Quick Start Guide

vCenter Server Heartbeat 5.5

vmware®

Quick Start Guide
Revision: 20090305
Item:

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. It guides you through the steps required to install vCenter Server Heartbeat and to perform basic configuration. It provides a brief introduction to basic administration tasks and advanced configuration features. For more information, the guide provides pointers to other manuals.

Intended Audience

The user guide assumes a working knowledge of networks including the configuration of the TCP/IP suite of protocols, a sound knowledge of domain administration on the Windows 2003 platform notably in Active Directory and DNS.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, 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 datastore

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current versions of this book and other books, go to http://www.vmware.com/support/pubs

Online and Telephone Support

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

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html

Support Offerings

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

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used 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. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

vCenter Server Heartbeat Introduction

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

vCenter Server Heartbeat Protection

vCenter Server Heartbeat is a Windows based system that has been specifically designed to provide high availability to server configurations in one product while not requiring any specialized hardware.

Server Protection

vCenter Server Heartbeat protects the active server's operating system or hardware from failing. Two instances of vCenter Server Heartbeat monitor each other by sending "I'm alive" messages and reciprocating with acknowledgments over a network connection termed the vCenter Server Heartbeat Channel. If the passive server detects that this process or heartbeat has failed, then a failover occurs as illustrated in Figure 0-1.

Figure 0-1 Failover
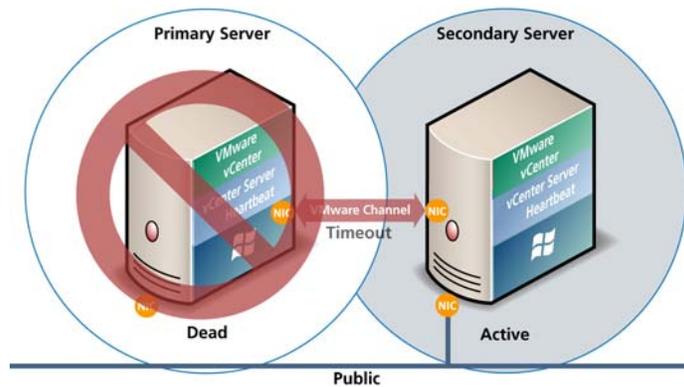
A failover is similar to a switchover but is used in more drastic situations. A failover happens when the passive server detects that the active server is no longer responding. This can occur when the active server hardware crashes or loses its network connections. Rather than the active server gracefully closing, the passive server determines that the active server has failed and requires no further operations. In a failover, the passive server immediately takes on the role of the active server.

Network Protection

vCenter Server Heartbeat proactively monitors the ability of the active server to communicate with the rest of the network by polling defined nodes around the network, including the default gateway, the primary DNS server, and the Global Catalog server at regular intervals. If all three nodes fail to respond, for example, in the case of a network card failure or a local switch failure, vCenter Server Heartbeat can initiate a switchover, allowing the secondary server to assume an identical network identity as the primary server.

Application Protection

vCenter Server Heartbeat running on the active server locally monitors the applications and services it has been configured to protect through the use of *plugins*.

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 initiates a switchover (2).

Figure 0-2 Switchover
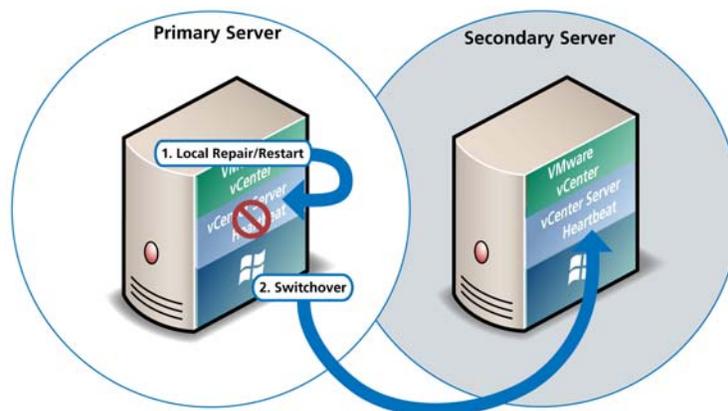
A switchover gracefully closes any protected applications that are running on the active server and restarts them on the passive server with the application or service that caused the failure as illustrated in Figure 0-2.

