

Installation Guide

VMware vCenter Server Heartbeat 6.3 Update 1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-000561-03

vmware[®]

You can find the most up-to-date technical documentation on the VMware Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book 5

Getting Started

- 1 Introduction 9
 - Overview 9
 - vCenter Server Heartbeat Concepts 9
 - Architecture 9
 - Protection Levels 11
 - Communications 14
 - vCenter Server Heartbeat Switchover and Failover Processes 15

Installation

- 2 vCenter Server Heartbeat Implementation 21
 - Overview 21
 - Environmental Prerequisites 21
 - Common Requirements 22
 - Server Architecture Options 23
 - Virtual to Virtual (V2V) 23
 - Physical to Virtual (P2V) 23
 - Physical to Physical (P2P) 24
 - Cloning Technology Options 24
 - Supported Pre-Clone Technologies 24
 - Supported Install Clone Technologies 25
 - vCenter Server with SQL Server on the Same Host 26
 - vCenter Server with SQL Server on a Separate Host 26
 - vCenter Server Only 26
 - Network Options 26
 - LAN 26
 - WAN 28
 - Antivirus Recommendations 29
 - Deployment Options Summary 29
 - Installation Options Checklist 30
- 3 Installing vCenter Server Heartbeat on Identical Nodes 31
 - Overview 31
 - Installation Process 31
 - Primary Server 32
 - Secondary Server 38
 - vCenter Server Heartbeat Console 44
 - Navigate vCenter Server Heartbeat Console 44
 - Add a vCenter Server Group 44
 - Add a New Connection 45
 - Post Installation Configuration 45

Configuring VirtualCenter Plug-in with the Correct Credentials	45
When Deployed in a WAN Environment	46
vCenter Server 2.5	46
Installing the View Composer Plug-in	47
Installation of Client Tools	47
4 Installing vCenter Server Heartbeat on Non-Identical Nodes	49
Overview	49
Installation Process	49
Installing vCenter Server Heartbeat on Non-Identical Nodes	50
Primary Server	50
Secondary Server	54
vCenter Server Heartbeat Console	58
Navigate vCenter Server Heartbeat Console	58
Add a vCenter Server Group	59
Add a New Connection	59
Post Installation Configuration	60
Configuring VirtualCenter Plug-in with the Correct Credentials	60
Configuring SQL Server Plug-in to run with the Correct Credentials	61
Installing the View Composer Plug-in	61
Installation of Client Tools	61
Appendix – Setup Error Messages	63
Glossary	65

About This Book

The *Installation Guide* provides information about installing VMware vCenter Server Heartbeat, including implementation in a Local Area Network (LAN) or Wide Area Network (WAN) and using identical nodes or non-identical nodes. To help you protect your VMware vCenter Server, the book provides an overview of protection offered by vCenter Server Heartbeat and the actions that vCenter Server Heartbeat can take in the event of a network, hardware, or application failure.

Intended Audience

This guide assumes the reader has working knowledge of networks including the configuration of TCP/IP protocols and domain administration on the Windows™ 2003 and 2008 platforms, notably in Active Directory and DNS.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation go to <http://www.vmware.com/support/pubs>.

Overview of Content

This guide is designed to give guidance on the installation vCenter Server 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 vCenter Server Heartbeat concepts including the Switchover and Failover processes.
- Chapter 2 — *vCenter Server Heartbeat Implementation* discusses environmental prerequisites and common requirements for installation, options for server architecture, cloning technology, application components, and network configurations. It also gives guidance on antivirus solutions, and provides a convenient summary and checklist to follow as you perform the installation.
- Chapter 3 — *Installing vCenter Server Heartbeat on Identical Nodes* describes the installation process, guides you through installation on the Primary and Secondary servers using identical nodes, and through post-installation configuration.
- Chapter 4 — *Installing vCenter Server Heartbeat on Non-Identical Nodes* describes the installation process, guides you through installation on the Primary and Secondary servers using non-identical nodes, 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.

Document Feedback

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

Abbreviations Used in Figures

The figures in this book use the abbreviations listed in [Table 1](#).

Table 1. Abbreviations

Abbreviation	Description
Channel	VMware 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 www.vmware.com/support/pubs.

Online and Telephone Support

Go to www.vmware.com/support to use online support to submit technical support requests, view your product and contract information, and register your products.

Go to www.vmware.com/support/phone_support.html to find out how to use telephone support for the fastest response on priority 1 issues (applies to customers with appropriate support contracts).

Support Offerings

Go to www.vmware.com/support/services to find out how VMware support offerings can help meet your business needs.

VMware Professional Services

Go to www.vmware.com/services to access information about education classes, certification programs, and consulting services. VMware Education 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 onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment.

Getting Started

Introduction

This chapter includes the following topics:

- [“vCenter Server Heartbeat Concepts”](#) on page 9
- [“vCenter Server Heartbeat Switchover and Failover Processes”](#) on page 15

Overview

vCenter Server Heartbeat is a Windows based service specifically designed to provide high availability protection for vCenter Server configurations without requiring any specialized hardware.

vCenter Server Heartbeat Concepts

Architecture

vCenter Server Heartbeat software is installed on a Primary (production) server and a Secondary (ready-standby) server. These names refer to the physical hardware (identity) of the servers.

Depending on the network environment, vCenter Server Heartbeat can be deployed in a Local Area Network (LAN) or Wide Area Network (WAN). Additionally, vCenter Server Heartbeat allows for installation using identical nodes (LAN and WAN) or non-identical nodes (LAN only). These features provide flexibility necessary to address most network environments.

Depending on the network environment and architecture selected, vCenter Server Heartbeat can be configured where the Primary and Secondary server have the same domain name and Principal (Public) IP address (identical nodes) or where the Primary and Secondary servers have different domain names but share the Principal (Public) IP address (non-identical nodes). In either architecture, the Secondary server will have the same file and data structure and can run all of the same applications and services as the Primary server. The vCenter Server Heartbeat software is symmetrical in almost all respects, and either the Primary server or the Secondary server can take the active role and provide protected applications to the user.

When deployed, vCenter Server Heartbeat uses two servers with either identical Principal (Public) IP addresses for identical nodes or a shared Principal (Public) IP address for non-identical nodes. One of the servers performs the role of the active server that is visible on the Public network while the other is the passive server that is hidden from the Public network but remains as a ready-standby server. Only one server can display the Principal (Public) IP address and be visible on the Public network at any given time.

Identical Nodes Configuration

When configured for identical nodes, vCenter Server Heartbeat uses two servers with the same domain name, Principal (Public) network IP address, file and data structure, applications, and services to ensure that vCenter Server is running and available. With a packet filter installed on both servers Principal (Public) NICs, vCenter Server Heartbeat applies the packet filter to the Principal (Public) NIC on the passive server thereby blocking communications and hiding the passive server from the Public network. When a switchover occurs, the packet

filter on the currently active server is enabled preventing communications on the Public network while the packet filter on the currently passive server is disabled thereby allowing the two servers to switch roles. From this point on, the previously passive server is now active and servicing the clients. The previously active server is now passive and hidden from the Public network.

In the event of a failover, the previously active server is deemed to have failed and no further actions are necessary. The packet filter on the previously passive server is disabled allowing the server to become visible on the Public network and service clients as the new active server.

Advantages of Identical Nodes Configuration

Identical node configuration provides for a simplified installation and supports Virtual to Virtual, Virtual to Physical, and Physical to Physical architectures. Additionally, identical node configuration supports use of both the Pre-clone and Install clone, installation techniques. When configured with identical nodes, vCenter Server Heartbeat provides two identical servers that can function as the active server servicing clients. Additionally, with identical nodes, organizations can deploy vCenter Server Heartbeat in WAN environments thereby extending protection over wide geographic distances.

Non-Identical Nodes Configuration

Non-identical node configuration provides enhanced management capabilities to the vCenter Heartbeat Server cluster by providing continuous access to the passive server simultaneously while the active server continues to service clients. When configured with non-identical nodes, vCenter Server Heartbeat uses unique server names for each server and enhanced IP address management capabilities to accommodate Microsoft (updatable) DNS servers and Locked Down mode or non-Microsoft DNS servers while providing the same levels of protection as when configured with identical nodes.

The Secondary server has a different Fully Qualified Domain Name (FQDN) than the Primary server but 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. With vCenter Server Heartbeat software symmetrical in almost all respects, either the Primary server or the Secondary server can assume the active role and provide protected applications to the user.

Additionally, this configuration allows the passive server to be easily accessed for maintenance purposes, updating anti-virus definition files, receiving operating system hot-fixes, updates and patches from third-party management software, and allows use of third-party monitoring tools.

Switchover/Failover Without Updating DNS Servers

Select the *Non-Identical* option when you want to deploy vCenter Server Heartbeat with non-identical nodes in an environment that does not permit updating DNS (a non-updatable Microsoft DNS server (or Locked Down Mode) or a non-Microsoft DNS server). This configuration requires vCenter Server vCenter Server 4.0 Update 1 or later, if SQL Server is deployed, it must be remote, and since DNS will not be updated automatically, you must prepopulate the DNS server with entries for the new management names and IP addresses of the Primary and Secondary servers. vCenter Server Heartbeat uses permanently assigned unique Management IP addresses on both the Primary and Secondary servers. Adjacent IP addresses should be reserved and used for the Principal (Public) IP address and the Management IP addresses for the Primary and Secondary Servers when installing vCenter Server Heartbeat on non-identical nodes on servers running Windows 2008. When vCenter Server Heartbeat is started, the shared Principal (Public) IP address is provided to the active server. When a switchover occurs, the shared Principal (Public) IP address is removed from the previously active server (making it passive) and provided to the previously passive server (making it active) allowing the servers to switch roles and the new active server to begin servicing clients.

Microsoft DNS Server Updated During Switchover/Failover

Select the *Non-identical (Updates MS DNS)* option when you want to deploy vCenter Server Heartbeat with non-identical nodes in an environment where vCenter Server 4.0 Update 1 or later is installed, if SQL Server is deployed it must be remote, a Microsoft DNS server that permits updates is used, and you want to take advantage of the enhanced passive server management capabilities. vCenter Server Heartbeat interacts with the DNS server and following a switchover, will ensure that servers are correctly identified on the network by updating DNS information. vCenter Server Heartbeat uses unique server names and Management IP

addresses for the Primary and Secondary servers separate from the shared Public (Principal) IP address. Clients connect to vCenter Server using a unique virtual service name configured in vCenter Server Heartbeat that resolves to the Public (Principal) IP address. When started, vCenter Server Heartbeat provides the passive server its unique Management IP address and provides the active server with the shared Principal (Public) IP address.

When a switchover occurs, vCenter Server Heartbeat removes the shared Principal (Public) IP address from the currently active server and replaces it with its unique Management IP address. On the currently passive server, vCenter Server Heartbeat removes the Management IP address and replaces it with the shared Principal (Public) IP address thereby allowing the servers to switch roles.

Advantages of Non-Identical Nodes Configuration

Deployment of non-identical nodes allows for easy access to the passive (hidden/ready standby) server at any time regardless of which server is active and servicing clients. Additionally, this configuration allows the passive server to be easily accessed for maintenance purposes, updating anti-virus 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

vCenter Server Heartbeat provides the following protection levels:

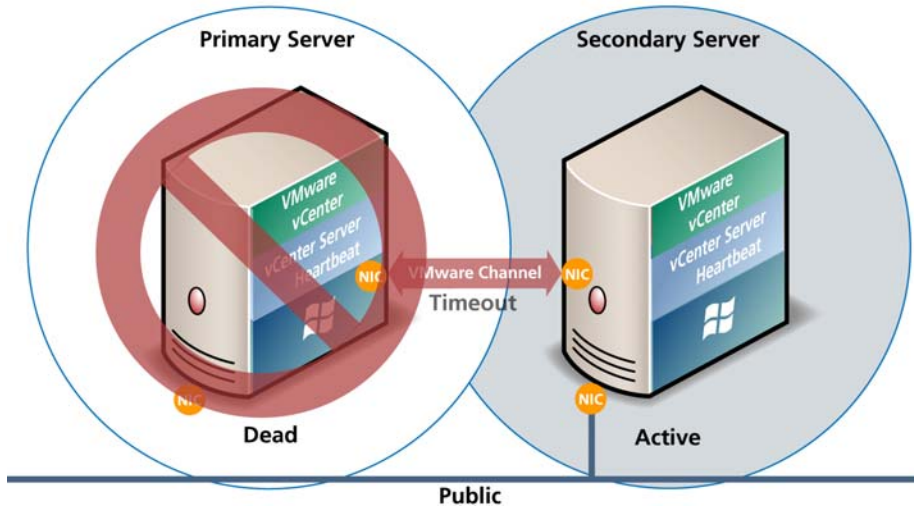
- **Server Protection** – vCenter Server Heartbeat provides continuous availability to end users through a hardware failure scenario or operating system crash. Additionally, vCenter Server Heartbeat protects the network identity of the production server, ensuring users are provided with a replica server on the failure of the production server.
- **Network Protection** – vCenter Server Heartbeat proactively monitors the network by polling up to three nodes to ensure that the active server is visible on the network.
- **Application Protection** – vCenter Server Heartbeat maintains the application environment ensuring that applications and services stay alive on the network.
- **Performance Protection** – vCenter Server Heartbeat proactively 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** – vCenter Server Heartbeat intercepts all data written by users and applications, and maintains a copy of this data on the passive server that can be used in the event of a failure.

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

Server Protection

vCenter Server Heartbeat provides continuous availability to end users through a hardware failure scenario or operating system crash. Additionally, vCenter Server Heartbeat protects the network identity of the production server, ensuring users are provided with a replica server including server name (single identity only) and IP address on the failure of the production server.

Two instances of vCenter Server Heartbeat regularly send “I’m alive” messages and message acknowledgments to one another over a network connection referred to as the VMware Channel to detect interruptions in responsiveness. If the passive server detects that this monitoring process (referred to as the heartbeat) has failed, it initiates a failover as illustrated in [Figure 1-1](#).

Figure 1-1. Failover

A failover is similar to a switchover but is used in more urgent situations, such as when the passive server detects that the active server is no longer responding. This can occur when the active server hardware fails, loses its network connections, or otherwise becomes unavailable. Rather than the active server gracefully closing, the passive server determines that the active server has failed and requires no further operations. In a failover, the passive server immediately assumes the active server role. The failover process is discussed later in this guide.

Network Protection

vCenter Server Heartbeat proactively monitors the network by polling up to three nodes to ensure that the active server is visible on the network. vCenter Server Heartbeat polls defined nodes around the network, including the default gateway, the primary DNS server, and the global catalog server at regular intervals. If all three nodes fail to respond, for example, in the case of a network card failure or a local switch failure, vCenter Server Heartbeat can initiate a switchover, allowing the Secondary server to assume an identical network identity as the Primary server.

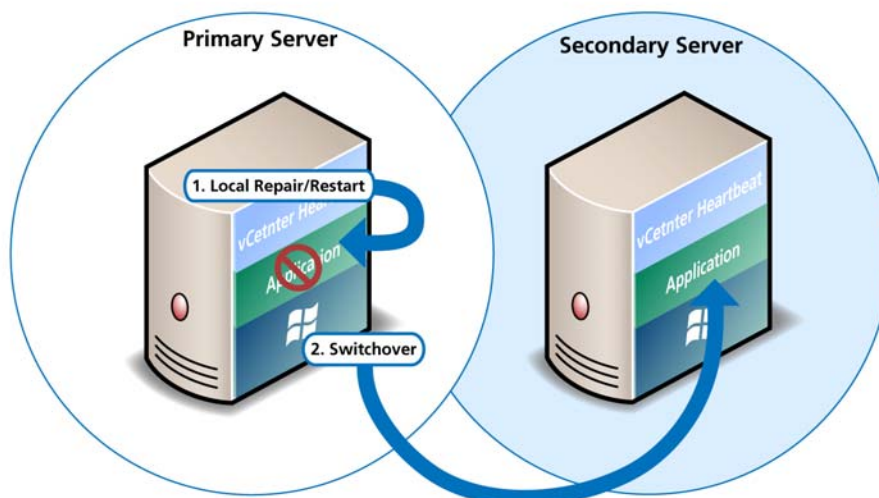
Application Protection

vCenter Server Heartbeat running on the active server locally monitors the applications and services it has been configured to protect (through the use of plug-ins) to verify that protected applications are operational and not in an unresponsive or stopped state. This level of monitoring is fundamental in ensuring that applications remain available to users.

