail Heartbeat Clusters.*

Depending on the network environment, Neverfail Heartbeat can be deployed in a Local Area Network (LAN) for High Availability or Wide Area Network (WAN) for Disaster Recovery, providing the flexibility necessary to address most network environments.

When deployed, one of the servers performs the *Role* of the *Active* server that is visible on the Public network while the other is *Passive* and hidden from the Public network but remains as a ready-standby server. The Secondary server has the same domain name, uses the same file and data structure, same Principal (Public) network address, and can run all the same applications and services as the Primary server. Only one server can display the Principal (Public) IP address and be visible on the Public network at any given time. Neverfail Heartbeat software is symmetrical in almost all respects, and any of the servers can take the active role and provide protected applications to the user.

Neverfail Heartbeat provides continuous access to the passive server simultaneously as the active server continues to service clients allowing the passive server to be easily accessed for maintenance purposes, updating anti-malware definition files, receiving operating system hot-fixes, updates and patches from third-party management software, and allows use of third-party monitoring tools.

Protection Levels

Neverfail Heartbeat provides the following protection levels:

- *Server Protection* – provides continuous availability to end users through a hardware failure scenario or operating system crash. Additionally, Neverfail Heartbeat protects the network identity of the production server, ensuring users are provided with a replica server on the failure of the production server.

- *Network Protection* – proactively monitors the network by polling up to three nodes to ensure that the active server is visible on the network.
- *Application Protection* – maintains the application environment ensuring that applications and services stay alive on the network.
- *Performance Protection* – monitors system performance attributes to ensure that the system administrator is notified of problems and can take pre-emptive action to prevent an outage.
- *Data Protection* – intercepts all data written by users and applications, and maintains a copy of this data on the passive server which can be used in the event of a failure.

Neverfail Heartbeat provides all five protection levels continuously, ensuring all facets of the user environment are maintained at all times, and that the Public network continues to operate through as many failure scenarios as possible.

Communications

Neverfail Heartbeat communications consist of two crucial components, the Neverfail Channel and the Principal (Public) network.

To accommodate communications requirements, Neverfail Heartbeat can be configured to use either multiple NICs (1 X Channel and 1 X Principal (Public) connection) on each server providing a separate dedicated Neverfail Channel network from the Principal (Public) network or a single NIC on each server to fulfill both the Neverfail Channel and Principal (Public) network connection requirements.

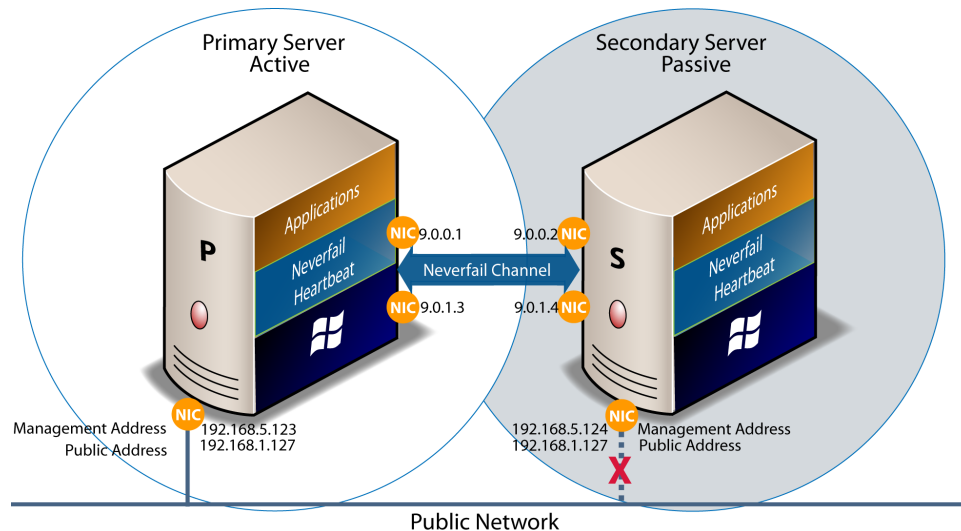


Figure 1: Communications Between Primary and Secondary Servers

Neverfail Channel

The first component is the Neverfail Channel which provides communications between the active and passive servers. The Neverfail Channel is used for control and data transfer from the active server to the passive servers and for monitoring of the active server's status by the passive servers.

The NICs on the active and passive servers used for the Neverfail Channel are normally configured with IP addresses outside of the Principal (Public) network subnet range and are referred to as the Neverfail Channel addresses. During installation, setup will disable NetBIOS for the Neverfail Channel(s) on the active and passive servers to prevent server name conflicts.

The NICs that support connectivity across the Neverfail Channel can be standard 100BaseT Ethernet cards providing a throughput of 100 Mbits per second across standard Cat-5 cabling. When using multiple NICs providing a separate dedicated Neverfail Channel, this channel requires no hubs or routers, but the direct connection does require crossover cabling.

When configured for a WAN deployment, configure the Neverfail Channel to use static routes over switches and routers to maintain continuous communications independent from corporate or public traffic.

Principal (Public) Network

The second component is the Principal (Public) network used by clients to connect to the active server. The Principal (Public) network provides access to the Principal (Public) IP address used by clients to connect to the active server.

The Principal (Public) IP address is a static IP address that is only available on the currently active server and is the IP address a client uses to connect to the active server. It must be configured as a static IP address, that is, not DHCP (Dynamic Host Configuration Protocol) enabled. In the figure above, the IP address is configured as 192 . 168 . 1 . 127. The Principal (Public) IP address is shared by the active and passive servers in a LAN and is always available on the currently active server in the cluster. In the event of a switchover or failover, the Principal (Public) NIC is blocked on the previously active server and is then available on the new active server. When configured, a Management IP address will provide access to a server regardless of the role of the server.

Management IP Address

All servers in the cluster can be configured with Management IP addresses that 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 Principal (Public) IP address or Neverfail Channel IP address and is always available for administrators to access the server.

Neverfail Heartbeat Switchover and Failover Processes

Neverfail Heartbeat uses four different procedures – managed switchover, automatic switchover, automatic failover, and managed failover – to change the role of the active and passive servers depending on the status of the active server.

- *Managed Switchover* – You can click **Make Active** on the Neverfail Heartbeat Management Client *Server: Summary* page to manually initiate a managed switchover. When a managed switchover is triggered, the running of protected applications is transferred from the active machine to the passive machine in the server pair. The server roles are reversed.
- *Automatic Switchover* – Automatic switchover (auto-switchover) is similar to failover (discussed in the next section) but is triggered automatically when system monitoring detects failure of a protected application.
- *Automatic Failover* – Automatic failover is similar to automatic switchover (discussed above) but is triggered when the passive server detects that the active server is no longer running properly and assumes the role of the active server.
- *Managed Failover* – Managed failover is similar to automatic failover in that the passive server automatically determines that the active server has failed and can warn the system administrator about the failure, but no failover actually occurs until the system administrator manually triggers this operation (the default configuration in a DR environment).

Chapter 2

Implementation

This chapter discusses the deployment options and prerequisites to successfully implement Neverfail Heartbeat and provides a step-by-step process to assist in selecting options required for installation.

Implementation Overview

Neverfail Heartbeat is a versatile solution that provides multiple configurations to suit user requirements. Neverfail Heartbeat can be deployed as a Pair in either a LAN or WAN, or as a Trio utilizing both a LAN and a WAN connection.

This chapter discusses the deployment options and the necessary prerequisites for each option, and provides a step-by-step process to assist you in selecting the options required to successfully implement Neverfail Heartbeat.

Prior to installing Neverfail Heartbeat, you must identify the preferred deployment options. The installation process requires you to select options throughout the procedure to achieve the best configuration for your requirements.

During the installation process, Neverfail Heartbeat performs a variety of checks to ensure the server meets the minimum requirements for a successful installation. If the server fails one of the checks, a *Critical Stop* or *Warning* message is displayed. [Setup Error Messages](#) provides an explanation of the messages. You must resolve Critical Stops before you can proceed with setup.

Common Requirements

The following requirements must be met to support a successful installation of Neverfail Heartbeat.

Environmental Prerequisites

The server protected by Neverfail Heartbeat must not be configured as a domain controller, global catalog, or DNS server. If it is, it must be reconfigured before installing Neverfail Heartbeat.

System Requirements

To support the installation of Neverfail Heartbeat, systems must meet the following minimum requirements:

- Supported Operating Systems

Important: *Neverfail Heartbeat requires that Microsoft™ .Net Framework 4 be installed prior to running Setup.exe. If .Net Framework 4 is not installed when you attempt to initiate Setup, Neverfail Heartbeat will prevent installation until .Net Framework 4 is installed.*

Windows Server 2003 must have Windows Imaging Component (WIC) installed prior to installing Microsoft .Net Framework 4.

