

Installation on Windows Server 2012 When the Secondary Server is Virtual

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
Neverfail Heartbeat Implementation.....	11
Environmental Prerequisites.....	11
Supported Environments.....	11
Unsupported Environments.....	11
Pre-Install Requirements.....	12
Server Deployment Architecture Options.....	12
Virtual to Virtual.....	12
Physical to Virtual.....	13
Cloning Technology Options.....	13
Application Component Options.....	14
Network Options.....	14
Local Area Network (LAN).....	15
Wide Area Network (WAN).....	15
Network Interface Card (NIC) Configuration.....	16
Firewall Configuration Requirements.....	18
Anti-Malware Recommendations.....	18
Chapter 3: Installing Neverfail Heartbeat	19
Pre-Installation Tasks.....	19
Installing Neverfail Heartbeat on the Primary Server.....	19
Installing Neverfail Heartbeat on the Secondary or Tertiary Server.....	24
Install Client Tools.....	26
Neverfail vSphere Client.....	27
Installing Neverfail vSphere Client.....	28
Launch Neverfail vSphere Client.....	29
Discover Neverfail Heartbeat Servers.....	31
Add Neverfail Clusters.....	32
Remove Neverfail Clusters.....	33
Managing Neverfail Heartbeat with Neverfail vSphere Client.....	33
Appendix A: Setup Error Messages.....	35
Appendix B: Installation Verification Testing.....	39
Testing a Neverfail Heartbeat Pair.....	39

Exercise 1 - Auto-switchover.....	39
Exercise 2 - Data Verification.....	41
Exercise 3 - Switchover.....	42
Testing a Neverfail Heartbeat Trio.....	42
Exercise 1 - Auto-switchover.....	43
Exercise 2 - Managed Switchover.....	44
Exercise 3 - Data Verification.....	46
Glossary.....	49

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 the Secondary server is virtual.

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 — *Installing* 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.

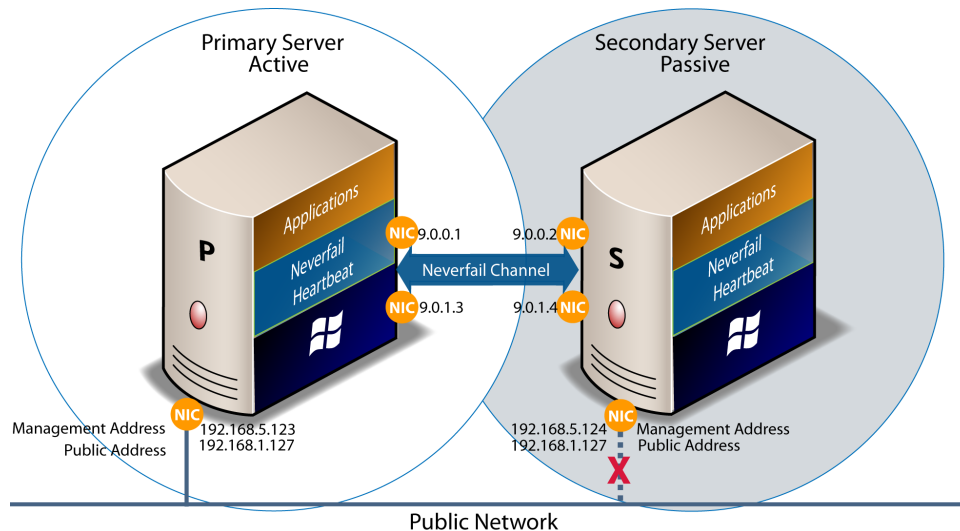


Figure 1: Communications Between Primary and Secondary Servers

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.

Neverfail Heartbeat Implementation

Neverfail Heartbeat is a versatile solution that provides multiple configurations to suit user requirements. It can be deployed in a LAN for high availability, a WAN to provide disaster recovery, or as a Trio utilizing both a LAN and a WAN connection.

During the installation process, Neverfail Heartbeat performs a variety of checks to ensure the server meets the minimum requirements for a successful installation. A critical stop or warning message appears if the server fails a check. Refer to the [Setup Error Messages](#) in this guide for a list of the checks and an explanation of the messages. You must resolve critical stops before you can proceed with setup. Prior to installing Neverfail Heartbeat, select the deployment options you intend to use. The installation process will prompt you to select options throughout the procedure to create the configuration you want.

Environmental Prerequisites

Neverfail Heartbeat supports the following environments listed below.

Supported Environments

- Neverfail Heartbeat is supported on the following versions of Windows Server 2012
 - Windows Server 2012 x64 Standard
 - Windows Server 2012 x64 Datacenter

Unsupported Environments

- The following environments are not supported by Neverfail Heartbeat
 - On a server deployed as a [Domain Controller \(DC\)](#)
 - On a server deployed as a [Global Catalog](#)
 - On a server deployed as a [DNS \(Domain Name System\) Server](#)
 - On an IA-64 Itanium Platform

Pre-Install Requirements

Prior to installing Neverfail Heartbeat, the following requirements must be met and are in addition to those required for installed applications.

- Verify that the Primary server is a member of the domain.
- Verify no other critical business applications (other than those to be protected) are installed on the server.
- Verify that there is a minimum of 1GB of available RAM (2GB recommended) in addition to any other memory requirements for the Operating System or installed applications.. 256MB of RAM must remain available to Neverfail Heartbeat at all times.
- Verify that a minimum 2GB of free disk space is available on the installation drive for Neverfail Heartbeat.

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.

- Obtain and use local administrator rights to perform Neverfail Heartbeat installation.

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

- Apply the latest Microsoft security updates.
- All applications that will be protected by Neverfail Heartbeat must be installed and configured on the Primary server prior to installing Neverfail Heartbeat.
- Verify that the Primary, Secondary, and Tertiary (if installed) servers have identical system date, time, and time Zone settings.
- Verify that Windows Server Backup Feature and Command Line Tools have been installed on all servers in the Cluster prior to installing Neverfail Heartbeat. Installation of Windows Server Backup Feature and Command Line Tools will also install Windows PowerShell.
- Verify that all services to be protected are running or set to *Automatic* prior to installation. During installation, protected services are set to manual to allow Neverfail Heartbeat to start and stop services depending on the role of the server. The target state of the services is normally running on the active server and stopped on the passive.

