QuickStart Guide

vCenter Server Heartbeat 6.3

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-000379-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About This Book

This *Quick Start Guide* provides an introduction to VMware vCenter Server Heartbeat and guides you through the steps required to install vCenter Server Heartbeat and to perform basic configuration. This guide also provides a brief introduction to basic administration tasks and advanced configuration features, and provides pointers to more detailed information in other manuals.

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.

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
SAN	Storage Area Network (type of datastore)

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current versions of this guide and other publications, 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.

vCenter Server Heartbeat Introduction 1

This chapter introduces vCenter Server Heartbeat and provides an overview of vCenter Server Heartbeat concepts. It contains the following sections:

vCenter Server Heartbeat Protection

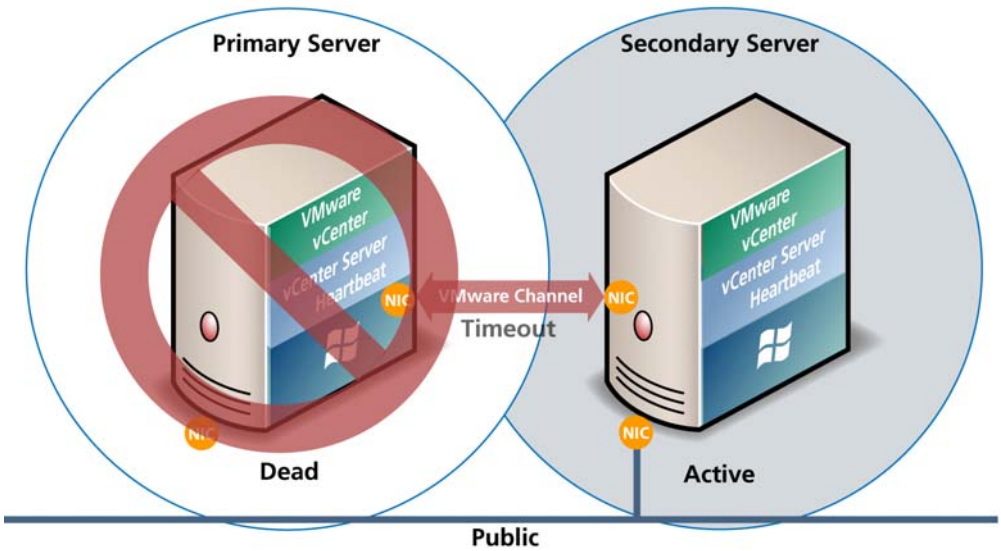
vCenter Server Heartbeat is a Windows based service specifically designed to provide high availability protection for vCenter Server configurations without requiring any specialized hardware.

Server Protection

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

Network Protection

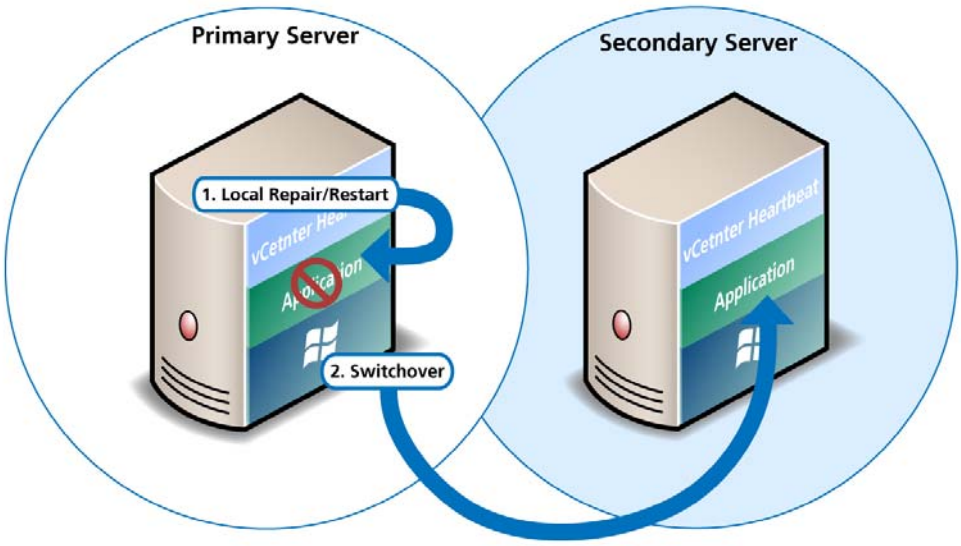
vCenter Server Heartbeat proactively monitors the network by polling up to three nodes to ensure that the active server is visible on the network. vCenter Server Heartbeat polls defined nodes around the network, including the default gateway, the primary DNS server, and the global catalog server at regular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

Application Protection

vCenter Server Heartbeat maintains the application environment ensuring that applications and services stay alive on the network. 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.