- Windows Server 2003 x86 and x64 Standard / Enterprise / R2 with SP2
- Windows Server 2008 x 86 and x64 Standard / Enterprise with SP1 or SP2
- Windows Server 2008 R2 x64 Standard / Enterprise / Datacenter and SP1
- Windows Server 2012 x64 Standard / Datacenter
- 1GB of available RAM (2GB recommended)

Note: *During the setup process, Neverfail Heartbeat verifies that a minimum of 1GB of RAM is available.*

To ensure proper operation, Neverfail Heartbeat requires a minimum of 1GB of RAM in addition to the memory requirements of the Operating System and installed applications. 256MB of RAM must remain available to the Neverfail Heartbeat application suite at all times.

- 2 GB of disk space available on the drive to receive the Neverfail Heartbeat installation

Note: *Although Neverfail Heartbeat requires only 2GB of available disk space on the drive to receive the Neverfail Heartbeat installation, once installed, the size of each send and receive queue is configured by default for 10GB. For Trio configurations the send and receive queues will by default require 20GB per server. You must ensure that sufficient disk space is available to accommodate the send and receive queues or modify the queue size configuration to prevent MaxDiskUsage errors.*

- Latest Microsoft security updates
- Local administrator rights for installation

Note: *Neverfail Heartbeat services are required to be run under the Local System account.*

Configuration Requirements

In addition to the system requirements listed above, the network environment must meet the following criteria to support the installation and operation of Neverfail Heartbeat:

- Plugs-ins on pre-cloned servers must be located with the same path as on the Primary server for a successful installation. For example, if the path on the Primary server is C:\temp\<pluginname.dll>, then the path to the plug-in on the pre-cloned server(s) also must be C:\temp\<pluginname.dll>.
- All applications intended to receive Neverfail Heartbeat protection must be installed and configured on the Primary server prior to installing Neverfail Heartbeat
- The Primary, Secondary, and Tertiary servers must be set to identical System Date, Time, and Time Zone. Once configured, do not change the Time Zone
- If installing on Windows Server 2003, verify that the Principal (Public) network adapter is listed as the first network adapter in the Network Connections Bind Order on each server. (**Network Connections > Advanced > Advanced Settings**)

Server Architecture Options

Neverfail Heartbeat supports Virtual to Virtual, Physical to Virtual, and Physical to Physical architectures for both pair and trio configurations. The selected server architecture determines the hardware requirements and impacts the technique used to clone the Primary server.

Virtual to Virtual (V2V)

In a V2V architecture, Neverfail Heartbeat allows cloning of the Primary server prior to the installation of Neverfail Heartbeat using VMware Converter, VMware vCenter Cloning Utility, and other 3rd party utilities. Benefits to this architecture include reduced hardware cost, shorter installation time, and use of the Pre-Clone technique for installation. Secondary and Tertiary virtual machines must meet the following minimum requirements:

- The configuration of Secondary and Tertiary virtual machines must match the Primary virtual machine:
 - Similar CPU, including resource management settings
 - Similar memory configuration, including resource management settings.
- Appropriate resource pool priorities
- Each virtual machine in a V2V configuration must be on a separate host to guard against failure at the host level
- Each virtual NIC must use a separate virtual switch (network)

Physical to Virtual (P2V)

P2V architecture is used when the environment requires a mix of physical and virtual machines, such as when Neverfail Heartbeat is installed on a physical server in an environment with limited available hardware. This architecture is appropriate if you must avoid adding additional physical servers or when you prefer to migrate to virtual technologies over a period of time. Secondary and Tertiary virtual machines must meet the following minimum requirements:

- The configuration of Secondary and Tertiary virtual machines must match the Primary physical server:
 - Similar CPU
 - Similar memory
- Secondary and Tertiary virtual machines require sufficient priority in resource management settings so that other virtual machines do not impact their performance.
- Each virtual NIC must use a separate virtual switch.

Physical to Physical (P2P)

P2P architecture is used in an environment that requires physical servers. Use of P2P architecture requires use of the Install Clone technique.

Primary Server

The Primary server in a P2P architecture must meet the hardware and software requirements specified in [Common Requirements](#).

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
 - Similar memory
- An identical number of NICs to the Primary server
- 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

Note: The Neverfail Heartbeat standard implementation process assumes that the Advanced Configuration and Power Interface (or ACPI) compliance of both machines are identical. If this is not the case, contact Neverfail Support at <http://extranet.neverfailgroup.com/support> for further information.

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 Heartbeat
- Set up in a Workgroup prior to installing Neverfail Heartbeat
- The System Date, Time, and Time Zone must be consistent with Primary server

Tertiary Server

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

Hardware

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

- Hardware must be equivalent to the Primary server:
 - Similar CPU
 - Similar memory
- A minimum of three NICs (one for each channel and one for the Principal (Public) connection)
- 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

Note: The Neverfail Heartbeat standard implementation process assumes that the Advanced Configuration and Power Interface (or ACPI) compliance of both machines are identical. If this is not the case, contact Neverfail Support at <http://extranet.neverfailgroup.com/support> for further information.

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 driver letter and directory as on the Primary server
- The Machine name must be different from the Primary and Secondary server prior to installing Neverfail Heartbeat
- Set up in a Workgroup prior to installing Neverfail Heartbeat
- System Date / Time and Time Zone must be consistent with Primary server

Cloning Technology Options

Cloning the Primary server to create nearly identical Secondary and/or Tertiary servers involves different techniques depending on the selected server architecture option.

Supported Pre-Clone Technologies

The following cloning technologies are supported for creating Pre-Cloned images for use as a Secondary or Tertiary server:

- VMware Converter for Physical to Virtual (P2V)
- VMware vCenter virtual machine cloning for Virtual to Virtual (V2V)
- Other third party utilities

Supported Install Clone Technologies

Installation of Neverfail Heartbeat provides support for NTBackup on Windows 2003 and Wbadmin on Windows Server 2008 for automated Install Cloning.

This process is automated, but all prerequisites for the Secondary and Tertiary (when deployed) server specified under *Physical to Physical (P2P)* requirements must be met.

Note: When installing in a Physical to Virtual (P2V) architecture, VMware Tools must not be installed on the Secondary/Tertiary server during the Neverfail Heartbeat installation process. If VMware Tools are currently installed on the Secondary/Tertiary server, you must fully uninstall VMware Tools prior to initiation of the Setup process. Once the installation of Neverfail Heartbeat has completed, you may reinstall VMware Tools.

Important: When installing on Windows Server 2003, verify that the Principal (Public) network adapter is listed first in the bind order of the **Network Connections > Advanced > Advanced Settings** dialog.

Network Options

Networking requirements are contingent upon how Neverfail Heartbeat is deployed. To deploy as a High Availability (HA) solution, a LAN configuration is required. To deploy Neverfail Heartbeat for Disaster Recovery (DR), a WAN configuration is required. Each network configuration has specific configuration requirements to ensure proper operation.

Note: *Neverfail recommends that the Neverfail Channel be configured on a different subnet than the Principal (Public) network. In the event that this is not possible, see KB 2527 — Configuring Neverfail Heartbeat Channel and Public Connections to use the Same Subnet.*

Neverfail Heartbeat can be configured to run using multiple NICs or a single NIC.

Multiple NICs

Neverfail Heartbeat supports use of multiple NICs on each server pair. When using multiple NICs, one NIC is configured with the Principal (Public) IP address for client access while a second dedicated NIC is configured with the Neverfail Channel IP address. Deploying with multiple NICs provides the advantage of redundancy and also removes the risk of single point of failure that exists in single NIC configurations. To configure using multiple NICs on each server, see [Multi-NIC Configuration](#).

Note: *Neverfail Heartbeat does NOT out-of-the-box support teams of NICs but can be configured to support teamed NICs with additional configuration steps when installing with teamed NICs present. See knowledge base article KB-114 — How to install the Neverfail Heartbeat Packet Filter Driver on a NIC team (Teamed NICs, NIC Teaming) for more information about teamed NICs.*

Single NIC

Neverfail Heartbeat also supports use of a single NIC configured to perform both functions, providing the Principal (Public) IP address to users and the Neverfail Channel for data transfer and control. To configure using a single NIC on each server, see [Single NIC Configuration](#).

Local Area Network (LAN)

When deployed in a LAN environment, Neverfail Heartbeat requires that both servers use the same Principal (Public) IP address. Each server also requires a Neverfail Channel IP address.

Wide Area Network (WAN)

Neverfail Heartbeat supports sites with different subnets. In this scenario, the Primary and Secondary servers in the Neverfail Heartbeat Pair or Secondary and Tertiary servers in a trio will require unique Principal (Public) IP addresses in each subnet and a unique Neverfail Channel IP address in each subnet for each server. During Setup, select the *Use different IP addresses for Secondary (Recommended for DR secondary)* and specify the Principal (Public) IP addresses of both the Secondary server and the Primary server in the pair. If deployed in a trio, during Setup, select the *Use same IP address for Secondary (Recommended for HA secondary)* and add the Principal (Public) IP address for the Tertiary server.