Server Deployment Architecture Options

The selected server architecture affects the requirements for hardware and the technique used to clone the Primary server.

Virtual to Virtual

Virtual to Virtual is the supported architecture if applications to be protected are already installed on the production (Primary) server running on a virtual machine. Benefits to this architecture include reduced hardware cost, shorter installation time, and use of the Pre-Clone technique for installation.

The Secondary/Tertiary virtual machine must meet the minimum requirements.

- The specifications of the Secondary/Tertiary virtual machine must match the specifications of the Primary virtual machine as follows:
 - Similar CPU (including resource management settings)
 - Memory configuration (including resource management settings)
 - Appropriate resource pool priorities
- Each virtual machine used in the Virtual to Virtual pair must be on a separate ESX host to guard against failure at the host level.
- If using more than one NIC, each virtual NIC must use a separate virtual switch.

Physical to Virtual

The Physical to Virtual architecture is used when the environment requires a mix of physical and virtual machines. This architecture is appropriate to avoid adding more physical servers or if you plan to migrate to virtual technologies over a period of time.

The Secondary Neverfail Heartbeat virtual machine must meet the minimum requirements.

- The specifications of the Secondary Neverfail Heartbeat virtual machine must match the Primary physical server as follows:
 - Similar CPU
 - Identical Memory
- The Secondary Neverfail Heartbeat virtual machine must have sufficient priority in resource management settings so that other virtual machines do not impact its performance.
- Each virtual NIC must use a separate virtual switch.

Cloning Technology Options

Cloning the Primary server to create a nearly identical Secondary server involves different technologies depending on the selected server architecture.

Cloning Prior to Installation (Pre-clone)

The following cloning technologies are supported for creating cloned images for use as a Secondary server before you begin installing Neverfail Heartbeat:

- Use VMware vCenter Converter when cloning in a Physical to Virtual environment.

Important: When installing in a Physical to Virtual architecture, VMware Tools must not be installed on the Secondary server during the Neverfail Heartbeat installation process. If VMware Tools are currently installed on the Secondary 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.

- Use VMware vCenter virtual machine cloning when cloning in a Virtual to Virtual environment.

Important: When installing in a Virtual to Virtual architecture, VMware Tools must be installed and running on the Primary server before starting the Neverfail Heartbeat installation process.

Application Component Options

Neverfail Heartbeat can accommodate any of the supported modules listed below:

Supported Plug-ins

- Neverfail ClusterProtector Solutions Pack for v6.6
- Neverfail for Blackberry Enterprise server
- Neverfail for Business Application
- Neverfail for Exchange
- Neverfail for File Server
- Neverfail for Good Mobile Messaging
- Neverfail for IIS
- Neverfail for Lotus Domino
- Neverfail for RightFax Server
- Neverfail for SharePoint Server
- Neverfail for SQL Server
- SCOM Solutions Pack for Neverfail v6.6

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.

Firewall Configuration Requirements

When firewalls are used to protect networks, you must configure them to allow traffic to pass through both the *Client Connection port* (52267) and the *Default Channel port* (57348).

Important: When installing on Windows Server 2012, Microsoft Windows may change the connection type from a Private network to an Unidentified network after you have configured the firewall port to allow channel communications resulting in the previously configured firewall changes to be reset for the new network type (Unidentified).

The firewall rules must be recreated to allow traffic to pass through for the Client Connection port and the Default Channel port. Neverfail recommends that the firewall be configured to allow the client to connect to the Client Connection port by process, `nfgui.exe`, rather than by a specific port. To enable channel communications between servers, change the Network List Manager Policy so that the Neverfail Channel network is identified as a Private Network, and not the default Unidentified Network, and configure the firewall to allow traffic to pass through on Port 57348, the Default Channel port.

Anti-Malware Recommendations

Consult with and implement the advice of your anti-malware provider, as Neverfail guidelines often follow these recommendations. Consult the Neverfail Knowledge Base for up to date information on specific anti-malware products.

Do not use file level anti-malware to protect application server databases, such as MS SQL Server databases. The nature of database contents can cause false positives in malware detection, leading to failed database applications, data integrity errors, and performance degradation.

Neverfail recommends that when implementing Neverfail Heartbeat, you do not replicate file level anti-malware temp files using Neverfail Heartbeat.

The file level anti-malware software running on the Primary server must be the same as the software that runs on the Secondary and Tertiary server. In addition, the same file level anti-malware must run during both active and passive roles.

Configure file level anti-malware to use the Management IP address on the passive servers for malware definition updates. If this is not possible, manually update malware definitions on the passive servers.

Exclude the following Neverfail directories from file level anti-malware scans (C:\Program Files\Neverfail\ is the default installation directory):

- C:\Program Files\Neverfail\r2\logs
- C:\Program Files\Neverfail\r2\log

Any configuration changes made to a file level anti-malware product on one server (such as exclusions) must be made on the other server as well. Neverfail Heartbeat does not replicate this information.

Chapter 3

Installing Neverfail Heartbeat

This chapter discusses the installation process used to implement Neverfail Heartbeat on Windows Server 2012 when the Secondary server is virtual. Prior to installing Neverfail Heartbeat, you must identify the deployment options you want. The installation process requires you to select options throughout the procedure to achieve your configuration goals.

After selecting implementation options, begin the installation process. During the installation process, Neverfail Heartbeat performs a variety of checks to ensure the server meets the minimum requirements for a successful installation. Should the server fail one of the checks, a critical stop or warning message appears. Refer to the [Setup Error Messages](#) in this guide for a list of the checks and an explanation of the messages. You must resolve critical stops before you can proceed with setup.

Pre-Installation Tasks

Procedure

This section provides the step-by-step process for preparing Neverfail Heartbeat for installation in Pair and Trio configurations using the *Pre-Clone* installation technique.

Note: The Pre-Clone method of installing Neverfail Heartbeat requires a true clone of the Primary server using VMware vCenter Converter for P2V, vCenter virtual machine cloning for V2V, or another third party utility. After the clones are created, you must follow the procedure outlined below prior to installing Neverfail Heartbeat. Failure to do so can cause IP address and network name conflicts.

- Clone the Primary server using either the VMware vCenter Converter for P2V, vCenter virtual machine cloning for V2V, or another 3rd Party Utility to create a cloned image of the Primary server. The clone must be 100% with no changes to the Name, SID, or domain membership.