If a protected application fails, vCenter Server Heartbeat first tries to restart the application on the active server (1) in [Figure 1-2](#).

If the application does not successfully restart, vCenter Server Heartbeat initiates a switchover (2) in [Figure 1-2](#). Refer to “[vCenter Server Heartbeat Switchover and Failover Processes](#)” on page 15 for further information about the switchover process.

Figure 1-2. Switchover



A switchover gracefully closes any protected applications that are running on the active server and restarts them on the passive server, including the application or service that caused the failure. In the example where the Primary server is active and the Secondary server is passive, the Primary server is demoted to a passive role and is hidden from the network when the Secondary server is promoted to an active role and is made visible to the network. The mechanics of switchovers are discussed in more detail later in this guide.

Performance Protection

Ensuring that your protected applications are operational and providing service at a level of performance adequate for users to remain productive is important. The vCenter Server Heartbeat plug-in provides these monitoring and pre-emptive repair capabilities.

vCenter Server Heartbeat proactively monitors system performance attributes to ensure that the system administrator is notified of problems and can take pre-emptive action to prevent an outage.

In addition to monitoring application services, vCenter Server Heartbeat can monitor specific application attributes to ensure that they remain within normal operating ranges. Similar to application monitoring, various rules can be configured to trigger specific corrective actions whenever these attributes fall outside of their respective ranges.

vCenter Server Heartbeat provides the same level of flexibility to define and perform multiple corrective actions in the event of problems on a service by service or even attribute by attribute basis.

Data Protection

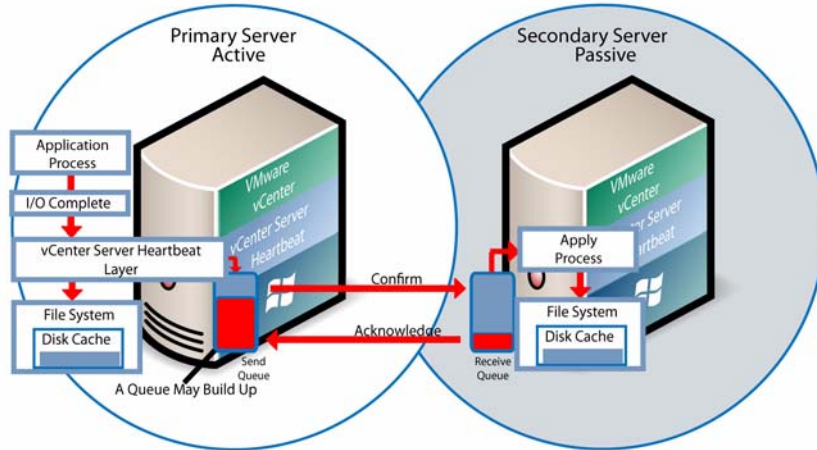
You can configure vCenter Server Heartbeat to protect the application environment. All data files that users or the applications require in the application environment are made available should a failure occur. After installation, vCenter Server Heartbeat configures itself to protect files, folders, and registry settings for vCenter Server on the active server by mirroring them in real time to the passive server. If a failover occurs, all files protected on the failed server are available to users after the failover, hosted on the Secondary server.

vCenter Server Heartbeat intercepts all file system I/O operations on the active server. If the intercepted write and update operations are within the protected set, these are placed in a queue on the active server referred to as the active server's send queue, pending transmission to the passive server. Each request is numbered to maintain its order in the queue.

With the request in the active server's send queue, vCenter Server Heartbeat allows the disk I/O to continue with the requested disk operation.

If the channel is connected, the active server's send queue is transferred to the passive server, which places all the requests in the passive server's receive queue. The passive server confirms the changes were logged by sending the active server an acknowledgement. The active server clears the data from its queue.

Figure 1-3. Apply Process



The apply process running on the passive server’s receive queue applies all updates in strict sequence, duplicating an identical set of file operations on the passive server as illustrated in [Figure 1-3](#).

Communications

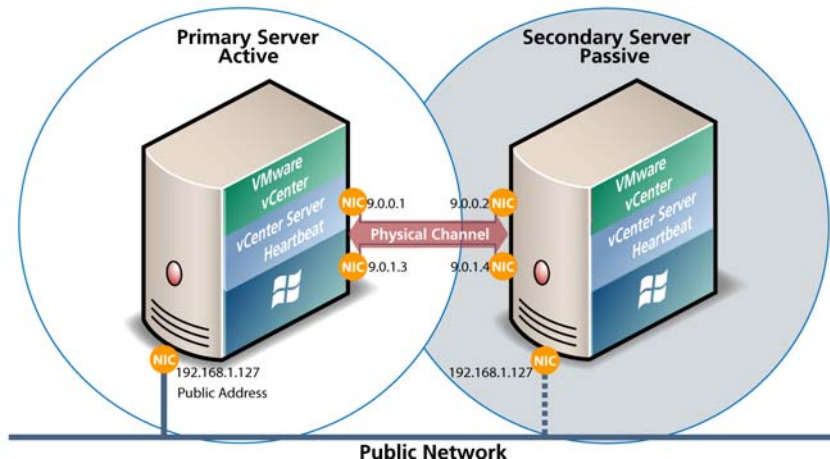
The VMware Channel is a crucial component of the setup and can be configured in a number of ways.

Both the Primary and Secondary servers must have two or more network interface connections (NICs).

The Principal (Public) network requires one NIC. The VMware Channel uses a separate NIC for the private connection between the servers used for control and data transfer between the pair of servers.

A second pair of NICs can be used to provide a degree of redundancy for the VMware Channel. In this configuration, the VMware Channel has a dual channel if more than one dedicated NIC is provided for the VMware Channel on each server. To provide added resilience, the communications for the second channel must be completely independent from the first channel. They must not share any switches, virtual switches, routers or the same WAN connection.

Figure 1-4. Communication Between Primary and Secondary Servers



The IP address a client uses to connect to the active server (the Principal (Public) IP address) 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.

NOTE Obtain the IP address: type **ipconfig** at the prompt in a DOS shell. For additional information about the IP configuration, add the switch **/All** to the **ipconfig** command.

The Principal (Public) NICs on the passive server are configured to use the same IP address as that of the active server but are prevented from communicating with the live network through an IP packet filtering system installed with vCenter Server Heartbeat. This packet filter prevents traffic using the Principal (Public) address from being committed to the wire. It also prevents NetBIOS traffic utilizing other IP addresses on the NIC from being sent to prevent NetBIOS name resolution conflicts.

The NICs on the active and passive servers used for the VMware Channel are configured so that their IP addresses are outside of the subnet range of the Principal (Public) network. These addresses are referred to as VMware Channel addresses.

During installation, setup will switch off NetBIOS for the VMware Channel(s) on the active and passive servers as this connection remains live and both the passive and active machines have the same NetBIOS name. Following restore and after the vCenter Server Heartbeat installation completes (runtime), NetBIOS is disabled across the channel(s). This occurs during installation to prevent a name conflict, which occurs when both servers have the same name.

The NICs that support connectivity across the VMware Channel can be standard 100BaseT Ethernet cards providing a throughput of 100 Mbits per second across standard Cat-5 cabling. In its most basic form, a dedicated channel requires no hubs or routers, but the direct connection requires crossover cabling.

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

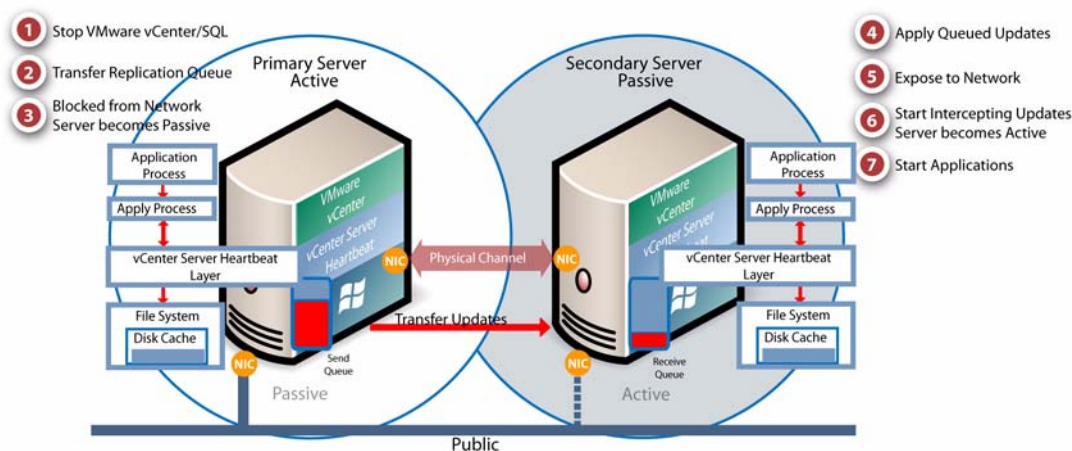
vCenter Server Heartbeat Switchover and Failover Processes

vCenter Server 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 **vCenter Server Heartbeat Console 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.

Figure 1-5. Switchover



A managed switchover performs the following steps:

- 1 Stop the protected applications on the active server. After the protected applications stop, no more disk updates are generated.
- 2 Send all updates that are still queued on the active server to the passive server. After this step, all updates are available on the passive server.

- 3 Re-designate the Secondary server as the new active server. After this step, vCenter Server Heartbeat:
 - Hides the previously active server from the network.
 - Makes the newly active server visible on the network. The newly active server has the same identity as the previously active server, and begins to intercept and queue disk I/O operations for the newly passive server.
- 4 vCenter Server Heartbeat causes the newly passive server to begin accepting updates from the active server.
- 5 vCenter Server Heartbeat starts the same protected applications on the new active server. The protected applications become accessible to users. The managed switchover is complete

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.

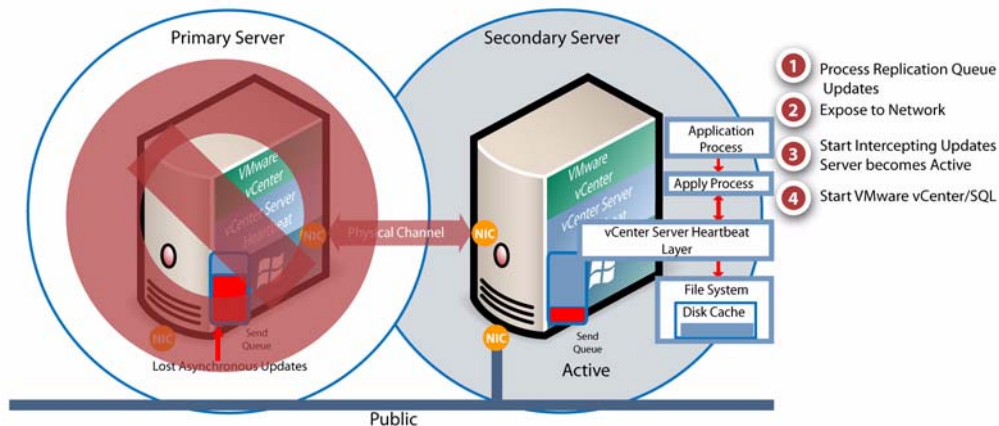
Like managed switchover, auto-switchover changes the server roles but then stops vCenter Server Heartbeat on the previously active server to allow the administrator to investigate the cause of the auto-switchover and verify the integrity of the data.

After the cause for the auto-switchover is determined and corrected, the administrator can use vCenter Server Heartbeat Console to return the server roles to their original state.

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.

Figure 1-6. Failover



During the automatic failover, the passive server performs the following steps:

- 1 Apply any intercepted updates currently in the passive server's receive queue as identified by the log of update records that are saved on the passive server but not yet applied to the replicated files.

The amount of data in the passive server's receive queue affects the time required to complete the failover process. If the passive server's receive queue is long, the system must wait for all updates to the passive server to complete before the rest of the process can take place. An update record can be applied only if all earlier update records are applied, and the completion status for the update is in the passive server's receive queue. When no more update records can be applied, any update records that cannot be applied are discarded.

- 2 Switch mode of operation from passive to active.

This enables the public identity of the server. The active and passive servers both use the same system name and same Principal (Public) IP address. This Principal (Public) IP address can be enabled only on one system at anytime. When the public identity is enabled, any clients previously connected to the server before the automatic failover are able to reconnect.

- 3 Start intercepting updates to protected data. Any updates to the protected data are saved in the send queue on the local server.
- 4 Start all protected applications. The applications use the replicated application data to recover, and then accept re-connections from any clients. Any updates that the applications make to the protected data are intercepted and logged.

At this point, the originally active server is offline and the originally passive server is filling the active role and is running the protected applications. Any updates that completed before the failover are retained. Application clients can reconnect to the application and continue running as before.

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.

Automatic Switchover and Failover in a WAN Environment

Automatic switchover and failover in a WAN environment differ from a automatic switchover and failover in a LAN environment due to the nature of the WAN connection. In a WAN environment, automatic switchover and failover are disabled by default in the event that the WAN connection is lost.

Should a condition arise that would normally trigger an automatic switchover or failover, the administrator will receive vCenter Server Heartbeat alerts. The administrator must manually click the **Make Active** button on the **Server: Summary** page of the vCenter Server Heartbeat Console to allow the roles of the servers to switch over the WAN.

To enable Automatic Switchover in a WAN

- 1 In the vCenter Server Heartbeat Console, click the **Network** tab to display the **Network Monitoring** page.
- 2 Click **Configure Auto-switchover**.
- 3 Select the **Auto-switchover if client network connectivity lost for** check box.
- 4 Configure the number of pings to wait before performing the auto-switchover.
- 5 Click **OK**.

Recovery from a Failover

Assuming that the Primary server was active and the Secondary server was passive before the failover, after the failover the Secondary server is active and the Primary server is passive.

NOTE When failover conditions such as a power failure cause both active and passive servers to fail, the condition may result that causes both servers to restart in passive mode. In this situation, manual intervention is required.

After rectifying the problem that initiated the failover, it is a simple process to reinstate the Primary server as the active server and the Secondary server as the passive server.

When vCenter Server Heartbeat starts on the failed Primary server, it detects that it did not stop cleanly the previous time. It disables the public identity by deploying the IP packet filter and halts vCenter Server Heartbeat so that the issues that caused the failure can be resolved.

To restore the previously failed server to the active role

- 1 Correct the conditions that caused the failover.
- 2 Verify the integrity of the disk data on the failed server.
- 3 Restart the failed, now passive, server after all issues are resolved.
- 4 Start vCenter Server Heartbeat on the passive server.

At this point, the instances of vCenter Server Heartbeat running on the servers connect and begin to re-synchronize the data on the Primary server.

- 5 Wait until vCenter Server Heartbeat is fully synchronized.

When the re-synchronization is complete, you can continue operating with this configuration (for example, the Secondary server is the active server and the Primary server is the passive server), or initiate a managed switchover.

- 6 Optionally, perform a managed switchover to return the Primary and Secondary servers to the same roles they had before the failover.

Installation

vCenter Server Heartbeat Implementation

2

This chapter includes the following topics:

- [“Overview”](#) on page 21
- [“Environmental Prerequisites”](#) on page 21
- [“Common Requirements”](#) on page 22
- [“Server Architecture Options”](#) on page 23
- [“Cloning Technology Options”](#) on page 24
- [“Application Component Options”](#) on page 25
- [“Network Options”](#) on page 26
- [“Antivirus Recommendations”](#) on page 29
- [“Deployment Options Summary”](#) on page 29

Overview

vCenter Server Heartbeat is a versatile solution that provides complete protection of vCenter Server and SQL Server. It can be deployed in a LAN for high availability or across a WAN to provide disaster recovery. vCenter Server Heartbeat can protect vCenter Server and SQL Server installed on the same server, or protect vCenter Server and SQL Server on separate servers. This flexibility enables vCenter Server Heartbeat to protect vCenter Server when using remote databases other than SQL Server.

This chapter discusses the deployment options and prerequisites to successfully implement vCenter Server Heartbeat and provides a step-by-step process to assist in selecting options required for installation. The deployment scenario table provides a visual reference to configuration options supported by vCenter Server Heartbeat.

During the installation process, vCenter Server 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 [Appendix – Setup Error Messages](#) in this guide for a list of the checks and an explanation of the message. You must resolve critical stops before you can proceed with setup.

Prior to installing vCenter Server Heartbeat, select the deployment options you intend to use. The installation process prompts you to select options throughout the procedure to create the configuration you want.

Environmental Prerequisites

vCenter Server Heartbeat cannot protect a server configured with the following roles: domain controller, global catalog, or DNS.