Neverfail Heartbeat, using multiple NICs, also supports sites with the same subnet. In this scenario the Neverfail Heartbeat shares a single Principal (Public) IP address between the Primary and Secondary server making it available on the active server. Although the Neverfail Channel addresses should be unique within the same subnet. During Setup, select the *Use same IP addresses for Secondary (Recommended*

for HA secondary) on the *Principal (Public) IP Address Configuration* page and specify the IP address to be shared by both servers.

WAN Requirements

WAN deployments require the following:

- Persistent static routing configured for the channel connection(s) where routing is required
- One NIC minimum, two NICs (1 x Public and 1 x Channel) are recommended
- At least one Domain Controller at the Disaster Recovery (DR) site
- If the Primary and DR site uses the same subnet:
 - During install, follow the steps for a LAN or VLAN on the same subnet
 - Both the Primary and Secondary servers in the pair or the Secondary and Tertiary servers in the trio use the same Public IP address
- If the Primary and DR site use different subnets:
 - During install, follow the steps for a WAN
 - The Primary and Secondary servers in the Neverfail Heartbeat pair or the Secondary and Tertiary servers in the trio require a separate Principal (Public) IP address and a Neverfail Channel IP address
 - Provide a user account with rights to update DNS using the `DNSUpdate.exe` utility provided as a component of Neverfail Heartbeat through Neverfail Heartbeat Management Client **Applications > Tasks > User Accounts**
 - Neverfail recommends integrating Microsoft DNS into AD so that `DNSUpdate.exe` can identify all DNS Servers that require updating
 - At least one Domain Controller at the DR site
 - Refer to the following articles in the Neverfail Knowledge Base:
 - ◆ Knowledge base article KB-1425 – Configuring DNS with Neverfail Heartbeat in a WAN Environment
 - ◆ Knowledge base article KB-1599 – Configuring Neverfail Heartbeat to Update BIND9 DNS Servers Deployed in a WAN

Bandwidth

Neverfail Heartbeat includes automatic bandwidth optimization in WAN environments. This feature compresses data transferred over the Neverfail Channel, optimizing the traffic for low bandwidth connections causing some additional CPU load on the active server.

Determine the available bandwidth and estimate the required volume of data throughput to determine acceptable latency for the throughput. Additionally, the bandwidth can affect the required queue size to accommodate the estimated volume of data. Neverfail recommends making a minimum of 1Mbit of spare bandwidth available to Neverfail Heartbeat.

Latency

Latency has a direct effect on data throughput. Latency on the link should not fall below the standard defined for a T1 connection.

Neverfail SCOPE Data Collector Service can assist in determining the available bandwidth, required bandwidth, and server workload. For more information about Neverfail SCOPE Data Collector Service, contact Neverfail Professional Services.

Network Interface Card (NIC) Configuration

Neverfail Heartbeat supports the use of both a single NIC or multiple NIC configuration on Primary, Secondary, and Tertiary (if installed) servers. The number of NICs present will determine how the NICs are configured.

Important: *The Primary, Secondary, and Tertiary (if installed) servers must have the same number of NICs.*

Multi-NIC Configuration

When Using multiple NICs, one NIC functions for client and management access while a second NIC functions as a dedicated Neverfail Channel.

Primary Server

The Primary server is configured with the following connections:

- A Principal (Public) network connection configured with a static Principal (Public) IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.
- Neverfail Channel connection(s) configured with a static IP address in a different subnet than the Principal (Public) IP address, and with a different IP address than the Secondary server channel NIC, and network mask. No gateway or DNS server address is configured. NetBIOS will be disabled during the installation process to prevent server name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared on the Neverfail Channel connection(s) prior to installing Neverfail Channel.

Secondary/Tertiary Server

The Secondary/Tertiary server must have the same number of NICs as the Primary server and is configured as follows:

- A Principal (Public) connection configured with a static IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.

Note: *If deploying as a pair in a WAN, the Principal (Public) IP address of the Secondary server may be in a different subnet than the Primary server.*

Note: *If configured in a trio, the Primary and Secondary servers are configured for LAN deployment and the Secondary and Tertiary servers are configured for WAN deployment.*

- Neverfail Channel network connection(s) configured on a separate dedicated NIC with a static IP address in a different subnet than the Secondary/Tertiary Principal (Public) IP address, and with a different IP address than the Primary or Secondary server's Neverfail Channel NIC, and a network mask. No gateway address or DNS server address is configured. NetBIOS will be disabled during the installation process to prevent server name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared on the Neverfail Channel connection(s) prior to installing Neverfail Channel.

Single NIC Configuration

Configuring Neverfail Channel using a single NIC requires that both functions (Client access and Channel operations) use the same physical or virtual NIC.

Primary Server

The Primary server requires a single NIC configured with the following IP addresses:

- A Principal (Public) IP address - configured using a static IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.
- A Neverfail Channel IP address - configured on the same NIC as the Principal (Public) IP address configured with a static IP address in a different subnet than the Principal (Public) IP address, and a network mask. No gateway address or DNS server address is configured. NetBIOS will be disabled during the installation process to prevent server name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared prior to installing Neverfail Channel.

Important: Ensure that your server has a persistent DNS entry in the DNS system for the Principal (Public) IP address.

Secondary/Tertiary Server

The Secondary/Tertiary server must have the same number of NICs as the Primary server and be configured as follows:

- A Neverfail Channel IP address - configured with a static IP address and the network mask. No gateway or DNS server address is configured. NetBIOS will be disabled during the installation process to prevent server name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared prior to installing Neverfail Channel.

Important: Ensure that your server has a persistent DNS entry in the DNS system for the Principal (Public) IP address. The Secondary/Tertiary server's Principal (Public) IP address will be configured during the Setup process.

Chapter 3

Command Line Installation

Command Line Usage

To perform an unattended installation, you must run the `start /wait Setup` command with the appropriate parameters from the command line. Additionally, you must create a `.txt` file (parameter file) that contains the information necessary to provide the intended options to the Setup application. The following information provides details about the parameters and parameter file necessary to successfully perform a command line installation.

Note: Users should not cut-and-paste from this .pdf document but should type the actual commands and parameters.

```
start /wait Setup [-h]
[-f<parameter file>] [-ni [-sp -se -sw -di]]
[-DNSPassword:<password>] [-BACKUPPassword:<password>]
[-secondaryInstall|-uninstall|-drvInstall|]
```

Table 1: Command Line Parameters

Parameter	Description
-h	Displays this usage information
-f:<parameter file>	Uses a file of parameters to run Important: If the file name/path contains any white space (space, tab) or special characters(-, /, etc.) then it must be enclosed in quotes "..."
-ni	Not interactive, suppresses the Graphical User Interface. This instructs Setup not to use the Graphical User Interface. If this parameter is not specified but a parameter file is specified, the Graphical User Interface pages will be fully populated and require that the Next or Proceed button be clicked and any popup dialog boxes be acknowledged.
-sp	Suppress Progress (Only for Non- interactive)
-se	Suppress Errors (Only for Non- interactive)

Parameter	Description
-sw	Suppress Warnings (Only for Non- interactive)
-di	Display Info (Only for Non- interactive)
-DNSPassword:<password>	The password used for DNSUpdate
-BACKUPPassword:<password>	The password used for WBADMIN
-uninstall	Do not use unless instructed to do so
-ADMINPassword:<Password>	The password to use for Administrator
-drvInstall	Do not use unless instructed to do so
-secondaryInstall	Do not use unless instructed to do so

Important: Only the DOS shell requires the "start /wait"

Table 2: Return Codes

Code	Description
0	: Success
1	: Incorrect Usage (not enough parameters)
2	: Invalid Parameter
3	: File cannot be opened (file cannot be found)
4	: File parse failed
5	: Unable to Run (See output for specific problems)
6	: Processing failed

Parameter File Elements

The parameter file is used to pass setup options to the Setup application and is made up of a sequence of tagged lines, with the tag indicating what the data describes.

For example: `INSTALLTYPE:Install`

Important: The parser is case insensitive. Any values containing white space must be enclosed with double quotes, for example "pre clone". If the file name/path contains any white space (space, tab) or special characters(-, /, etc.) then it must be enclosed in quotes "..."

Table 3: Parameter File Elements

Tag	Values	Comments
FORMATVERSION:	V1_0 (Default)	Used to indicate the Format of the tags listed after this line. This can be used multiple times.