Installing Neverfail Heartbeat on the Primary Server

Prerequisites

Prior to attempting installation of Neverfail Heartbeat on the Primary server, ensure that the server meets all of the pre-requisites stated in [Pre-Install Requirements](#). During the installation process, Neverfail Heartbeat will install Neverfail Heartbeat on all servers identified in the cluster and validate that all servers meet the minimum requirements for a successful installation.

1. Having verified all of the environmental prerequisites are met, download the Neverfail Heartbeat .zip file to an appropriate location on the Primary server.
2. Open *Network Connections*, right-click the Neverfail Channel network connection and select *Properties*.
3. Select *Internet Protocol Version 4 (TCP/IP)* and click **Properties**.
4. Click **Advanced**, select the *DNS* tab, and clear the *Register this connection's addresses in DNS* check box.
5. Select the *WINS* tab and select *Disable NetBIOS over TCP/IP*. Click **OK** three times to close the dialogs.
6. Extract the contents of the Neverfail Heartbeat .zip file and double-click the Setup.exe file to initiate the installation process.

Note: If you click **Exit** after Setup has started, you are prompted to save your settings. When you run Setup.exe later, you will be asked if you want to use the previously saved configuration.

7. The *Setup Type* page appears. Because this is a new installation of Neverfail Heartbeat, select *Install Neverfail Heartbeat* and click **Next**.
The *Physical Hardware Identity* page is displayed.

Note: The left pane of each page in the Setup wizard provides information about the setup process.

8. Select *Primary* for the *Physical Hardware Identity* and click **Next**.
The *Neverfail End User License Agreement* page is displayed.
9. Read the license agreement carefully and select *I accept terms of the License Agreement*. Click **Next**.
The *License Configuration* page is displayed.
10. Neverfail Heartbeat prompts you to enter a valid serial number. Click **Add** to enter a valid serial number and click **Next**. When entering multiple licenses, it may be easier to import this information from text files. Perform the following steps to import multiple license keys from a text file:
 - a) Create a text (.txt) file list of the license keys for each licensed Neverfail Heartbeat product or feature. Each license key must be on a separate line, for example:

 11111-22222-33333-44444-55555

 ABCDE-FGHIJ-KLMNO-PQRST-UVWXY
 - b) Click **Import** and browse to the location of the text file containing the license keys. After the license key information is entered or imported, the lower panel of the *License Configuration* page lists the licensed components, such as Neverfail Heartbeat that are being installed.
The *Select Topology* page is displayed.
11. Select *LAN*, *WAN*, or both *LAN* and *WAN (Trio)* for the intended network topology. Click **Next**.
The *Cloning Option* page is displayed.
12. On the *Cloning Option* page, select *Pre-clone*, then click **Next**.
The *Installation Paths* page is displayed.

Important: The path of the Neverfail Heartbeat installation folder cannot contain Unicode characters. If Neverfail Heartbeat is installed in a folder that has a path containing Unicode characters, it will cause the Neverfail Heartbeat Service to not start. The path of the Neverfail Heartbeat installation folder can only contain lower and upper case letters A to Z, digits from 0 to 9, and the following special characters: space \ _ - () . : Additionally, Neverfail Heartbeat does not support file or folder names ending with a period "." or space " ".

13. Configure the installation paths. The default installation location is `C:\Program Files\Neverfail\`, but can be changed by manually typing a path to another install location. Alternatively, click **Browse** to select a location. Select *Create icons on Desktop* and click **Next**.

If using multiple NICs, continue with [Step 14](#). If using a single NIC, go to [Step 15](#).

The *Channel Adapter Identification* page is displayed.

14. Identify the network adapter(s) for use in the Neverfail Channel on the *Channel Adapter Identification* page. Select the network adapters (NICs) for the Neverfail Channel from the list. Click the adapter name to display the selected NIC properties in the lower pane. You must select at least one NIC to proceed with the installation. If no NICs are available, click **Open Network Connections** to review the network configuration of your machine and verify that you have the correct number of NICs installed. After selecting the appropriate NIC, click **Next**.

The *Neverfail Channel IP Configuration* page is displayed.

Important: Only one channel can be configured for each NIC. To configure more than one channel you must identify more than one NIC. A disabled NIC does not appear in this list. Enable the NIC to display it. If a NIC is disconnected, its IP addresses do not appear in the lower pane.

15. The *Neverfail Channel IP Configuration* page allows you to configure the Neverfail Channel between servers. Neverfail Heartbeat Setup requires you to identify both ends of the channel by IP address whether configuring a Pair or Trio, or in a LAN or WAN. The steps required to configure the Neverfail Channels between servers depends on whether you are configuring a Pair or a Trio. If you are configuring a Pair, perform Step (a) and Step (b) below, and skip Step (c). If you are configuring a Trio, perform all three steps.
- Select the *IP Address On Primary* from the drop down list (the list contains all local IP addresses), and manually enter the reciprocal *IP Address On Secondary* into the corresponding text box. Click **OK**.
 - Click **Add** for each available channel connection. You must specify all Neverfail Channel IP addresses in subnets outside of the normal Principal (Public) IP addressing schema. Neverfail Channel traffic routing uses the Neverfail Channel network card rather than the Principal (Public) network card. When finished adding channel connections, click **Next**.
 - Skip this step if configuring a Pair. Perform Step (a) and Step (b) above to configure the Primary to Secondary Neverfail Channel, and then repeat the process using the IP addresses necessary to configure the Secondary to Tertiary Neverfail Channel and the Tertiary to Primary Neverfail Channel.
16. Review and adjust, if necessary, the default channel port. Click **Next**.
- If using multiple NICs, continue with [Step 17](#).
 - If using a single NIC, go to [Step 18](#).

The *Public Adapter Identification* page is displayed.

Important: When the implementation spans multiple sites with firewalls between the servers, configure the firewalls to allow traffic to pass through the default channel port or the manually configured channel port. See [Firewall Configuration Requirements](#) for additional information.

17. Select the Principal (Public) NIC(s). The IP address information is displayed for each NIC. Click **Next**.

The *Principal (Public) IP Address Configuration* page is displayed.

