

Enterprise Monitoring

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: Neverfail and Simple Network Management Protocol.....	7
Simple Network Management Protocol Overview.....	7
Neverfail SNMP Extension Agent.....	7
NeverfailHB-MIB.mib.....	8
Chapter 2: Neverfail and System Center Operations Manager.....	13
Neverfail Heartbeat Management Pack.....	13
Introduction to the Neverfail Heartbeat Management Pack.....	13
Getting Started.....	16
Understanding Management Pack Operations.....	17
Neverfail Heartbeat Management Pack Monitors.....	18
Troubleshooting.....	26
Glossary.....	27

About This Book

Intended Audience

This guide assumes a working knowledge of networks including the configuration of TCP/IP protocols, SNMP, System Center Operations Manager, and a sound knowledge of domain administration on the Windows™ 2003, 2008, and 2012 platforms, notably in Active Directory and DNS.

Using the Monitoring Guide

This guide is designed to provide information related to the monitoring your Neverfail Heartbeat Clusters and Groups with either SNMP when the Neverfail Heartbeat Extension Agent is installed or System Center Operations Manager when the Neverfail SCOM Plug-in is installed. The information contained in this guide is current as of the date of printing.

Overview of Content

This guide is designed to provide the information necessary to successfully monitor Neverfail Heartbeat using SNMP with Neverfail Heartbeat's Extension Agent. Additionally, it provides the information required to successfully monitor Neverfail Heartbeat via System Center Operations Manager using the Neverfail Management Pack and Neverfail SCOM Plug-in.

This guide 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 — Neverfail Heartbeat and Simple Network Management Protocol (SNMP) presents an overview of Neverfail Heartbeat's interaction with SNMP using the Neverfail Heartbeat Extension Agent and Neverfail Heartbeat MIB and provides a listing of objects and traps available to SNMP.
- Chapter 2 — Neverfail Heartbeat and Microsoft System Center Operations Manager (SCOM) discusses use of the Neverfail Management Pack to monitor Neverfail Heartbeat and provides information about its content.

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

The figures in this book use the abbreviations listed in the table below.

Table 1: Abbreviations

Abbreviation	Description
Channel	Neverfail Channel
NIC	Network Interface Card
SNMP	Simple Network Management Protocol
SCOM	System Center Operations Manager

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

Neverfail and Simple Network Management Protocol

Simple Network Management Protocol Overview

Simple Network Management Protocol (SNMP) allows a variety of management programs such as Tivoli and HP OpenView to monitor and control many networked devices. Systems managed by SNMP run SNMP agents, which provide information to the management program in one of the following ways:

- In response to GET operations (a specific request for information from the management system) and SET operations
- By sending a trap (an alert sent by the SNMP agent to notify the management system of a specific event or condition)

Information that can be provided by managed devices is identified using a Management Information Base (MIB) file.

Neverfail Heartbeat supports Microsoft SNMP on systems where the SNMP service is enabled. Neverfail Heartbeat only works with the Microsoft SNMP Service. Microsoft's SNMP Service only supports up to SNMP Version 2. Neverfail Heartbeat integrates with Microsoft's SNMP Service through the implementation of an SNMP Extension Agent.

Neverfail SNMP Extension Agent

The Neverfail SNMP Extension Agent is installed automatically on all Neverfail enabled servers within a Neverfail group. Installation of the Neverfail SNMP Extension Agent is performed during normal Neverfail Setup operations. If the user intends to use Neverfail's SNMP feature, they must enable Microsoft SNMP service.

The Neverfail SNMP Extension Agent serves as an interface between the management program and Neverfail Heartbeat allowing information from Neverfail Heartbeat to be captured by and forwarded to the management program. Neverfail does not support SET operations due to the lack of security in SNMP Version 2.

The Neverfail SNMP Extension Agent sends traps for all significant Heartbeat events. These traps contain a description of the event and are defined in the NeverfailHB-MIB.mib file.

NeverfailHB-MIB.mib

The NeverfailHB-MIB.mib file defines the objects used to report information about Neverfail Heartbeat to SNMP management software. The NeverfailHB-MIB.mib file is included in the Neverfail Heartbeat kit and can be found in the <install_location>\Neverfail\R2\bin folder.

The following tables contain a listing of the objects and traps provided by the NeverfailHB-MIB.mib file.

Table 2: Cluster Group

Object	ID Mapping	Description
clusterName	heartbeatClusterMIBObjects 1	The cluster name
clusterReplicationEnabled	heartbeatClusterMIBObjects 2	Whether replication is enabled on the cluster or not
clusterActiveServer	heartbeatClusterMIBObjects 3	The current active server. This can be Primary, Secondary or Tertiary
clusterGroupType	heartbeatClusterMIBObjects 4	The cluster group type, for example, Unary, Binary or Ternary
clusterApplicationState	heartbeatClusterMIBObjects 5	The rolled up application state, for example, Stopped, Started, etc.
clusterHeartbeatVersion	heartbeatClusterMIBObjects 6	The version of Neverfail Heartbeat installed
clusterTotalMissedPings	heartbeatClusterMIBObjects 7	The total number of missed network pings
clusterCurrentMissedPings	heartbeatClusterMIBObjects 8	The current number of missed network pings

Table 3: Heartbeat Server

The Heartbeat Server Table. This is the table of servers in the cluster. There will be a maximum of three rows in this table.

Object	ID Mapping	Description
hbServerTableIndex	hbServerTableEntry1	Index into the HB Server Table. Identifies the member of the cluster
hbServerIdentity	hbServerTableEntry2	Specifies whether this is the Primary, Secondary or Tertiary server
hbServerStatus	hbServerTableEntry3	The status of this Neverfail Heartbeat Server
hbServerRole	hbServerTableEntry4	The role of this Neverfail Heartbeat Server - Active or Passive
hbServerPublicIPAddress	hbServerTableEntry5	The Public IP Address for this server
hbServerHBUpTime	hbServerTableEntry6	The length of time this server has been up and running
hbServerFSSynchStatus	hbServerTableEntry7	The current state of File System Synchronization
hbServerFSPercentComplete	hbServerTableEntry8	The percentage of file system synchronization that is complete
hbServerRegistrySynchStatus	hbServerTableEntry9	The current state of Registry Synchronization
hbServerTimeSinceActiveLost	hbServerTableEntry10	Only valid on the Passive server, this is the length of time since the Active server was last seen
hbServerRecoveryPointEstimate	hbServerTableEntry11	The estimated point in time from which the server data can be recovered
hbServerPercentProcessorTime	hbServerTableEntry12	The percentage of Processor Time (Not supported in this version)