Tag	Values	Comments
INSTALLTYPE :	Install Install Client Tools Only Install AM(X) Install Service Pack Uninstall Uninstall Components	
LICENSEKEY :	Valid license key	
PLUGINPATH :	Must be a valid path and include the plug-in file name	Only one per line but can be defined multiple times
FEATUREFORINSTALLATION :	Neverfail Heartbeat	Only one per line but can be defined multiple times
SERVERROLE :	Primary Secondary	
TOPOLOGY :	HA DR	
ACCEPT_EULA :	True False	
DEFAULTCHANNELPORT :	Must be an integer	
DESTINATIONPATH :	Must be a valid path	
BACKUPDESTINATIONPATH :	Must be a valid path	Used to indicate where to write the pre-synchronization data
BCKUPSOURCEPATH :	Must be a valid path	Used to locate the pre-synchronization data for installation of the Secondary server
INCLUDEPROTECTEDDATAINBACKUP :	True False	
NETWORKTASKDOMAIN :		Used when the Principal (Public) IP addresses are different for different servers (usually for a DR topology)
NETWORKTASKUSER :		Used when the Principal (Public) IP addresses are different for different servers (usually for a DR topology)
LEAVEONNETWORK :	True False	
COMPUTERNAMEPOSTUNINSTALL :	Must be a string	
CLIENTCONNECTIONPORT :	Must be an integer	
SECONDARYCLONETYPE :	Full Merge Pre clone	<i>Note: The Full and Merge clone types are not supported for Command Line Installation</i>

Tag	Values	Comments
TERTIARYCLONETYPE :	Full Merge Pre clone	
BACKUPUSER :		
SECONDARYPRINCIPLEADDRESS :	Must be an IP address	Only one per line but can be defined multiple times
TERTIARYPRINCIPLEADDRESS :	Must be an IP address	Only one per line but can be defined multiple times
PRIMARYSECONDARYCHANNEL :	Must be an IP address	Only one per line but can be defined multiple times
SECONDARYTERTIARYCHANNEL :	Must be an IP address	Only one per line but can be defined multiple times
TERTIARYPRIMARYCHANNEL :	Must be an IP address	Only one per line but can be defined multiple times
STARTSERVICEATEND :	True False	

Command Line Installation of the Primary Server

Installation of Neverfail Heartbeat begins with the Primary server.

1. The following is an example of a parameter file (it must be modified before you use it).

<file_name.txt>

Tertiary Installation Example :

```

INSTALLTYPE:Install
ACCEPT_EULA:true
LICENSEKEY:<license serial number>
SERVERROLE:PRIMARY
TOPOLOGY:<"HA AND DR">
SECONDARYCLONETYPE:"pre clone"
TERTIARYCLONETYPE:full
DESTINATIONPATH:"C:\Program Files\
C:\Program Files\Neverfail\
"
PRIMARYSECONDARYCHANNEL:<10.0.1.1,10.0.1.2>
SECONDARYTERTIARYCHANNEL:<10.0.2.2,10.0.2.3>
TERTIARYPRIMARYCHANNEL:<10.0.3.3,10.0.3.1>
PRIMARYPRINCIPLEPADDESS:<192.168.99.111>
SECONDARYPRINCIPLEPADDESS:<192.168.99.111>
TERTIARYPRINCIPALADDRESS:<192.168.98.113>
NETWORKTASKDOMAIN:dnstest.com
NETWORKTASKUSER:administrator
CLIENTCONNECTIONPORT:52267
FEATUREFORINSTALLATION:"Neverfail Heartbeat"
BACKUPDESTINATIONPATH:\\<10.0.1.1\nf backup>
BACKUPUSER:Administrator
INCLUDEPROTECTEDDATAINBACKUP:true
//AMXPATH:
PLUGINPATH:"C:\nfsql\SqlServerNFPlugin.dll"
```



```
//DEFAULTCHANNELPORT:
//BACKUPSOURCEPATH:
STARTSERVICEATEND:True
```

Note: The parameters enclosed in <> can be enclosed in double quotes (") and should be if they contain spaces, dashes or other potentially confusing characters.

DR Installation Example:

```
INSTALLTYPE:Install
ACCEPT_EULA:true
LICENSEKEY:<license serial number>
SERVERROLE:PRIMARY
TOPOLOGY:<DR>
SECONDARYCLONETYPE:"pre clone"
DESTINATIONPATH:"
C:\Program Files\Neverfail\
"
PRIMARYSECONDARYCHANNEL:<10.0.1.1,10.0.5.2>
PRIMARYPRINCIPLEPADDESS:<192.168.99.111>
SECONDARYPRINCIPLEPADDESS:<192.168.98.104>
NETWORKTASKDOMAIN:dnstest.com
NETWORKTASKUSER:administrator
CLIENTCONNECTIONPORT:52267
FEATUREFORINSTALLATION:Neverfail Heartbeat
BACKUPDESTINATIONPATH:\\<10.0.1.1\nf backup>
BACKUPUSER:Administrator
INCLUDEPROTECTEDDATAINBACKUP:true
//AMXPATH:
PLUGINPATH:"C:\nfsql\SqlServerNFPlugin.dll"
//DEFAULTCHANNELPORT:
//BACKUPSOURCEPATH:
STARTSERVICEATEND:True
```

Note: The parameters enclosed in <> must be enclosed in double quotes (") if they contain spaces, dashes or other potentially confusing characters.

2. Download the Neverfail Heartbeat .exe to a suitable location on the Primary server.
3. Extract the contents of the Neverfail Heartbeat .zip file into a temporary folder.
4. Navigate to **Start > Run** and type CMD to open a command window.
5. Navigate to the to the location of the temporary folder.
6. Run the command :start /wait setup -f:<parameter file> -DNSPassword:<DNS Password> -BACKUPPassword:<backup password> -ni

Command Line Installation of a Virtual Secondary or Tertiary Server

Installation of the Secondary and Tertiary server is similar to installation of the Primary server

1. Create a .txt file containing the following configuration parameters: This is an example of a parameter file (it must be modified before you use it).

<file_name.txt>

```
INSTALLTYPE:Install
```

```
SERVERROLE:SECONDARY
BACKUPSOURCEPATH:\\<192.168.15.111\nf backup>
BACKUPUSER:Administrator
```

Note: The parameters enclosed in <> must be enclosed in double quotes (") if they contain spaces, dashes or other potentially confusing characters.

2. Download the Neverfail Heartbeat .exe to a suitable location on the Secondary server.
3. Extract the contents of the Neverfail Heartbeat .zip file into a temporary folder.
4. Navigate to **Start > Run** and type CMD to open a command window.
5. Navigate to the to the location of the temporary folder.
6. Run the command: start /wait setup -f:<parameter file>
-BACKUPPassword:<backup password> -ni

Command Line Installation of a Physical Secondary or Tertiary Server

Installation of the Secondary and Tertiary server is similar to installation of the Primary server

1. Create a .txt file containing the following configuration parameters: This is an example of a parameter file (it must be modified before you use it).

<file_name.txt>

```
InstallSecParas.txt
INSTALLTYPE:Install
SERVERROLE:SECONDARY
BACKUPSOURCEPATH:\\<192.168.15.111\nf backup>
BACKUPUSER:Administrator
```

Note: The parameters enclosed in <> must be enclosed in double quotes (") if they contain spaces, dashes or other potentially confusing characters.

2. Download the Neverfail Heartbeat .exe to a suitable location on the Secondary server.
3. Extract the contents of the Neverfail Heartbeat .zip file into a temporary folder.
4. Navigate to **Start > Run** and type CMD to open a command window.
5. Navigate to the to the location of the temporary folder.
6. Run the command: start /wait setup -f:<parameter file>
-BACKUPPassword:<backup password> -ni

Command Line Installation of Neverfail Heartbeat Client Tools

Neverfail Heartbeat allows installation of Neverfail Heartbeat Client Tools for remote management of Neverfail Heartbeat clusters.

Prerequisites

When installing Neverfail Heartbeat Client Tools on Windows XP, the following Service Pack levels are required.

- Windows XP 32 bit SP3
- Windows XP 64 bit SP2

1. Create a .txt file containing the following configuration parameters:

Important: The following is an example of a parameter file (it must be modified before you use it). The content within the characters < and > indicate example text and the actual < and > characters should not be present in the edited file.

```
INSTALLTYPE:"Install Client Tools Only"
```

```
ACCEPT EULA:true
```

```
DESTINATIONPATH:<C:\AutoInstall>
```

2. Download the Neverfail Heartbeat .exe to a suitable location on the workstation .
3. Extract the contents of the Neverfail Heartbeat .zip file into a temporary folder.
4. Navigate to **Start > Run** and type CMD to open a DOS window.
5. Navigate to the to the location of the temporary folder.
6. Run the command: `start /wait setup -f:<parameter file> -ni`
7. Upon completion of the unattended installation, the **Manage Server** icon will appear on the desktop.

Command Line Uninstall of Neverfail Heartbeat

Neverfail Heartbeat allows you to uninstall the product from your Server using the command line method.

1. Ensure all the Neverfail Heartbeat processes are stopped and close the Neverfail Heartbeat Management Client and System Tray icon.
2. Create a .txt file with the following configuration parameters:

Important: The following is an example of a parameter file (it must be modified before you use it). The content within the characters < and > indicate example text and the actual < and > characters should not be present in the edited file.

```
INSTALLTYPE:Uninstall
```

```
LEAVEONNETWORK:true
```

3. Extract the contents of the Neverfail Heartbeat .zip file into a temporary folder.
4. Navigate to **Start > Run** and type CMD to open a DOS window.
5. Navigate to the to the location of the temporary folder.
6. Run the command: `start /wait setup -f:<parameter file> -ni`

After the uninstall process completes, you will be notified of any files that could not be removed and advised to delete them manually.