18. The process of configuring the Principal (Public) IP Address depends on whether you are installing in a LAN, a WAN (with different subnets or different IP addresses within the same subnet), or configuring a Trio. For a LAN or same subnet WAN deployment, follow Step a. For a WAN (with different subnets or different IP addresses within the same subnet), follow Step b. For a Trio, follow Step c.
 - a) For LAN installation or same subnet WAN installs, select *Use same IP addresses for Secondary (Recommended for HA secondary)* and click **Add** to specify the IP address in a LAN or same subnet WAN. Repeat this step to define all addresses for your configuration. Click **Next**. Go to [Step 20](#).
 - b) When installing in a WAN with different subnets or different IP addresses within the same subnet, select *Use different IP addresses for Secondary (Recommended for DR secondary)* For a WAN environment, specify the IP addresses of the Secondary server as well as the Primary server. Repeat this step to define all addresses for your configuration. Click **Next**. Go to [Step 19](#).
 - c) When configuring a Trio, perform Step a and then specify the IP address of the Tertiary server (normally in a different subnet than the Primary and Secondary servers) in addition to the Primary server. Add each Principal (Public) network address until all addresses defining your configuration are present. Click **Next** and continue with [Step 19](#).
19. The *User Details* page allows you to enter the *Domain Name*, a domain administrator *Username* and *Password* in the respective text boxes and click **Next**.
When the Principal (Public) addresses on the Secondary/Tertiary server are different from those on the Primary server, Neverfail Heartbeat must perform additional tasks during failover or switchover. These additional tasks require clients to change their resolution of the active server to a different IP address and requires that Neverfail Heartbeat update the DNS entries for the active server across the enterprise. Such updates require the credentials for domain administrators (or an account with equivalent rights). The *Client Configuration* page is displayed.
20. The Neverfail Heartbeat server pair can be administered remotely on client machines using the Neverfail Heartbeat Management Client. The Neverfail Heartbeat Management Client connects to the IP address of the active server using the default client connection port of 52267. If this port is already in use, type an available client connection port in the text box. Click **Next**.
The *Licensed Feature Configuration* page is displayed.
21. The combination of licensed features and installed plug-ins determines the types of applications and data that are protected by Neverfail Heartbeat. The *Licensed Feature Configuration* page allows you to select the applications to protect. All licensed Neverfail Heartbeat features are listed. Clear the check box of any application that you do not intend to protect. All applications with the check box selected become protected upon completion of the installation. Click **Next**.
The *AM(X) Configuration* page is displayed.
22. To add an AM(X), click the **Add** button. In the resulting file selection dialog, select an AM(X) script file or Plug-in .dll and click **OK**. The script files usually have the file extension .amx or .vbs, and plug-ins have the file extension .dll.

Note: Downloading plug-in files can cause them to be marked as "Untrusted" by the Windows system, and untrusted plug-ins may fail to load. You can "unblock" an untrusted file by examining its properties using Windows Explorer and clicking on the **Unblock** button if it is present.

The *Pre-synchronization Data Configuration* page is displayed.

23. The *Pre-synchronization Data Configuration* page allows you to select a location to place the backup files. When installing into a Windows Server 2012 environment, provide the UNC path to the location for the backup files on the Secondary server. Click **Next**.
The *Installation Summary* page is displayed.
24. Review the summary of options and configuration information for the installation. Click **Next**.
The *Validate Collector Installation* page is displayed.

25. Enter the User account information (*Domain, Username, and Password*) for all remote servers. If installing a Pair, enter the User account information for the Secondary server. If installing in a Trio configuration, enter the User account information for both the Secondary and Tertiary servers.

Note: *If the server(s) are not members of a domain, the Domain field is not required and should be left empty.*

26. Click **Install** to install the Validate Collector on each server in the cluster. The results of the Validate Collector installation are displayed in the *Report* pane. If the Validate Collector is not successfully installed, click **Back** to reattempt installation.

Note: *If Validate does not successfully install on all remote servers in the cluster, verify the username, domain, and password values are correct. Additionally, ensure that there are no open connections to the remote servers. After verifying, click **Install** again.*

Note: *If the Validate Collector fails to install on the local server, or you wish to bypass Validation, click the **Skip Validation** button to continue the installation and go to [Step 30](#).*

27. After Validate Collector is successfully installed on the local server, click **Next**. The *Validate* page is displayed.

Important: *It is important to configure any firewalls to allow traffic to pass between the Primary, Secondary, and Tertiary servers before attempting to run Validate.*

28. Click **Start** to initiate the Validation process or click **Skip Validation** to bypass the Validation process. Validate Collector gathers required information from all servers in the cluster and provides the status of the gathering operation for each server. Upon completion of information gathering, high level results are displayed in the lower pane of the page with the color green and a check mark for success, a blue triangle with an exclamation mark for informational, a yellow triangle with exclamation mark for warning, or the color red and an "X" for failure. To re-run Validate, click **Retry**. To change the location of the Validate Report, type a new path or click **Browse** and select a new location for the Validate Report.
29. Click the **View** link at the lower left of the Validate pane and review the detailed report provided by Validate. A web browser is launched and the detailed contents of the Validate are displayed. Review the contents for failures, warnings, or recommendations. After reviewing the report, click **Next**. The *Pre-install Checks* page is displayed.
30. Pre-install checks run to ensure that the installation can continue. *Setup* checks the available disk space, system memory, operating system compatibility, and dependencies between modules. The Progress pane on the *Pre-Install Checks* page displays the progress of these checks. When finished, the *Report* pane displays the results.
31. Review the pre-install check results. If any of the pre-install checks are unsuccessful, go back through the wizard, make the necessary changes, and run the pre-install checks again. If the pre-install checks are successful, click **Next**. The *Install* page is displayed.
32. The *Install* page displays the progress of the installation. During this process, *Setup* installs the necessary files and folders onto your system and applies the configuration you specified. The *Packet Filter Installation* page is displayed.

33. The Neverfail Heartbeat Packet Filter driver installs on each network card of the production server. If you see warnings that the driver is unsigned or did not complete the Windows Logo tests, click **Install**. If Windows is configured to display Signed Driver warnings, you may see multiple warnings. The *Report* pane displays the results. Click **Next**.

By default, the Neverfail Heartbeat Packet Filter driver is applied to all Principal (Public) network cards present on the machine. The Neverfail Heartbeat Packet Filter is not applied to the network cards forming Neverfail Channel connections as these cards maintain unique IP addresses irrespective of the role of the server.

