Installation Guide

VMware vCenter Server Heartbeat 6.4 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-000727-00

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

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

Contents

Getting Started

Installation

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). 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* describes the installation process, guides you through installation on the Primary and Secondary servers, and through post-installation configuration.
- Appendix A— *Setup Error Messages* lists error messages that may appear during setup and tests that will help you resolve the errors.

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 1

This chapter includes the following topics:

- "vCenter Server Heartbeat Concepts" on page 9
- "vCenter Server Heartbeat Switchover and Failover Processes" on page 13

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) for High Availability or Wide Area Network (WAN) for Disaster Recovery, providing the 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 Principal (Public) IP address or where the Primary and Secondary servers share the Principal (Public) IP address.

When deployed, one of the servers performs the role of the active server that is visible on the Public network while the other is passive and hidden from the Public network but remains as a ready-standby server. The Secondary server has 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. Only one server can display the Principal (Public) IP address and be visible on the Public network at any given time. 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.

vCenter Server Heartbeat provides continuous access to the passive server simultaneously while the active server continues to service clients allowing 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.

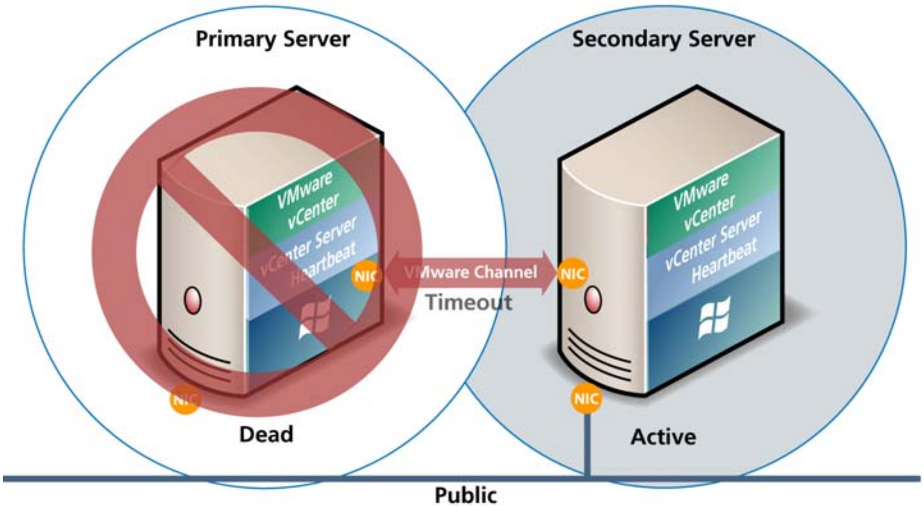
vCenter Server Heartbeat provides all five protection levels continuously, ensuring all facets of the user environment are maintained at all times, and that the network (Principal (Public) network) continues to operate through as many failure scenarios as possible.

Server Protection

vCenter Server Heartbeat provides continuous availability to end users through a hardware failure scenario or operating system crash. Additionally, vCenter Server Heartbeat ensures users are provided with a replica server 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 the same role as the Primary server.

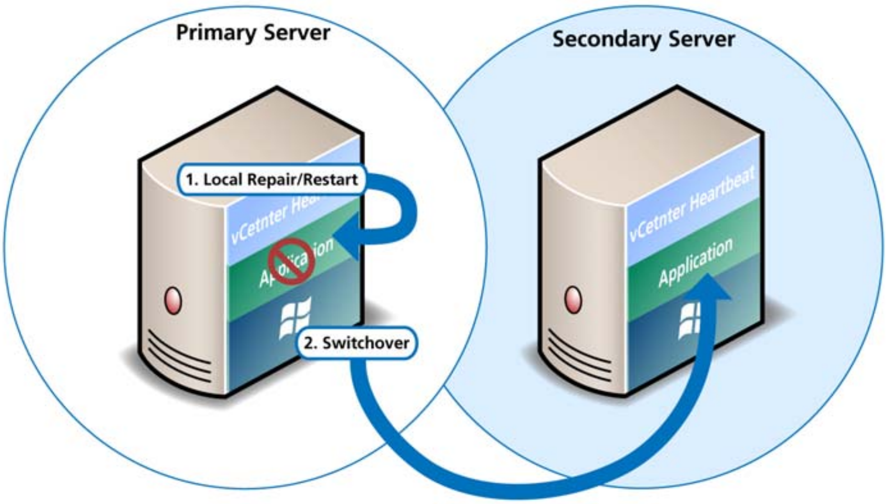
Application Protection

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 13 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.

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.

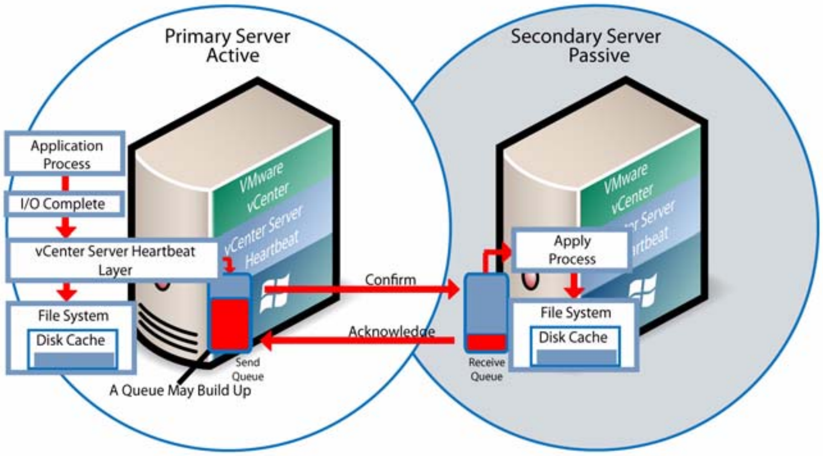
In addition to monitoring application services, vCenter Server Heartbeat can monitor specific application attributes to ensure that they remain within normal operating ranges. Similar to application monitoring, various rules can be configured to trigger specific corrective actions whenever these attributes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

Figure 1-3. Apply Process



Communications

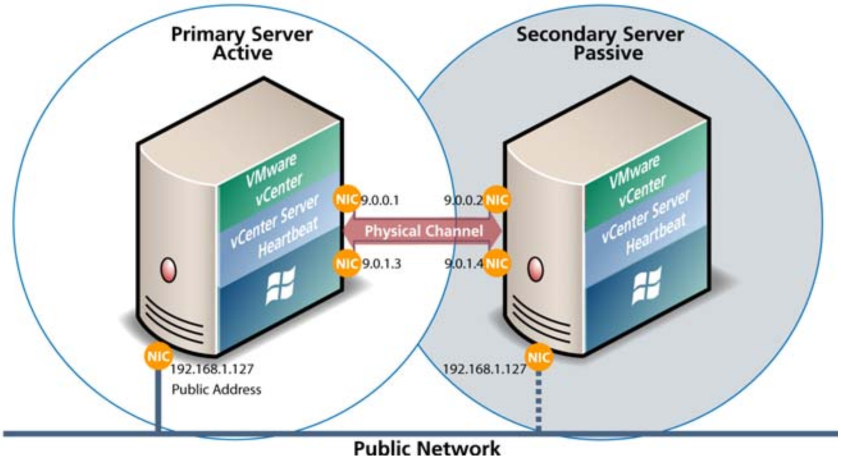
The VMware Channel is a crucial component of the setup and can be configured in a number of ways.

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.

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. Following restore and after the vCenter Server Heartbeat installation completes (runtime), NetBIOS is disabled across the channel(s).

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.

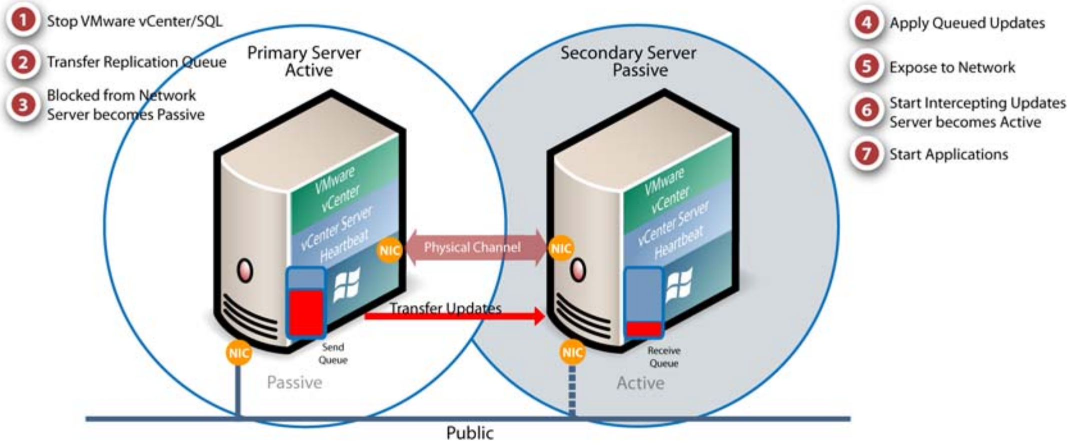
vCenter Server Heartbeat Switchover and Failover Processes

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 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.