Object	ID Mapping	Description
hbServerPercentDiskTime	hbServerTableEntry13	The percentage of Disk Time (Not supported in this version)
hbServerAvgDiskSecTransfer	hbServerTableEntry14	The measurement of the average time of each data transfer, regardless of the number of bytes read or written (Not supported in this version)
hbServerPercentCPUUtilization	hbServerTableEntry15	The percentage of CPU utilization (Not supported in this version)
hbServerMaxChannelThruPut	hbServerTableEntry16	The maximum throughput of this server's channels in mbits/sec
hbServerCurrentChannelThruPut	hbServerTableEntry17	The current throughput of this server's channels in mbits/sec

Table 4: Neverfail Channels

Neverfail Channel table information

Object	ID Mapping	Description
channelTableIndex	channelTableEntry 1	Index into the Channel Table
channelHost	channelTableEntry 2	The host for this Neverfail Channel - can be Primary, Secondary or Tertiary
channelPeer	channelTableEntry 3	The peer to which this Neverfail Channel is connected - can be Primary, Secondary or Tertiary
isConnected	channelTableEntry 4	Whether the Neverfail Channel is connected or not
numConnectedLinks	channelTableEntry 5	The number of connected physical links in the Neverfail Channel
waxEnabledCompressionType	channelTableEntry 6	The compression type that has been enabled on this channel
waxActiveCompressionType	channelTableEntry 7	The active compression type on this channel
waxTimeStarted	channelTableEntry 8	Time since WAN compression started
waxVolDataProcessed	channelTableEntry 9	The volume of data processed
waxAvgThruPutData	channelTableEntry 10	Average throughput of uncompressed data
waxCurrentThruPutData	channelTableEntry 11	Current throughput of uncompressed data
waxAvgCompressionFactor	channelTableEntry 12	Average data compression factor
waxCurrentCompressionFactor	channelTableEntry 13	Current data compression factor
sendQueueSize	channelTableEntry 14	Size of the send queue
sendQAgeOfOldestEntry	channelTableEntry 15	Age of the oldest entry on send queue in milliseconds

<i>Object</i>	<i>ID Mapping</i>	<i>Description</i>
receiveQueueSize	channelTableEntry 16	Size of the receive queue
receiveQAgeOfOldestEntry	channelTableEntry 17	Age of the oldest entry on receive queue in milliseconds

Table 5: Physical Links

Physical link table information

<i>Object</i>	<i>ID Mapping</i>	<i>Description</i>
linkTableIndex	linkTableEntry 1	Index into the Link Table
linkHost	linkTableEntry 2	The source server for the link
linkPeer	linkTableEntry 3	The destination server for the link
linkSourceIPAddress	linkTableEntry 4	The IP Address on the source server
linkDestinationIPAddress	linkTableEntry 5	The IP Address on the destination server
linkIsConnected	linkTableEntry 6	True or False depending on whether the link is connected or not

Table 6: Protected Applications

Protected application table information

<i>Object</i>	<i>ID Mapping</i>	<i>Description</i>
protectedApplicationIndex	protectedApplicationEntry 1	Index into the Protected Application table
protectedApplicationName	protectedApplicationEntry 2	The name of the protected application
protectedApplicationState	protectedApplicationEntry 3	The current status of the protected application
protectedApplicationHealth	protectedApplicationEntry 4	The current health of the protected application

Table 7: Traps

Traps used by Neverfail Heartbeat Extension Agent

<i>Trap</i>	<i>ID Mapping</i>	<i>Description</i>
ApplicationStarted	1	A protected application has started in the cluster

Trap	ID Mapping	Description
ApplicationStopped	2	A protected application has stopped in the cluster
FailoverPrevented	3	A failover has been prevented as the Active server is still visible to the Passive server
FailoverStarting	4	A failover has occurred in the cluster
DisconnectingServers	5	Neverfail Heartbeat Server1 has lost contact with Neverfail Heartbeat Server2
InvalidLicense	6	There is no valid license for Neverfail Heartbeat in the cluster
LicenseExpiryEvent	7	The Neverfail Heartbeat license has expired
ImpendingLicenseExpiry	8	The Neverfail Heartbeat license for this cluster will expire shortly
ServerMadeActive	9	This server has been made active
ServerMadePassive	10	This server has been made passive
ReplicationStarted	11	Replication has started in the cluster
ReplicationStopped	12	Replication has stopped in the cluster
ShuttingDown	13	Neverfail Heartbeat is shutting down in the cluster
HeartbeatStarted	14	Neverfail Heartbeat has started in the cluster
HeartbeatStopped	15	Neverfail Heartbeat has stopped on this server
NFChannelConnected	16	The Neverfail Channel has connected
NFChannelDisconnected	17	<i>Known issue: The Neverfail Heartbeat SNMP Extension Agent does not currently send traps to indicate when the Neverfail Channel has disconnected.</i>
ControllerAutoSwitched	18	An automatic switchover has completed
ControllerAutoSwitchover	19	An automatic switchover has started

Table 8: Error Events

The following are serious error events that occur very infrequently.

Variable	ID Mapping	Description
SplitBrain	20	A split-brain has occurred in the cluster. You will need to manually reconfigure the servers and restart Heartbeat
ApplyAccessDenied	21	The Apply module in Neverfail Heartbeat has been denied access to a file or directory on the passive server
ApplyDiskFull	22	The disk on the passive server is full. Neverfail Heartbeat can no longer apply changes to the passive server
ApplySharingViolation	23	There has been a sharing violation on the passive server. An unknown process is accessing the protected data on the passive server
NFChannelDiskUsageExceeded	24	The Neverfail Channel has exceeded its maximum disk usage
NFChannelOutOfDiskSpace	25	The Neverfail Channel is out of disk space
RollbackOperationFailed	26	A Neverfail Heartbeat rollback operation has failed

<i>Variable</i>	<i>ID Mapping</i>	<i>Description</i>
UnsupportedFeature	27	Neverfail Heartbeat has detected an unsupported feature. Please see KB???? for further information
LostMessage	28	Neverfail Heartbeat has detected that a message has been lost between the Active and Passive servers
BadPingConfiguration	29	The Network Monitoring ping configuration is invalid
InvalidISCPingTarget	30	The Server Monitoring ping configuration is invalid
ApplyDead	31	Critical internal error in Apply component

Chapter 2

Neverfail and System Center Operations Manager

Neverfail Heartbeat Management Pack

Neverfail offers a Neverfail Heartbeat Management Pack to provide the required configuration information for monitoring and reporting on Neverfail Heartbeat and protected application operations. When used in conjunction with Microsoft System Center Operations Manager (SCOM) and the Neverfail SCOM Plug-in, users can monitor the performance of Neverfail Heartbeat and use the data from SCOM reports to optimize both server and Neverfail Heartbeat performance.