NOTE Because vCenter Server Heartbeat only protects the vCenter Server and SQL Server applications, no other critical business applications should be installed on the server.

Common Requirements

The following requirements are in addition to those required for vCenter Server and SQL Server.

NOTE If you are intending to deploy vCenter Server Heartbeat with non-identical nodes, you must use vCenter Server 4.0 Update 1 or later.

- Supported vCenter Server Versions
 - VirtualCenter Server 2.5
 - VirtualCenter Server 2.5 Update 1
 - VirtualCenter Server 2.5 Update 2
 - VirtualCenter Server 2.5 Update 3
 - VirtualCenter Server 2.5 Update 4
 - VirtualCenter Server 2.5 Update 5
 - VirtualCenter Server 2.5 Update 6
 - vCenter Server 4.0
 - vCenter Server 4.0 Update 1
 - vCenter Server 4.0 Update 2
 - vCenter Server 4.1
 - vCenter Server 4.1 Update 1
- Operating Systems
 - Windows Server 2003 x86 Standard SP2
 - Windows Server 2003 x86 Enterprise SP1 and SP2
 - Windows Server 2003 x64 Standard/Enterprise SP2
 - Windows Server 2003 R2 x64 Standard/Enterprise SP2
 - Windows Server 2008 x86 Standard/Enterprise SP1 and SP2
 - Windows Server 2008 x64 Standard/Enterprise SP1 and SP2
 - Windows Server 2008 R2 Standard/Enterprise

NOTE vCenter Server Heartbeat supports protection of both standalone instances of vCenter Server 4.0.x and also when in Linked Mode groups.

- Prior to installing vCenter Server Heartbeat, verify that vCenter Guided Consolidation, vCenter Update Manager, and vCenter Converter are configured using Fully Qualified Domain Names (FQDN) rather than IP addresses.
- During the setup process, vCenter Server Heartbeat verifies that a minimum of 1GB RAM is available. To ensure proper operation, vCenter Server Heartbeat requires a minimum of 1GB RAM (2GB is recommended) in addition to any other memory requirement for the Operating System or vCenter Server.
- Verify that 2GB of disk space is available on the installation drive for vCenter Server Heartbeat.
- Obtain and use local administrator rights to perform vCenter Server Heartbeat installation.
- Apply the latest Microsoft security updates.
- All applications that will be protected by vCenter Server Heartbeat must be installed and configured on the Primary server prior to installing vCenter Server Heartbeat.

- Verify that both Primary and Secondary servers have identical system date, time, and time Zone settings. Once configured, do not change the time zone.
- Verify that the Principal (Public) network adapter is listed as the first network adapter in the Network Connections Bind Order. (**Network Connections > Advanced > Advanced Settings**).
- Verify that the Managed IP setting in the Virtual Infrastructure Client is the same IP address used for the vCenter Server Heartbeat Principal (Public) IP address.
- If installing in a Windows 2008 server environment, User Account Control (UAC) must be disabled during the installation process. After installation has completed, you may re-enable UAC.

Server Architecture Options

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

Virtual to Virtual (V2V)

V2V is the supported architecture if vCenter Server is 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.

NOTE The V2V architecture is supported when deploying vCenter Server Heartbeat with non-identical nodes.

The Secondary virtual machine must meet the minimum requirements.

- The specifications of the Secondary 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 V2V pair must be on a separate ESX host to guard against failure at the host level.
- Each virtual NIC must use a separate virtual switch.

Physical to Virtual (P2V)

P2V architecture is used when the environment requires a mix of physical and virtual machines, such as when vCenter Server is installed on a physical server in an environment where available hardware is limited. This architecture is appropriate if you must avoid adding more physical servers or if you plan to migrate to virtual technologies over a period of time. With P2V architecture, you can test vCenter Server running in a virtual environment or migrate from Physical to Virtual without any downtime. The Secondary virtual machine must meet the minimum requirements.

NOTE The P2V architecture is supported when deploying vCenter Server Heartbeat with non-identical nodes.

- The specifications of the Secondary virtual machine must match the Primary physical server as follows:
 - Similar CPU
 - Identical Memory
- The Secondary 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.

Physical to Physical (P2P)

P2P architecture is used in environments where both the Primary and Secondary servers are physical servers. Use of P2P limits installation options as it requires use of the Install Clone technique. This architecture requires attention to detail when preparing for installation as both hardware and software must meet specific prerequisites.

NOTE The P2P architecture is not supported when deploying vCenter Server Heartbeat with non-identical nodes.

Primary Server

The Primary server must meet the following requirements:

- Hardware as specified in “[Common Requirements](#)” on page 22.
- Software as specified in “[Common Requirements](#)” on page 22.

Secondary Server

The Secondary server operates as a near clone of the Primary server and must meet the following requirements.

Hardware

Hardware should be equivalent to the Primary server to ensure adequate performance when the server is in the active role:

- Similar CPU.
- Similar memory.
- Identical number of NICs to the Primary server.
- Drive letters must match the Primary server.
- Available disk space must be greater than or equal to the Primary server.
- Advanced Configuration and Power Interface (ACPI) compliance must match the Primary server. The vCenter Server Heartbeat Standard implementation process assumes identical ACPI compliance on both machines. If not, contact VMware Support at www.vmware.com/support for further information.

Software

Software on the Secondary server must meet the following requirements.

- OS version and Service Pack version must match the Primary server.
- OS must be installed to the same driver letter and directory as on the Primary server.
- Machine name must be different from the Primary server prior to installing vCenter Server Heartbeat.
- Set up in a workgroup prior to installing vCenter Server Heartbeat.
- System date, time, and time zone settings must be consistent with the Primary server.

Cloning Technology Options

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

Supported Pre-Clone Technologies

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

- VMware vCenter Converter for “[Physical to Virtual \(P2V\)](#)” on page 23.

- VMware vCenter virtual machine cloning for “[Virtual to Virtual \(V2V\)](#)” on page 23.

Supported Install Clone Technologies

Installation of vCenter Server Heartbeat provides support for NTBackup on Windows 2003 and Wbadmin on Windows Server 2008 for automated Install Cloning. This process is automated but requires meeting all prerequisites for the Secondary server specified in “[Physical to Physical \(P2P\)](#)” on page 24.

NOTE When using the Install Clone technique in a Physical to Virtual (P2V) architecture, VMware Tools must not be installed on the Secondary (cloned) server during the vCenter Server Heartbeat installation process. If VMware Tools are currently installed on the Secondary (cloned) server, you must fully uninstall VMware Tools prior to initiation of the Setup process. Once the installation of vCenter Server Heartbeat has completed, you may reinstall VMware Tools.

Application Component Options

vCenter Server Heartbeat can accommodate any of the supported vCenter Server configurations and protects the following components:

- VirtualCenter Server Version 2.5
 - VMware VirtualCenter Server
 - VMware Capacity Planner
 - VMware Converter Enterprise
 - VMware Update Manager
 - VMware License Server
 - VMware Virtual Infrastructure Client
- vCenter Server Version 4.0
 - VMware vCenter Server
 - VMware Guided Consolidation Service
 - VMware License Server
 - VMware ADAM
 - VMware vCenter Management Web Server
 - VMware vCenter Update Manager
 - VMware vCenter Converter
 - VMware vCenter Orchestrator
 - VMware vSphere Host Update Utility
 - VMware vSphere Client
- vCenter Server Version 4.1
 - VMware vCenter Server
 - VMware Guided Consolidation Service
 - VMware License Server
 - VMware ADAM
 - VMware vCenter Management Web Server
 - VMware vCenter Update Manager
 - VMware vCenter Converter
 - VMware vCenter Orchestrator
 - VMware vSphere Host Update Utility
 - VMware vSphere Client
- View Composer 1.1 and 2.0
 - VMware View Composer
 - VMware Universal File Access

- vCenter Converter Enterprise
- SQL Server Versions
 - Microsoft SQL Server 2005 SP1-SP3
 - Microsoft SQL Server 2008 including SP2

NOTE Ensure that all VMware components are bound to the Principal (Public) IP address on the Principal (Public) network adapter and that the Principal (Public) network adapter is listed first in the bind order of the **Network Connections > Advanced > Advanced Settings** page.

vCenter Server with SQL Server on the Same Host

To ensure adequate performance in 20+ host or 200+ virtual machine environments, VMware recommends that SQL Server and vCenter Server be installed on separate physical disk drives. VMDKs must be on separate datastores to avoid potential disk bottlenecks.

vCenter Server with SQL Server on a Separate Host

When installing vCenter Server Heartbeat in an environment where SQL Server is on a separate host from vCenter Server, repeat the installation process for the Primary and Secondary server specifically for the SQL Server.

To ensure proper failover, increase the default Heartbeat interval for the vCenter Server from 20 to 30 seconds.

NOTE If deploying with non-identical nodes, SQL Server must be installed remote to vCenter Server.

vCenter Server Only

The **vCenter Server Only** option requires a single iteration of the installation process because the database is not protected.

Network Options

Networking requirements are contingent upon how vCenter Server Heartbeat is deployed. To deploy as a High Availability (HA) solution, a LAN configuration is required. To deploy vCenter Server Heartbeat for Disaster Recovery (DR), a WAN configuration is required. Additionally, the server pair can be deployed with identical nodes or non-identical nodes. Each network configuration has specific configuration requirements to ensure proper operation.

NOTE vCenter Server 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 [1027288](#) for more information about teamed NICs.

LAN

When deployed in a LAN environment, vCenter Server Heartbeat requires that both servers use the same Principal (Public) IP address. Each server also requires a separate VMware Channel IP address on a separate dedicated subnet.

NOTE Deployment in a LAN environment is the only supported option when configuring for non-identical nodes.

Non-Identical Nodes

If configuring for non-identical nodes, vCenter Server Heartbeat supports updatable Microsoft DNS servers and non-updatable (Locked Down mode) or non-Microsoft DNS servers.

Microsoft DNS Server Updated During Switchover/Failover

Microsoft DNS servers must be updatable to allow operation of the `DNSUpdate.exe`. If using Microsoft Windows 2008 R2, the security level must be configured to permit changes to Windows Server 2008 R2 DNS servers.

Switchover/Failover Without Updating DNS Servers

If using Microsoft DNS servers in a Locked Down mode or non-Microsoft DNS servers, vCenter Server Heartbeat will not attempt to update DNS and therefore, the Administrator must prepopulate the DNS server with entries for the new management names and IP addresses that are to be used. Adjacent IP addresses should be reserved and used for the Principal (Public) IP address and the Management IP addresses for the Primary and Secondary Servers when installing vCenter Server Heartbeat on non-identical nodes on servers running Windows 2008.

Primary Server

Three NICs (1 x Public and 2 x Channel) are recommended for redundancy in the event one channel fails. A minimum of two NICs (one for the Channel, and one for the Public) are required in this configuration. Split-brain Avoidance should be configured.

- Principal (Public) network connection configured with the following:
 - Static IP address
 - Correct network mask
 - Correct Gateway address
 - Correct preferred and secondary (if applicable) DNS server address
 - NetBIOS enabled
- Channel Network connection(s) configured with the following:
 - Static IP address in a different subnet than the Principal (Public) network with a different IP address than the Secondary server channel NIC
 - Correct network mask
 - No Gateway IP address
 - No DNS server address
 - NetBIOS enabled (disabled during the installation process)

Secondary Server

Networking components on the Secondary server must be configured as follows:

- Same number of NICs as the Primary server
- Principal (Public) network connection configured with temporary network settings
- Channel network connection(s) configured with the following:
 - Static IP address in a different subnet than the Principal (Public) network with a different IP address than the Primary server channel NIC
 - Correct network mask
 - No Gateway IP address
 - No DNS IP address
 - NetBIOS enabled (setup will disable this during the installation process)
 - File and print sharing enabled

WAN

Deploying vCenter Server Heartbeat in a WAN environment requires additional considerations. Each server within the vCenter Server Heartbeat pair requires its own separate Principal (Public) IP address and a VMware Channel IP address in a separate dedicated subnet.

NOTE Non-identical nodes are not supported in a WAN environment.

WAN Requirements

WAN deployments require the following:

- Persistent static routing configured for the channel connection(s) where routing is required
- 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 use the same subnet:
 - During install, follow the steps for a LAN or VLAN on the same subnet
 - Both servers in the vCenter Server Heartbeat pair use the same Public IP address
- If the Primary and DR site use different subnets:
 - During install, follow the steps for a WAN
 - Both servers in the vCenter Server Heartbeat pair require a separate Principal (Public) IP address and a VMware Channel IP address in a separate dedicated subnet
 - Provide a user account with rights to update DNS using the DNSUpdate utility provided as a component of vCenter Server Heartbeat through vCenter Server Heartbeat Console **Applications > Tasks > User Accounts**
 - VMware recommends integrating Microsoft DNS into AD so that DNSUpdate can identify all DNS Servers that require updating
 - At least one Domain Controller at the DR site
 - Refer to the following articles in the VMware Knowledge Base:
 - [KB 1008571](#) – *Configuring DNS with VMware vCenter Server Heartbeat in a WAN Environment*
 - [KB 1008605](#) – *Configuring vCenter Server Heartbeat to Update BIND9 DNS Servers Deployed in a WAN*

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 and the Default Channel port. VMware recommends that the Client Connection port be configured by process rather than by specific port and that the Default Channel port be configured to allow traffic to pass through on the specific configured port.

Bandwidth

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. VMware recommends making a minimum of 1Mbit of spare bandwidth available to vCenter Server Heartbeat.

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

Latency

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

Heartbeat Diagnostics can assist in determining the available bandwidth, required bandwidth, and server workload. For more information about Heartbeat Diagnostics, contact VMware Professional Services.

Antivirus Recommendations

Consult with and implement the advice of your antivirus (AV) provider, as VMware guidelines often follow these recommendations. Consult the VMware knowledge base for up to date information on specific AV products.

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

VMware recommends that when implementing vCenter Server Heartbeat, you do not replicate file level AV temp files using vCenter Server Heartbeat.

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

Configure file level AV to use the management IP address on the passive server for virus definition updates. If this is not possible, manually update virus definitions on the passive server.

Exclude the following VMware directories from file level AV scans (C:\Program Files\VMware\VMware vCenter Server Heartbeat\ is the default installation directory):

- C:\Program Files\VMware\VMware vCenter Server Heartbeat\r2\logs
- C:\Program Files\VMware\VMware vCenter Server Heartbeat\r2\log

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

Deployment Options Summary

Table 2-1 provides all possible deployment options described in this section.

Table 2-1. Installation Options

	Network		Node Configuration		Clone Technique		Component		
	LAN	WAN	Identical Nodes	Non-identical Nodes	Pre-Clone	Install Clone	vCenter Server w/SQL Local	vCenter Server w/SQL Remote	vCenter Server Only
V2V	X	X	X	X	X		X	X	X
P2V	X	X	X	X	X	X	X	X	X
P2P	X	X	X			X	X	X	X

Installation Options Checklist

Verify the prerequisites:

Server architecture:

P2P

P2V

V2V

Cloning technology option:

Pre-Clone Install

Install Clone

Application components to protect:

vCenter Server with SQL Server on same host

vCenter Server with SQL Server on separate host

vCenter Server only

Network environment type:

LAN

WAN

Identity Mode:

Identical Nodes

Non-Identical Nodes (Only supported in LAN, using V2V or P2V, Pre-Cloned environments)

Microsoft DNS Server Updated During Switchover/Failover

Switchover/Failover Without Updating DNS Servers (Locked Down mode) or non-Microsoft DNS server

Is the subnet the same at the Secondary site?

- If Yes, an IP address is required for this subnet

Active Directory Integrated DNS?

- If Yes, a Domain Account with rights to update DNS is required.
- If No, refer to the knowledge base articles in [“Network Options”](#) on page 26.

Installing vCenter Server Heartbeat on Identical Nodes

3

This chapter includes the following topics:

- [“Overview”](#) on page 31
- [“Installation Process”](#) on page 31
- [“Primary Server”](#) on page 32
- [“Secondary Server”](#) on page 38
- [“vCenter Server Heartbeat Console”](#) on page 44
- [“Post Installation Configuration”](#) on page 45
- [“Installation of Client Tools”](#) on page 47

Overview

This chapter discusses the installation process used to implement vCenter Server Heartbeat on Windows Server 2003 and Windows Server 2008. The installation process for all scenarios follows the same basic procedure. Links to specific installation scenarios describing differences are identified by the blue hyperlinked text.

Prior to installing vCenter Server 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.