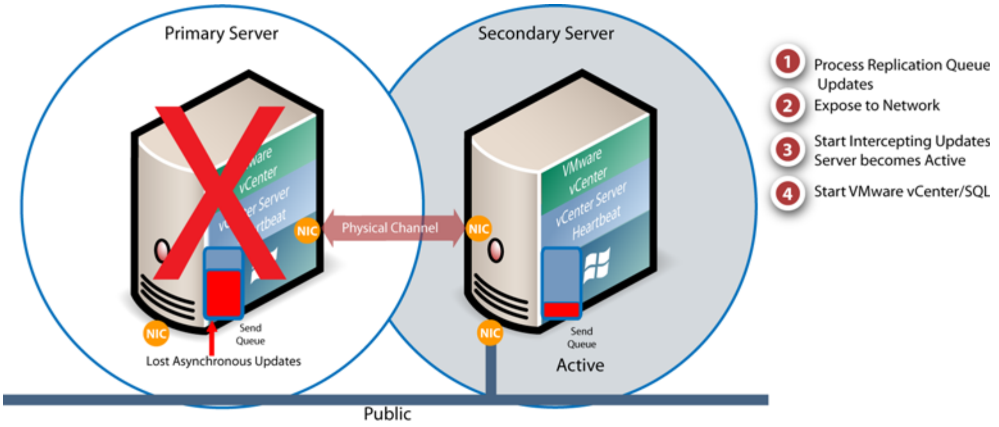
Like managed switchover, auto-switchover changes the server roles but then stops vCenter Server Heartbeat on the previously active server to allow the administrator to investigate the cause of the auto-switchover and verify the integrity of the data.

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


Primary Server
Secondary Server
1 Process Replication Queue Updates
2 Expose to Network
3 Start Intercepting Updates Server becomes Active
4 Start VMware vCenter/SQL
VMware vCenter vCenter Server Heartbeat
NIC
Physical Channel
NIC
NIC
NIC
Send Queue
Send Queue
Lost Asynchronous Updates
Active
Public

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 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**.

Installation

vCenter Server Heartbeat Implementation 2

This chapter includes the following topics:

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 its Database 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.

- Supported vCenter Server Versions
  - vCenter Server 4.0 Update 1
  - vCenter Server 4.0 Update 2
  - vCenter Server 4.0 Update 3
  - vCenter Server 4.1
  - vCenter Server 4.1 Update 1
  - vCenter Server 5.0
  - vCenter Server 5.0 Update 1
- Operating Systems
  - Windows Server 2003 x86 Standard/Enterprise/Datacenter SP1 and SP2
  - Windows Server 2003 x64 Standard/Enterprise/Datacenter SP2
  - Windows Server 2003 R2 x64 Standard/Enterprise/Datacenter SP2
  - Windows Server 2008 x86 Standard/Enterprise/Datacenter SP1 and SP2
  - Windows Server 2008 x64 Standard/Enterprise/Datacenter SP1 and SP2
  - Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1

  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 the Primary server is a member of the domain. The Domain for the Primary server will not change throughout the installation process although the Primary and Secondary server names will be changed as part of the installation procedure.
- 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.

- When installing into a Windows Server 2008 or 2008 R2 environment, verify that Windows Server Backup Feature and Command Line Tools have been installed on the Primary and Secondary servers prior to installing vCenter Server Heartbeat. Installation of Windows Server Backup Feature and Command Line Tools will also install Windows PowerShell.

Server Architecture Options

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

Virtual to Virtual

Virtual to Virtual is the supported architecture if 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.

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 Virtual to Virtual 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

The Physical to Virtual 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 Physical to Virtual 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.

- 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

The Physical to Physical architecture is used in environments where both the Primary and Secondary servers are physical servers. Use of Physical to Physical limits installation options as it requires cloning using vCenter Server Heartbeats native cloning during the installation process. This architecture requires attention to detail when preparing for installation as both hardware and software must meet specific prerequisites.

Primary Server

The Primary server must meet the following requirements:

- Hardware as specified in "Common Requirements" on page 20.

- Software as specified in "Common Requirements" on page 20.

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 technologies depending on the selected server architecture.

Cloning Prior to Installation

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

- VMware vCenter Converter for "Physical to Virtual" on page 21.
- VMware vCenter virtual machine cloning for "Virtual to Virtual" on page 21.

Cloning During Installation

Installation of vCenter Server Heartbeat provides support for NTBackup on Windows 2003 and Wbadmin on Windows Server 2008 for automated cloning during the installation process. The process is automated but requires meeting all prerequisites for the Secondary server specified in "Physical to Physical" on page 21.

Application Component Options

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

- 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 Sever
  - 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 5.0
  - VMware vCenter Server
  - VMware Guided Consolidation Service
  - VMware License Sever
  - 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
  - VMware Policy Based Storage Management Service
  - VMware Inventory Service
  - VMware USB Arbitration Service
  - VMware vSphere Web Client
  - VMware vSphere ESXi Dump Collector
  - VMware vSphere ESXi Dump Collector Web Server
  - VMware vSphere Auto Deploy Waiter
  - VMware vSphere Authentication Proxy
  - VMware vSphere Authentication Proxy Adapter
  - VMware Syslog Collector
- 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
  - Microsoft SQL Server 2008 R2

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.

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. 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.

Switchover/Failover

vCenter Server Heartbeat will not attempt to update DNS and therefore, the Administrator must pre-populate 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 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 a temporary IP address different from the Principal (Public) IP address but within the same subnet
- 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.

DNS Server Updated During Switchover/Failover

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.

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

Architecture	Network		Clone Technique		Component		
	LAN	WAN	Prior to Installation	During Installation	vCenter Server w/SQL Local	vCenter Server w/SQL Remote	vCenter Server Only
Virtual to Virtual	X	X	X		X	X	X
Physical to Virtual	X	X	X		X	X	X
Physical to Physical	X	X		X	X	X	X

Installation Options Checklist

Verify the prerequisites:

Server architecture:

___ Physical to Physical

___ Physical to Virtual

___ Virtual to Virtual

Cloning technology option:

___ Prior to Installation

___ During Installation

Application components to protect:

___ vCenter Server with SQL Server on same host

___ vCenter Server with its Database Server on separate host

___ vCenter Server only

Network environment type:

___ LAN

___ WAN

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 24.

Installing vCenter Server Heartbeat 3

This chapter includes the following topics:

- "Overview" on page 29
- "Installation Process" on page 29
- "Primary Server" on page 29
- "Secondary Server" on page 37
- "Post Installation Configuration" on page 47
- "VMware vCenter Server Heartbeat Console" on page 45
- "Installation of Client Tools" on page 49
- "Uninstall vCenter Server Heartbeat" on page 50

Overview

This chapter discusses the installation process used to implement vCenter Server Heartbeat on Windows Server 2003 or Windows Server 2008. 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.

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

vCenter Server Heartbeat is installed on both the Primary and Secondary server of a vCenter Server Heartbeat Pair. Installation of vCenter Server Heartbeat begins on the Primary server.

NOTE When protecting SQL Server, 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.

To install vCenter Server Heartbeat on the Primary server

1 Having verified all of the environmental prerequisites are met, download the vCenter Server Heartbeat self-extracting file to an appropriate location on the Primary server.

NOTE Ensure that the user is logged into the domain before installing vCenter Server Heartbeat.

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 Navigate to **Start** > **Administrative Tools** > **Services** to launch the Service Control Manager.

7 If protecting vCenter Server 5.0 or later, select the following services and set them to *Manual*.

- VMware VirtualCenter Server
- VMware vSphere Profile-Drive Storage
- vCenter Inventory Service
- VMware VirtualCenter Management Webservices

8 If the Secondary server is to be virtual, clone the Primary server using either VMware vCenter Converter, vCenter virtual machine cloning, 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.

9 Double-click the 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.

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

11 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.

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

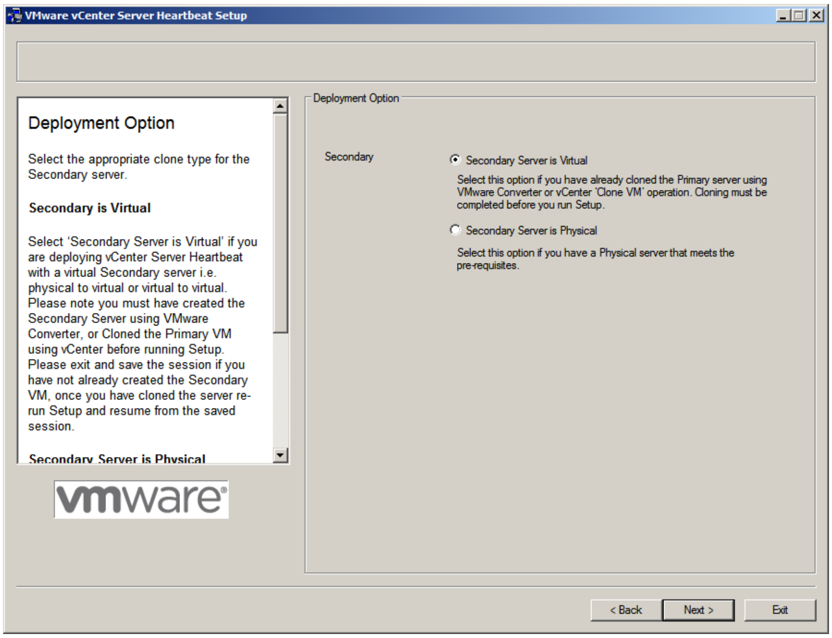
NOTE If .Net 2.0 SP2 is not currently installed on the server, vCenter Server Heartbeat Setup installs this required component, taking some additional time during the installation process.