The *Primary Installation Complete* page is displayed.

34. When the *Setup* wizard confirms the successful completion of the installation, click **Finish**.

Installing Neverfail Heartbeat on the Secondary or Tertiary Server

The process of installing Neverfail Heartbeat on the Secondary or Tertiary server is similar to installing Neverfail Heartbeat on the Primary server.

Prerequisites

Installation of Neverfail Heartbeat on the Primary server must be successfully completed before initiating installation of Neverfail Heartbeat on the Secondary or Tertiary server.

1. You have the following options:
 - If you are using a single NIC, continue with [Step 2](#).
 - If you are using multiple NICs, go to [Step 3](#).
2. Before powering on the Secondary (cloned) server image, right-click the server image and select *Edit Settings*.
 - a) Select the Principal (Public)/Neverfail Channel virtual network adapter and clear the *Connected* and *Connect at power on* check boxes.
 - b) Power on the Secondary (previously cloned) server image.
 - c) On the Secondary server, open *Network Connections*, right-click the Principal (Public)/Neverfail Channel network connection, and select *Properties*. Select *Internet Protocol Version 4 (TCP/IP)* and click **Properties**.
 - d) Configure the appropriate Neverfail Channel IP address. Click **Advanced**.
 - e) Click the *WINS* tab and select *Disable NetBIOS over TCP/IP* and clear the *Register this connection's addresses in DNS* check box.
 - f) Click **OK** three times to close the dialogs.
 - g) Right-click the Secondary (cloned) server image and select *Edit Settings*.
 - h) Select the single virtual network adapter and select the *Connected* and *Connect at power on* check boxes. IP communications with the Secondary server go through the Neverfail Channel.
 - i) Go to [Step 4](#).
3. Before powering on the Secondary (cloned) server image, right-click the server image and select *Edit Settings*.
 - a) Select the Principal (Public) virtual network adapter and clear the *Connected* and *Connect at power on* check boxes.
 - b) Repeat the process on the Neverfail Channel virtual network adapter.
 - c) Power on the Secondary (previously cloned) server image.

- d) On the Secondary server, open *Network Connections*, right-click the Neverfail Channel network connection, and select *Properties*. Select *Internet Protocol Version 4 (TCP/IP)* and click **Properties**.
- e) Configure the appropriate Neverfail Channel IP address and subnet mask. Click **Advanced**.
- f) Click the *WINS* tab, select *Disable NetBIOS over TCP/IP*. Select the *DNS* tab and clear the *Register this connection's addresses in DNS* check box. Click **OK** three times to close the dialogs.
- g) Right-click the Principal (Public) network connection and select *Properties*. Select *Internet Protocol Version 4 (TCP/IP)* and click **Properties**. Configure the Principal (Public) IP address, subnet mask, and default gateway.
- h) Click **OK** three times to close the dialogs.
- i) Right-click the Secondary (cloned) server image and select *Edit Settings*.
- j) Select the Neverfail Channel virtual network adapter and select the *Connected* and *Connect at power on* check boxes. IP communications with the Secondary server go through the Neverfail Channel.

Important: Do not connect the Principal (Public) virtual network adapter at this time to prevent an IP address conflict on the network.

4. Extract the contents of the Neverfail Heartbeat .zip file and double-click the Setup.exe file to initiate the installation process.
5. The *Setup Type* page appears. As with the installation on the Primary server, select *Install Neverfail Heartbeat* and click **Next**.
The *Physical Hardware Identity* page is displayed.
6. Select the identity of the server on the *Physical Hardware Identity* page. Select *Secondary or Tertiary* as the server identity and click **Next**.
The *Identify Microsoft Windows Backup Folder* page is displayed.
7. Identify the location of the folder containing the backup file from the Primary server. Manually type the location path in the text box. Click **Next**.

Note: You must use the UNC path to identify the folder location of the backup files, for example, \\192.168.1.6\backup.

If you selected to *Skip Validation* on the Primary server, go to [Step 12](#), otherwise, the *Validate Collector Installation* page is displayed.

8. If the *Validate Collector* was not successfully installed on the Secondary server during the Primary server installation, click the **Install** button to install the *Validate Collector* on the Secondary/Tertiary server or click the **Skip Validation** to bypass the *Validate* process.
The results of the *Validate Collector* installation are displayed in the *Report* pane. If the *Validate Collector* is not successfully installed, click **Back** to reattempt installation.

Note: If the *Validate Collector* fails to install on the local server or you wish to bypass *Validation*, click the **Skip Validation** button to continue the installation and go to [Step 12](#).

9. After *Validate Collector* is successfully installed on the local server, click **Next**.
The *Validate* page is displayed.
10. Click **Start** to initiate the *Validation* process or click **Skip Validation** to bypass the *Validation* process.
Validate Collector gathers required information from all servers in the cluster and provides the status of the gathering operation for each server. Upon completion of information gathering, high level results are displayed in the lower pane of the page with the color green and a check mark for success, a blue triangle with an exclamation mark for informational, a yellow triangle with

exclamation mark for warning, or the color red and an "X" for failure. To re-run Validate, click **Retry**. To change the location of the Validate Report, type a new path or click **Browse** and select a new location for the Validate Report.

11. Click the **View** link at the lower left of the Validate pane and review the detailed report provided by Validate. A web browser is launched and the detailed contents of the Validate are displayed. Review the contents for failures, warnings, or recommendations. After reviewing the report, click **Next**.
The *Pre-install Checks* page is displayed.
12. The pre-install checks run. Click **Next**.
If any of the pre-install checks are unsuccessful, go back through the wizard, make the necessary changes, and run the pre-install checks again.
13. The next page displays the progress of the installation. During this process, Setup installs the necessary files and folders onto your system and applies the configuration you specified.
14. The *Report* pane displays the results of the installation. Click **Next**.
The *Packet Filter Installation* page is displayed.
15. The progress of the Neverfail Heartbeat Filter installation is displayed. Click **Next**.
 - a) The Packet Filter is installed on the Principal (Public) NIC and the Principal (Public) network adapter can be reconnected. Right-click the Secondary server image name and select *Edit Settings*.
 - b) Select the Principal (Public) virtual network adapter, select the *Connected* and *Connect at power on* check boxes, and click **OK**.
16. In the *Channel Adapter Identification* page, select the appropriate adapter and review the IP address configuration in the lower pane. Click **Next**.
The *Public Adapter Identification* page is displayed.
17. Configure the Principal (Public) adapter on the Secondary server through the *Public Adapter Identification* page. When you select the Principal (Public) adapter, a caution message notifies you that the IP address on the Principal (Public) adapter does not match the IP address on the Primary server (LAN configuration only).
The *Secondary Installation Complete* page is displayed.
18. When the *Setup* wizard confirms the successful completion of the installation, click **Finish**.