Introduction to the Neverfail Heartbeat Management Pack

The Neverfail Heartbeat Management Pack provides the configuration information necessary to monitor the health, performance, and availability of Neverfail Heartbeat servers running on Windows Server 2003, 2008, and 2012 operating systems. The Neverfail Heartbeat Management Pack provides the necessary information to allow SCOM to collect server performance data that can be used for routine management and configuration modifications to optimize servers.

This Neverfail Heartbeat Management Pack download supports the following operating systems:

- Windows Server® 2012
- Windows Server® 2008 R2
- Windows Server® 2008
- Windows Server® 2003

This diagram provides an overview of the SCOM Agent communications for monitoring Neverfail Heartbeat and protected applications.

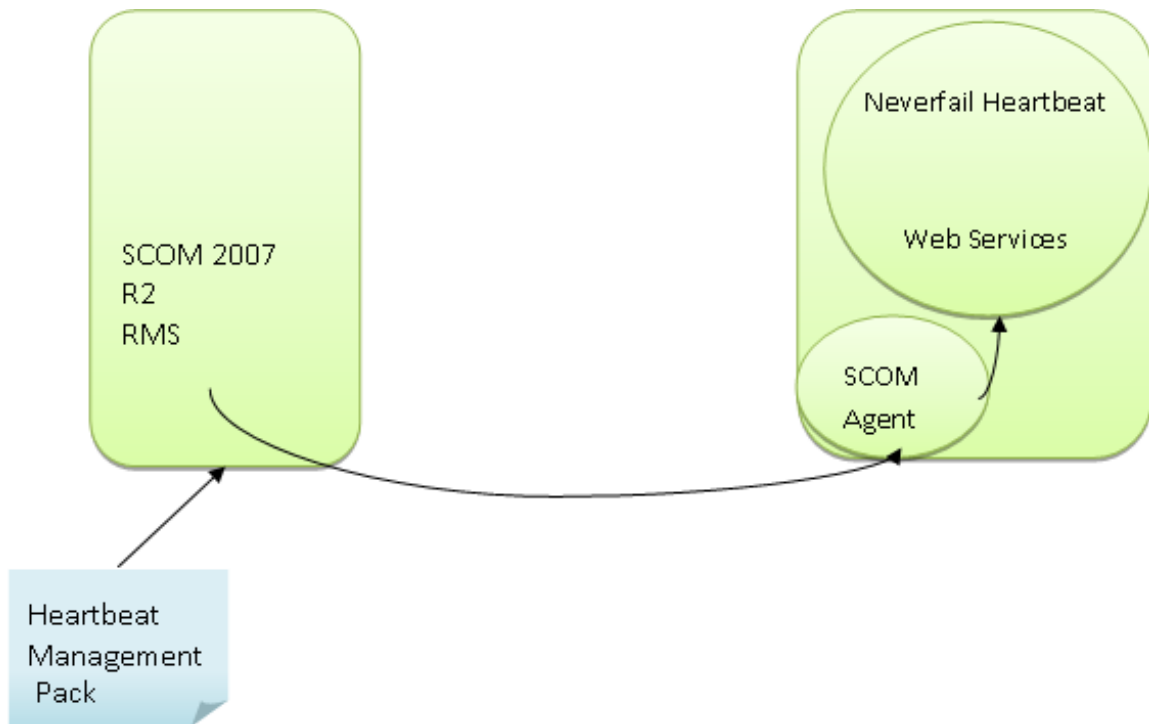


Figure 1: SCOM Agent Communications

This diagram provides an overview of the relationships between the classes and identifies the hosting objects, contained objects, containing objects and inheritance characteristics of the Neverfail Heartbeat Management Pack.