If a protected application fails, vCenter Server Heartbeat first tries to restart the application on the active server (1). If restarting the application fails, then vCenter Server Heartbeat can initiate a switchover (2).

Figure 1-2. Switchover



A switchover gracefully closes any protected applications that are running on the active server and restarts all of them on the passive server, including the application or service that caused the failure as illustrated in Figure 1-2.

Performance Protection

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

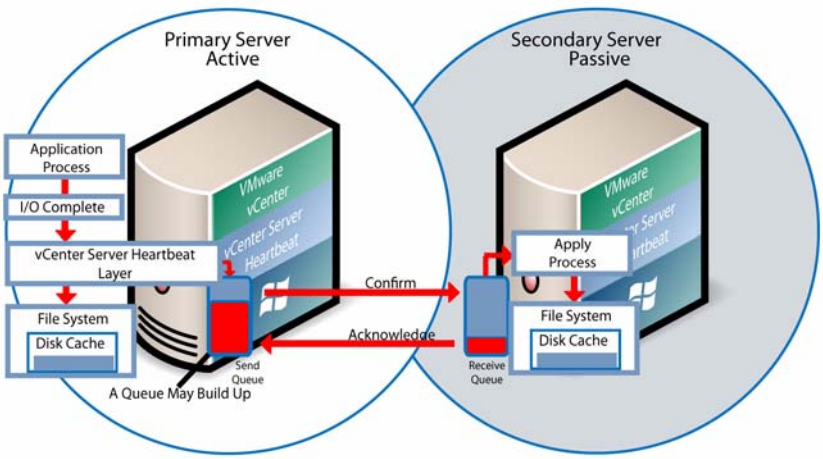
In addition to monitoring application services, vCenter Server Heartbeat can monitor specific application attributes to ensure that they remain within normal operating ranges. Similar to application monitoring, various rules can be configured to trigger specific corrective actions whenever these attributes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

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 configures itself to protect files, folders, and even the registry settings for vCenter Server on the active server by mirroring these in real-time to the passive server. If a failover occurs, all files protected on the failed server are available after the failover, hosted on the Secondary server.

Figure 1-3. Apply Process



Communications

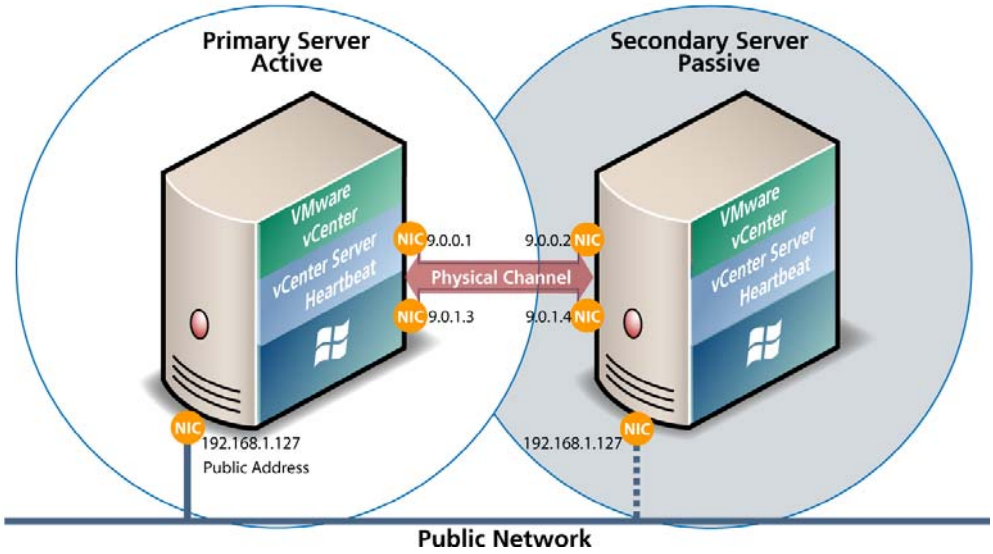
The VMware Channel is a crucial component of the setup and can be configured in a number of ways.