Installation Process

After selecting implementation options, begin the installation process. During the installation process, vCenter Server 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 [Appendix – Setup Error Messages](#) in this guide for a list of the checks and an explanation of the message. You must resolve critical stops before you can proceed with setup.

Primary Server

Installation of vCenter Server Heartbeat begins on the Primary server.

NOTE vCenter Server Heartbeat prompts you to enter a valid production serial number during the installation process. If you do not enter a valid production serial number during the installation process, vCenter Server Heartbeat installs in the evaluation mode.

To install the Primary Server

- 1 Having verified all of the environmental prerequisites are met, download the vCenter Server Heartbeat WinZip self-extracting file to an appropriate location on the Primary server (either Physical or Virtual).

You have the following options:

- For P2P, go to [Step 2](#) to continue the installation.
- For V2V or P2V installations with the Pre-Clone technique selected, begin with [Step a](#) below to configure the network settings on the Secondary server.
 - a Clone the Primary server using either the VMware vCenter Converter for P2V, vCenter virtual machine cloning for V2V, or another third-party utility to create a cloned image of the Primary server. The clone must be completely identical with no changes to the Name, SID, or domain membership.
 - b After creating the cloned image, but before powering on the cloned image, edit the image settings.
 - c On the Secondary (previously cloned) server image, select the Public virtual network adapter and clear the **Connected** and **Connect at power on** check boxes.
 - d Repeat the process on the Channel virtual network adapter.
 - e Power on the Secondary (previously cloned) server image.
 - f After the Secondary starts, open Network Connections, right-click the VMware Channel network connection and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**.
 - g Configure the appropriate VMware Channel IP address and subnet mask. Click **Advanced**
 - h Click the **DNS** tab, clear the **Register this connection's addresses in DNS** check box.
 - i Click the **WINS** tab, select **Disable NetBIOS over TCP/IP** and click **OK** twice.
 - j Select the Principal (Public) network connection, right-click and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**. Set the appropriate IP address (same as the Primary server for LAN installations), Subnet Mask, and Default Gateway, and click **OK**.
 - k In **Network Connections**, click **Advanced** and select **Advanced Settings**. Verify that the Principal (Public) NIC IP address is listed first in the Bind Order, and click **OK**.
 - l Right-click the Secondary (cloned) server image and select **Edit Settings**.
 - m Select the VMware Channel virtual network adapter and select the **Connected** and **Connect at power on** check boxes. IP communications with the Secondary server go through the VMware Channel.

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

- 2 On the Primary server, double-click the WinZip Self-Extracting file to initiate the installation process. The **Setup Introduction** dialog appears. Review the information and click **OK**.

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.

- 3 The **WinZip Self-Extractor** dialog appears. Click **Setup** to continue.

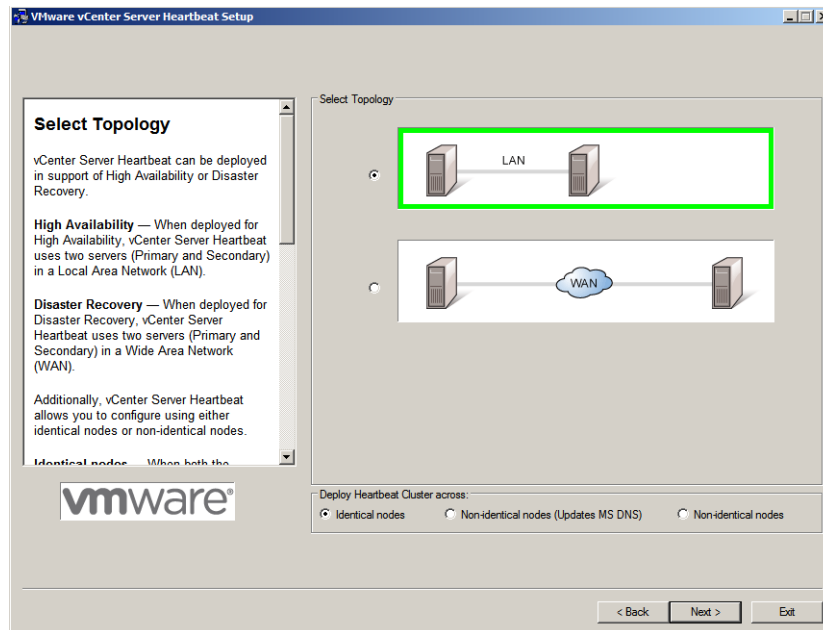
- 4 The **Setup Type** page appears. Because this is a new installation of vCenter Server Heartbeat, select **Install vCenter Server Heartbeat** and click **Next**.

NOTE The left pane of each page in the setup wizard provides information about the setup process.

- 5 Select the physical identity of the server on the **Physical Hardware Identity** page. Select **Primary** as the server identity and click **Next**.

NOTE If .Net 2.0 is not currently installed on the server, vCenter Server Heartbeat Setup installs this required component, taking some additional time during the installation process.

- 6 Read the license agreement carefully and select **I accept terms of the License Agreement**. Click **Next**.
- 7 Click **Add** to enter a valid production serial number for production mode or click **Next** to install in the evaluation mode.
- 8 Select the intended topology of the installation. Select either **LAN** (if the Primary and Secondary server will use the same Principal (Public) IP address) or **WAN** (if the Primary and Secondary server will use different Principal (Public) IP addresses).



- 9 Select the intended identity mode. Select **Identical nodes** since the servers will use the same Fully Qualified Domain Names (FQDN). Click **Next**.

- 10 Select the cloning options.

You have the following options:

- For installation using the Install Clone technique, continue with [Step 11](#).
- For installation using the Pre-Clone technique, continue with [Step 12](#).

- 11 Select **Not a clone of the Primary server**, click **Next**, and go to [Step 13](#).
- 12 If a virtual Secondary server was created using vCenter Converter, the cloning option in the Virtual Infrastructure Client, or a third-party utility, select **Pre-cloned** and click **Next**.
- 13 Configure the installation paths. The default installation location is `C:\Program Files\VMware\VMware vCenter Server Heartbeat`, but you can change it by manually typing a path to another install location.

NOTE The path of the VMware installation folder cannot contain Unicode characters. If vCenter Server Heartbeat is installed in a folder that has a path containing Unicode characters, this causes the Neverfail Server R2 service to fail to start. The path of the VMware 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, vCenter Server Heartbeat does not support file or folder names ending with a period "." or space " ".

Alternatively, click **Browse** to select one of these locations. Select **Create icons on Desktop** and click **Next**.

- 14 Identify the network adapter(s) for use in the VMware Channel on the **Channel Adapter Identification** page. Select the network adapters (NICs) for the VMware 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**.

NOTE 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 **VMware Channel IP Configuration** page prompts you to configure the VMware Channel(s) IP network addresses. Click **Add** for each available channel connection. For the Primary server, select from a drop-down menu that lists all local IP addresses. Type the reciprocal IP address on the Secondary server into the **IP Address On Secondary** text box. You must specify all VMware Channel IP addresses in subnets outside of the normal Principal (Public) IP addressing schema so that VMware Channel traffic routing uses the VMware Channel network card rather than the Principal (Public) network card. Click **OK**. Repeat this step for additional NICs.
- 16 Review and adjust, if necessary, the default channel port. Click **Next**.

NOTE 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. Consult the VMware knowledge base for additional information.

- 17 Select the Principal (Public) NIC(s). The IP address information is displayed for each NIC. Click **Next**.
- vCenter Server Heartbeat software can be deployed in a configuration where both servers have the same Principal (Public) IP address, for instance, in a standard Local Area Network (LAN) deployment where both machines are in the same subnet.

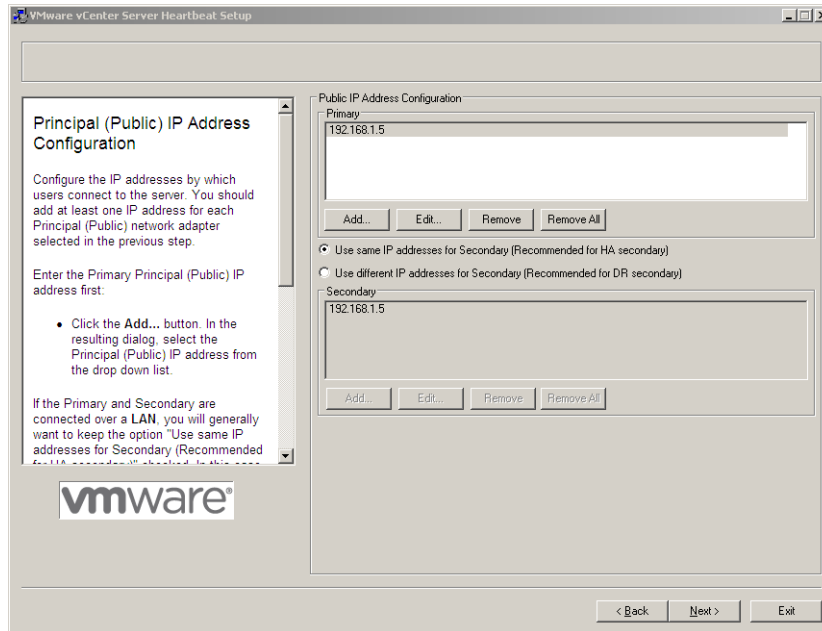
Alternatively, vCenter Server Heartbeat can be deployed where the Principal (Public) IP addresses differ, for instance, in a Wide Area Network (WAN) deployment where the Primary and Secondary servers are located in different sites and subnets where client access is therefore bound by the standard network routing to allow the correct connectivity to the server according to its locale.

- 18 Select **Use same IP addresses for Secondary (Recommended for HA secondary)** or **Use different IP addresses for Secondary (Recommended for DR secondary)**.

You have the following options:

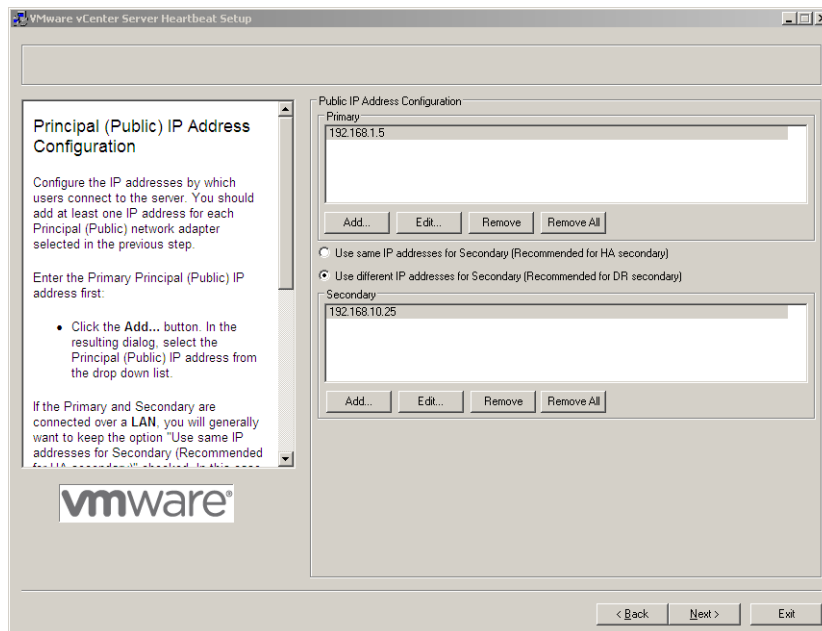
- For a WAN installation with different subnets, go to [Step 20](#).
- For LAN installation or same subnet WAN installs, continue with [Step 19](#).

- 19 For a LAN environment, click **Add** to specify the IP address. Click **Next**.



If installing in a LAN or when the WAN uses the same subnet, go to [Step 23](#).

- 20 For a WAN environment, specify IP addresses of the Secondary server and the Primary server.



- 21 Add each Principal (Public) network address until all addresses are present. Click **Next**.
- 22 When the Principal (Public) addresses on the Secondary server are different from those on the Primary server, vCenter Server 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 vCenter Server Heartbeat update the DNS entries for the active server across the enterprise. Such updates require credentials for domain administrators (or an account with equivalent rights). Type the **Domain Name**, a domain administrator **Username** and **Password** in the respective text boxes and click **Next**.

- 23 The vCenter Server Heartbeat server pair can be administered remotely on client machines using the vCenter Server Heartbeat Console. The vCenter Server Heartbeat Console connects to an 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**.
- 24 Select the applications to protect. All licensed vCenter Server Heartbeat features are listed.
- If installing vCenter Server only, or vCenter Server locally and the SQL Server on a separate server, select **Protect Virtual Center only**.
 - If installing SQL Server remotely, upon completion of the vCenter Server installation locally, repeat the installation procedure at the remote SQL Server location and select **Protect SQL Server only**.
 - If installing both vCenter Server and SQL Server locally, select **Protect Virtual Center and SQL Server**.
 - If View Composer is installed, select the **View Composer** check box to provide protection for View Composer.
- 25 To facilitate the clone of the Primary server onto the Secondary server, you must back up pertinent components of the Primary server for restoration on to the Secondary server. Where VMware Channel communications are fast and reliable, for instance in a LAN topology, you can directly create the backup files over the VMware Channel connections to a partition on the Secondary server.

Where the VMware Channel connection is slower than 10 Mbit/s or risks an interruption in connection, for example in a WAN topology, save the backup file locally and manually port the file to the Secondary server.

Microsoft Windows Backup Configuration options. Including the applications' protected data greatly increases the backup file size and therefore increases the time of the backup operation. Due to the potential large size of the backup file, careful consideration is required when including application data and specifying the backup folder location.

Depending on the network topology between the servers, backup files can include or exclude application data. Including application data in the backup file decreases the time to initially verify and synchronize the applications data on first start up of vCenter Server Heartbeat. This is useful where VMware Channel connections are slower than LAN speed, such as in a WAN implementation.

To estimate the maximum size of the backup file, add together the size of each volume that contains system data and application data. Although the actual size of the backup file can be smaller, using this rule of thumb helps ensure a successful installation.

You have the following options:

- For installation on Windows Server 2003 using the Pre-Clone technique, go to [Step 26](#) on [page 37](#).
- For installation on Windows Server 2003 using the Install Clone technique, continue with [Step a](#) of [Step 25](#).
- For installation on Windows Server 2008 using the Pre-Clone technique, go to [Step d](#) of [Step 26](#)
- For installation on Windows Server 2008 using the Install Clone technique, go to [Step d](#) of [Step 25](#).

Continue with [Step a](#).

- a To perform a direct backup, click **Map Network Drive** and specify a network mapping to the Secondary server. Type in the path or **Browse** to the location to receive the backup file.
- b Select an appropriate drive letter for the mapping and specify the required share on the Secondary server using the channel address of the Secondary server as the server name, for example: \\10.0.0.6\Backup. Verify that the mapped partition has enough free space, a minimum of 2GB, to accommodate the backup file.

- c Specify the path to an appropriate location for storing the backup file by either manually typing the path into **Backup File Folder** or click **Browse** to locate the folder or network mapping. Click **Next**. Go to [Step 27](#).
 - d Select a location to place the backup files through the **Microsoft Windows Backup Configuration** page. When installing into a Windows Server 2008 environment, you must specify a UNC path to the backup file location. Type a UNC path to a location using the machine name or IP address and shared folder into the **Folder** text box. Type a **User** and **Password** that grants access to the shared folder. Click **Next**. Go to [Step 27](#).
- 26 When the Pre-Clone technique is selected, Setup backs up two small files, nfsetup.dat and primary.csv, from the Primary server and restores them to the Secondary server for proper configuration.

Continue with [Step a](#).

- a To perform this direct backup, click **Map Network Drive** and specify a network mapping to the Secondary server. Type the path or **Browse** to the location to receive the backup file.
- b Select an appropriate drive letter for the mapping and specify the required share on the Secondary server using the channel address of the Secondary server as the server name, for example: \\10.0.0.6\Backup.
- c Specify the path to an appropriate location for storing the backup file by either manually typing the path into **Backup File Folder** or click **Browse** to locate the folder or network mapping. Click **Next**. Continue with [Step 27](#)
- d Type the machine name or IP address and the path to the shared folder to receive the backup files, for example: \\10.0.0.16\Backup.

With both Windows Server 2003 and Windows Server 2008, vCenter Server Heartbeat takes the backup using the Windows Volume Shadow Service and does not stop services, thereby preventing downtime. Click **Next**.

- 27 Review the summary of options and configuration information for the installation. Click **Next**.
- 28 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 Report pane displays the results of the pre-install checks.
- 29 If some 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**.