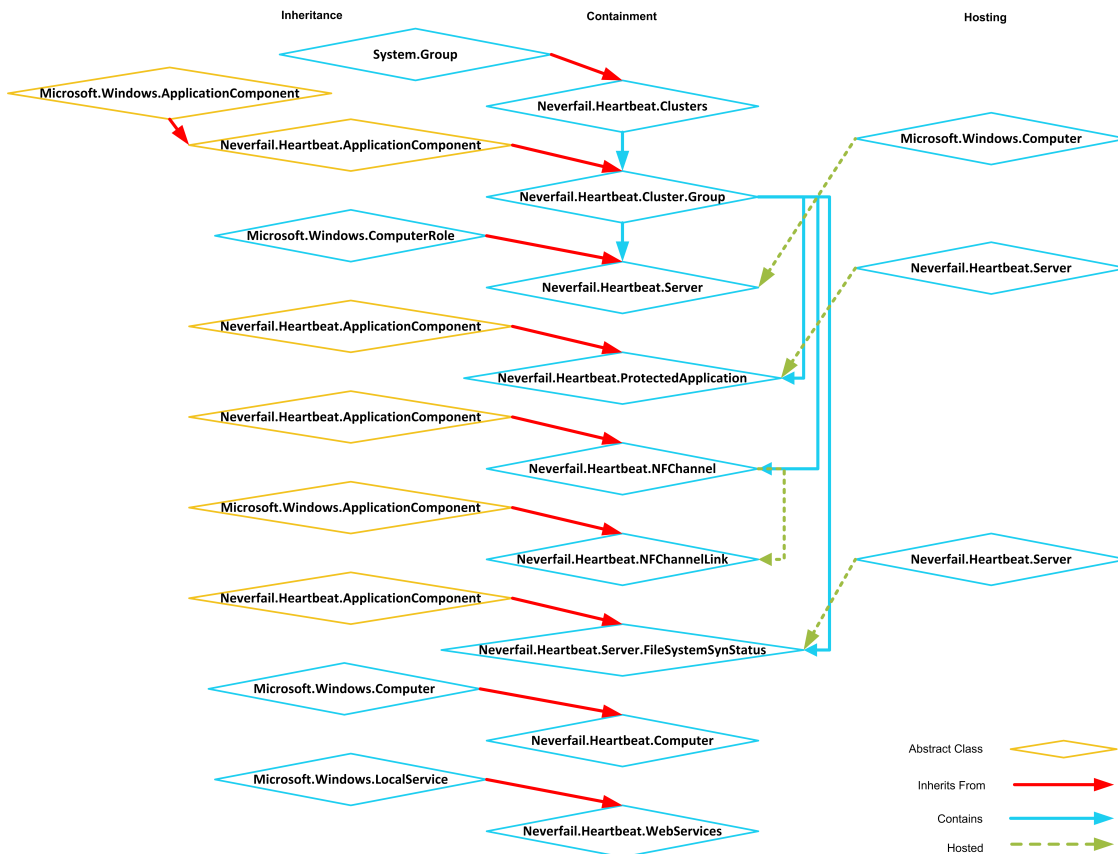


Figure 2: The Neverfail Heartbeat Management Pack Service Model

Getting the Latest Management Pack and Documentation

The Neverfail Heartbeat Management Pack, `Neverfail.Heartbeat.mp` file, is included in the Neverfail Heartbeat kit .zip file and as a component of the `SCOMSolutionsPackNeverfail-v6-6.zip` file that can be downloaded from the [Neverfail Extranet](#) by navigating to **Products / Downloads > Heartbeat** and selecting the appropriate version of the `SCOMSolutionsPackNeverfail-v6-6.zip` file.

The Neverfail SCOM Plugin supports the following versions of SCOM:

- SCOM version 2007
- SCOM version 2007 R2
- SCOM version 2012

Contents of the Neverfail SCOM Pack

The `SCOMSolutionsPackNeverfail-v6-6.zip` file contains the following components:

- `Neverfail.Heartbeat.mp` file
- `Neverfail Heartbeat for System Center Operations Manager.pdf`
- `SCOMNFPlugin.dll` file

Changes in This Update

This is the first version of this document.

Supported Configurations

The Neverfail Heartbeat Management Pack provides support for Neverfail Heartbeat v6.7.0 and later in the following configurations:

- High Availability (Pair) in a LAN
- Disaster Recovery (Pair) in a WAN
- High Availability (LAN)+ Disaster Recovery (WAN) (Tertiary)

Getting Started

This section provides the prerequisites to importing the Management Pack, steps to perform after importing the Management Pack, and information about customization.

Before You Import the Management Pack

Before importing the `Neverfail.Heartbeat.mp` file, the following tasks must be performed.

1. Neverfail Heartbeat must be installed and configured before importing `Neverfail.Heartbeat.mp`
2. The server on which Neverfail Heartbeat is installed must be configured in the SCOM Operations Console to act as an Agent Proxy before importing `Neverfail.Heartbeat.MP`. This will allow the Neverfail Active server to report performance and configuration information for the Neverfail passive servers.
3. Install the SCOM Plug-in following the steps below:

Important: *Plug-ins should be installed only on the active server. Installation of a plug-in on a passive server may cause an Exception to occur.*

- a. Launch the Neverfail Heartbeat Management Client.
- b. Navigate to **Applications > Plug-ins**.
- c. Right-click on an existing plug-in from the Plug-ins list and select **Install** from the menu or click **Install** at the top of the page.

The **Install Plug-in** dialog is displayed.

- d. Type a path to the `SCOMNFPlugin.dll` location (case-sensitive), or click **Browse** and navigate to the plug-in (recommended).
- e. Click **OK** to install the plug-in or click **Cancel** to close the dialog without installing a plug-in.

The Neverfail SCOM Plug-in works to manage the HealthService service ensuring that it is stopped on the passive server at all times and running on the active server. During a switchover, the Neverfail SCOM Plug-in automatically stops the HealthService service on the machine that was previously active and starts it on the machine that will become active.

Additionally, the Neverfail SCOM Plug-in changes the HealthService service Startup type on the passive machine to *Manual* and on the active machine to *Automatic* ensuring that the HealthService service is always run on the active server regardless of whether Neverfail Heartbeat itself is running or stopped.

Files in This Management Pack

The Neverfail Heartbeat Management Pack consists of the following files:

- `Neverfail.Heartbeat.mp`

After You Import the Management Pack

After the Neverfail Heartbeat Management Pack has been imported, perform the following tasks:

1. Review the Performance Monitors for enablement.
2. Set the any overrides for frequency of discovery.

Low-Privilege Environments

By default, the Neverfail Heartbeat Management Pack will use the agent action account to perform discoveries and to run monitors, rules and tasks. The agent action account can run as Local System or as a named account. If running as the Local System account the user will have the privileges required to run tasks, rules and discovery actions provided by the Neverfail Heartbeat Management Pack.

Note: *If you configure the agent to use a low-privilege account Neverfail discoveries, monitors, rules and tasks will not run successfully.*

Understanding Management Pack Operations

Neverfail Heartbeat operations are divided into two areas, Discovery and Monitoring:

Discovery

Each object in the Neverfail Heartbeat Management pack must be discovered by SCOM before it can be viewed by the user. To enable this, the Neverfail Heartbeat Management Pack contains two Discoveries - *Neverfail.Heartbeat.Computer.Discover* and *Neverfail.Heartbeat.Discover.All*.

- The *Neverfail.Heartbeat.Computer.Discover* allows for discovery of the *Neverfail.Heartbeat.Computer* class. This is the first discovery that runs and will query the registry of each computer in the network to determine if Neverfail Heartbeat is installed. If Neverfail Heartbeat is found, it will check the version. If the version found matches the version listed in the Management Pack, an object will be created.
- The *Neverfail.Heartbeat.Discover.All* discovery targets each *Neverfail.Heartbeat.Computer* class found in the previous discovery. For each computer it runs a single script to retrieve all data on the servers within the Neverfail Cluster.