Note: *The SupportLogs directory is also left behind. This is intentional and should not be deleted in the event you need to submit a support report.*

Appendix

A

Setup Error Messages

Table 5: Setup Error Messages

<i>Message</i>	<i>Pri</i>	<i>Sec</i>	<i>Level</i>	<i>Test</i>
10 - 'The pre install check data file does not have the correct format. Setup cannot continue'.	No	Yes	Critical Stop	Check that the file adheres to the correct formatting and structure for use in analysis on the Secondary.
Setup has detected incompatible versions of the collector version \$x and the analyzer version \$y dll. This would suggest different versions of Setup have been run on the Primary and Secondary servers.	No	Yes	Critical Stop	Check that the analyzer and collector dlls are compatible.
File \$x cannot be analyzed it - may be corrupt Setup is unable to continue. If the file has been opened check that it has not been saved with Word Wrap.		Yes	Critical Stop	Check file format is correct.
190 - This server is a #1# domain controller. Neverfail Heartbeat must not be installed on a domain controller.	Yes	Yes	Critical Stop	Test whether the server is a domain controller.
173 - Neverfail Heartbeat does not support the '/3GB' switch on Windows 2000 Standard Edition.	Yes	Yes	Critical Stop	Test for /3GB on Windows 2000

Message	Pri	Sec	Level	Test
175 - Neverfail Heartbeat requires Windows 2003 Standard Edition SP1 or later if '/3GB' switch is on.	Yes	Yes	Critical Stop	
103 - Neverfail Heartbeat does not support #1#. The following are supported Windows 2000 Server SP4 or greater; Windows Server 2003 SP1 or greater.	Yes	Yes	Warning	
200 - Your #1# server uses the Intel ICH7 chipset and Windows 2000 has been detected. This combination is incompatible with Neverfail Heartbeat.	Yes	Yes	Critical Stop	
217 - Neverfail Heartbeat is not supported on Windows Storage Server Edition.	Yes	Yes	Warning	
106 - Primary and Secondary OS - versions are not identical, #1# vs. #2#: and require the same Service Pack level.		Yes	Critical Stop	Compatibility check on secondary.
208 - You are running a 64-bit - version of Windows on one of your servers and a 32-bit version of Windows on the other. This is not supported.		Yes	Critical Stop	Compatibility check on secondary.
111 - The system folders on primary and secondary system must be the same. Setup has detected that the secondary system folder is #2# and the primary was #1#.	-	Yes	Critical Stop	Compatibility check on secondary.
113 - You do not have enough total memory to install Neverfail Heartbeat on your #1# server. You must have at least 1GB.	Yes	Yes	Critical Stop	
Neverfail recommends a minimum of 2GB. Note actual memory requirements depend on the application load; and may require more memory.	Yes	Yes	Warning	
117 - You do not have enough free disk space to install Neverfail Heartbeat You must have at least 2GB available.	Yes	Yes	Critical Stop	

Message	Pri	Sec	Level	Test
118 - For every volume on the primary system that contains protected data a corresponding volume must exist on the secondary server. In most cases this means that for every volume on the primary server a volume with the same drive letter (such as D:\) must exist on the secondary server. If this is not the case, the secondary server must be modified to meet this requirement.	-	Yes	Warning	Compatibility check on secondary.
204 - Your operating system on your #1# server is #2# and you are running with a Windows 2000 driver for your NC77xx NIC(s). In order to prevent system crashes you must upgrade to a Windows 2003 driver; the name for those drivers ends with '57XP32.sys' and not with '57W2K.sys'	Yes	Yes	Critical Stop	
212 - The number of Free System Page Table Entries on this server has dropped to #1#. This is too low. You should have at least #2# Free System Page Table Entries available.	Yes	Yes	Critical Stop	
201 - #1#: This service is incompatible with running Neverfail Heartbeat and must be stopped before Neverfail Heartbeat can be installed.	Yes	Yes	Warning	
209 - Double-Take drivers have been detected on this server. To avoid compatibility problems please uninstall Double-Take before re-running setup.	Yes	Yes	Critical Stop	

Appendix

B

Installation Verification Testing

Testing a Neverfail Heartbeat Pair

Important: The following procedure provides information about performing Installation Verification testing on a Neverfail Heartbeat pair to ensure proper installation and configuration. Additionally, this procedure provides step-by-step procedures to perform a controlled switchover in the event of an application failure and failover in the event of network or hardware failure resulting in excessive missed heartbeats.

Note: In this document, the term “Pair” refers to a Neverfail Heartbeat pair. Refer to the for more information about Neverfail Heartbeat Pairs.

Exercise 1 - Auto-switchover

Neverfail Heartbeat monitors Neverfail services and the system environment to ensure that protected services are available for end users. To monitor services and the system environment, Neverfail Heartbeat uses plug-ins which are designed for Neverfail services and the system.

If a protected service or the system begins to operate outside of preconfigured thresholds, Neverfail Heartbeat can automatically switch to make the passive server the active server in the pair that provides services for end users.

Important: These exercises are examples and should be performed in order. Neverfail recommends against attempting to test failover on a properly operating pair by methods such as unplugging a power cord. At the moment power is lost, any data not written to the passive server is lost. Neverfail recommends that all actions intended to verify operation of the passive server be performed as a switchover rather than a failover.

Starting Configuration

Prior to initiating the Installation Verification process in a pair, Neverfail Heartbeat must be configured with the Primary server as active and the Secondary server as passive. Additionally, the following prerequisites must be met:

- The Secondary server must be synchronized with the Primary server.

- All protected services must be operating normally.
- If installed in a LAN environment, verify that *Failover from Primary server to Secondary server if channel heartbeat is lost for failover timeout* is selected from the **Server: Monitoring > Configure Failover** dialog (default setting).
- If installed in a WAN environment, you must manually select *Failover from Primary server to Secondary server if channel heartbeat is lost for failover timeout* in the **Server: Monitoring > Configure Failover** dialog.

Important: Prior to starting the Installation Verification process, ensure that a known good backup of the Primary server exists and examine the Windows event logs for recent critical errors.

Neverfail provides an executable, `nfavt.exe`, to emulate conditions that result in auto-switchover so you can verify that your Neverfail Heartbeat installation performs as expected. This section guides you through the steps necessary to perform this verification.

Steps to Perform

Important: If you encounter errors and or find it necessary to back out the changes made by this exercise, you can stop at any point and perform the steps described in the [Back-out Procedure \(Auto-switchover\)](#) to return the Pair to its original operating configuration and state.

Table 6: Perform the following procedure to verify Auto-Switchover in a Pair configuration.

Machine ID	Activity	Results
Primary	Open a command prompt.	
	Change directory to <code>C:\Program Files\Neverfail\R2\Bin</code>	
	Execute <code>nfavt.exe</code> . When prompted, “Are you sure you wish to continue”, click Continue .	Service is switched to the Secondary server and Neverfail Heartbeat shuts down on the Primary.
Secondary	Login to the Neverfail Heartbeat Management Client.	
	In the <i>Servers</i> pane of the Neverfail Heartbeat Management Client, select the server pair.	The <i>System Overview</i> screen indicates that the Secondary server is active.
	Verify all protected applications have started on the Secondary.	Services are running on the Secondary.
	Verify data is present.	Data is present.

Successful completion of this procedure leaves the Neverfail Heartbeat pair in the state necessary to perform the second part of the Installation Verification process, detailed in [Exercise 2 - Data Verification](#).

Back-out Procedure (Auto-switchover)

Important: Do not perform this back-out procedure if you intend to continue the Installation Verification process.

If for any reason you find it necessary to back out of this exercise, you can stop at any point and return the pair to the state it was in at the beginning of this exercise by performing the following steps:

1. Shut down Neverfail Heartbeat and protected services on all servers.
2. Complete the following on both servers:
 - a. Open the *Configure Server* wizard.
 - b. Select the *Machine* tab.
 - c. Select the *Primary* server as active.
 - d. Click **Finish**.
3. On the Secondary server, right-click the taskbar icon and select *Start Neverfail Heartbeat*.
4. Verify that the Secondary server is passive (S/-).
5. On the Primary server, right-click the taskbar icon and select *Start Neverfail Heartbeat*.
6. After Neverfail Heartbeat starts, login to the Neverfail Heartbeat Management Client.
7. Verify that applications have started and replication to the passive server has resumed.

Exercise 2 - Data Verification

The Data Verification exercise validates that data is synchronized between the servers resulting in current data on the active server following the Auto-switchover exercise performed previously. The objective is to take a working active server (the Secondary server) and synchronize it with the passive (Primary server). This exercise also demonstrates that all the correct services stopped when the Primary server became passive.

Starting Configuration

Neverfail Heartbeat is running on the Secondary active server. Using the *System Tray* icon, verify that the server status displays **S/A**. Neverfail Heartbeat is not running on the Primary server which is set to passive. Using the *System Tray* icon, verify that the server status displays **-/-** to indicate that Neverfail Heartbeat is not running.