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

14 vCenter Server Heartbeat prompts you to enter a valid serial number. If you do not enter a valid serial number, vCenter Server Heartbeat installs in the evaluation mode. Click **Add** to enter a valid serial number for production mode or click **Next** to install in the evaluation mode.

15 Select **LAN** or **WAN** for the intended network topology. Click **Next**.

16 Select the Deployment Option.



VMware vCenter Server Heartbeat Setup

Deployment Option

Select the appropriate clone type for the Secondary server.

Secondary is Virtual

Select 'Secondary Server is Virtual' if you are deploying vCenter Server Heartbeat with a virtual Secondary server i.e. physical to virtual or virtual to virtual. Please note you must have created the Secondary Server using VMware Converter, or Cloned the Primary VM using vCenter before running Setup. Please exit and save the session if you have not already created the Secondary VM, once you have cloned the server re-run Setup and resume from the saved session.

Secondary Server is Physical

Deployment Option

Secondary

● Secondary Server is Virtual

Select this option if you have already cloned the Primary server using VMware Converter or vCenter 'Clone VM' operation. Cloning must be completed before you run Setup.

○ Secondary Server is Physical

Select this option if you have a Physical server that meets the pre-requisites.

You have the following options:

- For installations where the Secondary server is virtual, continue with Step 17.
- For installations where the Secondary server is physical, continue with Step 18.

17 Select **Secondary Server is Virtual** if you created a clone of the Primary server prior to running Setup. Click **Next** and go to Step 19.

18 Select **Secondary Server is Physical** if you are going to use a physical Secondary server, click **Next**.

19 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 VMware vCenter Server Heartbeat is installed in a folder that has a path containing Unicode characters, this causes the VMware vCenter Server Heartbeat 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, VMware 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**.

20 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.

21 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.

NOTE If the Secondary server is virtual, you will receive a warning message that the Secondary server cannot be contacted. Disregard the warning and click **No** to proceed.

22 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.

23 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 use 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.

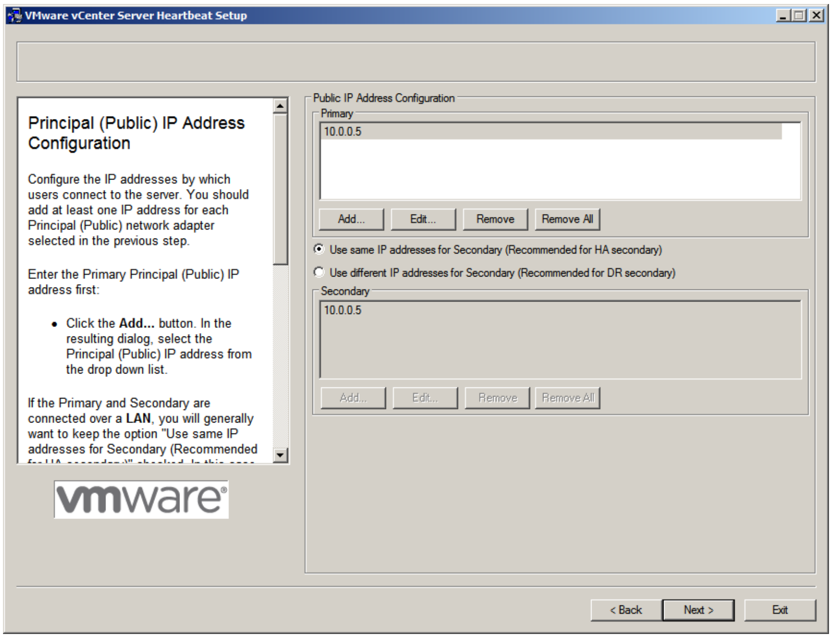
NOTE Adjacent IP addresses should be reserved and used for the Principal (Public) IP address and the Management IP addresses for the Primary and Secondary Servers when installing vCenter Server Heartbeat on servers running Windows 2008.

24 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 LAN installation or same subnet WAN installs, continue with Step 25.
- For a WAN installation with different subnets, go to Step 26.

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



VMware vCenter Server Heartbeat Setup

Principal (Public) IP Address Configuration

Configure the IP addresses by which users connect to the server. You should add at least one IP address for each Principal (Public) network adapter selected in the previous step.

Enter the Primary Principal (Public) IP address first:

- Click the **Add...** button. In the resulting dialog, select the Principal (Public) IP address from the drop down list.

If the Primary and Secondary are connected over a **LAN**, you will generally want to keep the option "Use same IP addresses for Secondary (Recommended

Public IP Address Configuration

Primary: 10.0.0.5

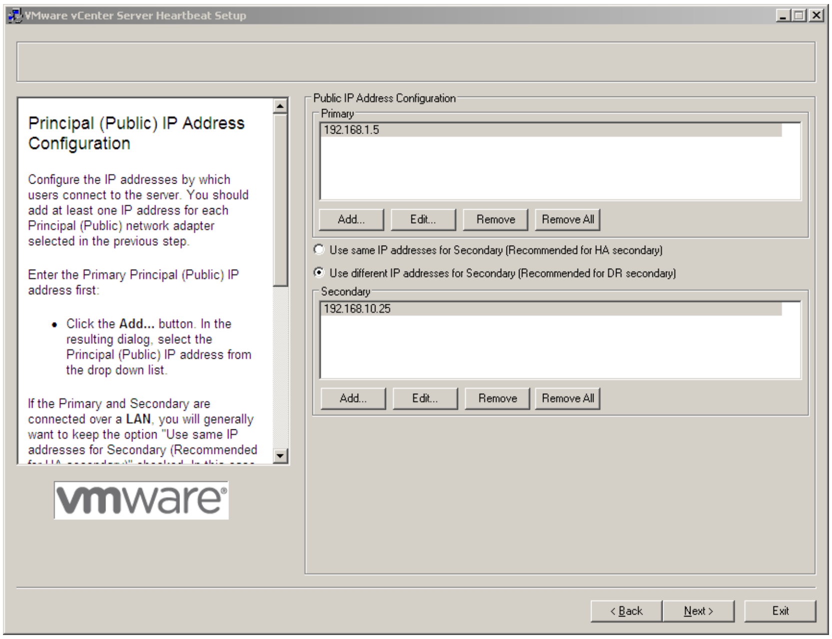
● Use same IP addresses for Secondary (Recommended for HA secondary)

○ Use different IP addresses for Secondary (Recommended for DR secondary)

Secondary: 10.0.0.5

If installing in a LAN or in a WAN that uses the same subnet, go to Step 29.

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



VMware vCenter Server Heartbeat Setup

Principal (Public) IP Address Configuration

Configure the IP addresses by which users connect to the server. You should add at least one IP address for each Principal (Public) network adapter selected in the previous step.

Enter the Primary Principal (Public) IP address first:

- Click the **Add...** button. In the resulting dialog, select the Principal (Public) IP address from the drop down list.

If the Primary and Secondary are connected over a **LAN**, you will generally want to keep the option "Use same IP addresses for Secondary (Recommended

Public IP Address Configuration

Primary: 192.168.1.5

○ Use same IP addresses for Secondary (Recommended for HA secondary)

● Use different IP addresses for Secondary (Recommended for DR secondary)

Secondary: 192.168.10.25

27 Add each Principal (Public) network address until all addresses are present. Click **Next**.

28 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 the 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**.

29 The vCenter Server Heartbeat server pair can be administered remotely on client machines using the vCenter Server Heartbeat Console or using the vSphere plug-in. The vCenter Server Heartbeat Console connects to the IP address of the active server using the default client connection port of `52267`. If this port is already in use, type an available client connection port in the text box. Click **Next**.

30 Select the applications to protect. All licensed vCenter Server Heartbeat features are listed. If View Composer is installed, select the **View Composer** check box to provide protection for View Composer.

NOTE If you are protecting vCenter only or vCenter and SQL Server, provide a Username and Password for an account with rights to Virtual Infrastructure.

- If installing vCenter Server or other componenets such as VMware Update Manager, Support Tools, etc. locally and the SQL Server Database on a separate server, select **Protect Virtual Center only** and click **Next**.
- 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** and click **Next**.
- If installing both vCenter Server and SQL Server locally, select **Protect Virtual Center and SQL Server** and click **Next**.

31 You have the following options:

- For installations where the Secondary server is virtual, go to Step 36.
- For installations where the Secondary server is physical, go to Step 32.

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

33 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.

34 If any of the pre-install checks are unsuccessful, go back through the wizard, make the necessary changes, and run the pre-install checks again. If the pre-install checks are successful, click **Next**.

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

35 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. Click **Next** after vCenter Server Heartbeat components are complete.

NOTE If a previous version of Heartbeat Diagnostics is detected, vCenter Server Heartbeat Setup updates it to the current version.