The following objects are created:

- *Neverfail.Heartbeat.ClusterGroup*
- *Neverfail.Heartbeat.Server*
- *Neverfail.Heartbeat.ProtectedApplication*
- *Neverfail.Heartbeat.NFChannel*
- *Neverfail.Heartbeat.NFChannel.Link*
- *Neverfail.Heartbeat.WebServices*
- *Neverfail.Heartbeat.Server.FileSystemSyncStatus*

Note: *The Neverfail Heartbeat Management Pack schedules both discoveries to run once every four hours. This is inline with the recommended Microsoft discovery interval. To run discovery more frequently, you must override this value. Administrators must determine the appropriate frequency based upon their configuration and environment.*

The Neverfail.Heartbeat.ComputerDiscovery identifies new Neverfail Heartbeat installations and does not need to run frequently. The Neverfail.Heartbeat.Discover.All discovery identifies changes in Neverfail Heartbeat configuration - for example the addition or deletion of Neverfail Heartbeat servers or channels;

or changes to Neverfail Heartbeat server roles (active/passive). This discovery requires running a single script on the SCOM Agent.

When determining how often to run discovery, it is important to balance the additional memory consumption required by SCOM with the need for more frequent discovery. For example, if discovery is run with the default configuration (once every 4 hours), when a failover/switchover occurs, the Monitors in the Neverfail Heartbeat Management Pack will update the overall status of the Neverfail Heartbeat objects promptly (and display any Alerts or Events that have been generated) however it will take up to 4 hours before the SCOM Operations Console accurately reflects the new roles of the Neverfail Heartbeat servers.

Additionally, instances of the following relationships are created:

- *Neverfail.Heartbeat.ClusterGroup.Contains.ProtectedApplications*
- *Neverfail.Heartbeat.ClusterGroup.Contains.Neverfail.Heartbeat.NFChannel*
- *Neverfail.Heartbeat.ClusterGroup.Contains.Heartbeat.Servers*
- *Neverfail.Heartbeat.ClusterGroup.Contains.WebServices*
- *Neverfail.Heartbeat.Server.Hosts.Neverfail.Heartbeat.ProtectedApplications*
- *Neverfail.Heartbeat.Server.Hosts.Neverfail.Heartbeat.FileSystemSyncStatus*
- *Neverfail.Heartbeat.NFChannel.Hosts.Neverfail.Heartbeat.NFChannel.Link*

Monitoring

With a combination of Availability and Performance monitors the Neverfail Heartbeat Management Pack monitors all discovered objects for Health and performance related issues with the monitors running in varying intervals between 3 and 5 minutes. Unit monitors roll-up in state views to produce near real-time health state views that can be used to determine the current health of all Neverfail services. Event views provide a historical view of the components health in situations where historical context is required to provide insight into Neverfail-related problems or when the user wants to see the health status over an extended period of time.

Neverfail Heartbeat Management Pack Monitors

Unit Monitors

Unit monitors gather state information from contained objects and provide and report the overall state of the object to the SCOM Console.

Table 9: Unit Monitors

Monitor	Type	Alert	Description
State Monitor for Heartbeat Server	Availability	Yes	<p>Monitors the Status of the Heartbeat Server. The SCOM state will indicate <i>Warning/Degraded</i> for the following controller states:</p> <ul style="list-style-type: none"> • Service Shutdown • Not Replicating • Stopping Replication • Service Shutting Down • Switching Active Server • Disconnecting from Peer Server • Not Participating • Server Not Responding

Monitor	Type	Alert	Description
			<ul style="list-style-type: none"> Previously Active Awaiting Peer Server (following an unclean shutdown) <p>The SCOM state will indicate <i>Critical</i> for the following:</p> <ul style="list-style-type: none"> Lost Active Server Active Following Failover <p><i>Note: For all other events, the SCOM state will indicate OK.</i></p>
State Monitor for Protected Applications	Availability	Yes	<p>Monitors the availability State of the protected application by looking at the Health and State values of the protected application.</p> <ul style="list-style-type: none"> If the Health is OK and the state is Stopped or Stopping, then indicate a <i>Warning/Degraded</i> state. If the Health is OK and the State is Starting or Started then indicate an <i>OK</i> state. If Health is Critical then indicate a <i>Critical</i> state. For any other Health state (for example Potential problem, warning, unknown or unmonitored) indicate a <i>Warning/Degraded</i> state.
State Monitor for Neverfail Channel's Physical Link	Availability	Yes	Monitors whether the Neverfail Channel Physical link is connected or not.
Web Service Monitor	Availability	Yes	This monitor checks whether the WebServices service is running or not. If it is not running a <i>Critical</i> alert is generated. A manual recovery action is also implemented which restarts the service. This recovery action can be run by the user in the SCOM Health Explorer.

Dependency Monitors

Dependency monitors allow the state of an object to affect the state of a monitor containing the object thereby allowing for a roll-up of states.

Table 10: Dependency Monitors

Monitor	Type	Alert	Description
<i>Neverfail.Heartbeat.CGdependsPA_DependencyMonitor</i>	Dependency	No	This monitor updates the state of the Cluster Group to reflect the state of the Protected Application. The health state is determined by the worst state of any protected application in the cluster.
<i>Neverfail.Heartbeat.CGdependsHB_DependencyMonitor</i>	Dependency	No	This monitor updates the state of the Cluster Group to reflect the state of the Heartbeat Servers. The health state is determined by the worst state of any Heartbeat Server in the cluster.
<i>Neverfail.Heartbeat.NFChannel.depends_Link.Monitor</i>	Dependency	No	This monitor updates the state of the Neverfail Channel to reflect the state of the Channel Links. The health state is determined

Monitor	Type	Alert	Description
			by the best state of any link within the Neverfail Channel.
<i>Neverfail.Heartbeat.CGdependsWebServices_DependencyMonitor</i>	Dependency	No	This monitor updates the state of the Cluster Group to reflect the state of the Web Services service.

Health Roll-ups

The following diagram illustrates how health states of components roll-up.