Install 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

Note: *Neverfail Heartbeat Client Tools 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 Client Tools will prevent installation until .Net Framework 4 is installed.*

1. To install the Neverfail Heartbeat Client Tools, download, extract the contents, and initiate Neverfail Heartbeat `setup.exe`.
 - a) Download Neverfail Heartbeat to a suitable location.
 - b) Extract the contents of the Neverfail Heartbeat `.zip` file.
 - c) Double-click the `setup.exe` file to initiate the installation process.

The **Setup Type** page is displayed.

2. On the **Setup Type** page, select *Install Client Tools Only* and click **Next**.
3. Read the license agreement carefully and select *I accept terms of the License Agreement*. Click **Next**.
4. Configure the installation paths. The default installation location is `C:\Program Files\Neverfail\` but can be changed by manually typing a path to another install location. Alternatively, click **Browse** to select one of these locations. Select *Create icons on Desktop* and click **Next**.

Note: The path of the Neverfail Heartbeat Client Tools installation folder cannot contain Unicode characters. The path of the Neverfail Heartbeat Client Tools installation folder can only contain lower and upper case letters A to Z, digits from 0 to 9, and the following special characters: space \ _ . :

Additionally, Neverfail Heartbeat Client Tools does not support file or folder names ending with a period "." or space " ".

5. Review the summary of options and configuration information for the installation. Click **Next**. Pre-install checks run to ensure that the installation can continue. The *Report* pane displays the results of the pre-install checks. If some pre-install checks are unsuccessful, go back through the wizard, make the necessary changes, and run the pre-install checks again.
6. If the pre-install checks are successful, click **Next**. The next page displays the progress of the installation. During this process, Neverfail Heartbeat Setup installs the necessary files and folders onto your system and applies the configuration you specified.
7. Click **Next** after Neverfail Heartbeat Client Tools components are complete. The **Client Tools Installation Complete** page is displayed.
8. Click **Finish**.

Neverfail vSphere Client

Neverfail vSphere Client is an optional feature that employs the Neverfail vSphere Client Extension Plug-in and integrates Neverfail vSphere Client with VMware's vSphere Client. Neverfail vSphere Client allows administrators to manage Neverfail Heartbeat Clusters and Groups from within the VMware vSphere Client. Neverfail vSphere Client allows administrators to Discover Neverfail Clusters and Groups, manually Add and Remove Neverfail Heartbeat servers, perform a switchover using the Make Active command, Start Replication, Stop Replication, and Shutdown Neverfail Heartbeat.

Additionally, the Neverfail vSphere Client allows administrators to view the current status of Neverfail Heartbeat servers previously discovered or added to Neverfail vSphere Client. Administrators can view Replication status, Application health, File and Registry Synchronization status, and the role of the server.

Note: If the Neverfail Management on vCenter Server features was not previously included in your Neverfail Heartbeat license, you must regenerate your license and install it using the Configure Server wizard to add

the new feature. The Neverfail Management on vCenter Server feature will only be available for installation once the feature has been added to your license and the license installed.

Installing Neverfail vSphere Client

Installation of Neverfail vSphere Client is performed on the server running vCenter Server using Neverfail Heartbeat Setup similar to installation of Neverfail Heartbeat.

Prerequisites

- Neverfail Heartbeat v6.6 or later installed on all physical Neverfail Heartbeat servers
- An appropriate Neverfail license for the Pair or Trio for Management on vCenter Server
- vCenter Server installed on a single server to manage virtual servers in a the site

Note: *If vCenter Sever Heartbeat is installed on the vCenter Server, then Neverfail Heartbeat Management on vCenter Server must be installed on both the active and passive servers. If Neverfail Heartbeat Management of vCenter Server is installed on the Primary vCenter Server before installing vCenter Server Heartbeat, the cloning process used during the installation of vCenter Server Heartbeat will automatically install Neverfail Management of vCenter Server on the Secondary server.*

1. Download the Neverfail Heartbeat .zip file to a suitable location on the server running vCenter Server.

Note: *Before attempting to unzip the Neverfail Heartbeat .zip file, verify that the file is not blocked. Right-click the Neverfail Heartbeat .zip file and select Properties. If the file is shown as blocked, click the **Unblock** button.*

2. Extract the contents of the Neverfail Heartbeat .zip file.
3. Double-click the setup.exe file to initiate the installation process.
The **Setup Type** page is displayed.

Note: *If you click **Exit** any time after Setup.exe starts, you are prompted to save the current settings. When you run Setup.exe later, you are offered the option to use the previously saved settings.*

If .Net 4.0 is not currently installed on the server, Neverfail Heartbeat Setup prompts you to download and install .Net 4.0 before allowing you to install Neverfail Heartbeat Management on vCenter Server. You must exit the installation process, download and install .Net 4.0, and restart the installation process.

The left panel of each page in the Neverfail Heartbeat Setup wizard provides information about the setup process. Select the configuration options in the panel on the right.