36 The **Microsoft Windows Backup Configuration** is displayed.

When the Secondary server is virtual, Setup backs up two small files, `nfsetup.dat` and `primary.csv`, into a shared folder from the Primary server and restores them to the Secondary server for proper configuration.

When the Secondary server is physical you are prompted to select options to facilitate the clone of pertinent components of the Primary server onto 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 connection to a shared folder on a partition on the Secondary server.

Backup files can be configured to 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.

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.

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.

37 You have the following options:

- For installation on Windows Server 2003 where the Secondary server is virtual, go to Step 38.
- For installation on Windows Server 2003 where the Secondary server is physical, continue with Step a of Step 37.
- For installation on Windows Server 2008 where the Secondary server is virtual, go to Step d of Step 38.
- For installation on Windows Server 2008 where the Secondary server is physical, go to Step d of Step 37.

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.

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 44.

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, for example:`\\10.0.0.16\Backup`. Type a **User** and **Password** that grants access to the shared folder. Click **Next**. Go to Step 44.

38 When the **Secondary Server is Virtual** has been selected, Setup backs up two small files, `nfsetup.dat` and `primary.csv`, from the Primary server and restores them to the Secondary server during the Secondary server installation for proper configuration.

Continue with Step a.

a To perform a direct backup, create a shared folder on the Primary server to store the back up files. Click **Map Network Drive** and specify a network mapping to the shared folder previously created by typing 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 using the channel address of the Primary 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 go to Step 39.

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**.

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

40 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.

41 If any of the pre-install checks are unsuccessful, go back through the wizard, make the necessary changes, and run the pre-install checks again. If the pre-install checks are successful, click **Next**.

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

42 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.

43 Click **Next** after vCenter Server Heartbeat components are complete. Go to Step 47.

44 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.

45 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.

46 A summary page displays the results of the backup operation. Review the backup report and click **Next**.

47 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**.

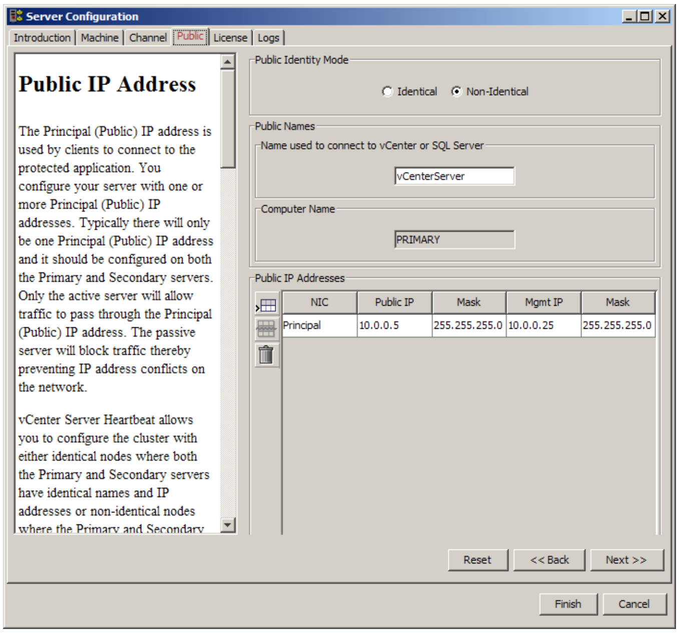
By default, the vCenter Server Heartbeat Packet Filter driver is applied to all Principal (Public) network cards present on the machine. The vCenter Server Heartbeat Packet Filter is not applied to the network cards forming VMware Channel connections as these cards maintain unique IP addresses irrespective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

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

49 The Configure Server wizard is launched.

50 Click the **Public** tab.

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.



Public IP Address

The Principal (Public) IP address is used by clients to connect to the protected application. You configure your server with one or more Principal (Public) IP addresses. Typically there will only be one Principal (Public) IP address and it should be configured on both the Primary and Secondary servers. Only the active server will allow traffic to pass through the Principal (Public) IP address. The passive server will block traffic thereby preventing IP address conflicts on the network.

vCenter Server Heartbeat allows you to configure the cluster with either identical nodes where both the Primary and Secondary servers have identical names and IP addresses or non-identical nodes where the Primary and Secondary

Public Identity Mode: ○ Identical ● Non-Identical

Public Names

Name used to connect to vCenter or SQL Server: vCenterServer

Computer Name: PRIMARY

Public IP Addresses

NIC	Public IP	Mask	Mgmt IP	Mask
Principal	10.0.0.5	255.255.255.0	10.0.0.25	255.255.255.0

51 Enter the **Name used to connect to vCenter or SQL Server**.

NOTE The *Name used to connect to vCenter or SQL Server* 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 *Name used to connect to vCenter or SQL Server* and it is the same on all servers in the cluster.

52 In the **NIC** drop-down, select the Principal (Public) NIC.

53 In the **Public IP** drop-down, select the Principal (Public) IP address assigned to the Principal (Public) NIC.

54 In the first **Mask** field, enter the Subnet Mask of the Principal (Public) IP address.

55 In the **Mgmt IP** field, enter the reserved Management IP address for the Primary server.

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

56 In the second **Mask** field, enter the Subnet Mask of the Management IP address.

57 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

You have the following options:

- If the Secondary server is virtual, continue with Step 1

- If the Secondary server is physical, go to Step 2

1. Before powering on the Secondary (cloned) image, right-click the server image and select **Edit Settings**.

   a. Select the Principal (Public) virtual network adapter and clear the **Connected** and **Connect at power on** check boxes.

   b. Repeat the process on the VMware Channel virtual network adapter.

   c. Power on the Secondary (previously cloned) server image.

   d. On the Secondary server, 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, download vCenter Server Heartbeat to the Secondary server (either physical or virtual) to a suitable location. Execute the 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 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 SP2 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 If the Secondary server is virtual, 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 any of the 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 8.
- If installing on Windows Server 2008, go to Step 29.

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.

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**.

You have the following options:

- If the Secondary server is physical, go to Step 11.
- If the Secondary server is virtual, 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**.

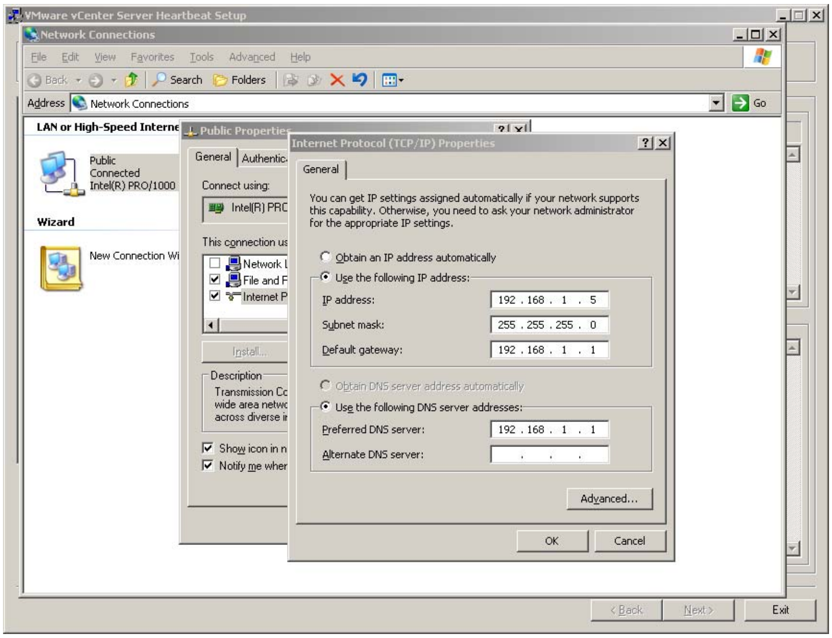
11 In the **Channel Adapter Identification** page, select the appropriate adapter and review the IP address configuration in the lower pane. Click **Next**.

You have the following options:

- If the Secondary server is physical, continue to Step 12.
- If the Secondary server is virtual, go to Step 15.

12 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**.

13 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).



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 5
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server: . . .

14 If in a WAN environment, verify the Secondary Principal (Public) adapter IP address configuration. Click **Next** and go to Step 16.

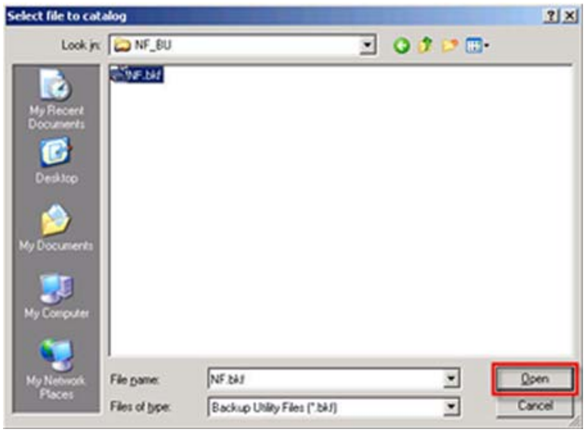
15 When the Secondary server is virtual, although you previously configured the IP address of the Principal (Public) network connections, you can make any last minute changes on the Secondary server through vCenter Server Heartbeat. Click **Next** and go to Step 29.

16 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**.

17 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.

18 Click **Next** in the Restore Wizard. Click **Browse** to locate the previously generated backup file.

19 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**.