NOTE The Progress pane on the **Pre-Install Checks** page displays the progress of these checks. When finished, the Report pane displays the results.

- 30 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. Setup also installs Heartbeat Diagnostics and configures it with the default settings.

NOTE If a previous version of Heartbeat Diagnostics is detected, vCenter Server Heartbeat Setup updates it to the current version. To learn more about Heartbeat Diagnostics, see *Getting Started with Heartbeat Diagnostics* on the VMware Web site.

- 31 Click **Next** after vCenter Server Heartbeat components are complete.

You have the following options:

- If using the Pre-Clone installation technique, go to [Step 35](#).
- If using the Install Clone installation technique, continue to [Step 32](#).

- 32 The next page displays the Microsoft Windows Backup page. Click **Proceed**. The automated backup is saved in the previously defined location.

NOTE When installing into a Windows Server 2008 environment, vCenter Server Heartbeat verifies that the Windows Server Backup Feature and Command Line Tools are installed. If they are not installed, you must install them now. You are not required to exit the installation to install the Windows Server Backup Feature. Navigate to the Server Manager and under Features, add the Windows Backup Feature and Command Line Tools. When installing Windows Server Backup Feature, Windows PowerShell is also necessary.

- 33 The progress of the backup operation is displayed in the Progress pane. When finished, a report on the backup is displayed in the Report pane. Review the backup report to verify successful completion. Click **OK** on the dialog and click **Next** on the page.
- 34 A summary page displays the results of the backup operation. Review the backup report and click **Next**.
- 35 The vCenter Server 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 **Continue Anyway** (Windows Server 2003) or **Install** (Windows Server 2008). If Windows is configured to display Signed Driver warnings, you can see multiple warnings. The Report pane displays the results. Click **Next**.

By default, the vCenter Server Heartbeat Packet Filter driver is applied to all Principal (Public) network cards present on the machine. The vCenter Server Heartbeat Packet Filter is not applied to the network cards forming VMware Channel connections as these cards maintain unique IP addresses irrespective of the role of the server. vCenter Server Heartbeat also disables NetBIOS on the Channel NIC(s) to prevent domain name conflicts on the subnet.
- 36 When the setup wizard confirms the successful completion of the installation, click **Finish**.

Secondary Server

The process of installing vCenter Server Heartbeat on the Secondary server is similar to installing vCenter Server Heartbeat on the Primary server.

To install the Secondary server

- 1 To install the vCenter Server Heartbeat on the Secondary server, download vCenter Server Heartbeat to the Secondary server (either Physical or Virtual) to a suitable location. Execute the WinZip self extracting file to start the installation process. The **Setup Introduction** dialog appears. Review the information and click **OK**.

NOTE If you click **Exit** after Setup has started, you are prompted to save your settings. When you run the self extracting WinZip file again later, you will be asked if you want to use the previously saved configuration.

- 2 The **WinZip Self-Extractor** dialog appears. Click **Setup** to continue.
- 3 The **Setup Type** page appears. As with the installation on the Primary server, select **Install VMware vCenter Server Heartbeat** and click **Next**.

NOTE The left pane of each page in the setup wizard provides information about the setup process.

- 4 Select the identity of the server on the **Physical Hardware Identity** page. Select **Secondary** as the server identity and click **Next**.

NOTE If .Net 2.0 is not currently installed on the server, vCenter Server Heartbeat Setup installs this required component, taking some additional time during the installation process.

- 5 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 For Windows Server 2003 installations you can alternatively click **Browse** and locate the folder. On Windows Server 2008 installations, you must use the UNC path.

- 6 The pre-install checks run. Click **Next**.

If some pre-install checks are unsuccessful, go back through the wizard, make the necessary changes, and run the pre-install checks again.

You have the following options:

- If installing on Windows Server 2003, continue with [Step 7](#).
- If installing on Windows Server 2008, go to [Step 28](#).

- 7 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. Setup also installs Heartbeat Diagnostics and configures it with the default settings. To learn more about Heartbeat Diagnostics see *Getting Started with Heartbeat Diagnostics*.

- 8 The Report pane displays the results of the installation. Click **Next**.

- 9 The progress of the VMware vCenter Server Heartbeat Packet Filter installation is displayed. Click **Next**.

You have the following options:

- If the Secondary server is physical, such as in P2P, go to [Step 10](#).
- If the Secondary server is virtual, such as in P2V or V2V, continue with [Step a](#).
 - 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**.

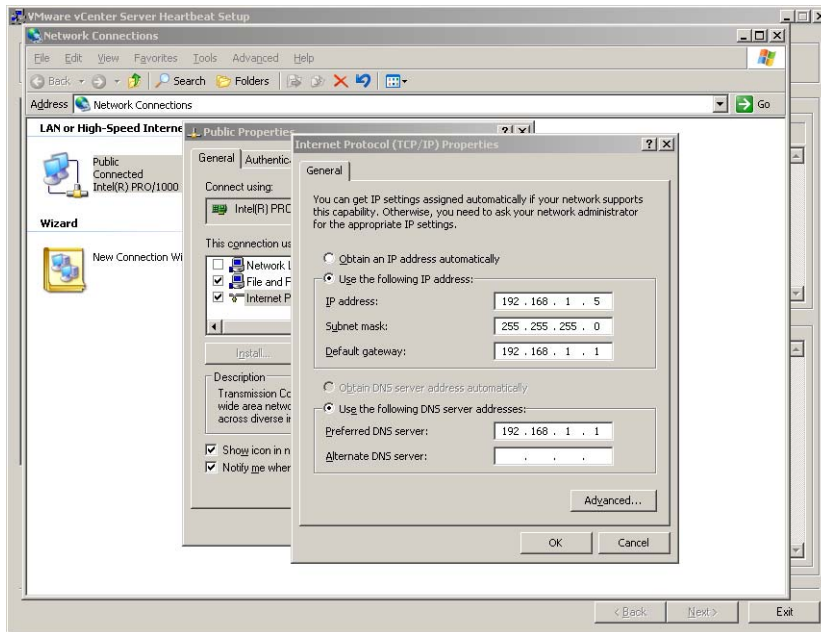
- 10 In the **Channel Adapter Identification** page, select the appropriate adapter and review the IP address configuration in the lower pane. Click **Next**.

You have the following options:

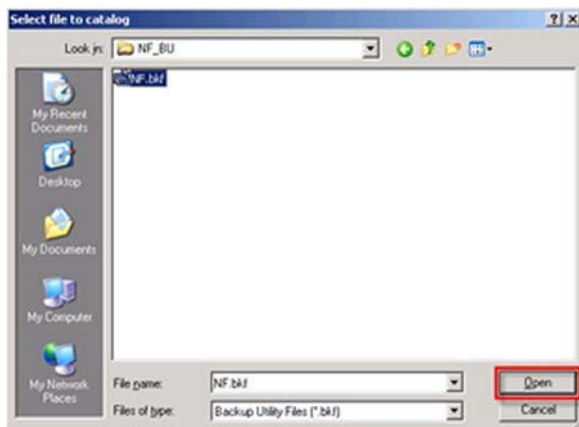
- If using the Install Clone installation technique, continue to [Step 11](#).
- If using the Pre-Clone installation technique, go to [Step 14](#).

- 11 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). Click **OK**.

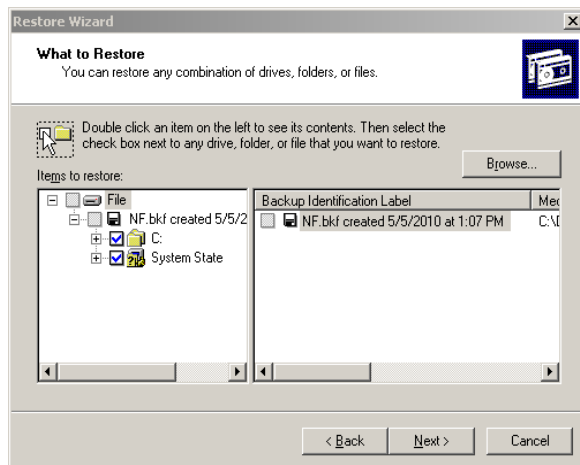
- 12 Click **Open Network Connections** to change the static IP address of the Principal (Public) adapter to match that of the Primary server (LAN configuration only).



- 13 If in a WAN environment, verify the Secondary Principal (Public) adapter IP address configuration. Click **Next** and go to [Step 15](#).
- 14 When using the Pre-Clone installation technique, although you previously configured the IP address of the Principal (Public) network connections, you can make any last minute changes on the Secondary server through vCenter Server Heartbeat. Click **Next** and go to [Step 28](#).
- 15 The **Microsoft Windows Backup Restore** page shows the process of unbinding the vCenter Server Heartbeat Packet Filter and disabling NetBIOS from the VMware Channel NIC(s). A caution message appears, advising you that the restore process is initiating and upon completion, the server must be restarted. After restarting, Plug and Play (PnP) can require you to restart the machine again. Click **Next**.
- 16 The NTBackup wizard launches. If NTBackup has never run before, the software searches for backup devices. Close any open wizards and click **Restore Wizard** on the **Welcome** page.
- 17 Click **Next** in the Restore Wizard. Click **Browse** to locate the previously generated backup file.
- 18 Navigate to the partition and select the folder in which the backup file was created, select the backup file, click **Open** and then click **OK**.



- 19 Expand the file tree structure to see the System State file in the left pane. Click **OK** to build indexes where required. Select all items listed under the media created tree and click **Next**.



- 20 With **Where to restore** at the default **Original location**, click **Next**. Click **Finish**.



- 21 A warning message alerts you that the restore process is going to overwrite the existing System State files. Click **OK**.
- 22 When the restoration process completes, click **Close**.
- 23 To apply the newly restored system state, you must restart the machine. Click **Yes** to restart the server.
- 24 Following the restart of the server, log in to the Secondary server using a domain administrator account.
- 25 PnP can require multiple restarts of the server as it reidentifies the actual hardware makeup of the Secondary server as opposed to that restored from the backup file of the Primary server.

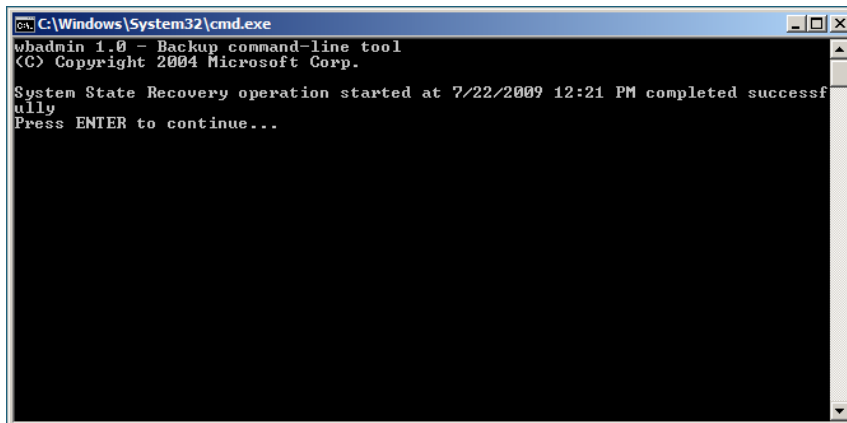
NOTE vCenter Server Heartbeat starts each time the Secondary server restarts. Manually shut down vCenter Server Heartbeat before initiating a restart.

- 26 Click **Yes** at each restart prompt to allow each PnP cycle to complete.
- 27 When all PnP cycles complete, the vCenter Server Heartbeat Setup is complete.
- 28 You have the following options:
- For installations on Windows Server 2003, go to [Step 44](#) on [page 43](#).
 - For installations on Windows Server 2008 using the Install Clone technique, continue with [Step 29](#) on [page 42](#).
 - For installations on Windows Server 2008 using the Pre-Clone technique, go to [Step 39](#) on [page 43](#)

- 29 The **Microsoft Windows Backup Restore** page is displayed. The **Microsoft Windows Backup Restore** page shows the progress of unbinding the packet filter and disabling NetBIOS from the channel NIC(s). After this process completes, a caution message advises you that the restore process is initiating and upon completion of the restore process, the server requires a restart. After restarting, Plug-and-Play (PnP) can require you to restart the machine more than once. Click **OK**.
- 30 The progress of the backup restore is displayed in the Progress pane. When finished, a report on the restore is displayed in the Report pane. Review the backup restore report to verify successful completion. Click **Next**.
- 31 The **Disconnect Network Cables** page is displayed. To disable the NICs is NOT sufficient. You must physically disconnect the network cables from the NICs. After disconnecting the network cables from the NICs, click **Finish**. A confirmation dialog is displayed. You must restart the machine to apply the newly restored System State. Click **Yes** to restart the server.

NOTE If this server is running in a virtual environment, disconnect the NICs from the virtual environment.

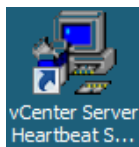
- 32 Following the restart of the server, log in to the Secondary server using the domain administrator account. A DOS window is presented stating that the restore of the System State was successful. Press Enter. Click **Yes** at each restart prompt to allow each PnP cycle to complete.



NOTE PnP can require multiple restarts of the server as it identifies the actual hardware makeup of the Secondary server as opposed to that restored from the backup file of the Primary server.

vCenter Server Heartbeat starts each time the Secondary server restarts. Manually shut down vCenter Server Heartbeat before initiating a restart.

- 33 After all PnP cycles complete, log in to the server and double-click the newly created **vCenter Server Heartbeat Setup Completion** icon created on the Desktop to continue the setup process.



- 34 The **Post-Reboot Configuration** page is displayed. vCenter Server Heartbeat Setup installs the packet filter. When complete, click **Next**.

NOTE If you receive 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 can receive multiple warnings.

- 35 The **Reconnect Network Cables** page is displayed. Follow the instructions on this page to reconnect all of the previously disconnected network cables. After all network cables are connected, click **Next**.
- 36 The **Channel Adapter Identification** page is displayed. Use this opportunity to reconfigure the VMware Channel NICs. During the cloning process, the IP address for the channel adapter on the Secondary server is reset to the IP address for the Primary server. To prevent network conflicts and to properly configure the VMware Channel, click **Open Network Connections** to display the network connections. Configure the Secondary Channel connection to the appropriate IP address (different from the IP address for the Primary Channel connection). After completing this configuration, select the check boxes for all channel connections and click **Next**.
- 37 The **Public Adapter Identification** page is displayed. Select the Principal (Public) connection. Verify that the IP address configuration is correct.
- 38 The **Duplicate Installation Complete** page is displayed. Do not select the **Start vCenter Server Heartbeat** check box. Click **Finish**.
- 39 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. Setup also installs Heartbeat Diagnostics and configures it with the default settings. To learn more about Heartbeat Diagnostics see *Getting Started with Heartbeat Diagnostics*.
- 40 The Report pane displays the results of the installation. Click **Next**.
- 41 The progress of the VMware vCenter Server Heartbeat Packet Filter installation is displayed. Click **Next**.
You have the following options:
 - If the Secondary server is Physical such as in P2P, go to [Step 42](#).
 - If the Secondary server is Virtual such as in P2V or V2V, continue with [Step a](#).
 - 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**.
- 42 In the **Channel Adapter Identification** page, select the appropriate adapter and review the IP address configuration in the lower pane. Click **Next**.
- 43 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).
- 44 The **Secondary Installation Complete** page is displayed. Do not select the **Start vCenter Server Heartbeat** check box. Click **Finish**.
- 45 Before starting vCenter Server Heartbeat, verify the time synchronization between the Primary and Secondary servers. When a difference exists, synchronize the Secondary (passive) server to the Primary (active) server across the VMware Channel. Type the following command at the command prompt:


```
net time \\<Primary_Channel_IP_address> /set
```

Start vCenter Server Heartbeat on the Primary server. Right-click the vCenter Server Heartbeat System Tray icon and select **Start VMware vCenter Server Heartbeat**. The icons change from a double dash to a **P**, indicating the server is the Primary server, and an **A** indicating the server is acting in an active role.

Start vCenter Server Heartbeat on the Secondary server. Right-click the vCenter Server Heartbeat System Tray icon and select **Start VMware vCenter Server Heartbeat**. The icon changes from a double dash to an **S**, indicating that the server is the Secondary server, and a dash (–), indicating that the server is in a passive role.
- 46 The Primary and Secondary servers establish a handshake and commence replication.

NOTE The installation is complete if vCenter Server was installed with a local SQL Server or only vCenter Server was installed with no separate SQL Server.

If vCenter Server only was installed and you want to install a separate SQL Server, repeat the installation process for the Primary and Secondary servers at the remote site and select **SQL Server only**.