Steps to Perform

Table 7: Perform the following steps to verify that data is synchronized following Auto-switchover in a Pair configuration.

<i>Machine ID</i>	<i>Activity</i>	<i>Results</i>
Primary	Right-click the taskbar icon and select <i>Start Neverfail Heartbeat</i> .	Neverfail Heartbeat successfully starts.
	Login to Neverfail Heartbeat Management Client.	
	In the <i>Servers</i> pane of the Neverfail Heartbeat Management Client, select the server pair.	The <i>System Overview</i> screen is displayed.
	Navigate to the <i>Server: Summary</i> tab to show the connection from the Secondary (active) to Primary (passive).	The <i>Server: Summary</i> page shows a connection from the Secondary server to the Primary server.
	Select the <i>Data: Replication</i> tab and wait for both the <i>File System</i> and the <i>Registry</i> status to display as <i>Synchronized</i> . Access the Neverfail Heartbeat logs and confirm that no exception errors occurred during the synchronization process.	Data replication resumes from the Secondary server back to the Primary server. Both the <i>File System</i> & <i>Registry</i> status become <i>Synchronized</i> .

Successful completion of this procedure leaves the Neverfail Heartbeat Pair in the state necessary to perform the final part of the Installation Verification process, detailed in [Exercise 3 - Switchover](#).

Exercise 3 - Switchover

The Switchover exercise demonstrates the ability to switch the functionality and operations of the active server on command to the other server in the pair using the Neverfail Heartbeat. Perform this exercise only after successfully completing the Auto-switchover and Data Verification Exercises.

Starting Configuration

Neverfail Heartbeat is running on the Secondary active server. Using the *System Tray* icon, verify that the server status displays **S/A**. Neverfail Heartbeat is running on the Primary server which is set to passive. Using the *System Tray* icon, verify that the server status displays **P/-** to indicate that Neverfail Heartbeat is running on the Primary server and that the Primary server is passive

Steps to Perform

Table 8: Perform the following steps to switch functionality and operations on command from the active server to the ready standby server.

Machine ID	Activity	Results
Secondary	Launch Neverfail Heartbeat Management Client and select the <i>Data: Replication</i> tab. Verify that both the <i>File System</i> and <i>I</i> status are <i>Synchronized</i> .	
	Select the <i>Server: Summary</i> tab. Select the Primary server icon and click Make Active .	The Neverfail Heartbeat Management Client <i>Server: Summary</i> page displays the applications stopping on the active server. Once all applications are stopped, the active server becomes passive and the passive server becomes active. The Console shows the applications starting on the newly active server. Both the <i>File System</i> and <i>Registry</i> status are <i>Synchronized</i> .
	Confirm application performance and availability meets previously defined criteria. Verify that client applications are running as expected after the switchover process.	Services continue to be provided as before the switchover occurred. You may need to refresh or restart some client applications as a result of a switchover.

Successful completion of this procedure indicates a successful outcome from the Installation Verification process.

Testing a Neverfail Heartbeat Trio

Important: The following procedure provides information about performing Installation Verification testing on a Neverfail Heartbeat trio to ensure proper installation and configuration. Additionally, this procedure provides step-by-step procedures to perform a controlled switchover in the event of an application failure and failover in the event of network or hardware failure resulting in excessive missed heartbeats.

Note: In this document, the term “Cluster” refers to a Neverfail Heartbeat Cluster. Refer to the [Glossary](#) for more information about Neverfail Heartbeat trios.

Exercise 1 - Auto-switchover

Neverfail Heartbeat monitors services and the system environment to ensure that protected services are available for end users. To monitor services and the system environment, Neverfail Heartbeat uses plug-ins which are designed for Neverfail services and the system.

If a protected service or the system begins to operate outside of preconfigured thresholds, Neverfail Heartbeat can automatically switch to and make active the passive server in the pair to provide services for end users.

Important: These exercises are examples and should be performed in order. Neverfail recommends against attempting to test failover on a properly operating Cluster by methods such as unplugging a power cord. At the moment power is lost, any data not written to the passive server is lost. Neverfail recommends that all actions intended to verify operation of the passive server be performed as a switchover rather than a failover.

Neverfail provides an executable, `nfavt.exe`, to emulate conditions that result in auto-switchover so you can verify that your Neverfail Heartbeat installation performs as expected. This section guides you through the steps necessary to perform this verification.

Starting Configuration

Prior to initiating the Installation Verification process in a Trio, Neverfail Heartbeat must be configured with the Primary server as active, the Secondary server as 1st passive, and the Tertiary server as 2nd passive. All servers must be synchronized with the Primary server, and all protected applications must be operating normally.

Important: Prior to starting the Installation Verification process, ensure that a known good backup of the Primary server exists and examine the Windows event logs for recent critical errors.

Neverfail provides an executable, `nfavt.exe`, to emulate conditions that result in auto-switchover so you can verify that your Neverfail Heartbeat installation performs as expected. This section guides you through the steps necessary to perform this verification.

Prior to initiating this procedure, download `nfavt.exe` from the Neverfail Extranet by navigating to **Product / Downloads > Utilities > Neverfail Acceptance Verification Tester Utility** to
`<installation_location>\Neverfail\R2\Bin`

Steps to Perform

Important: If you encounter errors and or find it necessary to back out the changes made by this exercise, you can stop at any point and perform the steps described in the [Back-out Procedure \(Auto-switchover\)](#) to return the Pair to its original operating configuration and state.

Table 9: Perform the following procedure to verify Auto-Switchover in a Pair configuration.

Machine ID	Activity	Results
Primary	Open a command prompt.	

Machine ID	Activity	Results
	Change directory to C:\Program Files\Neverfail\R2\Bin	
	Execute <code>nfavt.exe</code> When prompted, "Are you sure you wish to continue", click Continue .	Service is switched to the Secondary server and Neverfail Heartbeat shuts down on the Primary.
Secondary	Login to the Neverfail Heartbeat Management Client.	
	In the <i>Servers</i> pane of the Neverfail Heartbeat Management Client, select the server Cluster.	The <i>System Overview</i> screen indicates that the Secondary server is active.
	Verify all protected applications have started on the Secondary.	Services are running on the Secondary.
	Verify data is present and is replicating to the Tertiary server.	Data is present and replicating.
Tertiary	Verify that the Tertiary server is passive and in-sync	The <i>System Overview</i> page indicates that the Tertiary server is passive and in-sync

Successful completion of this procedure leaves the Neverfail Heartbeat pair in the state necessary to perform the second part of the Installation Verification process, detailed in [Exercise 2 - Managed Switchover](#).

Back-out Procedure (Auto-switchover)

Important: Do not perform this back-out procedure if you intend to continue the Installation Verification process.

If for any reason you find it necessary to back out of this exercise, you can stop at any point and return the Cluster to the state it was in at the beginning of this exercise by performing the following steps:

1. Shut down Neverfail Heartbeat and protected services on all servers.
2. Complete the following on all three servers:
 - a. Open the *Configure Server* wizard.
 - b. Select the *Machine* tab.
 - c. Select the *Primary* server as active.
 - d. Click **Finish**.
3. On the Secondary and Tertiary servers, right-click the taskbar icon and select *Start Neverfail Heartbeat*.
4. Verify that the Secondary and Tertiary servers are passive (S/- and T/-).
5. On the Primary server, right-click the taskbar icon and select *Start Neverfail Heartbeat*.
6. After Neverfail Heartbeat starts, login to the Neverfail Heartbeat Management Client.
7. Verify that applications have started and replication to the passive server has resumed.

Exercise 2 - Managed Switchover

Neverfail Heartbeat provides manual control over switching the active server role to another server in the Cluster. On command, Neverfail Heartbeat gracefully stops replication and the protected applications on the currently active server and then starts the protected applications and replication on the server selected to assume the active role.

Use this exercise to validate seamless switching of the active server role to another server in the Cluster. At the end of this section are instructions on how to back out of the exercise (such as if errors are encountered) and return the Cluster to its original operating configuration and state.

Starting Configuration

Neverfail Heartbeat is running on the Secondary active server (S/A) and Tertiary server (T/-). Neverfail Heartbeat is not running on the Primary server (-/-)

Steps to Perform

Important: If you encounter errors and or find it necessary to back out the changes made by this exercise, you can stop at any point and perform the steps described in the Back-out Procedure (Managed Switchover) below to return the Cluster to its original operating configuration and state.

Table 10: Perform the following steps to verify Managed Switchover in a Trio configuration.