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 example in Figure 1-4, the IP address is configured as 192.168.1.127.

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

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

Following restore and after the vCenter Server Heartbeat installation completes (runtime), NetBIOS is disabled across the channel(s). This occurs during installation to prevent a name conflict, which occurs when both servers have the same name.

The NICs that support connectivity across the VMware Channel can be standard 100BaseT Ethernet cards providing a throughput of 100Mbits per second across standard Cat-5 cabling.

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

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

The Secondary server has the same name, same file and data structure, same network address, and can run all the same applications and services as the Primary server.

Only one server name and network address can be visible on the same network at any one time. One of these two servers is live on the Principal (Public) network and serves the protected applications. This is the active server. The other server is hidden from the Principal (Public) network, remains as a ready standby server, and is the passive server.

The vCenter Server Heartbeat software is symmetrical in almost all respects, and either the Primary Server or the Secondary server can take the active role and provide the protected application to users.

vCenter Server Heartbeat Installation 2

This chapter discusses the installation of vCenter Server Heartbeat and provides an overview of the prerequisites for successful installation. It contains the following sections:

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 on separate servers. This flexibility enables vCenter Server Heartbeat to protect vCenter Server when using remote databases other than SQL Server.

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 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
  - VirtualCenter Server 2.5

- VirtualCenter Server 2.5 Update 1
- VirtualCenter Server 2.5 Update 2
- VirtualCenter Server 2.5 Update 3
- VirtualCenter Server 2.5 Update 4
- VirtualCenter Server 2.5 Update 5
- VirtualCenter Server 2.5 Update 6
- vCenter Server 4.0
- vCenter Server 4.0 Update 1
- vCenter Server 4.0 Update 2
- vCenter Server 4.1

- Operating Systems
  - Windows Server 2003 x86 Standard SP2
  - Windows Server 2003 x86 Enterprise SP1 and SP2
  - Windows Server 2003 x64 Enterprise SP2
  - Windows Server 2008 x86 SP1 and SP2
  - Windows Server 2008 x64 SP1 and SP2
  - Windows Server 2008 R2

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

- Prior to installing vCenter Server Heartbeat, verify that vCenter Guided Consolidation, vCenter Update Manager, and vCenter Converter are configured using Fully Qualified Domain Names (FQDN) rather than IP addresses.
- During the setup process, vCenter Server Heartbeat verifies that a minimum of 1GB RAM is available. To ensure proper operation, vCenter Server Heartbeat requires a minimum of 1GB RAM (2GB is recommended) in addition to any other memory requirement for the Operating System or vCenter Server.
- Verify that 2GB of disk space is available on the installation drive for vCenter Server Heartbeat.
- Obtain and use local administrator rights to perform vCenter Server Heartbeat installation.
- Apply the latest Microsoft security updates.
- All applications that will be protected by vCenter Server Heartbeat must be installed and configured on the Primary server prior to installing vCenter Server Heartbeat.
- Verify that both Primary and Secondary servers have identical system date, time, and time zone settings. Once configured, do not change the time zone.
- Verify that the Principal (Public) network adapter is listed as the first network adapter in the network connections bind order. (**Network Connections** > **Advanced > Advanced Settings**).
- Verify that the Managed IP setting in the Virtual Infrastructure Client is the same IP address used for the vCenter Server Heartbeat Principal (Public) IP address.

Server Architecture Options

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

Virtual to Virtual (V2V)

V2V is the supported architecture if vCenter Server is already installed on the production (Primary) server running on a virtual machine. 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
  - OS version and Service Pack
- Each virtual machine used in the V2V pair must be on a separate ESX host to guard against failure at the host level.
- Each virtual NIC must use a separate virtual switch.

Physical to Virtual (P2V)

The P2V architecture is used when the environment requires a mix of physical and virtual machines. 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
  - OS version and Service Pack
- The Secondary virtual machine must have sufficient priority in resource management settings so that other virtual machines do not impact its performance.
- Each virtual NIC must use a separate virtual switch.