To install SQL Server on a separate host from the vCenter Server, go to [“Primary Server”](#) on page 32

- 47 See [“Post Installation Configuration”](#) on page 45 for additional instructions on configuring vCenter Server Heartbeat.

vCenter Server Heartbeat Console

To administer a pair of servers you must connect to them through the vCenter Server Heartbeat Console. vCenter Server Heartbeat Console does not connect until vCenter Server Heartbeat initializes.

You can start vCenter Server Heartbeat Console from any server in the vCenter Server Heartbeat Pair.

To start vCenter Server Heartbeat Console

- 1 Right-click the VMware vCenter Server Heartbeat interactive status icon on the Windows taskbar (located on the right side of the Windows tool bar). The vCenter Server Heartbeat quick access menu opens.
- 2 Select **Manage Server**. The vCenter Server Heartbeat Console opens in a window and shows the Heartbeat Servers (overview) pane.

Alternatively you can start vCenter Server Heartbeat Console from the VMware program group on the Windows Start menu. This is the only method supported if vCenter Server Heartbeat Console has been installed on a workstation that is not part of the Pair.

Navigate vCenter Server Heartbeat Console

After vCenter Server Heartbeat Console is running, use the navigation panel on the left of the vCenter Server Heartbeat Console window to view and select Groups and Pair connections you can manage with vCenter Server Heartbeat Console.

NOTE A Group is an arbitrary collection of vCenter Server Heartbeat Pairs used for organization.

A Connection, or Pair Connection allows vCenter Server Heartbeat Console to communicate with a vCenter Server Heartbeat Pair either on the same machine or remotely.

See [“Add a vCenter Server Group”](#) on page 44 and [“Add a New Connection”](#) on page 45 for information on how to add Groups and Pair Connections to vCenter Server Heartbeat Console.

The selection of Group or Pair you make in the navigation panel “points” the vCenter Server Heartbeat Console to that Group or Pair and vCenter Server Heartbeat Console provides information related to only the selected Group or Pair. To avoid confusion, pay particular attention to the selection in the navigation panel when you are managing more than one Group or Pair.

NOTE Groups and Pairs are not automatically detected by vCenter Server Heartbeat Console. Each Group or Pair you want to manage must be added to vCenter Server Heartbeat Console before you can use it to view status or change settings for that Group or Pair Connection.

Select a Pair in the navigation panel of vCenter Server Heartbeat to show a set of tabs and sub-tabs that offer detailed status and control of the associated vCenter Server Heartbeat servers in the Pair.

Add a vCenter Server Group

The Add Group feature in vCenter Server Heartbeat Console allows you to add new vCenter Server Heartbeat Groups to manage.

To add a vCenter Server Heartbeat Group

- 1 Open vCenter Server Heartbeat Console and click **Add Group** in the tool bar, select **Add Group** from the **File** menu, or right-click an existing group in the navigation panel and select **Add Group** from the menu.
- 2 Type the name for the new group into the text box and click **OK**. The newly created group appears in the navigation panel on the left of the vCenter Server Center Heartbeat window.

Add a New Connection

The Add Connection feature in the vCenter Server Heartbeat Console allows you to add a new Pair Connection to an existing vCenter Server Heartbeat Group.

To Add a new connection

- 1 In the navigation panel, select the vCenter Server Heartbeat Group to receive the new connection. Click **Add Connection** in the tool bar, select **Add Connection** from the **File** menu, or right-click an existing group in the navigation panel and select **Add Connection** to invoke the **Add Connection** dialog.
- 2 Type the Host Name or IP address for the new connection into the text box, select the Port Number (if different from the default value of 52267), and select a group from the **Add to Group** drop-down list (to add the connection to a Group other than the one currently selected).

NOTE When you attempt to connect to vCenter Server Heartbeat for the first time, you are presented the option to accept the SSL certificate from the server. To continue connecting to vCenter Server Heartbeat, you must accept the SSL certificate.

- 3 Click **OK**. The newly created connection appears in the navigation panel on the left of the vCenter Server Heartbeat Console window, and the **Server: Summary** page updates to represent any existing network relationships of the added server.

NOTE You may be prompted to login. If so, login using a valid administrator-level Username and Password for the server for which you are adding a connection, and click **OK**.

- 4 Enter the remaining connections necessary to define the new vCenter Server Heartbeat Group.

Post Installation Configuration

Upon completion of installation, a series of tasks must be performed to ensure that vCenter Server Heartbeat is properly configured.

Configuring VirtualCenter Plug-in with the Correct Credentials

After installation is complete, you must enter the credentials for an account with rights to the Virtual Infrastructure.

To add the Virtual Infrastructure credentials

- 1 Navigate to the **Applications: Plug-ins** page.
- 2 Select the VirtualCenter Plug-in.
- 3 Click **Edit**.
- 4 Type the Username and Password for an account with rights to the Virtual Infrastructure.
- 5 Click **OK**.

When Deployed in a WAN Environment

When deployed in a WAN environment with VMware Orchestrator and the Primary and Secondary servers in different subnets, you must configure an Exclusion File Filter following the steps below:

- 1 Launch **vCenter Server Heartbeat Console**.
- 2 Click **Data** and click the **File Filters** tab.
- 3 Click **Add Exclusion Filter** and type the following path:
`$INSTALL_PATH_TO_ORCHESTRATOR/app-server/bin/boot.properties`
- 4 Click **OK**.
- 5 Perform a switchover so that the Secondary server becomes active.
- 6 Launch the **vCenter Orchestrator Web Configuration** wizard and select **Network**. In the **IP address** field select the Principal (Public) IP address of the Secondary server. Click **Apply changes**.
- 7 In the **vCenter Orchestrator Web Configuration** wizard, select **Startup Options**, and click **Restart service**.
- 8 From **vCenter Server Heartbeat Console**, select **Applications** and then **Services**. Verify that **VMware vCenter Orchestrator Server** service is included in the protected services. If not, manually run the **Protected Service Discovery** task from **VMware vCenter Heartbeat Console > Applications > Tasks > VMware VirtualCenter - Protected Service Discovery**

vCenter Server 2.5

The post installation configuration tasks are determined by the type of network environment.

LAN

For LAN deployments, perform the following:

- 1 If a Management IP address is configured, no additional tasks are required.
- 2 If a Management IP address is not configured, configure a VMware Managed IP address using the Virtual Infrastructure Client.
 - a Launch the Virtual Infrastructure Client.
 - b In the Virtual Infrastructure Client, navigate to **Administration > VirtualCenter Management Server Configuration > Runtime Settings**.
 - c In the **Managed IP** field, type the Principal (Public) IP address.
 - d Click **OK**.

WAN

For WAN deployments, regardless of whether a Management IP address exists, vCenter Server Heartbeat provides a task that can be configured to update the ESX hosts with the new Managed IP address during a switchover or failover. The task requires setting the Managed IP in either the `vpxd.cfg` file or in the registry.

To configure the Managed IP in the Vpxd file

- 1 The `vpxd.cfg` file is located at `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter`.
- 2 On the active server, locate the `<vpxd>` element in the `vpxd.cfg` file and add a new element `<managedIP>` that contains the Principal (Public) IP address of the vCenter server.

To configure the Managed IP in the registry

At `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VirtualCenter`, create a new string value called `<managedIP>` and set it with the Public (Principal) IP address of the currently active server.

IMPORTANT Do not configure the VMware Managed IP address using the Virtual Infrastructure Client. The Managed IP field from **Administration > VirtualCenter Management Server Configuration > Runtime Settings** must be clear.

Installing the View Composer Plug-in

Installation of the View Composer Plug-in can occur during the installation of vCenter Server Heartbeat as a part of the installation process or can be installed post-installation.

To install the View Composer Plug-in after vCenter Server Heartbeat has been installed

- 1 Ensure that View Composer has been installed on both the Primary and Secondary servers with the same configuration settings.
- 2 Launch the vCenter Server Heartbeat Console.
- 3 Navigate to **Applications: Plug-ins** and click **Install**.
- 4 Browse to the plug-in file located at:
<unzipped_folder>\<vCenterServerHeartbeatVersion-x86/x64>\plugins\ViewComposer\ViewComposerNFPlugin.dll
- 5 Click **OK** to install the View Composer Plug-in.

Installation of Client Tools

vCenter Server Heartbeat allows installation of vCenter Server Heartbeat Client Tools for remote management of vCenter Server Heartbeat clusters.

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

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

To install vCenter Server Heartbeat Client Tools

- 1 Copy the WinZip Self-Extracting file to the client where it is to be installed.
- 2 Double-click the WinZip Self-Extracting file to initiate the installation process. The **Setup Introduction** dialog appears. Review the information and click **OK**.
- 3 The **WinZip Self-Extractor** dialog appears. Click **Setup** to continue.
- 4 The **Setup Type** page appears. Because this is a vCenter Server Heartbeat Client Tools installation, select **Install Client Tools Only** and click **Next**.
- 5 Read the license agreement carefully and select **I accept terms of the License Agreement**. Click **Next**.
- 6 Configure the installation paths. The default installation location is `C:\Program Files\VMware\VMware vCenter Server Heartbeat`, but you can change it by manually typing a path to another install location.

NOTE The path of the VMware installation folder cannot contain Unicode characters. The path of the VMware 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, vCenter Server Heartbeat does not support file or folder names ending with a period "." or space " ".

Alternatively, click **Browse** to select one of these locations. Select **Create icons on Desktop** and click **Next**.

- 7 Review the summary of options and configuration information for the installation. Click **Next**.

- 8 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. If the pre-install checks are successful, click **Next**.
- 9 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. Click **Next** after vCenter Server Heartbeat Client Tools components are complete.
- 10 The **Client Tools Installation Complete** page is displayed. Click **Finish**.

Installing vCenter Server Heartbeat on Non-Identical Nodes

4

This chapter includes the following topics:

- [“Overview”](#) on page 49
- [“Installation Process”](#) on page 49
- [“Installing vCenter Server Heartbeat on Non-Identical Nodes”](#) on page 50
- [“Post Installation Configuration”](#) on page 60
- [“vCenter Server Heartbeat Console”](#) on page 58
- [“Installation of Client Tools”](#) on page 61

Overview

This chapter discusses the installation process used to implement vCenter Server Heartbeat on Windows Server 2003 or Windows Server 2008 on non-identical nodes. The installation process for both scenarios follows the same basic procedure. Links to specific installation scenarios describing differences are identified by the blue hyperlinked text.

This installation is only supported for LAN deployments using the V2V or P2V architecture, Pre-Cloned installation technique. The installation process requires you to select options throughout the procedure to achieve your configuration goals.

Installation Process

After selecting implementation options, begin the installation process. During the installation process, vCenter Server 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 [Appendix – Setup Error Messages](#) in this guide for a list of the checks and an explanation of the message. You must resolve critical stops before you can proceed with setup.

Installing vCenter Server Heartbeat on Non-Identical Nodes

vCenter Server Heartbeat is installed on both the Primary and Secondary server of a vCenter Server Heartbeat cluster.

NOTE When protecting SQL Server in a non-identical nodes environment, the SQL Server instance service must run under an account with administrator rights rather than the Network Service or Local System account. If required, change the **Log On AS** property by navigating to **Start > Administrative Tools > Services**. Select the SQL Service instance and click **Properties**. Select the **Log On** tab and select **This account**. Provide the new account credentials and click **OK**. Once complete, restart the SQL Server instance service.

Primary Server

Installation of vCenter Server Heartbeat begins on the Primary server.

To install vCenter Server Heartbeat on the Primary server

NOTE vCenter Server Heartbeat prompts you to enter a valid production serial number during the installation process. If you do not enter a valid production serial number during the installation process, vCenter Server Heartbeat installs in the evaluation mode.

- 1 Having verified all of the environmental prerequisites are met, download the vCenter Server Heartbeat WinZip self-extracting file to an appropriate location on the Primary server.
- 2 Open **Network Connections**, right-click the VMware Channel network connection and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**.
- 3 Click **Advanced**, select the **DNS** tab, and clear the **Register this connection's addresses in DNS** check box. Click **OK** three times to close the dialogs.
- 4 Right-click the Principal (Public) network connection and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**.
- 5 Click **Advanced**, select the **DNS** tab, and clear the **Register this connection's addresses in DNS** check box. Click **OK** three times to close the dialogs.
- 6 Clone the Primary server using either the VMware vCenter Converter for P2V, vCenter virtual machine cloning for V2V, or another third-party utility to create a cloned image of the Primary server. The clone must be completely identical with no changes to the Name, SID, or domain membership. Do not start the cloned server.
- 7 Double-click the WinZip Self-Extracting file to initiate the installation process on the Primary server. The **Setup Introduction** dialog appears. Review the information and click **OK**.

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.

- 8 The **WinZip Self-Extractor** dialog appears. Click **Setup** to continue.
- 9 The **Setup Type** page appears. Because this is a new installation of vCenter Server Heartbeat, select **Install vCenter Server Heartbeat** and click **Next**.

NOTE The left pane of each page in the setup wizard provides information about the setup process.

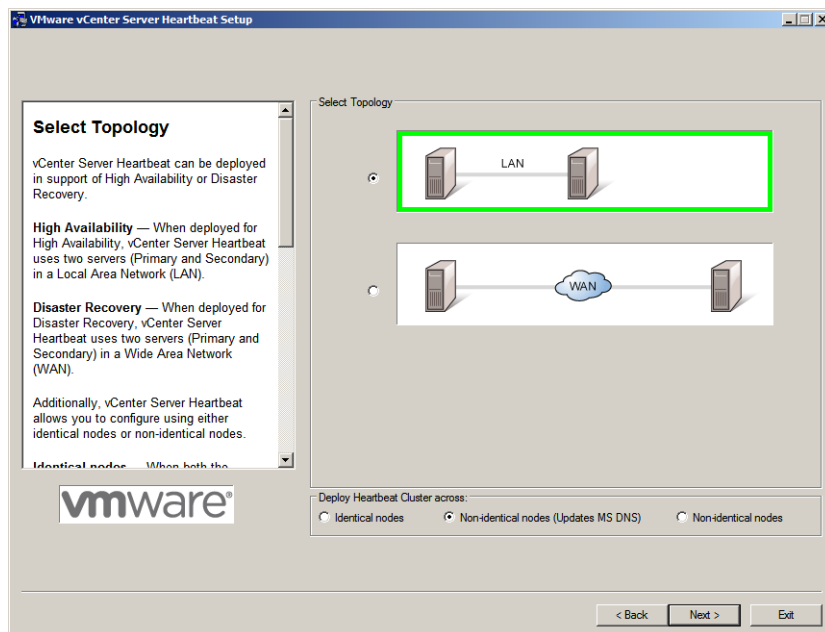
- 10 Select the physical identity of the server on the **Physical Hardware Identity** page. Select **Primary** as the server identity and click **Next**.

NOTE If .Net 2.0 is not currently installed on the server, vCenter Server Heartbeat Setup installs this required component, taking some additional time during the installation process.

- 11 Read the license agreement carefully and select **I accept terms of the License Agreement**. Click **Next**.

- 12 Click **Add** to enter a valid production serial number for production mode or click **Next** to install in the evaluation mode.
- 13 Select **LAN** for the network topology and in the **Deploy Heartbeat Cluster across** pane, select either **Non-identical (Updates MS DNS)** if you are using an updatable Microsoft DNS server or **Non-identical** if you are using a non-updatable Microsoft DNS server or non-Microsoft DNS server. Click **Next**.

NOTE Non-identical nodes without updatable DNS is not supported in a WAN.



- 14 Select the **Pre-Clone** option and click **Next**.
- 15 Configure the installation paths. The default installation location is `C:\Program Files\VMware\VMware vCenter Server Heartbeat`, but you can change it by manually typing a path to another install location.

NOTE The path of the VMware installation folder cannot contain Unicode characters. If vCenter Server Heartbeat is installed in a folder that has a path containing Unicode characters, this causes the Neverfail Server R2 service to fail to start. The path of the VMware 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, vCenter Server Heartbeat does not support file or folder names ending with a period "." or space " ".

Alternatively, click **Browse** to select one of these locations. Select **Create icons on Desktop** and click **Next**.

- 16 Identify the network adapter(s) for use in the VMware Channel on the **Channel Adapter Identification** page. Select the network adapters (NICs) for the VMware 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**.

NOTE 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.