4. Because the Neverfail vSphere Client Extension Plug-in is being installed, in the **Setup Type** page, select **Install Neverfail Heartbeat Management on vCenter Server**. Click **Next**.
The **End User License Agreement** page is displayed.
5. Review the contents of the End User License Agreement and select *I accept terms of the License Agreement* to continue installation of Neverfail vSphere Client Plug-in. If you select *I do not accept terms of the License Agreement*, the **Next** button remains inactive and the dialog allows only the **Back** and **Exit** button to be active. Click **Next** to continue.
The **Installation Paths** page is displayed.
6. The **Installation Paths** page displays the location where Neverfail Heartbeat Management on vCenter Server is to be installed. Click **Next**

- The **vCenter Management Tool Registration** page is displayed.
7. Enter the *Username* and *Password* used to connect to vCenter Server and click **Next**.
Neverfail Setup verifies the details provided. After the details have been verified, the **Installation Summary** page is displayed.
 8. Review the results of the **Installation Summary** page. Click **Next**.
 9. Neverfail Heartbeat Setup automatically performs pre-install checks to ensure that the installation can continue. If a problem is encountered, click **Back** to return to the appropriate screen to make the changes required to resolve the issue. After making changes, run the pre-install check again to verify that the problem has been resolved and no new issues were created. Once the pre-install check successfully completes, click **Next** to proceed with the installation.
The **Install** page is displayed.
 10. The progress of the installation is displayed in the upper pane of the **Install** page. When the installation has completed, the results of the installation are displayed in the lower pane of the **Install** page. Once installation has successfully completed, click **Next** to continue.
The **Installation Complete** page is displayed.

Launch Neverfail vSphere Client

Prerequisites

Use of Neverfail vSphere Client requires that Adobe Flash Player 10.0 is installed.

***Note:** If Adobe Flash Player 10.0 is not installed prior to installation of Neverfail vSphere Client Extension Plug-in, selecting the double-clicking the Neverfail Heartbeat tab in vSphere Client for the first time will provide an opportunity to download Adobe Flash Player 10.0 from the internet and install it.*

1. Login to VMware vSphere Client.



Figure 2: vSphere Client Login

2. A security certificate is presented. Select the check box to install the security certificate.

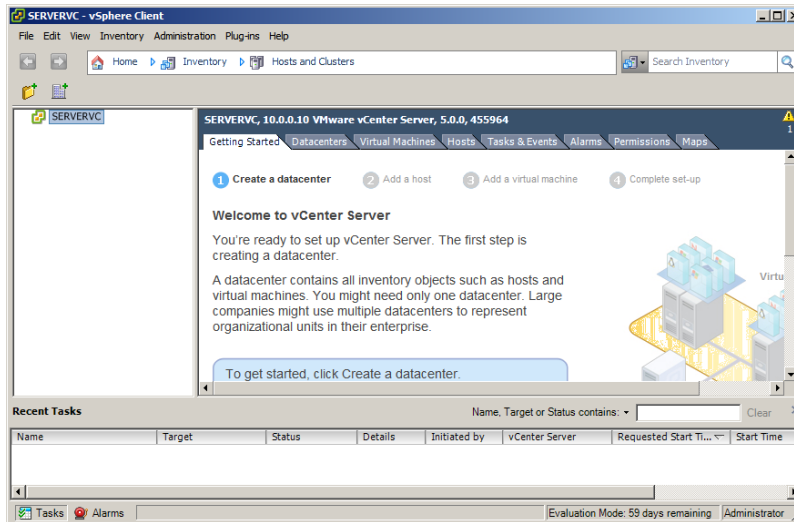


Figure 3: vSphere Client

3. Navigate to **Home > Solutions and Applications**.

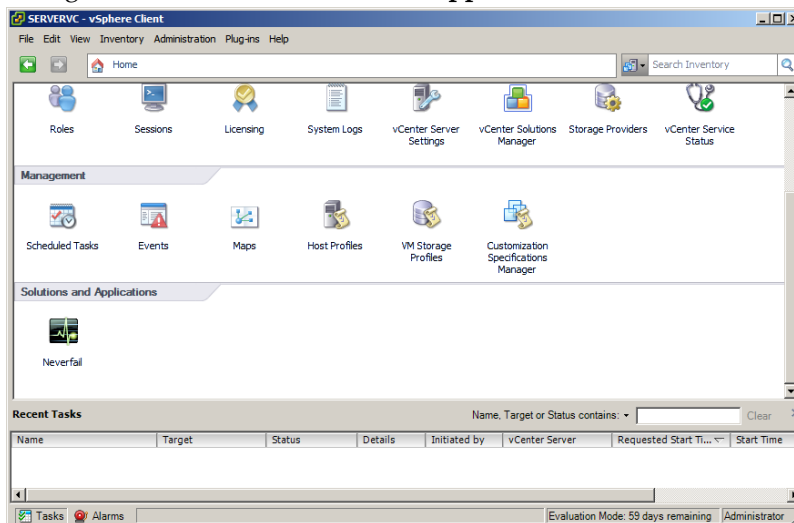


Figure 4: vSphere Client Solutions and Applications

4. Double-click the Neverfail Heartbeat icon in the *Solutions and Applications* pane. Neverfail vSphere Client displays the Neverfail Heartbeat page.

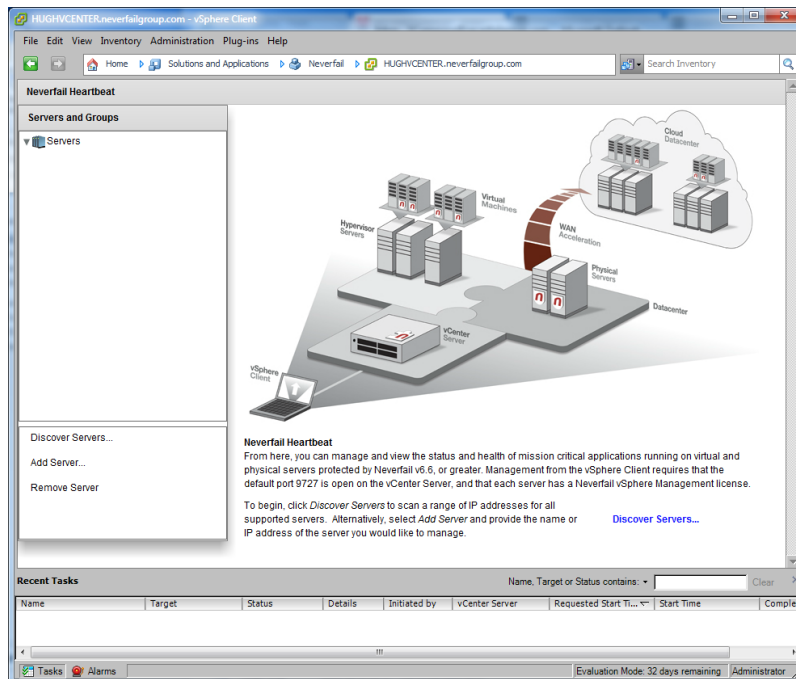


Figure 5: Neverfail Heartbeat page

Discover Neverfail Heartbeat Servers

Neverfail vSphere Client provides the ability to run discovery to identify all Neverfail Heartbeat Clusters and Groups.