Physical to Physical (P2P)

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

Primary Server

The Primary server must meet the hardware and software requirements specified in "Common Requirements" on page 11.

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 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 near identical Secondary server involves different techniques depending on the selected server architecture.

Supported Pre-Clone Technologies

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

- VMware Converter for "Physical to Virtual (P2V)" on page 13.
- VMware vCenter virtual machine cloning for "Virtual to Virtual (V2V)" on page 13.

Supported Install Clone Technologies

Installation of vCenter Server Heartbeat provides support for NTBackup on Windows 2003 and Wbadmin on Windows Server 2008 for automated Install Cloning. This process is automated but requires meeting all prerequisites for the Secondary server specified in "Physical to Physical (P2P)" on page 13.

Application Component Options

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

- VirtualCenter Server Version 2.5
  - VMware VirtualCenter Server
  - VMware Capacity Planner
  - VMware Converter Enterprise
  - VMware Update Manager
  - VMware License Server
  - VMware Virtual Infrastructure Client
- vCenter Server Version 4.0
  - VMware vCenter Server
  - VMware Guided Consolidation Service
  - VMware License 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 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
- VMware View Composer 1.1 and 2.0
  - VMware View Composer
  - VMware Universal File Access
- vCenter Converter Enterprise
- SQL Server 2005 SP1–SP3
- SQL Server 2008 including SP1

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** window.

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.

To ensure proper failover, increase the default Heartbeat interval from 20 to 30 seconds on the server running vCenter Server. This configuration is required anytime SQL Server is not installed on the same host as vCenter Server.

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.

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.

Primary Server

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

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

Secondary Server

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

- Same number of NICs as the Primary server
- Principal (Public) network connection configured with temporary network settings
- Channel network connection(s) configured with the following:
  - Static IP address in a different subnet than the Principal (Public) network with a different IP address than the Primary server channel NIC
  - Correct network mask
  - No Gateway IP address
  - No DNS IP address
  - NetBIOS enabled (disabled 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.

WAN Requirements

When deploying vCenterServer Heartbeat in a WAN environment, the following components must be configured:

NOTE Prior to installing vCenter Server Heartbeat, verify that vCenter Update Manager and vCenter Converter are configured using Fully Qualified Domain Names (FQDN) rather than IP addresses.

- Persistent static routing configured for the channel connection(s) where routing is required
- Two NICs (1 x Public; 1 x Channel) 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 when prompted during the setup process
  - Recommend 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 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*

Bandwidth

Determine the available bandwidth and estimate the volume of data throughput to determine acceptable latency for the throughput. Available 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 must not fall below the standard defined for a T1 connection.

Installation Process

After selecting implementation options, begin the installation process. The installation process for all scenarios follows the same basic procedure.

Installation Options Checklist

Server architecture:

____ P2P

____ P2V

____ V2V

Cloning technology option:

____ Pre-Clone Install

____ Install Clone

Application components to protect:

____ vCenter Server with SQL Server on same host

____ vCenter Server with SQL Server on separate host

____ vCenter Server only

Network environment type:

____ LAN

____ WAN

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, then refer to the knowledge base articles in "Network Options" on page 16.

Installation

Primary Server

After reviewing the setup prerequisites to ensure the servers in the pair (either physical or virtual) meet the minimum requirements and completing the pre-installation tasks (Pre-Cloning for V2V and P2V environments and configuring the VMware Channel), you can begin the setup process.

NOTE vCenter Server Heartbeat installs in the evaluation mode. Refer to "Post Installation Tasks" on page 20 for instructions on how to enter a production serial number.

To set up the Primary server

1 Double-click the WinZip Self-Extracting file on the Primary server.

2 The **Setup Introduction** dialog is displayed. Click **OK**.

3 The **WinZip Self-Extractor** dialog is displayed. Click **Setup** to open the **Install VMware vCenter Server Heartbeat** window.

4 The first installation option to configure is the **Setup Type**. Select **Install VMware vCenter Server Heartbeat**.

5 On the following step, set the **Server Identity**. Select **Primary**.

6 Setup allows you to enter a production serial number for production installations or click next without a serial number to install in the evaluation mode.

NOTE If you need help during the setup process, the left panel of the setup window explains each step or option.