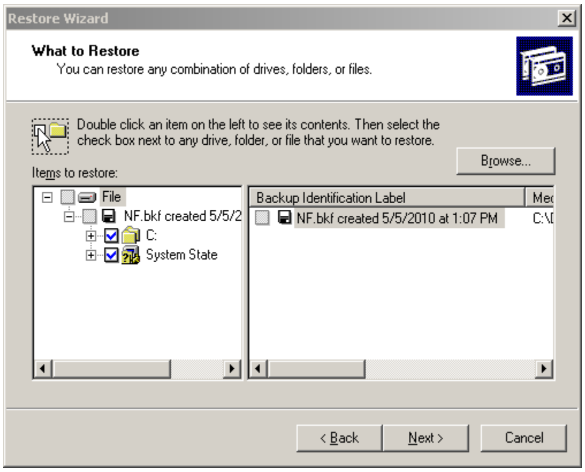
Look in: NF_BU

NF.bkf

File name: NF.bkf

Files of type: Backup Utility Files (*.bkf)

20 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**.



Restore Wizard

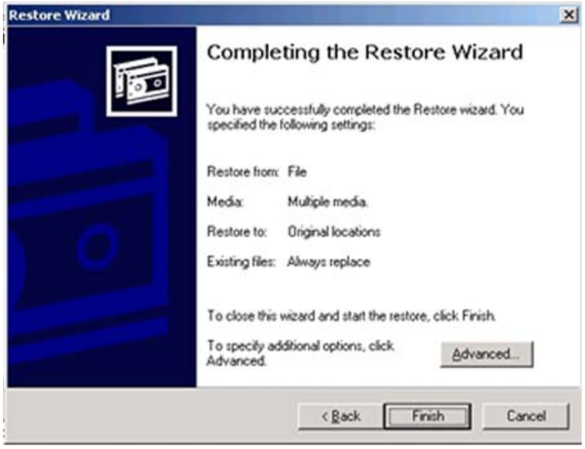
What to Restore

You can restore any combination of drives, folders, or files.

Double click an item on the left to see its contents. Then select the check box next to any drive, folder, or file that you want to restore.

Items to restore:

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



Restore Wizard

Completing the Restore Wizard

You have successfully completed the Restore wizard. You specified the following settings:

Restore from: File

Media: Multiple media.

Restore to: Original locations

Existing files: Always replace

To close this wizard and start the restore, click Finish.

To specify additional options, click Advanced.

22 A warning message alerts you that the restore process is going to overwrite the existing System State files. Click **OK**.

23 When the restoration process completes, click **Close**.

24 To apply the newly restored system state, you must restart the machine. Click **Yes** to restart the server.

25 Following the restart of the server, log in to the Secondary server using a domain administrator account.

26 Plug-and-Play 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.

27 Click **Yes** at each restart prompt to allow each Plug-and-Play cycle to complete.

28 When all Plug-and-Play cycles complete, the vCenter Server Heartbeat Setup is complete.

29 You have the following options:

- For installations on Windows Server 2003, go to Step 42 on page 43.
- For installations on Windows Server 2008 where the Secondary server is physical, continue with Step 30 on page 42.

- For installations on Windows Server 2008 where the Secondary server is virtual, go to Step 40 on page 43

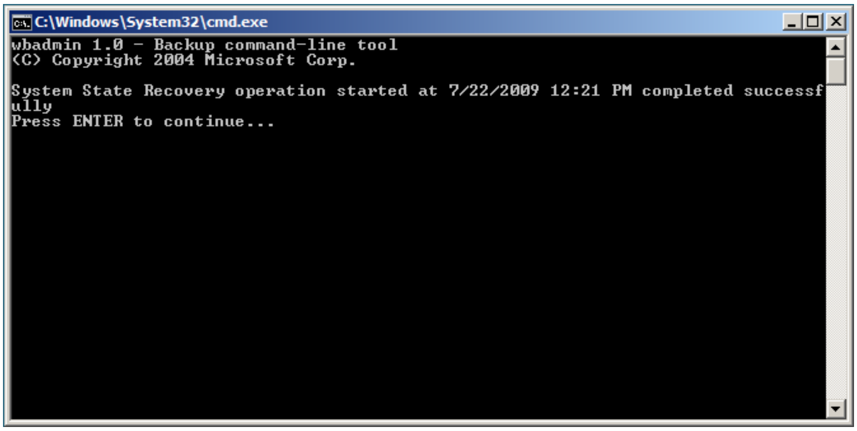
30 The **Microsoft Windows Backup Restore** page is displayed. The **Microsoft Windows Backup Restore** page shows the progress of unbinding the packet filter and disabling NetBIOS from the channel NIC(s). After this process completes, a caution message advises you that the restore process is initiating 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**.

31 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**.

32 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.

33 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 Plug-and-Play cycle to complete.



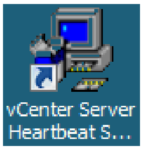
```
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

System State Recovery operation started at 7/22/2009 12:21 PM completed successf
ully
Press ENTER to continue...
```

NOTE Plug-and-Play 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.

34 After all Plug-and-Play 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.



35 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.

36 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**.

37 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**.

38 The **Public Adapter Identification** page is displayed. Select the Principal (Public) connection. Verify that the IP address configuration is correct.

39 The **Duplicate Installation Complete** page is displayed. Do not select the **Start vCenter Server Heartbeat** check box. Click **Finish**. Go to Step 46.

40 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.

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

42 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, go to Step 43.
- If the Secondary server is virtual, 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**.

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

44 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).

45 The **Secondary Installation Complete** page is displayed. Click **Finish**.

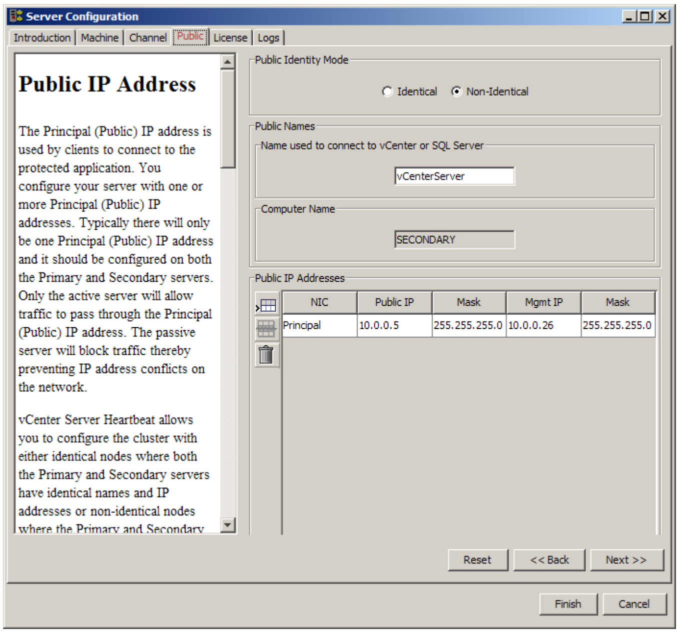
46 The Configure Server wizard is launched and allows you to configure the Secondary.

47 Click the **Public** tab.

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.

48 Enter the **Name used to connect to vCenter or SQL Server**.

> **NOTE** The *Name used to connect to vCenter or SQL Server* 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 *Name used to connect to vCenter or SQL Server* and it is the same on all servers in the cluster.



Server Configuration

Introduction | Machine | Channel | Public | License | Logs

Public IP Address

The Principal (Public) IP address is used by clients to connect to the protected application. You configure your server with one or more Principal (Public) IP addresses. Typically there will only be one Principal (Public) IP address and it should be configured on both the Primary and Secondary servers. Only the active server will allow traffic to pass through the Principal (Public) IP address. The passive server will block traffic thereby preventing IP address conflicts on the network.

vCenter Server Heartbeat allows you to configure the cluster with either identical nodes where both the Primary and Secondary servers have identical names and IP addresses or non-identical nodes where the Primary and Secondary

Public Identity Mode: ○ Identical ● Non-Identical

Public Names

Name used to connect to vCenter or SQL Server: vCenterServer

Computer Name: SECONDARY

Public IP Addresses

NIC	Public IP	Mask	Mgmt IP	Mask
Principal	10.0.0.5	255.255.255.0	10.0.0.26	255.255.255.0

49 In the **NIC** drop-down, select the Principal (Public) NIC.

50 In the **Public IP** drop-down, select the Principal (Public) IP address assigned to the Principal (Public) NIC.

51 In the first **Mask** field, enter the Subnet Mask of the Principal (Public) IP address.

52 In the **Mgmt IP** field, enter a reserved Management IP address for the Secondary server.

> **NOTE** Do not change the IP address for the Principal (Public) NIC. You need only enter the Management IP address in the *Mgmt IP* field. The Management IP address is unique for each server in the cluster.

53 In the second **Mask** field, enter the Subnet Mask of the Management IP address.

54 Click **Finish**. Do not start vCenter Server Heartbeat.

55 Verify that the pre-populated 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

vCenter Server Heartbeat requires unique server names to operate properly. To create the unique names you must rename both the Primary and Secondary servers to ensure proper configuration and prevent name resolution problems when clients attempt to access the vCenter Server application.