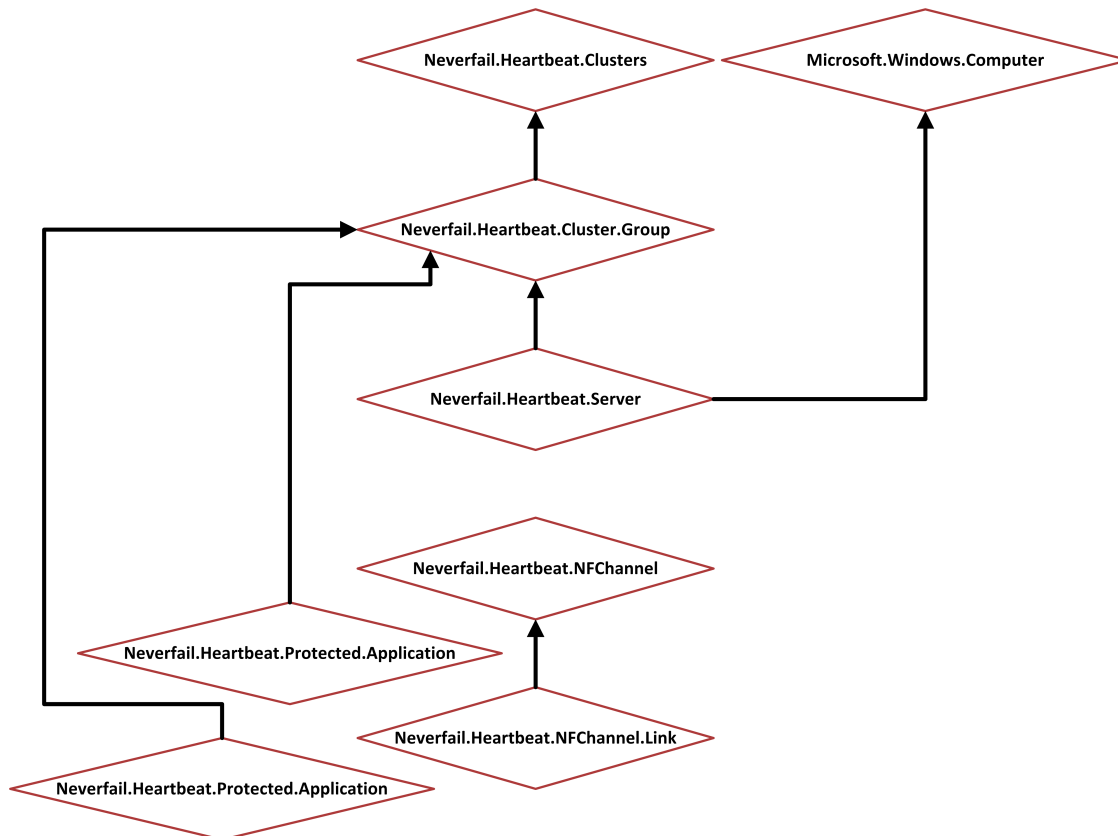


Figure 3: Neverfail Health Roll-ups

Performance Monitors

The following is a list of performance monitors that target the `Neverfail.Heartbeat.Server` class. These monitors are disabled by default. To enable these monitors, you must override the threshold values with values that are suitable for your environment.

Table 11: Performance Monitors

Monitor	Description
<code>Neverfail.Heartbeat.Server.Monitor.CurrentThroughPut</code>	A three-state performance monitor which monitors the current through put of the Heartbeat Server.

Monitor	Description
Neverfail.Heartbeat.Server.Monitor.MaxThroughPut	A three-state performance monitor which monitors the maximum through put of the Heartbeat Server.
Neverfail.Heartbeat.Server.Monitor.RecoveryPointMS	A three-state performance monitor which monitors the recovery point interval for the Heartbeat Server.
Neverfail.Heartbeat.Server.WinMonitor.AvgDiskQLen	A two-state performance monitor which monitors the Logical Disk, Average Disk Queue Length.
Neverfail.Heartbeat.Server.WinMonitor.AvgDiskSecRead	A two-state performance monitor which monitors the Logical Disk: Avg Disk/sec Read.
Neverfail.Heartbeat.Server.WinMonitor.AvgDiskSecTransfer	A two-state performance monitor which monitors the Logical Disk: Avg Disk/sec Transfer.
Neverfail.Heartbeat.Server.WinMonitor.CurrentDiskQueueLength	A two-state performance monitor which monitors the Logical Disk: Current Disk Queue Length.
Neverfail.Heartbeat.Server.WinMonitor.LogicalDisk.AvgDiskSecWrite	A two-state performance monitor which monitors the Logical Disk: Avg Disk/sec Write performance counter.
Neverfail.Heartbeat.Server.WinMonitor.LogicalDisk.DiskReadSec	A two-state performance monitor which monitors the Logical Disk: Disk Reads/sec performance counter.
Neverfail.Heartbeat.Server.WinMonitor.LogicalDisk.DiskWritesSec	A two-state performance monitor, which monitors the Logical Disk: Disk Writes/sec performance counter.
Neverfail.Heartbeat.Server.WinMonitor.LogicalDisk.PercetFreeSpace	A three-state performance monitor, which monitors the Logical Disk % Free Space performance counter.
Neverfail.Heartbeat.Server.WinMonitor.Processor.PercentProcessorTime	A two-state performance monitor, which monitors the Processor: % Processor Time performance counter.

Collection Rules

Rules collect historical data from sources such as Event Logs, Log Files, and Perfmon that data is stored In the Operations Manager database.

Note: Rules from different data sources are run at different times to minimize impact on system resources during the run. Additionally, rules that use the same data source are "cooked-down" to ensure that the collection script is run only once for all related rules.

Neverfail Channel Performance Data Collection Rules

The Neverfail Channel Performance Data rules target *Neverfail.Heartbeat.NFChannel* and use a script to retrieve the information.

Table 12: Neverfail Channel Performance Data Collection Rules

Name	Description
Neverfail.Heartbeat.CollectChannel.Q.ReceiveQOldestEntry	Collects the Channel's Receive Queue-oldest entry performance data.
Neverfail.Heartbeat.CollectChannel.Q.ReceiveQSizeBytes	Collects the Receive Queue Size in bytes
Neverfail.Heartbeat.CollectChannel.Q.SendQOldestEntry	Collects the Send Queue oldest entry performance counter.

<i>Name</i>	<i>Description</i>
Neverfail.Heartbeat.CollectChannel.Q.SendQSizeBytes	Collects the Send Queue Size in Bytes performance counter.
Neverfail.Heartbeat.CollectChannel.WAX.AvgCompressionFactor	Collects the WAX Average Compression Factor
Neverfail.Heartbeat.CollectChannel.WAX.AvgThruPut	Collects the WAX Average Through Put
Neverfail.Heartbeat.CollectChannel.WAX.CurrentCompressionFactor	Collects the WAX Current Compression Factor
Neverfail.Heartbeat.CollectChannel.WAX.CurrentThruPut	Collects the WAX Current Through Put
Neverfail.Heartbeat.CollectChannel.WAX.CurVolDataProcessed	Collects the WAX Current Volume Data Processed
Neverfail.Heartbeat.CollectChannel.WAX.VolDataProcessed	Collects the WAX Average Volume Data Processed

Physical Link Performance Data Collection Rules

The Physical Link Performance Data Collection rules provides information about the throughput of the physical link and uses a script to retrieve the information.