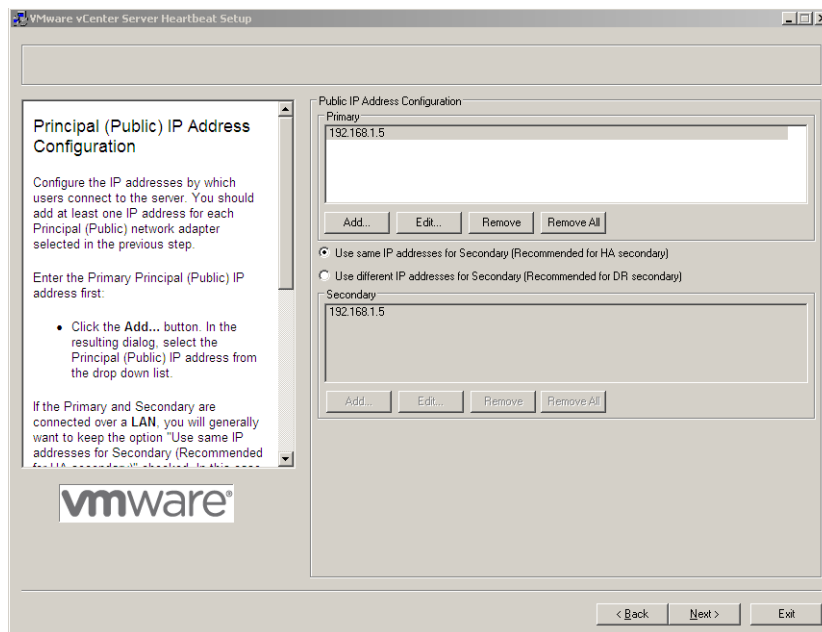
- 17 The **VMware Channel IP Configuration** page prompts you to configure the VMware Channel(s) IP network addresses. Click **Add** for each available channel connection. For the Primary server, select from a drop-down menu that lists all local IP addresses. Type the reciprocal IP address on the Secondary server into the **IP Address On Secondary** text box. You must specify all VMware Channel IP addresses in subnets outside of the normal Principal (Public) IP addressing schema so that VMware Channel traffic routing uses the VMware Channel network card rather than the Principal (Public) network card. Click **OK**. Repeat this step for additional NICs.
- 18 Review and adjust, if necessary, the default channel port. Click **Next**.

NOTE 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. Consult the VMware knowledge base for additional information.

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

NOTE Adjacent IP addresses should be reserved and used for the Principal (Public) IP address and the Management IP addresses for the Primary and Secondary Servers when installing vCenter Server Heartbeat on non-identical nodes on servers running Windows 2008.

- 20 Select **Use same IP addresses for Secondary (Recommended for HA secondary)** and click **Add** to specify the IP address.
- 21 Add the Principal (Public) network address. Click **Next**.



- 22 The vCenter Server Heartbeat server pair can be administered remotely on client machines using the vCenter Server Heartbeat Console. The vCenter Server Heartbeat Console connects to an 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**.
- 23 Select the applications to protect. All licensed vCenter Server Heartbeat features are listed.
 - If installing vCenter Server only, or vCenter Server locally and the SQL Server on a separate server, select **Protect Virtual Center only**.

- If installing SQL Server remotely, upon completion of the vCenter Server installation locally, repeat the installation procedure at the remote SQL Server location and select **Protect SQL Server Only**.

NOTE When deploying with non-identical nodes, vCenter Server Heartbeat only supports SQL Server installed on a separate server (remotely). Therefore the option **Protect Virtual Center and SQL Server** should *not* be selected. Instead, select **Protect Virtual Center Only** or **Protect SQL Server Only** as appropriate.

- If View Composer is installed, select the **View Composer** check box to provide protection for View Composer.
- 24 The **Microsoft Windows Backup Configuration** page prompts you to select options to facilitate the clone of the Primary server onto the Secondary server. The cloning process requires pertinent components of the Primary server for restoration on to the Secondary server. With the Pre-Clone technique selected, Setup backs up two small files, nfsetup.dat and primary.csv, from the Primary server and restores them to the Secondary server for proper configuration..

You have the following options:

- For installation on Windows Server 2003, continue with [Step a](#) below.
- For installation on Windows Server 2008, go to [Step d](#) of [Step 24](#).

Continue with [Step a](#).

- To perform a direct backup, click **Map Network Drive** and specify a network mapping to the Secondary server. Type the path or **Browse** to the location to receive the backup file.
- Select an appropriate drive letter for the mapping and specify the required share on the Secondary server using the channel address of the Secondary server as the server name, for example: \\10.0.0.6\Backup.
- Specify the path to an appropriate location for storing the backup file by either manually typing the path into **Backup File Folder** or click **Browse** to locate the folder or network mapping. Continue with [Step 25](#).
- Select a location to place the backup files through the **Microsoft Windows Backup Configuration** page. When installing into a Windows Server 2008 environment, you must specify a UNC path to the backup file location. Type a UNC path to a location using the machine name or IP address and shared folder into the **Folder** text box, for example: \\10.0.0.16\Backup. Type a **User** and **Password** that grants access to the shared folder. Click **Next**.

With both Windows Server 2003 and Windows Server 2008, vCenter Server Heartbeat takes the backup using the Windows Volume Shadow Service and does not stop services, thereby preventing downtime. Click **Next**.

- 25 Review the summary of options and configuration information for the installation. Click **Next**.
- 26 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 Report pane displays the results of the pre-install checks.
- 27 If some 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**.

NOTE The Progress pane on the **Pre-Install Checks** page displays the progress of these checks. When finished, the Report pane displays the results.

- 28 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. Setup also installs Heartbeat Diagnostics and configures it with the default settings.

NOTE If a previous version of Heartbeat Diagnostics is detected, vCenter Server Heartbeat Setup updates it to the current version. To learn more about Heartbeat Diagnostics, see *Getting Started with Heartbeat Diagnostics* on the VMware Web site.

- 29 Click **Next** after vCenter Server Heartbeat components are complete.
- 30 The vCenter Server 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 **Continue Anyway** (Windows Server 2003) or **Install** (Windows Server 2008). 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 vCenter Server Heartbeat Packet Filter driver is applied to all Principal (Public) network cards present on the machine. The vCenter Server Heartbeat Packet Filter is not applied to the network cards forming VMware Channel connections as these cards maintain unique IP addresses irrespective of the role of the server. vCenter Server Heartbeat also disables NetBIOS on the Channel NIC(s) to prevent domain name conflicts on the subnet.

- 31 When the Setup wizard confirms the successful completion of the installation, click **Finish**.
- 32 The Configure Server wizard is launched and allows you to configure the Primary server for use with non-identical nodes.
- 33 Click the **Public** tab and select **Non-Identical (Updates MS DNS)** or **Non-Identical** (for Locked Down mode or non-Microsoft DNS server) as appropriate.

NOTE If installing into an environment that uses Windows Server 2008 R2 for DNS, you must configure a security level on the DNS server that permits changes to DNS.

- 34 Enter the **Service Name** for the vCenter Server or SQL Server.

NOTE The *Service Name* is the DNS name by which application clients connect to the application. Normally this is the original name of the vCenter Server or SQL Server. There is only one *Service Name* and it is the same on all servers in the cluster.

- 35 In the **NIC** drop-down, select the Principal (Public) NIC.
- 36 In the **Public IP** drop-down, select the Principal (Public) IP address assigned to the Principal (Public) NIC.
- 37 In the first **Mask** field, enter the Subnet Mask of the Principal (Public) IP address.
- 38 In the **Passive IP** field, enter a reserved Management IP address for the Primary server.

NOTE The Management IP address is unique for each server in the cluster.

- 39 In the second **Mask** field, enter the Subnet Mask of the Management IP address.
- 40 Click **Finish**. Do not start vCenter Server Heartbeat.

Secondary Server

The process of installing vCenter Server Heartbeat on the Secondary server is similar to installing vCenter Server Heartbeat on the Primary server.

To install vCenter Server Heartbeat on the Secondary server

- 1 Before powering on the cloned image, edit the image 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 VMware Channel virtual network adapter.
 - c Power on the Secondary (previously cloned) server image.
 - d After the Secondary server starts, open **Network Connections**, right-click the VMware Channel network connection, and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**.
 - e Configure the appropriate VMware Channel IP address and Subnet Mask. Click **Advanced**
 - f Click the **WINS** tab, select **Disable NetBIOS over TCP/IP** and Click **OK** three times to close the dialogs.
 - g Right-click the Principal (Public) network connection and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**. Configure the Principal (Public) IP address (same as the Primary server), 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 VMware Channel virtual network adapter and select the **Connected** and **Connect at power on** check boxes. IP communications with the Secondary server go through the VMware Channel.

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

- 2 To install the vCenter Server Heartbeat on the Secondary server, execute the WinZip self-extracting file to start the installation process. The **Setup Introduction** dialog appears. Review the information and click **OK**.

NOTE If you click **Exit** after Setup has started, you are prompted to save your settings. When you run the self-extracting WinZip file again later, you will be asked if you want to use the previously saved configuration.

- 3 The **WinZip Self-Extractor** dialog appears. Click **Setup** to continue.
- 4 The **Setup Type** page appears. As with the installation on the Primary server, select **Install VMware vCenter Server Heartbeat** and click **Next**.

NOTE The left pane of each page in the setup wizard provides information about the setup process.

- 5 Select the identity of the server on the **Physical Hardware Identity** page. Select **Secondary** as the server identity and click **Next**.

NOTE If .Net 2.0 is not currently installed on the server, vCenter Server Heartbeat Setup installs this required component, taking some additional time during the installation process.

- 6 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 For Windows Server 2003 installations you can alternatively click **Browse** and locate the folder. On Windows Server 2008 installations, you must use the UNC path.

- 7 The pre-install checks run. Click **Next**.

NOTE The pre-install checks will return the message that the Primary and Secondary server's names match. This is expected and installation will be allowed to continue.

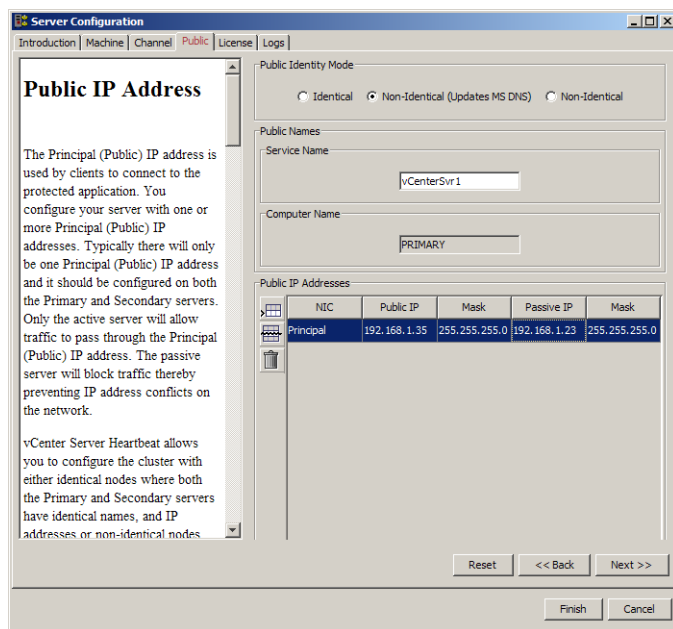
If some pre-install checks are unsuccessful, go back through the wizard, make the necessary changes, and run the pre-install checks again.

- 8 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. Setup also installs Heartbeat Diagnostics and configures it with the default settings. To learn more about Heartbeat Diagnostics see *Getting Started with Heartbeat Diagnostics*.
- 9 The Report pane displays the results of the installation. Click **Next**.
- 10 The progress of the VMware vCenter Server Heartbeat Packet Filter installation is displayed. Click **Next**.
- 11 The Packet Filter is installed on the Principal (Public) NIC. Once complete, the Principal (Public) network adapter can be reconnected. Right-click the Secondary server image name and select **Edit Settings**.
- 12 Select the Principal (Public) virtual network adapter, select the **Connected** and **Connect at power on** check boxes, and click **OK**.
- 13 In the **Channel Adapter Identification** page, select the appropriate adapter and review the IP address configuration in the lower pane. Click **Next**.
- 14 When using the Pre-Clone installation technique, although you previously configured the IP address of the Principal (Public) network connections, you can make any last minute changes on the Secondary server through vCenter Server Heartbeat. Click **Next**.
- 15 The **Duplicate Installation Complete** page is displayed. Do not select the **Start vCenter Server Heartbeat** check box. Click **Finish**.
- 16 The Configure Server wizard is launched and allows you to configure the Secondary server for use with non-identical nodes.
- 17 Click the **Public** tab and select **Non-Identical (Updates MS DNS)** or **Non-Identical** (for Locked Down mode or non-Microsoft DNS server) as appropriate.

NOTE If installing into an environment that uses Windows Server 2008 R2 for DNS and you have selected Non-identical (Updates MS DNS), you must configure a security level on the DNS server that permits changes to DNS.

- 18 Enter the **Service Name** for the vCenter Server or SQL Server.

NOTE The *Service Name* is the DNS name by which application clients connect to the application. Normally this is the original name of the vCenter Server or SQL Server. There is only one *Service Name* and it is the same on all servers in the cluster.



- 19 In the **NIC** drop-down, select the Principal (Public) NIC.
- 20 In the **Public IP** drop-down, select the Principal (Public) IP address assigned to the Principal (Public) NIC.
- 21 In the first **Mask** field, enter the Subnet Mask of the Principal (Public) IP address.
- 22 In the **Passive IP** field, enter a reserved Management IP address for the Secondary server.

NOTE The Management IP address is unique for each server in the cluster.

- 23 In the second **Mask** field, enter the Subnet Mask of the Management IP address.
- 24 Click **Finish**. Do not start vCenter Server Heartbeat.
- 25 If you have configured vCenter Server Heartbeat to use non-updating Microsoft DNS servers (Locked Down mode) or non-Microsoft DNS servers, verify that the prepopulated management names and IP addresses to be used are configured and available in the DNS servers before starting vCenter Server Heartbeat for the first time.

Renaming the Servers

Configuration for non-identical nodes in the cluster require unique server names.

To rename the Secondary server

- 1 Navigate to **Start > Administrative Tools > Services** and set the Neverfail Server R2 service to **Manual, Stopped**, and close the dialog.
- 2 Right-click the Secondary server image and select **Edit Settings**.
- 3 Disable the virtual network adapters for both the VMware Channel and Principal (Public) NICs.
- 4 Open Network Connections, right-click the Principal (Public) network connection and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**.

- 5 Change the IP address to the match that of the Secondary management IP address previously entered in the Configure Server wizard. Click **OK** twice to close the dialogs.
- 6 Navigate to the server's **System Properties**, select the **Computer Name** tab, and click **Change** to rename the Secondary server and join a Workgroup. When requested, restart the server.
- 7 Right-click the Secondary server image and select **Edit Settings**.
- 8 Re-enable the virtual network adapters for both the VMware Channel and Principal (Public) NICs.
- 9 Navigate to the server's **System Properties**, select the **Computer Name** tab, and click **Change** to join the domain. When requested, restart the server.

To rename the Primary Server

- 1 Navigate to **Start > Administrative Tools > Services** and set the Neverfail Server R2 service to **Manual, Stopped**, and close the dialog.
- 2 Navigate to the server's **System Properties**, select the **Computer Name** tab, and click **Change** to rename the Primary server. When requested, restart the server.

Post Installation

On both the Primary and Secondary servers, navigate to **Start > Administrative Tools > Services** and set the Neverfail Server R2 service to **Automatic**, and close the dialog. See [“Post Installation Configuration”](#) on page 60.

vCenter Server Heartbeat Console

To administer a pair of servers you must connect to them through the vCenter Server Heartbeat Console. vCenter Server Heartbeat Console does not connect until vCenter Server Heartbeat initializes.

You can start vCenter Server Heartbeat Console from any server in the vCenter Server Heartbeat Pair.

To start vCenter Server Heartbeat Console

- 1 Right-click the VMware vCenter Server Heartbeat interactive status icon on the Windows tool tray (located on the right side of the Windows tool bar). The vCenter Server Heartbeat quick access menu opens.
- 2 Select **Manage Server**. The vCenter Server Heartbeat Console opens in a window and shows the Heartbeat Servers (overview) pane.

Alternatively you can start vCenter Server Heartbeat Console from the VMware program group on the Windows Start menu. This is the only method supported if vCenter Server Heartbeat Console has been installed on a workstation that is not part of the Pair.