The next option is the cloning technique. When you select the cloning option, the subsequent setup screens display the setup process for the selected cloning technology.

During the setup process, you have the opportunity to identify:

- The Program Installation location
- VMware Channel IP addresses
- The Principal (Public) IP addresses
  - A single IP for a LAN installation
  - Two IPs for a WAN installation
- The applications to protect (vCenter Server and SQL Server, vCenter Server only, SQL only, and View Composer)
- The location to store the clone files

NOTE When installing into a Windows Server 2008 environment, you must specify a UNC path to the backup file location.

Setup runs a pre-install check process to verify that the server meets the minimum requirements before installing vCenter Server Heartbeat.

When using the Install Clone technique, setup makes a backup. When using the Pre-Clone setup, setup copies two small files to the storage location configured on the Secondary server.

A Packet Filter is installed on the Principal (Public) NIC and the setup process completes on the Primary server.

Secondary Server

To set up the Secondary server

1 Double-click the WinZip Self-Extracting file to start the setup process for the Secondary server (physical or virtual).

2 The **Setup Introduction** dialog is displayed. Click **OK**.

3 The **WinZip Self-Extractor** dialog is displayed. Click **Setup** to open the **Install VMware vCenter Server Heartbeat** window.

4 The first installation option to select is the **Setup Type**. Select **Install VMware vCenter Server Heartbeat.**

5 Select **Secondary** for the **Server Identity** option.

6 Specify the location of the folder containing the backup file from the Primary server. Type the location path in the text box or click **Browse** and locate the folder. Click **Next**.

7 Setup identifies the backup file location and runs pre-install checks before installing vCenter Server Heartbeat on the Secondary server.

8 The next step installs the Packet Filter and identifies the VMware Channel and Principal (Public) NICs.

9 When using an Install Clone setup in a LAN environment, configure the Principal (Public) NIC to the same IP address as the Primary server. After reconfiguring the Principal (Public) NIC (if necessary), start the restore process.

10 Following completion of the restore process, if the Secondary server is a physical server, Windows Plug and Play might run multiple times to detect hardware differences and require one or more system restarts.

NOTE When installing into a Windows Server 2008 environment, after completion of the restore process, you must restart the server and run the vCenter Server Heartbeat Setup Completion executable located on the Desktop. At this point, the Packet Filter is installed and the VMware Channel and Principal (Public) NICs are identified.

11 After Plug and Play completes detection, the setup process displays the **Finish** window.

Post Installation Tasks

After installation, complete the following tasks:

1 Ensure that vCenter Server Heartbeat is shut down.

2 Start VMware vCenter Server Heartbeat on the Primary server.

3 Verify that the Date and Time and Time Zone on the Secondary server are identical to that of the Primary server.

4 Start VMware vCenter Server Heartbeat on the Primary server.

After successfully installing vCenter Server Heartbeat on the server pair, if SQL Server is not on the same host as vCenter Server, repeat the setup process at the separate location where SQL Server is hosted.

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: Plugins** page.

2 Select the VirtualCenter Plug-in.

3 Click **Edit**.

4 Type the Username and Password for an account with rights to the Virtual Infrastructure.

5 Click **OK**.

When Deployed in a WAN Environment

NOTE Before proceeding with this task, ensure that vCenter Server Heartbeat is running on the pair, and System Status is **Replicating**.

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

1 Launch **vCenter Server Heartbeat Console**.

2 Click **Data** and select the **File Filters** tab.

3 Click **Add Exclusion Filter** and enter or browse to the following path:

```
$INSTALL_PATH_TO_ORCHESTRATOR/app-server/bin/boot.properties
```

4 Click **OK.**

5 Perform a switchover so that the Secondary server becomes active.

6 Launch the **vCenter Orchestrator Web Configuration** wizard and select **Network**. In the **IP address** field select the Principal (Public) IP address of the Secondary server. Click **Apply changes**.

7 If VMware Orchestrator Server is configured as a service, perform the following steps.

8 Launch the **vCenter Orchestrator Web Configuration** wizard, select **Startup Options**, and click **Restart service**.

9 From **vCenter Server Heartbeat Console**, select **Applications** and then **Services**. Verify that **VMware vCenter Orchestrator Server** service is included in the protected services. If not, manually run the **Protected Service Discovery** task from **VMware vCenter Heartbeat Console** > **Applications** > **Tasks** > **VMware VirtualCenter - Protected Service Discovery**).