For example, before installing vCenter Server Heartbeat your vCenter Server is named “vCenterServer”. During the vCenter Server Heartbeat installation process on “vCenterServer” you clone “vCenterServer” (the Primary server) to create a Secondary server.

After installation you rename the Secondary server to “vCSHB-Secondary” and then rename the Primary server to “vCSHB-Primary”. You then use the Configure Server wizard and identify the *Name used to connect to vCenter or SQL Server* as “vCenterServer” thereby allowing access to vCenter Server on either the Primary or Secondary servers.

To rename the Secondary server

1. Navigate to **Start** > **Administrative Tools** > **Services** and set the VMware vCenter Server Heartbeat 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 *Mgmt* (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 VMware vCenter Server Heartbeat 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.

NOTE The Primary server is currently configured with the Principal (Public) IP address and should not be changed.

Post Installation

On both the Primary and Secondary servers, navigate to **Start** > **Administrative Tools** > **Services** and set the VMware vCenter Server Heartbeat service to **Automatic**, and close the dialog. See "Post Installation Configuration" on page 47.

Resulting IP Configuration

After installing VMware vCenter Server Heartbeat on both the Primary and Secondary servers, the IP addressing configuration should reflect:

- When the Primary server is active
  - Primary (active) server - Principal (Public) IP address and the Primary Management IP address
  - Secondary (passive) server - Secondary Management IP address
- When the Secondary server is active
  - Primary (passive) server - Primary Management IP address
  - Secondary (active) server - Principal (Public) IP address and the Secondary Management IP address

VMware vCenter Server Heartbeat Console

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

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

To start vCenter Server Heartbeat Console

1 Right-click the VMware vCenter Server Heartbeat interactive status icon on the Windows too 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 46 and "Add a New Connection" on page 46 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** form 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 VMware 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 VMware vCenter Server Heartbeat is properly configured.

1 Before starting VMware 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
```

2 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.

NOTE vCenter Server Heartbeat will not attempt to update DNS and therefore, the Administrator must pre-populate the DNS server with entries for the new management names and IP addresses that are to be used. Use adjacent IP addresses for the Principal (Public) IP address and the Management IP address for the Primary and Secondary Servers when installing vCenter Server Heartbeat on servers running Windows 2008.

3 On the Primary server, navigate to **Start** > **Administrative Tools** > **Services** and set the VMware vCenter Server Heartbeat service to **Automatic** and close the dialog.

4 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.

5 On the Secondary server, navigate to **Start** > **Administrative Tools** > **Services** and set the VMware vCenter Server Heartbeat service to **Automatic** and close the dialog.

6 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.

7 Verify that Nslookup resolves as shown below:

   - Nslookup resolves Service Name to Public IP
   - Nslookup resolves Primary Name to Primary Management IP
   - Nslookup resolves Secondary Name to Secondary Management 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**.

8 To install vCenter Server Heartbeat on SQL Server when installed on a separate host from the vCenter Server, go to "Primary Server" on page 29

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

When protecting SQL Server, 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.

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 Administrators group, Enterprise Administrators 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 Administrators group, Enterprise Administrators 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 Post Installation

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.

Configure the Application Timeout Exception

vCenter Server Heartbeat can alert the Administrator if the time taken to start or stop the entire application exceeds the expected time during the following operations:

- vCenter Heartbeat startup
- Shutdown with protected applications
- Switchover
- Failover
- When the Administrator selects **Start Application**
- When the Administrator selects **Stop Application**

NOTE vCenter Server Heartbeat does not issue the timeout warning when it is performing the service restart recovery action provided by the periodic service monitoring. If there are multiple applications installed, vCenter Server Heartbeat will total the individual timeouts set for each application and issue a single *Application Timeout Exception* alert.

Configure timeout settings

NOTE The *Start Timeout* value should be configured according to vCenter inventory size and the *Stop Timeout* value according to inventory size and operational load. For example, if the inventory is large (more than 500 hosts and 15K Virtual machines, the Start time can be 20-30 minutes. Use the *Start Timeout* experienced as a guide to assist in determining the *Stop Timeout* value.

6. Right-click on the application and select **Edit** from the menu or select the application and click **Edit** at the top of the pane to invoke the **Edit Application** dialog.
7. Enter new values into the **Stop Timeout** and **Start Timeout** text boxes or use the arrow buttons to adjust the values (seconds). Click **OK**.

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**.

Uninstall vCenter Server Heartbeat

Under normal conditions it is not necessary to uninstall vCenter Server Heartbeat. Should the need arise, vCenter Server Heartbeat can be uninstalled easily allowing you to retain current log information.

Uninstalling vCenter Server Heartbeat

> **NOTE** You should leave only the currently active server on the network. If the passive server is a virtual machine, the image can be deleted and the uninstall procedure applied only to the active server.

1 From the Windows *Start* menu, navigate to the VMware vCenter Server Heartbeat program group and select *Uninstall or Modify*. The Setup wizard starts and detects the presence of installed components and provides a means for their removal.

2 Select the *Uninstall* option and click **Next**.

3 Follow the instructions provided in the Setup wizard to stop vCenter Server Heartbeat. You can shut down vCenter Server Heartbeat from the system tray icon or from its console.

4 After the application is stopped, click **Next**.

5 Verify that all programs associated with VMware vCenter Server Heartbeat are closed. Click **Next**.

6 The Setup wizard prompts you to select whether to leave the current server on the network. In a typical uninstall process, the active server remains on the network to continue providing application services to end users, and the passive server is removed from the network.

7 Select whether to leave the server on the network or to remove it from the network following completion of the uninstall process.

- If you select *Leave this server on the network after uninstall* and click **Next** to proceed to the next step, the uninstall process starts and the vCenter Server Heartbeat components are removed.
- If you select *Leave this server off the network after uninstall*, the *Rename server to* text box becomes active and you can specify the new computer name for the server that will be renamed. Click **Next** starts the uninstall process.

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

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

8 Click **Next**. The Setup wizard notifies you that VMware vCenter Server Heartbeat and its associated components have been uninstalled from the system.

9 Click **Finish**. A restart is required to finish removing certain components and to apply new settings. When you are prompted to perform this restart, click **Yes**.

10 After the server has restarted, launch a web browser and navigate to `http://<vCenter server name or IP>>/mob`

11 Click on **Content**

12 Click on **ExtensionManager**

13 In the *Properties* pane, identify the values *extensionlist["com.vmware.heartbeat"]* and *extensionlist["com.neverfail.heartbeat"]*

14 In the *Methods* pane, click the **UnregisterExtension** option and a new window will appear.

15 In the *Value* field, type `com.vmware.heartbeat` and click **Invoke Method** to remove the plug-in.

16 In the *Value* field, type `com.neverfail.heartbeat` and click **Invoke Method** to remove the plug-in.

17 Close the pop-up window.

18 Refresh the *Managed Object Type: ManagedObjectReference:ExtensionManager* window and the plug-in should be removed from the list.

19 Repeat the entire uninstall procedure on the other server in the pair to uninstall vCenter Server Heartbeat.

Unattended Installation of vCenter Server Heartbeat

4

This chapter includes the following topics:

Overview

This chapter discusses the unattended 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.

Prior to installing vCenter Server Heartbeat, you must prepare the configuration parameters file used during the unattended installation to achieve your configuration goals.

Installation Process

Setup should only be run after verifying that the server (virtual or physical) has met all of the prerequisites listed in "Common Requirements" on page 20.

Unattended installation of vCenter Server Heartbeat requires use of command line options and a configuration parameters file. The configuration parameters file must be created prior to running the unattended installation to provide the configuration parameters for Setup.

Unattended Installation Command Line Usage

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