Navigate vCenter Server Heartbeat Console

After vCenter Server Heartbeat Console is running, use the navigation panel on the left of the vCenter Server Heartbeat Console window to view and select Groups and Pair connections you can manage with vCenter Server Heartbeat Console.

NOTE A Group is an arbitrary collection of vCenter Server Heartbeat Pairs used for organization.

A Connection, or Pair Connection allows vCenter Server Heartbeat Console to communicate with a vCenter Server Heartbeat Pair either on the same machine or remotely.

See [“Add a vCenter Server Group”](#) on page 59 and [“Add a New Connection”](#) on page 59 for information on how to add Groups and Pair Connections to vCenter Server Heartbeat Console.

The selection of Group or Pair you make in the navigation panel “points” the vCenter Server Heartbeat Console to that Group or Pair and vCenter Server Heartbeat Console provides information related to only the selected Group or Pair. To avoid confusion, pay particular attention to the selection in the navigation panel when you are managing more than one Group or Pair.

NOTE Groups and Pairs are not automatically detected by vCenter Server Heartbeat Console. Each Group or Pair you want to manage must be added to vCenter Server Heartbeat Console before you can use it to view status or change settings for that Group or Pair Connection.

Select a Pair in the navigation panel of vCenter Server Heartbeat to show a set of tabs and sub-tabs that offer detailed status and control of the associated vCenter Server Heartbeat servers in the Pair.

Add a vCenter Server Group

The Add Group feature in vCenter Server Heartbeat Console allows you to add new vCenter Server Heartbeat Groups to manage.

To add a vCenter Server Heartbeat Group

- 1 Open vCenter Server Heartbeat Console and click **Add Group** in the tool bar, select **Add Group** from the **File** menu, or right-click an existing group in the navigation panel and select **Add Group** from the menu.
- 2 Type the name for the new group into the text box and click **OK**. The newly created group appears in the navigation panel on the left of the vCenter Server Center Heartbeat window.

Add a New Connection

The Add Connection feature in the vCenter Server Heartbeat Console allows you to add a new Pair Connection to an existing vCenter Server Heartbeat Group.

NOTE When a you attempt to connect to vCenter Server Heartbeat for the first time, you are presented the option to accept the SSL certificate from the server. To continue connecting to vCenter Server Heartbeat, you must accept the SSL certificate.

To Add a new connection

- 1 In the navigation panel, select the vCenter Server Heartbeat Group to receive the new connection. Click **Add Connection** in the tool bar, select **Add Connection** from the **File** menu, or right-click an existing group in the navigation panel and select **Add Connection** to invoke the **Add Connection** dialog.
- 2 Type the Host Name or IP address for the new connection into the text box, select the Port Number (if different from the default value of 52267), and select a group from the **Add to Group** drop-down list (to add the connection to a Group other than the one currently selected).

NOTE When a you attempt to connect to vCenter Server Heartbeat for the first time, you are presented the option to accept the SSL certificate from the server. To continue connecting to vCenter Server Heartbeat, you must accept the SSL certificate.

- 3 Click **OK**. The newly created connection appears in the navigation panel on the left of the vCenter Server Heartbeat Console window, and the **Server: Summary** page updates to represent any existing network relationships of the added server.

NOTE You may be prompted to login. If so, login using a valid administrator-level Username and Password for the server for which you are adding a connection, and click **OK**.

- 4 Enter the remaining connections necessary to define the new vCenter Server Heartbeat Group.

Post Installation Configuration

Upon completion of installation, a series of tasks must be performed to ensure that vCenter Server Heartbeat is properly configured.

- 1 When protecting SQL Server, verify that the `SetSPN.exe` tool present on both the Primary and the Secondary servers at the following locations:
 - On Windows Server 2003 environments, in `Program Files\Support Tools`. If Support Tools are not installed on your system, download them from <http://support.microsoft.com/?kbid=926027> and copy `SetSPN.exe` to `<install_path>\R2\bin`.
 - On Windows Server 2008 environments, in `Windows\System32`. This is normally present as a component of the Windows 2008 operating system.

`SetSPN.exe` is a Microsoft command-line tool that reads, modifies, or deletes the Service Principal Names (SPN) directory property for an Active Directory service account and is required to be present on both servers prior to starting vCenter Server Heartbeat for the first time.

- 2 Start vCenter Server Heartbeat on the Primary server. Right-click the vCenter Server Heartbeat System Tray icon and select **Start VMware vCenter Server Heartbeat**. The icons change from a double dash to a **P**, indicating the server is the Primary server, and an **A** indicating the server is acting in an active role.
- 3 Start vCenter Server Heartbeat on the Secondary server. Right-click the vCenter Server Heartbeat System Tray icon and select **Start VMware vCenter Server Heartbeat**. The icon changes from a double dash to an **S**, indicating that the server is the Secondary server, and a dash (-), indicating that the server is in a passive role.

The Primary and Secondary servers establish a handshake and commence replication.

- 4 Verify that Nslookup resolves as shown below:
 - Nslookup resolves Service Name to Public IP
 - Nslookup resolves Primary Name to Public IP
 - Nslookup resolves Secondary Name to Secondary Passive IP

If vCenter Server only was installed and you want to install a separate SQL Server, repeat the installation process for the Primary and Secondary servers at the remote site and select **Protect SQL Server Only**.

- 5 To install vCenter Server Heartbeat on SQL Server when installed on a separate host from the vCenter Server, go to [“Primary Server”](#) on page 32

Configuring VirtualCenter Plug-in with the Correct Credentials

After installation is complete, you must enter the credentials for an account with rights to the Virtual Infrastructure.

To add the Virtual Infrastructure credentials

- 1 Navigate to the **Applications: Plug-ins** page.
- 2 Select the VirtualCenter Plug-in.
- 3 Click **Edit**.
- 4 Type the Username and Password for an account with rights to the Virtual Infrastructure.
- 5 Click **OK**.

Configuring SQL Server Plug-in to run with the Correct Credentials

- 1 Launch the vCenter Server Heartbeat Console and navigate to the **Applications: Tasks** page.
- 2 Click **User Accounts**. Verify that the user account under which you installed vCenter Server Heartbeat is present in the list of User Accounts. If it is present and is a member of the Domain Admins group, Enterprise Admins group, or has been delegated Administrator rights, go to Step 6.
- 3 In the **User Accounts** dialog, click **Add**.
- 4 Enter the credentials of a domain account that is a member of the Domain Admins group, Enterprise Admins group, or one that has been delegated Administrator rights and click **OK**.
- 5 Once the account has been successfully added to the list, click **Close**.
- 6 In the **Task** pane, select the Network Configuration task *Set SPN (Primary)*.
- 7 Click **Edit**.
- 8 In the **Edit Task** dialog, in the **Run As:** drop-down field, select an account with appropriate rights (the account previously added).
- 9 Click **OK**.
- 10 Repeat the procedure for the Network Configuration task *Set SPN (Secondary)*.
- 11 After successfully configuring the correct credentials, select the *Set SPN (Primary)* task and click **Run Now**.

Installing the View Composer Plug-in

Installation of the View Composer Plug-in can occur during installation of vCenter Server Heartbeat or can be installed post-installation.

To install the View Composer Plug-in after vCenter Server Heartbeat has been installed

- 1 Ensure that View Composer has been installed on both the Primary and Secondary servers with the same configuration settings.
- 2 Launch the vCenter Server Heartbeat Console.
- 3 Navigate to **Applications: Plug-ins** and click **Install**.
- 4 Browse to the plug-in file located at:
<unzipped_folder>\<vCenterServerHeartbeatVersion-x86/x64>\plugins\ViewComposer\ViewComposerNFPlugin.dll.
- 5 Click **OK** to install the View Composer Plug-in.

Installation of Client Tools

vCenter Server Heartbeat allows installation of vCenter Server Heartbeat Client Tools for remote management of vCenter Server Heartbeat clusters.

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

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

To install vCenter Server Heartbeat Client Tools

- 1 Copy the WinZip Self-Extracting file to the client where it is to be installed.
- 2 Double-click the WinZip Self-Extracting file to initiate the installation process. The **Setup Introduction** dialog appears. Review the information and click **OK**.

- 3 The **WinZip Self-Extractor** dialog appears. Click **Setup** to continue.
- 4 The **Setup Type** page appears. Because this is a vCenter Server Heartbeat Client Tools installation, select **Install Client Tools Only** and click **Next**.
- 5 Read the license agreement carefully and select **I accept terms of the License Agreement**. Click **Next**.
- 6 Configure the installation paths. The default installation location is `C:\Program Files\VMware\VMware vCenter Server Heartbeat`, but you can change it by manually typing a path to another install location.

NOTE The path of the VMware installation folder cannot contain Unicode characters. The path of the VMware 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, vCenter Server Heartbeat does not support file or folder names ending with a period "." or space " ".

- Alternatively, click **Browse** to select one of these locations. Select **Create icons on Desktop** and click **Next**.
- 7 Review the summary of options and configuration information for the installation. Click **Next**.
 - 8 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. If the pre-install checks are successful, click **Next**.
 - 9 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. Click **Next** after vCenter Server Heartbeat Client Tools components are complete.
 - 10 The **Client Tools Installation Complete** page is displayed. Click **Finish**.

Appendix – Setup Error Messages

Table A-1. Setup Error Messages

Message	Pri	Sec	Level	Test
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. vCenter Server Heartbeat must not be installed on a domain controller.	Yes	Yes	Critical Stop	Test whether the server is a domain controller.
173 – vCenter Server Heartbeat does not support the '/3GB' switch on Windows 2000 Standard Edition.	Yes	Yes	Critical Stop	Test for /3GB on Windows 2000
175 – vCenter Server Heartbeat requires Windows 2003 Standard Edition SP1 or later if '/3GB' switch is on.	Yes	Yes	Critical Stop	
103 - vCenter Server 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 vCenter Server Heartbeat.	Yes	Yes	Critical Stop	
217 - vCenter Server 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.

Table A-1. Setup Error Messages (Continued)

Message	Pri	Sec	Level	Test
113 - You do not have enough total memory to install vCenter Server Heartbeat on your #1# server. You must have at least 1GB.	Yes	Yes	Critical Stop	
VMware recommend 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 vCenter Server Heartbeat. You must have at least 2GB available.	Yes	Yes	Critical Stop	
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 vCenter Server Heartbeat and must be stopped before vCenter Server 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	

Glossary

A **Active**

The functional state or role of a server visible through the network by clients running protected applications and servicing client requests.

Alert

A notification 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 among proprietary services. vCenter Server Heartbeat switchovers and failovers require no changes to AD, resulting in switchover and failover times measured in seconds.

Active – Passive

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

Active Server Queue

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

Advanced Configuration and Power Interface (ACPI)

A specification that dictates how the operating system can interact with hardware using power saving schemes. Primary and Secondary servers must have the same ACPI compliance.

Asynchronous

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

B **Basic Input/Output System (BIOS)**

The program a personal computer's microprocessor uses to start the computer system 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.

C **Cached Credentials**

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

Channel Drop

An event in which the dedicated communications link between the Primary and Secondary server 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 VMware Channel.

Cloned Servers

Two servers in a pair with the same configuration settings, names, applications, Security Identifiers (SIDs) and IP addresses, following the installation of vCenter Server Heartbeat.

Cloning Process

The vCenter Server Heartbeat process whereby all installed applications, configuration settings, the machine name, security identifier (SID), and IP address are copied to a second server.

Crossover Cable

A network cable that crosses transmit and receive lines.

D Data Replication

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

Device Drivers

A program that controls a hardware device, linking it to the operating system.

Disaster Recovery (DR)

A term indicating how you maintain and recover data in light of a disaster such as a hurricane or fire. vCenter Server Heartbeat achieves DR protection by placing the Secondary server at an offsite facility and replicating the data through a WAN link.

DNS (Domain Name System) Server

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

Domain

A logical group of client server based machines where the administration 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 2000 and above domains.

F Failover

The process by which the 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 server crash.

Full System Check (FSC)

The internal process programmatically started at the initial connection of a server pair or manually triggered through the vCenter Server Heartbeat Console. The FSC verifies the files and registry keys, and synchronizes 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.

G Graceful (Clean) Shutdown

vCenter Server Heartbeat shuts down with no data loss after completing replication using the vCenter Server Heartbeat Console.

- H** **Hardware Agnostic**
A key vCenter Server Heartbeat feature enabling the use of servers from different manufacturers, models, and processing power in a single vCenter Server Heartbeat server pair.
- Heartbeat**
The packet of information issued by the passive server across the VMware Channel, which the active server responds to, indicating its presence.
- Heartbeat Diagnostics**
The umbrella name for the VMware process and tools used to check the production server health and applicability to the implementation of the vCenter Server Heartbeat solution.
- 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 used to address a problem in a product.
- I** **Identical Nodes**
The use of two servers identical in name, IP address, and security identifier (SID).
- Identity**
The reference of a server's position in the server pair based upon hardware, either the Primary server or the Secondary server.
- L** **Low Bandwidth Module (LBM)**
A vCenter Server Heartbeat Module that compresses and optimizes data replicated between a Primary and Secondary server, thereby delivering maximum data throughput and improving application response time on congested WAN links.
- M** **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**
One physical Secondary server (hosting more than one virtual server) can provide protection to multiple physical Primary servers.
- N** **Network Monitoring**
Monitoring the active server's capability to communicate with the rest of the network by polling defined nodes around the network at regular intervals.
- Non-Identical Nodes**
Two servers in a cluster using differing names, Passive IP addresses, and security identifiers (SIDs).
- P** **Passive**
The functional state or role of a server that is not delivering service to clients and is hidden from the rest of the network.
- 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 passive server's disk or registry.

Pathping

A route-tracing tool that sends 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. When starting the computer, Plug and Play (PnP) configures the necessary IRQ, DMA and I/O address settings for the attached peripheral devices.

Plug-in

An optional module that can be installed into a vCenter Server Heartbeat server to provide additional protection for a specific application.

Pre-Installation Checks

A list of system and environmental checks performed before the installation of vCenter Server Heartbeat.

Principal IP address

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

Principal NIC

The network card that hosts the Principal IP address.

Protected Application

An application protected by vCenter Server Heartbeat.

Q**Quality of Service (QoS)**

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

R**Remote Desktop Protocol (RDP)**

This multi-channel protocol connects 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 VMware Channel, and applying them to the passive server so both servers are maintained in a synchronized state.

Role

The functional state of the server in the pair that can be either active or passive.

Rule

A set of actions vCenter Server Heartbeat to perform when defined conditions are met.

S**Security Identifier (SID)**

A unique alphanumeric character string that identifies each operating system and each user in a network of Windows NT, Windows Server 2000, Windows Server 2003, and Windows Server 2008 systems.

Server Monitoring

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

Server Pair

The generic term used to describe the coupling of the Primary and Secondary server in vCenter Server Heartbeat.

Shared Nothing

A key vCenter Server Heartbeat feature whereby hardware is not shared between the Primary and Secondary servers, thus preventing a single point of failure.

SMTP

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

Split-brain Avoidance

A unique feature of vCenter Server Heartbeat that uses various checks to overcome a scenario where both 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 where both the Primary and Secondary servers in a vCenter Server Heartbeat server pair are operating in the active mode and attempting to service clients, causing different data updates to be applied independently to each server.

SSL

(Secure Sockets Layer) establishes a secure session by electronically authenticating each end of an encrypted transmission.

Subnet

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

Storage Area Network (SAN)

A high-speed special-purpose network or (sub-network) 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 VMware Channel from the active server to the passive server. The data on the passive server is a mirror image of the protected data on the active server, a required condition for data replication on a vCenter Server Heartbeat server pair.

System State

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

T**Task**

An action performed by vCenter Server Heartbeat when defined conditions are met.

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 the computer and a specified destination computer.

U**Ungraceful (Unclean) Shutdown**

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

Unprotected Application

An application that is not monitored or its data replicated by vCenter Server Heartbeat.

V VMware Channel

The IP communications link used by vCenter Server Heartbeat for heartbeat and replication traffic.

VMware vCenter Server Heartbeat

The core replication and system monitoring component.

VMware vCenter Server Heartbeat Packet Filter

The network component installed on both servers that controls network visibility.

VMware vCenter Server Heartbeat Switchover and Failover Process

A vCenter Server Heartbeat unique process whereby the passive server gracefully (Switchover) or unexpectedly (Failover) assumes the role of the active server providing application services to connected clients.

Virtual Private Network (VPN)

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

VMware Web Site

The VMware web site dedicated to support partners and customers providing technical information, software updates, and license key generation.

W Windows Management Instrumentation (WMI)

A management technology using 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, and groups.