Table 13: Physical Link Performance Data Collection Rules

<i>Name</i>	<i>Description</i>
Neverfail.Heartbeat.CollectLink.BytesReceived	Collects the Bytes Received on the physical link.
Neverfail.Heartbeat.CollectLink.BytesSent	Collects the Bytes Sent on the physical link.

Heartbeat Server Performance Data Collection Rules

The Heartbeat Server Performance Data Rules provide information about the physical Heartbeat server.

Table 14: Heartbeat Server Performance Data Collection Rules

<i>Name</i>	<i>Description</i>
Neverfail.Heartbeat.CollectServer.CurrentThroughPut	Collects Current Through Put performance data
Neverfail.Heartbeat.CollectServer.MaxThroughPut	Collects Max Through Put performance data
Neverfail.Heartbeat.CollectServer.LogicalDiskC.AvgDiskQLen	Collects the AvgDiskQLen for the Logical Disk windows performance counter.
Neverfail.Heartbeat.CollectServer.LogicalDiskC.AvgDiskSecRead	Collects the AvgDiskSecRead for the Logical Disk windows performance counter.
Neverfail.Heartbeat.CollectServer.LogicalDiskC.AvgDiskSecTransfer	Collects the AvgDiskSecTransfer for the Logical Disk Windows performance counter.
Neverfail.Heartbeat.CollectServer.LogicalDiskC.AvgDiskSecWrite	Collects the AvgDiskSecWrite for the Logical Disk Windows performance counter.
Neverfail.Heartbeat.CollectServer.LogicalDiskC.CurrentDiskQueueLength	Collects the CurrentDiskQueueLength for the Logical Disk Windows performance counter.
Neverfail.Heartbeat.CollectServer.LogicalDiskC.DiskBytesSec	Collects the DiskBytesSec for the Logical Disk Windows performance counter.
Neverfail.Heartbeat.CollectServer.LogicalDiskC.DiskReadsSec	Collects the DiskReadsSec for the Logical Disk Windows performance counter.

<i>Name</i>	<i>Description</i>
Neverfail.Heartbeat.CollectServer.LogicalDiskC.DiskWritesSec	Collects the DiskWritesSec for the Logical Disk Windows performance counter.
Neverfail.Heartbeat.CollectServer.LogicalDiskC.FreeMegabytes	Collects the FreeMegabytes for the Logical Disk Windows performance counter.
Neverfail.Heartbeat.CollectServer.LogicalDiskC.PercentFreeSpace	Collects the %FreeSpace for the Logical Disk Windows performance counter.
Neverfail.Heartbeat.CollectServer.Processor_Total.PercentProcessorTime	Collects the %ProcessorTime for the Processor Windows performance counter.
Neverfail.Heartbeat.CollectServer.RecoveryPointMS	Collects the Recovery Point M/s performance counter from Heartbeat.

Event Collection Rules

The administrator must configure the frequency at which the rules run based upon the configuration and environment. Administrators should balance the consumption of system resources against the need for immediate collection of events. If the configuration and environment allows, Neverfail recommends that Event Collection Rules are configured to run every 5 minutes.

Table 15: Event Collection Rules

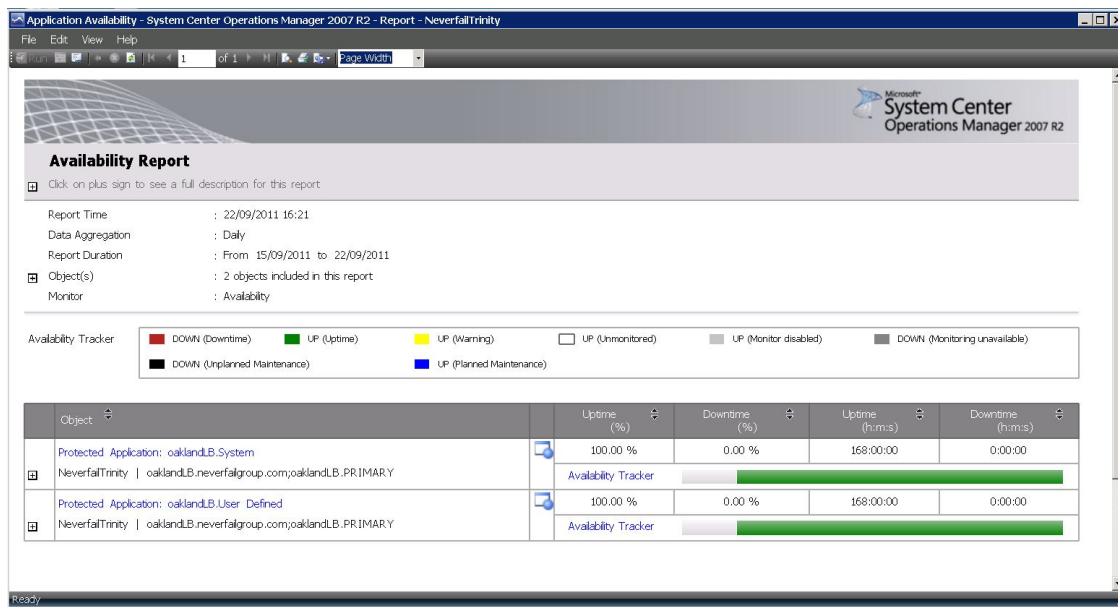
<i>Name</i>	<i>Target</i>	<i>Description</i>
Neverfail.Heartbeat.ServerEvents.Collection	Neverfail.Heartbeat.Server	A script-based rule that retrieves all events associated with the Neverfail Server object.
Neverfail.Heartbeat.NFChannelEvents.Collection	Neverfail.Heartbeat.NFChannel	A script-based rule that retrieves all events associated with the Neverfail Channel objects.
Neverfail.Heartbeat.PAEvents.Collection	Neverfail.Heartbeat.ProtectedApplications	A script-based rule that retrieves all events associated with the Protected Applications
Neverfail.Heartbeat.ServerShuttingDown.Collection	Neverfail.Heartbeat.Server	A rule used to check for a Heartbeat Shutting Down event and generates a corresponding alert.
Neverfail.Heartbeat.ImpendingLicenseExpiry.Collection	Neverfail.Heartbeat.Server	A rule used to check for an Impending License Expiry event and generates a corresponding alert.
Neverfail.Heartbeat.FailoverEvent.Collection	Neverfail.Heartbeat.Server	A rule used to check for Failover events and generates a corresponding alert.
Neverfail.Heartbeat.AutoSwitchoverEvent.Collection	Neverfail.Heartbeat.Server	A rule used to check for Auto-switchovers and generates a corresponding alert.