Performance Protection

vCenter Server Heartbeat monitors application services as well as specific application attributes to ensure that protected applications are operational and not in an unresponsive or stopped state. This level of monitoring is fundamental in ensuring that applications are available to users.

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

Data Protection

Once installed, vCenter Server Heartbeat configures itself automatically to protect files, folders, and even the registry settings for vCenter Server on the active server by mirroring them in real-time to the passive server. This means that if a failover occurs, all the files protected on the failed server are available after the failover, hosted on the secondary server.

Figure 0-3 Apply Process
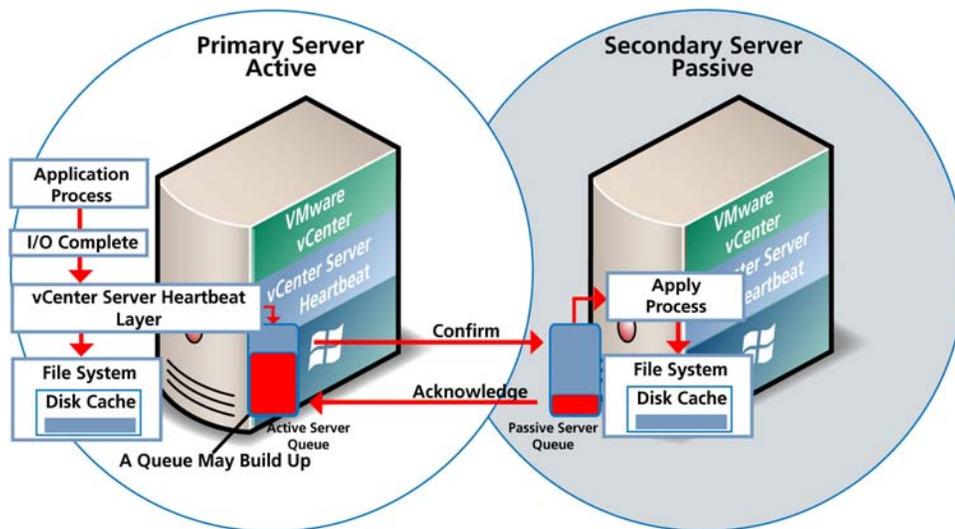
Communications

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 vCenter Server Heartbeat Channel uses a separate NIC, a private connection between the servers used for control and data transfer between the pair of servers.

The vCenter Server Heartbeat Channel might use a second pair of NICs to provide a degree of redundancy. In this case, the VMware Channel has a Dual Channel if more than one dedicated

NIC is provided for the vCenter Server Heartbeat 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 0-4 Communication between Primary and Secondary Servers
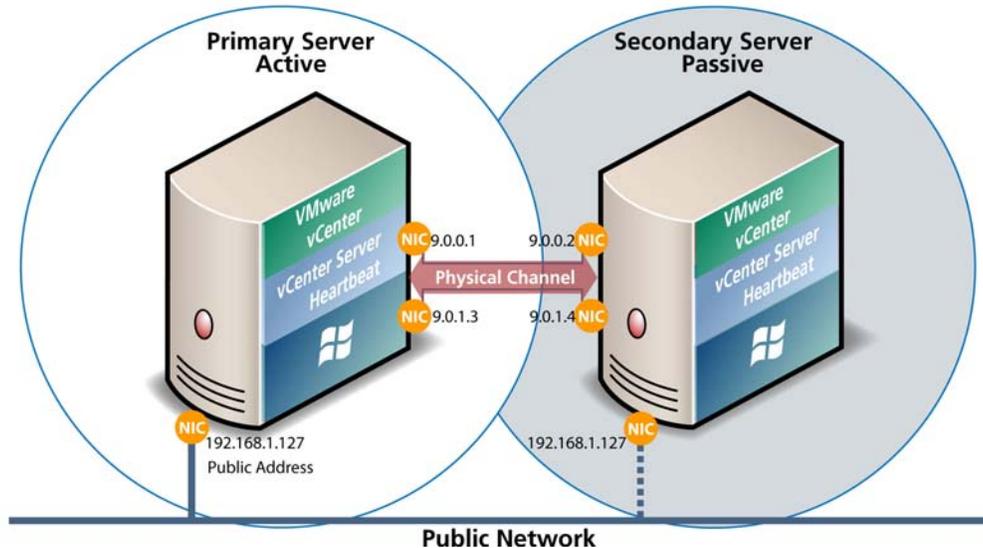
The IP address used by a client to connect to the active server (the Principal (Public) IP address) must be configured to use a static IP address (Not DHCP enabled). In the example in Figure 0-4, the IP address is configured as 192.168.1.127.