Machine ID	Activity	Results
Secondary	Login to the Neverfail Heartbeat Management Client.	
	Click Rollback .	The <i>Rollback</i> screen is displayed.
	Under <i>Shadows</i> , click Create . In the <i>Create Shadow</i> dialog, select <i>Secondary</i> , and then click OK .	A rollback point is created prior to testing Secondary to Tertiary switchover.
	In the <i>Servers</i> pane of the Neverfail Heartbeat Management Client, select the server Cluster.	The <i>System Overview</i> screen is displayed.
	In the <i>System Overview</i> page, select the Tertiary server and then click Make Active .	Neverfail Heartbeat performs a managed switchover to the Tertiary server and makes the Tertiary server active.
Tertiary	Login to the Neverfail Heartbeat Management Client.	
	In the <i>Servers</i> pane of the Neverfail Heartbeat Management Client, select the server Cluster.	The <i>System Overview</i> screen is displayed.
	Verify that all protected applications have started.	Services are running on the Tertiary server.
	Verify that data is present and replicating to the Secondary server.	Data is present and replicating.
Secondary	Verify that the Secondary server is passive and in-sync.	The <i>System Overview</i> screen indicates that the Secondary server is passive and in sync.

Successful completion of this procedure leaves the Cluster in the state necessary to perform the third part of the Installation Verification process, detailed in [Exercise 3 - Data Verification](#).

Back-out Procedure (Managed Switchover)

Important: Do not perform this back-out procedure if you intend to continue the Installation Verification process.

If for any reason you find it necessary to back out of this exercise, you can stop at any point and return the Cluster to the state it was in at the beginning of this exercise by performing the following steps:

1. Shut down Neverfail Heartbeat and protected applications on the Secondary and Tertiary servers.

2. Complete the following on the Tertiary server:
 - a. Open the *Configure Server* wizard.
 - b. Select the *Machine* tab.
 - c. Select the *Secondary* server as active.
 - d. Click **Finish**.
 - e. Right-click the taskbar icon and select *Start Neverfail Heartbeat*.
 - f. Verify that the Tertiary server is passive (T/-) and then shut down Neverfail Heartbeat.
3. On the Secondary, right-click the taskbar icon and select *Start Neverfail Heartbeat*.
4. After Neverfail Heartbeat starts on the Secondary server, login to the Neverfail Heartbeat Management Client.
5. Click **Rollback**.
6. Under *Shadows*, select the previously created shadow on the Secondary server and click **Rollback**.
7. The *Rollback Shadow* dialog is displayed. Select *Restart applications and replication automatically after rollback*, and then click **OK**.
8. The *Rollback Status & Control* dialog is displayed. Click **Yes**.
9. Once the rollback is complete, verify applications have started and are operating as expected.
10. On the Tertiary server, right-click the taskbar icon and select *Start Neverfail Heartbeat*.
11. Verify that replication to the passive server has resumed.

Exercise 3 - Data Verification

The Data Verification exercise validates that data is synchronized between the servers resulting in current data on the active server following a Managed Switchover. The objective is to take a working active server (the Secondary server) and synchronize it with the passive (Tertiary server).

Starting Configuration

Neverfail Heartbeat is running on the Secondary and Tertiary servers. Using the *System Tray* icon, verify that the server status displays **S/A**. Neverfail Heartbeat is not running on the Primary server which is set to passive. Using the *System Tray* icon, verify that the server status displays **-/-** to indicate that Neverfail Heartbeat is not running.

Important:

If you encounter errors and or find it necessary to back out the changes made by this exercise, you can stop at any point and perform the steps described in the [Back-out Procedure \(Data Verification\)](#) below to return the Cluster to its original operating configuration and state.

Steps to Perform

Table 11: Perform the following steps to verify that data is synchronized following Managed Switchover in a Trio configuration.

Machine ID	Activity	Results
Primary	Right-click the taskbar icon and select <i>Start Neverfail Heartbeat</i> .	Neverfail Heartbeat successfully starts.
	Login to Neverfail Heartbeat Management Client.	

Machine ID	Activity	Results
	In the <i>Servers</i> pane of the Neverfail Heartbeat Management Client, select the server Cluster.	The <i>System Overview</i> screen is displayed.
	Click on the Primary server icon to select the <i>Primary</i> server and verify that it is in a synchronized state.	Ensure that the full system check is complete.
Tertiary	Login to the Neverfail Heartbeat Management Client.	
	Click Rollback .	The <i>Rollback</i> screen is displayed.
	Under <i>Shadows</i> , click Create . In the <i>Create Shadow</i> dialog, select <i>Tertiary</i> , and then click OK .	A rollback point is created prior to testing Tertiary to Primary switchover.
Primary	In the <i>System Overview</i> screen, select the <i>Primary</i> server and click Make Active.	Neverfail Heartbeat performs a managed switchover to the Primary server and makes the Primary server active.
	Verify that all protected applications have started.	Services are running on the Primary server.
	Verify that data is present.	Data is present on the Primary server and is synchronized.
	Verify that all three servers are connected and replicating.	

Successful completion of this procedure indicates a successful outcome from the Installation Verification process.

Back-out Procedure (Data Verification)

Important: Do not perform this back-out procedure if you intend to continue the Installation Verification process.

If for any reason you find it necessary to back out of this exercise, you can stop at any point and return the Cluster to the state it was in at the beginning of this exercise by performing the following steps:

1. Shut down Neverfail Heartbeat and protected applications on all servers.
2. Complete the following on the Primary and Secondary servers:
 - a. Open the *Configure Server* wizard.
 - b. Select the *Machine* tab
 - c. Select the *Tertiary* server as active.
 - d. Click **Finish**.
 - e. Right-click the taskbar icon and select *Start Neverfail Heartbeat*.
 - f. Verify that the Primary and Secondary servers are passive (**P/-** and **S/-**).

Glossary

Active

The functional state or role of a server when it is visible to clients through the network, running protected applications, and servicing client requests.

Alert

A notification provided by Neverfail Heartbeat sent to a user or entered into the system log indicating an exceeded threshold.

Active Directory (AD)

Presents applications with a single, simplified set of interfaces so users can locate and use directory resources from a variety of networks while bypassing differences between proprietary services. Neverfail Heartbeat switchovers and failovers require no changes to AD resulting in switchover/failover times typically measured in seconds.

Active–Passive

The coupling of two servers with one server visible to clients on a network and providing application service while the other server is not visible and not providing application service to clients.

Advanced Configuration and Power Interface (ACPI)

A specification that dictates how the operating system can interact with the hardware especially where power saving schemes are used. The Primary, Secondary, and Tertiary servers must have identical ACPI compliance.

Asynchronous

A process whereby replicated data is applied (written) to the passive server independently of the active server.

Basic Input/Output System (BIOS)

The program a personal computer's microprocessor uses to get the computer system started after you turn it on. It also manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse, and printer.

Cached Credentials

Locally stored security access credentials used to log into a computer system when a Domain Controller is not available.

Channel Drop

An event in which the dedicated communications link between servers fails, often resulting in the passive server becoming active and consequently creating a split-brain syndrome.

Channel NIC (Network Interface Card)

A dedicated subnet used by the Neverfail Channel.

Checked

The status reported for user account credential (username/password) validation.

Cloned Servers

Servers that have identical configuration settings, names, applications, Security Identifiers (SIDs) and IP addresses, following the installation of Neverfail Heartbeat.

Cloning Process

The Neverfail Heartbeat process whereby all installed programs, configuration settings, and the machine name, Security Identifier (SID), and IP address are copied to another server.

Cluster

A generic term for a Neverfail Heartbeat Pair or Trio and the set of machines (physical or virtual) involved in supporting a single protected server. A Neverfail Heartbeat Cluster can include the machines used in a VMware or Microsoft cluster.

Connection

Also referred to as Cluster Connection. Allows the Neverfail Heartbeat Management Client to communicate with a Neverfail Heartbeat Cluster, either on the same machine or remotely.

Crossover Cable

A network cable that crosses the transmit and receive lines.

Data Replication

The transmission of protected data changes (files and registry) from the active to the passive server via the Neverfail Channel.

Data Rollback Module

A Neverfail Heartbeat module that allows administrators to rollback the entire state of a protected application, including files and registry settings, to an earlier point-in-time. Typically used after some form of data loss or corruption.

Degraded

The status reported for an application or service that has experienced an issue that triggered a Rule.

Device Driver

A program that controls a hardware device and links it to the operating system.

Disaster Recovery (DR)

A term indicating how you maintain and recover data with Neverfail Heartbeat in event of a disaster such as a hurricane or fire. DR protection can be achieved by placing the Secondary server (in a Pair) or the Tertiary server (in a Trio) at an offsite facility, and replicating the data through a WAN link.

DNS (Domain Name System) Server

Provides a centralized resource for clients to resolve NetBIOS names to IP addresses.

Domain

A logical grouping of client server based machines where the administration of rights across the network are maintained in a centralized resource called a domain controller.

Domain Controller (DC)

The server responsible for maintaining privileges to domain resources; sometimes called AD controller in Windows 2003 and above domains.

Dualed

A way to provide higher reliability by dedicating more than one NIC for the Neverfail Channel on each server.

Failover

Failover is the process by which the first passive server assumes the active role when it no longer detects that the active server is alive as a result of a critical unexpected outage or crash of a server.