Linked Reports

The following linked reports are provided.

Table 16: Linked Reports

Name	Target	Description
Neverfail Channel Performance Report	Neverfail.Heartbeat.NFChannel	Reports Channel Performance over a configurable period of time.
WAN Access Performance Report	Neverfail.Heartbeat.NFChannel	Reports WANSmart Performance over a configurable period of time
Protected Application Availability Report	Neverfail.Heartbeat.ProtectedApplication	Reports availability of Protected Applications over a configurable period of Time.
Heartbeat Server Availability Report	Neverfail.Heartbeat.Server	Reports availability of Neverfail Heartbeat over a configurable period of time.

**Figure 4: Example - Application Availability Report**

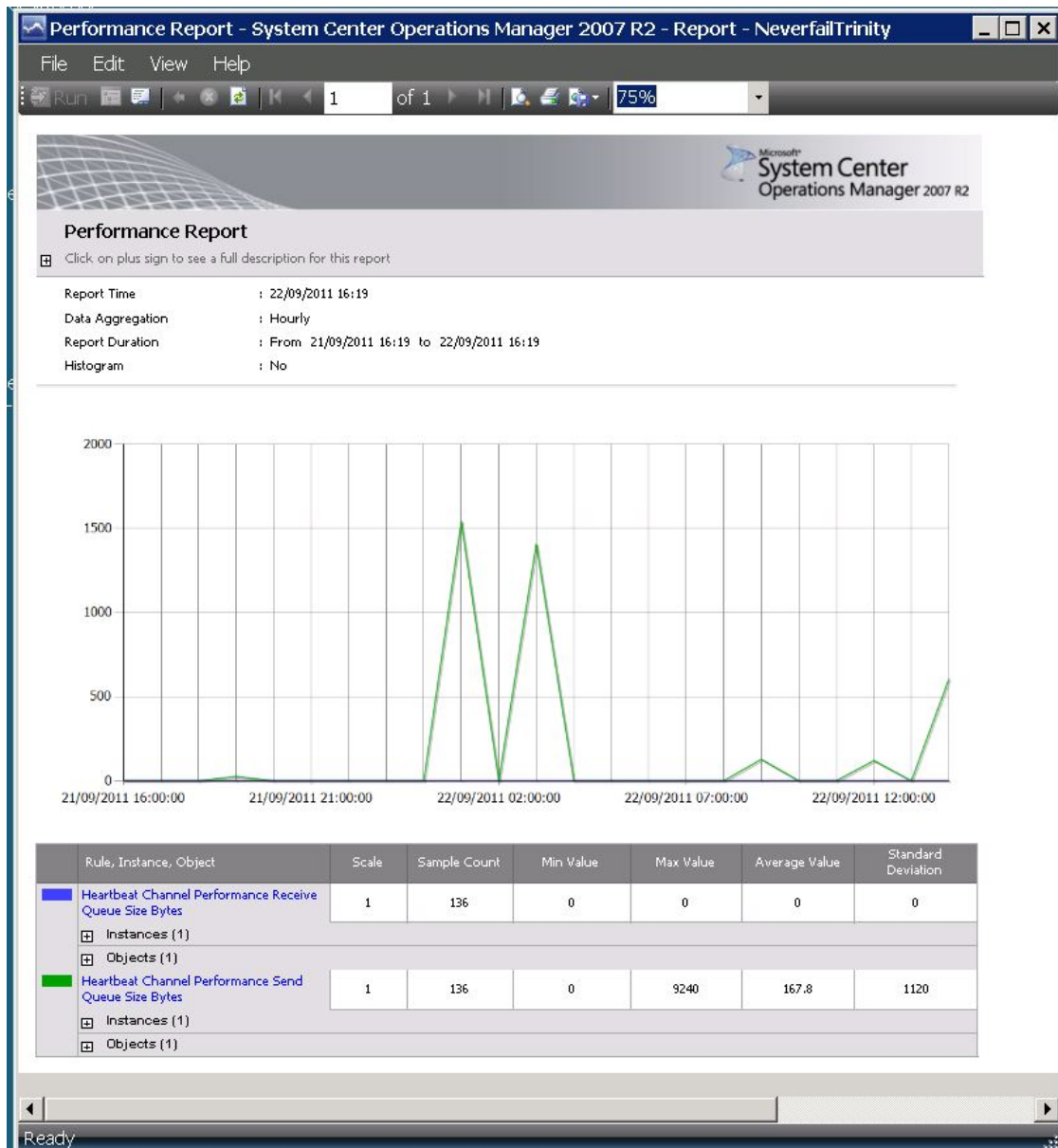


Figure 5: Example - Performance Report

Neverfail Recovery

The Neverfail Recovery task is used to perform an action on the Neverfail server such as restart a service.

Table 17: Neverfail Recovery

Name	Target	Description
Neverfail.Heartbeat.WebServicesRecovery	Neverfail.Heartbeat.Computer	Restarts the Neverfail WebServices service. This recovery is not run automatically on failure of the monitor, but must be run manually by the user.

Troubleshooting

Use of Management IPs (Backdoor IP addresses) or Alternate IP addresses on a passive server may result in erroneous or duplicate Alerts being raised and may cause problems in communications between the SCOM Operations Console and the SCOM Agent.

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.

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 Server Queue

The staging area of the active server used to store intercepted data changes before being transported across the Channel to the passive server.

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.

Alert

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

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 1st 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.

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 Replicator

A functionally limited version of the Neverfail Heartbeat product.

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.

Passive Server Queue

The staging area on the passive server used to store changes received from the active server before they are applied to the disk/registry on the passive server.

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 (Public) Network

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

Principal NIC

The network card which hosts the Principal IP address.

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 1st 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 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.

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.

Subnet

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

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 1st passive server or from the 1st passive server to the 2nd 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.