Prerequisites

Each server to be managed by Neverfail vSphere Client requires a Neverfail vSphere Management license.

1. From the **Neverfail Heartbeat** page, click **Discover Servers** in the left pane of the page. The **Discover Server** dialog is displayed.

Discover Servers

Discover Neverfail-protected servers to manage

Please specify a range of IP addresses in which to search.

Begin

End

Port Number

Please specify the credentials for connecting to the servers.

Domain accounts should use the syntax username@domain.

Username

Password

OK Cancel

Figure 6: Discover Servers dialog

- Identify the IP address range to search by adding a beginning and ending IP address in the *Begin* and *End* fields.
Neverfail recommends leaving the *Port Number* field with the default port unless the default port is in use by another application and a custom port has been configured.
- Add a username and password used to connect to Neverfail Heartbeat in the *Username* and *Password* fields.

Note: If the username is a domain account, use the following format: *username@domain.xxx*

- Click **OK** to run Neverfail Heartbeat server discovery.
Neverfail vSphere Client displays all Neverfail Clusters and Groups discovered.

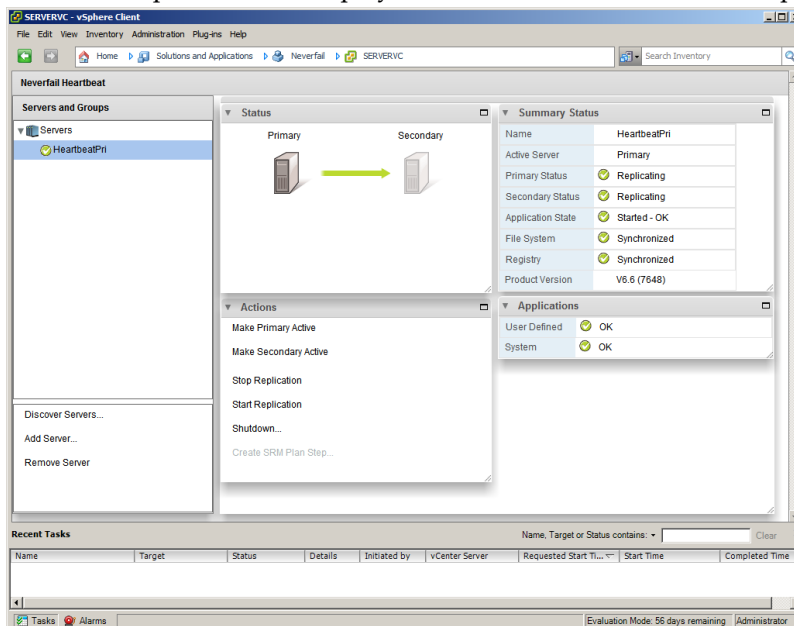


Figure 7: Neverfail Cluster in Neverfail vSphere Client

Add Neverfail Clusters

- Neverfail vSphere Client allows you to add individual Clusters which may be part of a Group. Click **Add Server** in the left pane of Neverfail vSphere Client to add a server. The **Add Server** dialog is displayed.

Figure 8: Add Server dialog

2. Enter the hostname or IP address of server to be added in the *Host* field.
Neverfail recommends leaving the *Port Number* field with the default port unless the default port is in use by another application and a custom port has been configured.
3. Add a username and password used to connect to Neverfail Heartbeat in the *Username* and *Password* fields.

Note: *If the username is a domain account, use the following format: username@domain.xxx.*

4. Click **OK** to add the Neverfail Cluster or Group.
Neverfail vSphere Client adds the Neverfail Heartbeat Cluster or Group to the left pane of the Neverfail Heartbeat page.

Remove Neverfail Clusters

Neverfail vSphere Client allows the removal of specific Neverfail Clusters from the Neverfail vSphere Client using the steps below.

1. Select the server Cluster to be removed from Neverfail vSphere Client.
2. Click **Remove Server**.
The intended Neverfail Cluster is removed from Neverfail vSphere client.

Note: *To define and configure Groups, you must use the Neverfail Heartbeat Management Client.*

Managing Neverfail Heartbeat with Neverfail vSphere Client

Neverfail vSphere Client allows administrators to manage Neverfail Heartbeat Clusters and Groups similar to the Neverfail Heartbeat Management Client. Neverfail vSphere Client provides the ability to perform a switchover, Start Replication, Stop Replication, and Shutdown Neverfail Heartbeat.

Additionally, Neverfail vSphere Client identifies the current active server and provides the Replication status of the servers in the Cluster, the Application State, and the File System and Registry State.

Note: *Neverfail Tasks and Events are not logged in vCenter 4.0 and earlier so will not appear in the vSphere Client.*

Perform a Switchover

- To make the Primary server of the Neverfail Cluster active, click the **Make Primary Active** button. The **Make Primary Active** dialog asks you to verify that you want to make the Primary server active. Click **OK** to make the Primary Server Active.
- To make the Secondary server of the Neverfail Cluster active, click the **Make Secondary Active** button. The **Make Secondary Active** dialog asks you to verify that you want to make the Secondary server active. Click **OK** to make the Secondary Server Active.
- If a Tertiary server is installed, you can make the Tertiary server active by click the **Make Tertiary Active** button. The **Make Tertiary Active** dialog asks you to verify that you want to make the Tertiary server active. Click **OK** to make the Tertiary server active.

Start Replication

When replication is stopped, click the **Start Replication** to initiate replication between the servers. Neverfail Heartbeat responds by starting replication between the servers.

Stop Replication

To stop replication, click the **Stop Replication** button. The **Stop Replication** dialog asks you to verify that you want to stop replication. Click **OK** to stop replication.

Shutdown Neverfail Heartbeat

To shutdown Neverfail Heartbeat, click the **Shutdown** button. The **Shutdown Options** dialog is displayed. Select one or more servers in the Neverfail Cluster to shutdown. Click **OK** to stop Neverfail Heartbeat on the selected servers in the Cluster.

Appendix

A

Setup Error Messages

Table 2: 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 3: 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 4: 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 5: 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 6: 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 7: 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 8: 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.