```
start /wait Setup [-h]
```

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

Table 4-1. Command Line Parameters

Parameter	Description
`–h`	Displays this usage information
`–f:<parameter file>`	Uses a file of parameters to run **Note:** if the file name/path contains any white space (space, tab) or special characters(-, /, etc.) then it must be enclosed in quotes "..."
`–ni`	:Not interactive, suppresses the Graphical User Interface. This instructs Setup not to use the Graphical User Interface. If this parameter is not specified but a parameter file is specified, the Graphical User Interface pages will be fully populated and require that the **Next** or **Proceed** button be clicked and any popup dialog boxes be acknowledged.
`–sp`	Suppress Progress (Only for Non- interactive)
`–se`	Suppress Errors (Only for Non- interactive)
`–sw`	Suppress Warnings (Only for Non- interactive)
`–di`	Display Info (Only for Non- interactive)
`–DNSPassword:<password>`	The password used for DNSUpdate
`–BACKUPPassword:<password>`	The password used for WBADMIN
`–uninstall`	Do not use unless instructed to do so
`–drvInstall`	Do not use unless instructed to do so
`–secondaryInstall`	Do not use unless instructed to do so

NOTE Only the DOS shell requires the "`start /wait`"

Table 4-2. Return Codes

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

Parameter File Elements

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

For example: “`INSTALLTYPE:Install`”

NOTE The parser is case insensitive and the value data can be quoted using double quotes (“).

Table 4-3. Parameter File Elements

Tag	Values	Comments
FORMATVERSION:	V1_0 (Default)	Used to indicate the Format of the tags listed after this line. This can be used multiple times.
INSTALLTYPE:	Install Install Client Tools Only Install AM(X) Install Service Pack Uninstall Uninstall Components	
LICENSEKEY:	Valid license key	Not required for vCenter Server Heartbeat
PLUGINPATH:	Must be a valid path.	Only one per line but can be defined multiple times.
FEATUREFORINSTALLATION:	VMware vCenter Server Heartbeat	Only one per line but can be defined multiple times.
SERVERROLE:	Primary Secondary	
TOPOLOGY:	HA DR	
ACCEPT_EULA:	True False	
DEFAULTCHANNELPORT:	Must be an integer	
DESTINATIONPATH:	Must be a valid path	
BACKUPDESTINATIONPATH:	Must be a valid path	Used to indicate where to write the pre-synchronization data.
BCKUPSOURCEPATH:	Must be a valid path	Used to locate the pre-synchronization data for installation of the Secondary server.
INCLUDEPROTECTEDDATAINBACKUP:	True False	
NETWORKTASKDOMAIN:		Used when the Principal (Public) IP addresses are different for different servers (usually for a DR topology).
NETWORKTASKUSER:		Used when the Principal (Public) IP addresses are different for different servers (usually for a DR topology).
LEAVEONNETWORK:	True False	
COMPUTERNAMEPOSTUNINSTALL:	Must be a string	
CLIENTCONNECTIONPORT:	Must be an integer	
SECONDARYCLONETYPE:	Full Merge Pre clone	Full is only valid for Windows 2008 Merge is only valid for Windows 2003
BACKUPUSER:		
VCUSERNAME:		
SECONDARYPRINCIPLEADDRESS:	Must be an IP address	Only one per line but can be defined multiple times.
PRIMARYSECONDARYCHANNEL:	Must be an IP address	Only one per line but can be defined multiple times.

Unattended Setup of the Primary Server

Installation of vCenter Server Heartbeat begins with the Primary server

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

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

<parameter.txt>

```
INSTALLTYPE:Install

ACCEPT_EULA:true

LICENSEKEY:<license serial number>

SERVERROLE:PRIMARY

TOPOLOGY:<HA or DR>

SECONDARYCLONETYPE:pre clone

DESTINATIONPATH:C:\AutoInstall

PRIMARYSECONDARYCHANNEL:<10.0.1.1,10.0.1.2>

PRIMARYPRINCIPLEADDRESS:<192.168.99.111>

SECONDARYPRINCIPLEADDRESS:<192.168.99.111>

NETWORKTASKDOMAIN:dnstest.com

NETWORKTASKUSER:administrator

CLIENTCONNECTIONPORT:52267

FEATUREFORINSTALLATION:VMware vCenter Server Heartbeat

PLUGINPATH:<C:\User\Desktop\Plugins>

BACKUPDESTINATIONPATH:\\<10.0.1.1\nf backup>

BACKUPUSER:Administrator

INCLUDEPROTECTEDDATAINBACKUP:true

VCUSERNAME:administrator

//STARTSERVICEATEND:

//AMXPATH:

//DEFAULTCHANNELPORT:

//BACKUPSOURCEPATH:
```

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

2 Rename the self-extracting file from `<name>.exe` to `<name>.zip`

3 Extract the contents of the self-extracting file into a temporary folder.

4 Navigate to **Start** > **Run** and type `CMD` to open a command window.

5 Navigate to the to the location of the temporary folder.

6 Run the command:

```
start /wait setup -f:<parameter file> –DNSPassword:<DNS Password>
–BACKUPPassword:<backup password> –VCENTERPASSWORD:<vCenterPassword> –ni
```

7 Upon completion of the unattended installation, a message instructing to launch the Configure Server wizard is displayed. Using the desktop icon, launch the Configure Server wizard.

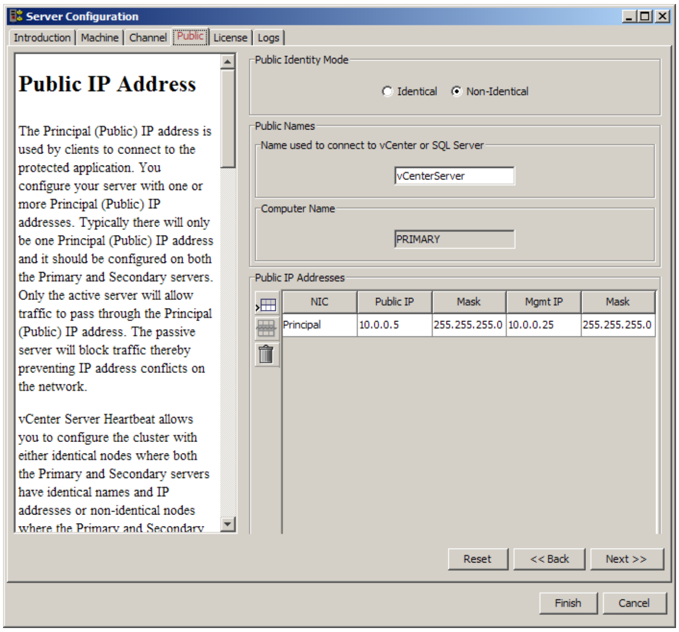
8 Click the **Public** tab.

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.

9 In the Public Identity/Mode pane, select **Non-Identical**.

10 Enter the **Name used to connect to vCenter or SQL Server**.

NOTE The *Name used to connect to vCenter or SQL Server* 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 *Name used to connect to vCenter or SQL Server* and it is the same on all servers in the cluster.



Public IP Address

The Principal (Public) IP address is used by clients to connect to the protected application. You configure your server with one or more Principal (Public) IP addresses. Typically there will only be one Principal (Public) IP address and it should be configured on both the Primary and Secondary servers. Only the active server will allow traffic to pass through the Principal (Public) IP address. The passive server will block traffic thereby preventing IP address conflicts on the network.

vCenter Server Heartbeat allows you to configure the cluster with either identical nodes where both the Primary and Secondary servers have identical names and IP addresses or non-identical nodes where the Primary and Secondary

Public Identity Mode

○ Identical ● Non-Identical

Public Names

Name used to connect to vCenter or SQL Server: vCenterServer

Computer Name: PRIMARY

Public IP Addresses

NIC	Public IP	Mask	Mgmt IP	Mask
Principal	10.0.0.5	255.255.255.0	10.0.0.25	255.255.255.0

11 In the **NIC** drop-down, select the Principal (Public) NIC.

12 In the **Public IP** drop-down, select the Principal (Public) IP address assigned to the Principal (Public) NIC.

13 In the first **Mask** field, enter the Subnet Mask of the Principal (Public) IP address.

14 In the **Mgmt IP** field, enter the reserved Management IP address for the Primary server.

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

15 In the second **Mask** field, enter the Subnet Mask of the Management IP address.

16 Click **Finish**. Do not start vCenter Server Heartbeat.

Unattended Setup of a Virtual Secondary Server

Installation of the Secondary server is similar to installation of the Primary server.

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

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

```
<file_name.txt>

    INSTALLTYPE:Install
```

```
SERVERROLE:SECONDARY

BACKUPSOURCEPATH:\\<192.168.15.111\nf backup>

BACKUPUSER:Administrator
```

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

2 Rename the self-extracting file from `<name>.exe` to `<name>.zip`

3 Extract the contents of the self-extracting file into a temporary folder.

4 Navigate to **Start** > **Run** and type `CMD` to open a command window.

5 Navigate to the to the location of the temporary folder.

6 Run the command:

```
start /wait setup -f:<parameter file> -BACKUPPassword:<backup password> -ni
```

7 Upon completion of the unattended installation, launch the Configure Server wizard to configure the Secondary server.

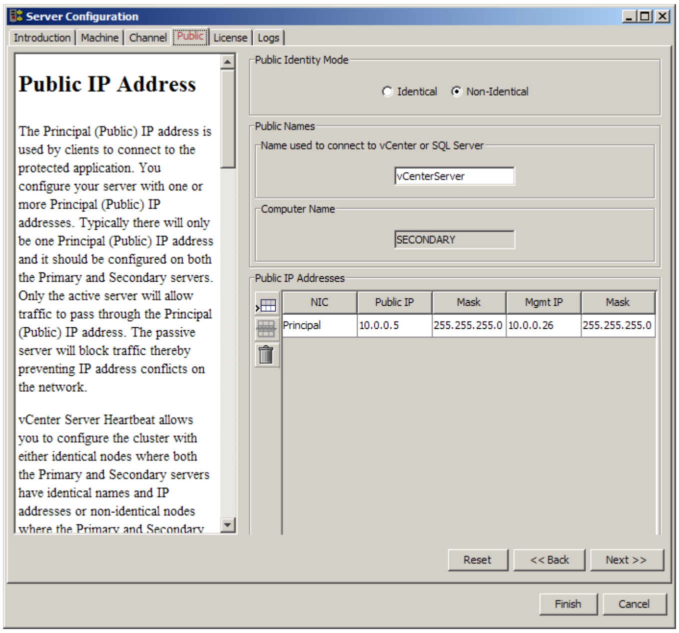
8 Click the **Public** tab.

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.

9 In the Public Identity/Mode pane, select **Non-Identical**.

10 Enter the **Name used to connect to vCenter or SQL Server**.

NOTE The *Name used to connect to vCenter or SQL Server* 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 *Name used to connect to vCenter or SQL Server* and it is the same on all servers in the cluster.



Public IP Address

The Principal (Public) IP address is used by clients to connect to the protected application. You configure your server with one or more Principal (Public) IP addresses. Typically there will only be one Principal (Public) IP address and it should be configured on both the Primary and Secondary servers. Only the active server will allow traffic to pass through the Principal (Public) IP address. The passive server will block traffic thereby preventing IP address conflicts on the network.

vCenter Server Heartbeat allows you to configure the cluster with either identical nodes where both the Primary and Secondary servers have identical names and IP addresses or non-identical nodes where the Primary and Secondary

Public Identity Mode: ○ Identical ● Non-Identical

Public Names

Name used to connect to vCenter or SQL Server: vCenterServer

Computer Name: SECONDARY

Public IP Addresses

NIC	Public IP	Mask	Mgmt IP	Mask
Principal	10.0.0.5	255.255.255.0	10.0.0.26	255.255.255.0

11 In the **NIC** drop-down, select the Principal (Public) NIC.

12 In the **Public IP** drop-down, select the Principal (Public) IP address assigned to the Principal (Public) NIC.

13 In the first **Mask** field, enter the Subnet Mask of the Principal (Public) IP address.

14 In the **Mgmt 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.

15 In the second **Mask** field, enter the Subnet Mask of the Management IP address.

16 Click **Finish**. Do not start vCenter Server Heartbeat.

17 Verify that the pre-populated 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.

Unattended Setup of a Physical Secondary Server

This is a two phase process, Installation and Restore, and then configuration after the post restore reboot of the server.

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

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

`<file_name.txt>`