First Passive

The passive server in a Neverfail Heartbeat Pair or Trio communicating with and receiving replicated data directly from the active server.

Full System Check (FSC)

The internal process automatically started at the initial connection or manually triggered through the Manage Server GUI to perform verification on the files and registry keys and then synchronize the differences.

Fully Qualified Domain Name (FQDN)

Also known as an absolute domain name, a FQDN specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain, relative to the root domain. Example: somehost.example.com., where the trailing dot indicates the root domain.

Global Catalog

A global catalog is a domain controller that stores a copy of all Active Directory objects in a forest. The global catalog stores a full copy of all objects in the directory for its host domain and a partial copy of all objects for all other domains in the forest.

Graceful (Clean) Shutdown

A shutdown of Neverfail Heartbeat based upon completion of replication by use of the Neverfail Heartbeat Neverfail Heartbeat Management Client, resulting in no data loss.

Group

An arbitrary collection of Neverfail Heartbeat Clusters used for organization.

Hardware Agnostic

A key Neverfail Heartbeat feature allowing for the use of servers with different manufacturers, models, and processing power in a single Neverfail Heartbeat Cluster.

Heartbeat

The packet of information issued by the passive server across the channel, which the active server responds to indicating its presence.

High Availability (HA)

Keeping users seamlessly connected to their applications regardless of the nature of a failure. LAN environments are ideally suited for HA.

Hotfix

A single, cumulative package that includes one or more files that are used to address a problem in a product.

Identity

The position of a given server in the Neverfail Heartbeat Cluster: Primary, Secondary, or Tertiary.

Install Clone

The installation technique used by Neverfail Heartbeat to create a replica of the Primary server using NTBackup or Wbadmin and to restore the replica to the Secondary and/or Tertiary servers.

Low Bandwidth Module (LBM)

A Neverfail Heartbeat module that compresses and optimizes data replicated between servers over a WAN connection. This delivers maximum data throughput and improves application response time on congested WAN links.

Machine Name

The Windows or NETBIOS name of a computer.

Management IP Address

An additionally assigned unfiltered IP address used for server management purposes only.

Many-to-One

The ability of one physical server (hosting more than one virtual server) to protect multiple physical servers.

Network Monitoring

Monitoring the ability of the active server to communicate with the rest of the network by polling defined nodes across the network at regular intervals.

Neverfail Channel

The IP communications link used by the Neverfail system for the heartbeat and replication traffic.

Neverfail Extranet

The Neverfail web site dedicated to supporting partners and customers by providing technical information, software updates, and license key generation.

Neverfail Heartbeat

The core replication and system monitoring component of the Neverfail solution.

Neverfail Heartbeat Packet Filter

The network component, installed on all servers, that controls network visibility.

Neverfail License Key

The key obtained from the Neverfail extranet that allows the use of components in the Neverfail suite; entered at install time, or through the Configure Server Wizard.

Neverfail Pair

Describes the coupling of the Primary and Secondary server in a Neverfail solution.

Neverfail Plug-ins

Optional modules installed into a Neverfail Heartbeat server to provide additional protection for specific applications.

Neverfail SCOPE

The umbrella name for the Neverfail process and tools used to verify the production servers health and suitability for the implementation of a Neverfail solution.

Neverfail SCOPE Report

A report provided upon the completion of the Neverfail SCOPE process that provides information about the server, system environment, and bandwidth.

Neverfail Switchover/Failover Process

A process unique to Neverfail in which the passive server gracefully (switchover) or unexpectedly (failover) assumes the role of the active server providing application services to connected clients.

Neverfail Trio

Describes a set of three coupled servers (Primary, Secondary, and Tertiary) in a Neverfail solution.

Pair

See Neverfail Heartbeat Pair above.

Passive

The functional state or role of a server when it is not delivering service to clients and is hidden from the rest of the network. For a Neverfail Heartbeat Trio, see also First Passive and Second Passive.

Pathping

A route-tracing tool that works by sending packets to each router on the way to a final destination and displays the results of each hop.

Plug-and-Play (PnP)

A standard for peripheral expansion on a PC. On starting the computer, PnP automatically configures the necessary IRQ, DMA and I/O address settings for the attached peripheral devices.

Plug-in

An application specific module that adds Neverfail Heartbeat protection for the specific application.

Pre-Clone

An installation technique whereby the user creates an exact replica of the Primary server using VMware vCenter Converter or other 3rd party utility prior to the initiation of installation and uses the replica as a Secondary and or Tertiary server.

Pre-Installation Checks

A set of system and environmental checks performed as a prerequisite to the installation of Neverfail Heartbeat.

Primary

An identity assigned to a server during the Neverfail Heartbeat installation process that normally does not change during the life of the server and usually represents the production server prior to installation of Neverfail Heartbeat.

Principal (Public) IP Address

An IP address used by clients to contact the server through drive mappings, UNC paths, DNS resolved paths, etc. to gain access to the server's services and resources.

Principal NIC

The network card which hosts the Principal IP address.

Principal (Public) Network

The network used by clients to connect to server applications protected by Neverfail Heartbeat.

Protected Application

An application protected by the Neverfail Heartbeat solution.

Quality of Service (QoS)

An effort to provide different prioritization levels for different types of traffic over a network. For example, Neverfail Heartbeat data replication may have a higher priority than ICMP traffic, as the consequences of interrupting data replication are more obvious than slowing down ICMP traffic.

Receive Queue

The staging area on a server used to store changes received from another server in the replication chain before they are applied to the disk/registry on the passive server.

Remote Desktop Protocol (RDP)

A multi-channel protocol that allows a user to connect to a computer running Microsoft Terminal Services.

Replication

The generic term given to the process of intercepting changes to data files and registry keys, transporting the changed data across the channel, and applying them to the passive server(s) so the servers are maintained in a synchronized state.

Role

The functional state of a server in the Neverfail Heartbeat Cluster: active or passive.

Rule

A set of actions performed by Neverfail Heartbeat when defined conditions are met.

Second Passive

The passive server in a Neverfail Heartbeat Trio communicating with and receiving replicated data directly from the first passive server.

Secondary

An identity assigned to a server during the Neverfail Heartbeat installation process that normally does not change during the life of the server and usually represents the standby server prior to installation of Neverfail Heartbeat.

Security Identifier (SID)

A unique alphanumeric character string that identifies each operating system and each user in a network of 2003/2008/2012 systems.

Send Queue

The staging area on a server used to store intercepted data changes before being transported across to a passive server in the replication chain.

Server Monitoring

Monitoring of the active server by the passive server, using a heartbeat message, to ensure that the active server is functional.

Shared Nothing

A key feature of Neverfail Heartbeat in which no hardware is shared between the Primary, Secondary, and Tertiary servers. This prevents a single point of failure.

SMTP

A TCP/IP protocol used in sending and receiving e-mail between servers.

SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks.

Split-Brain Avoidance

A unique feature of Neverfail Heartbeat that prevents a scenario in which Primary and Secondary servers attempt to become active at the same time leading to an active-active rather than an active-passive model.

Split-Brain Syndrome

A situation in which more than one server in a Neverfail Heartbeat Cluster are operating in the active mode and attempting to service clients, resulting in the independent application of different data updates to each server.

Subnet

Division of a network into an interconnected but independent segment or domain, intended to improve performance and security.

Storage Area Network (SAN)

A high-speed special-purpose network or (subnetwork) that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users.

Switchover

The graceful transfer of control and application service to the passive server.

Synchronize

The internal process of transporting 64KB blocks of changed files or registry key data, through the Neverfail Channel, from the active server to the first passive server or from the first passive server to the second passive server to ensure the data on the passive server is a mirror image of the protected data on the active server.

System Center Operations Manager (SCOM)

System Center Operations Manager is a cross-platform data center management server for operating systems and hypervisors.

System State

Data that comprises the registry, COM+ Class Registration database, files under Windows File Protection, and system boot file; other data may be included in the system state data.

Task

An action performed by Neverfail Heartbeat when defined conditions are met.

Tertiary

An identity assigned to a server during the Neverfail Heartbeat installation process that normally does not change during the life of the server and usually represents the disaster recovery server prior to installation of Neverfail Heartbeat.

Time-To-Live (TTL)

The length of time that a locally cached DNS resolution is valid. The DNS server must be re-queried after the TTL expires.

Traceroute

A utility that records the route through the Internet between your computer and a specified destination computer.

Trio

See Neverfail Heartbeat Trio above.

Ungraceful (Unclean) Shutdown

A shutdown of Neverfail Heartbeat resulting from a critical failure or by shutting down Windows without first performing a proper shutdown of Neverfail Heartbeat, resulting in possible data loss.

Unprotected Application

An application not monitored nor its data replicated by Neverfail Heartbeat.

Virtual Private Network (VPN)

A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Windows Management Instrumentation (WMI)

A management technology allowing scripts to monitor and control managed resources throughout the network. Resources include hard drives, file systems, operating system settings, processes, services, shares, registry settings, networking components, event logs, users, clusters, and groups.