Installation Verification 3

This chapter includes the following topics:

Verifying vCenter Server Heartbeat

The Installation Verification process validates the installation and tests the software operation.

The following exercises are examples and must be performed in order. VMware does not recommend attempting to test a failover on a properly operating server pair using methods such as unplugging a power cord. When power is lost, any data not written to the passive server is lost. VMware recommends performing a switchover rather than a failover to test the operation of the passive server.

Exercise One

This exercise demonstrates that the Secondary server can function as the Primary Server without the test data being immediately replicated back to the original server. During the exercise, stop the Primary server from providing service and hide it from the network, then introduce the Secondary to the network and allow it to provide service.

Starting Conditions

The Primary server is active. The Secondary server is passive. Both the File System and the Registry Status are **Synchronized**.

Local users are aware that the service is unavailable for the duration of this exercise.

Actions

Table 3-1. Exercise One Actions

Machine	Activity	Result
Primary	Shut down vCenter Server Heartbeat. Select Stop VMware vCenter Server Heartbeat and all protected applications, then click **OK**.	vCenter Server Heartbeat stops all monitored services and exits.
	With vCenter Server Heartbeat shut down, on the Primary server, go to **Start > All Programs > VMware > VMware vCenter Server Heartbeat > Configure Server** to launch the Configure Server wizard. In the wizard, change the Primary server's role to passive.	Primary server becomes passive
	Start vCenter Server Heartbeat. Then shut down Heartbeat and select Stop VMware vCenter Server Heartbeat and all protected applications, and then click **OK**.	This activates the network filter hiding the Primary server from the network.
Secondary	Go to **Start > All Programs > VMware > VMware vCenter Server Heartbeat > Configure Server** to launch the Configure Server wizard. In the wizard, change the Secondary server's role to active. Then start vCenter Server Heartbeat.	The Secondary server starts as the active server.
Client	Compares application functional status to the predefined criteria for availability and performance.	Secondary server behaves as the Primary server.

Results

The Secondary server provides the expected functionality of the Primary server.

Exercise Two

This exercise follows Exercise One. The objective is to take a working active server (Secondary) and synchronize it with the passive (Primary). This exercise also demonstrates that all the correct services stopped when the Primary server became passive.

Starting Conditions

vCenter Server Heartbeat is running on the Secondary Server, which is active. vCenter Server Heartbeat is not running on the Primary server and is set to passive without starting vCenter Server Heartbeat.

Local users are aware that the service is unavailable for the duration of this exercise.

Actions

Table 3-2. Exercise Two Actions

Machine	Activity	Result
Primary	Start vCenter Server Heartbeat.	vCenter Server Heartbeat starts. The vCenter Server Heartbeat Console shows the connection from the Secondary (active) to Primary (passive).
	Wait for both the Registry and the File System to become Synchronized. Access the vCenter Server Heartbeat logs and confirm that no exception errors occurred during synchronization.	Data replication resumes from the Secondary server back to the Primary server. Both the File System & Registry status become **Synchronized**.

Results

Both machines are resynchronized. All the data changed on the Secondary machine while the Primary was not running vCenter Server Heartbeat is updated onto the Primary machine. The Secondary (active) machine continues to provide service.

Exercise Three

Perform a switchover using vCenter Server Heartbeat Console. Perform this exercise after completing Exercises One and Two.

Local users are aware that the service is unavailable for the duration of this exercise.

Starting Conditions

Both the File System and Registry Status are **Synchronized**.

Actions

Table 3-3. Exercise Three Actions

Machine	Activity	Result
vCenter Server Heartbeat Console	Click **Switchover** and confirm.	The vCenter Server Heartbeat Console displays the services stopping on the active server. Once all services are stopped, the active server becomes passive and the passive server becomes active. The Console shows the services starting on the newly active server. Both the File and Registry status are **Synchronized**.
Any	Confirm application performance and availability meets previously defined criteria. Verify that client applications are running as expected after the switchover process.	Service as usual. You might have to refresh or restart some client applications as a result of a switchover.

Results

Application service transferred from the originally active machine to the originally passive machine. Document the application-client behavior for future reference.