```
InstallSecParas.txt

INSTALLTYPE:Install

SERVERROLE:SECONDARY

BACKUPSOURCEPATH:\\<10.0.3.1\nf backup>

BACKUPUSER:Administrator
```

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

2 Rename the self-extracting file from `<name>.exe` to `<name>.zip`

3 Extract the contents of the self-extracting file into a temporary folder.

4 Navigate to **Start** > **Run** and type `CMD` to open a command window.

5 Navigate to the to the location of the temporary folder.

6 Run the command:

```
start /wait setup -f:<parameter file> –BACKUPPassword:<backup password> –ni
```

7 Disconnect the Network cables (as instructed).

8 Reboot (as instructed).

9 Configure the NICs with the correct IP addresses.

10 Navigate to **Start** > **Run** and type `CMD` to open a command window.

11 Navigate to the to the location of the temporary folder.

12 Run the command:

```
start /wait setup –secondaryInstall-f:<parameter file> –ni
```

13 Upon completion of the unattended installation, launch the Configure Server wizard to configure the Secondary server.

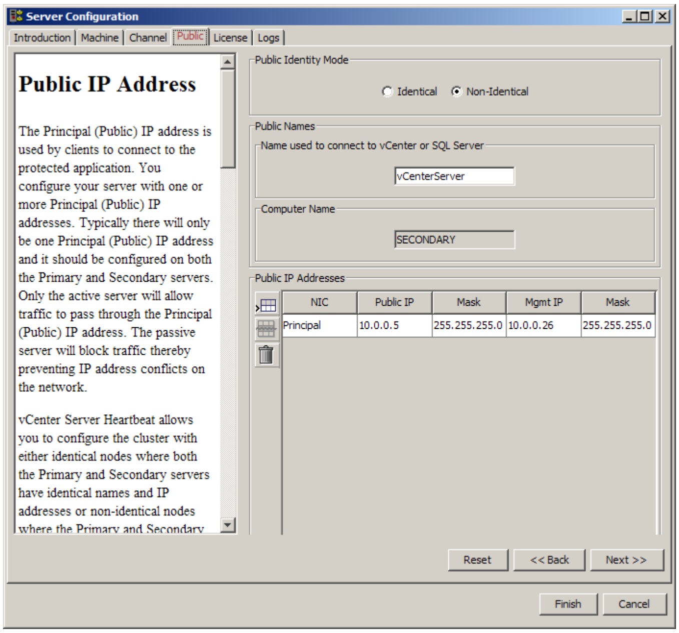
14 Click the **Public** tab.

> **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.

15. In the Public Identity/Mode pane, select **Non-Identical**.

16. Enter the **Name used to connect to vCenter or SQL Server**.

    NOTE The *Name used to connect to vCenter or SQL Server* 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 *Name used to connect to vCenter or SQL Server* and it is the same on all servers in the cluster.



Public IP Address

The Principal (Public) IP address is used by clients to connect to the protected application. You configure your server with one or more Principal (Public) IP addresses. Typically there will only be one Principal (Public) IP address and it should be configured on both the Primary and Secondary servers. Only the active server will allow traffic to pass through the Principal (Public) IP address. The passive server will block traffic thereby preventing IP address conflicts on the network.

vCenter Server Heartbeat allows you to configure the cluster with either identical nodes where both the Primary and Secondary servers have identical names and IP addresses or non-identical nodes where the Primary and Secondary

Public Identity Mode: ○ Identical ● Non-Identical

Public Names

Name used to connect to vCenter or SQL Server: vCenterServer

Computer Name: SECONDARY

Public IP Addresses

NIC	Public IP	Mask	Mgmt IP	Mask
Principal	10.0.0.5	255.255.255.0	10.0.0.26	255.255.255.0

17. In the **NIC** drop-down, select the Principal (Public) NIC.

18. In the **Public IP** drop-down, select the Principal (Public) IP address assigned to the Principal (Public) NIC.

19. In the first **Mask** field, enter the Subnet Mask of the Principal (Public) IP address.

20. In the **Mgmt 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.

21. In the second **Mask** field, enter the Subnet Mask of the Management IP address.

22. Click **Finish**. Do not start vCenter Server Heartbeat.

23. Verify that the pre-populated 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

vCenter Server Heartbeat requires unique server names to operate properly. To create the unique names you must rename both the Primary and Secondary servers to ensure proper configuration and prevent name resolution problems when clients attempt to access the vCenter Server application.

For example, before installing vCenter Server Heartbeat your vCenter Server is named “vCenterServer”. During the vCenter Server Heartbeat installation process on “vCenterServer” you clone “vCenterServer” (the Primary server) to create a Secondary server.

After installation you rename the Secondary server to “vCSHB-Secondary” and then rename the Primary server to “vCSHB-Primary”. You then use the Configure Server wizard and identify the *Name used to connect to vCenter or SQL Server* as “vCenterServer” thereby allowing access to vCenter Server on either the Primary or Secondary servers.

To rename the Secondary server

1. Navigate to **Start** > **Administrative Tools** > **Services** and set the VMware vCenter Server Heartbeat 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 Passive (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 VMware vCenter Server Heartbeat 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.
3. On both the Primary and Secondary servers, navigate to **Start** > **Administrative Tools** > **Services** and set the VMware vCenter Server Heartbeat service to **Automatic**, and close the dialog. See "Post Installation Configuration" on page 61 for additional instructions on configuring vCenter Server Heartbeat.

Post Installation Configuration

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

1. Before starting VMware 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
   ```

2. 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.

3. 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.

4 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.

5 Verify that Nslookup resolves as shown below:

  - Nslookup resolves Service Name to Public IP
  - Nslookup resolves Primary Name to Primary Management IP
  - Nslookup resolves Secondary Name to Secondary Management 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 edit the `parameter.txt` file parameter `PLUGINPATH:` to reflect the path to the SQL Server Plug-in.

6 To install vCenter Server Heartbeat on SQL Server when installed on a separate host from the vCenter Server, go to "Unattended Setup of the Primary Server" on page 56

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

When protecting SQL Server, 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.

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 Post Installation

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.

Unattended 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 Create a `.txt` file containing the following configuration parameters:

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

<parameter.txt>

```
INSTALLTYPE:Install Client Tools Only

ACCEPT_EULA:true

DESTINATIONPATH:C:\AutoInstall
```

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

2 Rename the self-extracting file from `<name>.exe` to `<name>.zip`

3 Extract the contents of the self-extracting file into a temporary folder.

4 Navigate to **Start** > **Run** and type `CMD` to open a command window.

5 Navigate to the to the location of the temporary folder and run the command:

```
start /wait setup -f:<parameter file> –ni
```

6 Upon completion of the unattended installation, the Manage Server icon will appear on the desktop.

Unattended Uninstall of vCenter Server Heartbeat

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

Uninstall vCenter Server Heartbeat from the command line

1 Ensure all the vCenter Server Heartbeat processes are stopped and close the vCenter Server Heartbeat Console and System Tray icon.

2 Create a `.txt` file with the following configuration parameters:

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

```
<file_name.txt>

//FORMATVERSION:

INSTALLTYPE:Uninstall

LEAVEONNETWORK: true
```

3 Rename the self-extracting file from `<name>.exe` to `<name>.zip`.

4 Extract the contents of the self-extracting file into a temporary folder.

5 Navigate to **Start** > **Run**, type `CMD` and click **OK** to open a command window.

6 Navigate to the to the location of the temporary folder.

7 Run the command:

```
Start /wait setup -f :<parameter file> -ni
```

8 Upon completion of the unattended uninstallation you will be asked to restart the server.

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 on 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 and Management IP addresses.

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.