The passive server's Principal (Public) NICs 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.

Configure the NICs on the active and passive servers used for the vCenter Server Heartbeat Channel so that their IP addresses are outside of the Principal (Public) networks subnet range. These addresses are termed the vCenter Server Heartbeat Channel addresses.

You must switch off NetBIOS for the vCenter Server Heartbeat Channel(s) on the active and passive servers as this connection remains live, and both the passive and active machines have the same NetBIOS name. After restore and after the vCenter Server Heartbeat installation complete (runtime), NetBIOS is disabled across the channel(s). This occurs automatically during installation. If NetBIOS was not disabled, a name conflict occurs as both servers now have the same name.

The NICs that allow the connectivity across the vCenter Server Heartbeat 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, vCenter Server Heartbeat 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

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 provides a versatile solution that deploys multiple configurations in either a LAN or WAN environment with the protected applications on either a single server or multiple servers. When deployed with SQL Server, vCenter Server Heartbeat allows vCenter Server to be installed on a local server while SQL server is installed on a remote server. Additionally, vCenter Server Heartbeat can be deployed with vCenter Server alone.

Prior to installing vCenter Server Heartbeat, you must identify the desired deployment options. The installation process requires you to select options throughout the procedure to achieve the desired configuration.

Environmental Prerequisites

The server protected by vCenter Server Heartbeat can **NOT** be configured as a domain controller / global catalog or DNS.

Common Requirements

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

- Supported vCenter Server Versions 2.5.0, 2.5.1, 2.5.2, 2.5.3

- Operating System Windows Server 2003 x86 Sp1 or SP2

- Additional 512 MB (minimum), 1 GB RAM (recommended)

- 2 GB of disk space available on the drive where vCenter Server Heartbeat is installed

- Local administrator rights for vCenter Server Heartbeat installation

- Latest Microsoft security updates

- All applications to be protected by vCenter Server Heartbeat must be installed and configured on the Primary server prior to installing vCenter Server Heartbeat.

- The primary and secondary servers must be set to identical System Date / Time and Time Zone. Once configured, do not change the Time Zone.

Primary Server

Hardware and software as specified in the Common Requirements section.

Secondary Server

Hardware

- Hardware must match the Primary server to ensure adequate performance when the server is in the active role:
    - Similar CPU
    - 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.

- ACPI compliance must match the Primary server. The vCenter Server Heartbeat Standard implementation process assumes that the Advanced Configuration and Power Interface (or ACPI) compliance of both machines are the same. If this is not the case, contact VMware Support at http://www.vmware.com/support for further information.

Software

- OS version and Service Pack version must match the Primary server.

- OS must be installed to 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 must be consistent with Primary server.

Server Architecture Options

The selected server architecture determines the requirements for hardware and impacts 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 that of the Primary Virtual Machine as follows:
  - Similar CPU (including resource management settings)
  - Memory configuration (including resource management settings)
  - Appropriate resource pool priorities
- Each virtual machine used in the V2V pair must be on a separate ESX host to guard against failure at the host level.
- Each virtual NIC must use a separate virtual switch.

Physical to Virtual (P2V)

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
  - Memory
- The Secondary Virtual Machine must have enough 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)

The P2P architecture is used in an environment where it is necessary to have both the Primary and Secondary servers as physical servers. Use of P2P limits the installation options as it requires using the Install Clone technique. Additionally, this architecture requires attention to detail when preparing for installation as both current hardware and software must meet the specific prerequisites listed.

Cloning Technology Options

Cloning the Primary server to create a near identical Secondary server involves different techniques depending on the chosen server architecture option.

Supported Pre-Clone Technologies

To create Pre-Cloned images for use as a Secondary server, use the following cloning technologies:

- VMware Converter for Physical To Virtual (P2V)

- VMware vCenter virtual machine cloning for Virtual To Virtual (V2V)

Supported Install Clone Technologies

vCenter Server Heartbeat supports NTBackup on Windows 2003 for automated Install Cloning. This automated process requires meeting all prerequisites for the Secondary server specified in the Physical to Physical (P2P) section.

Application Component Options

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

- VMware vCenter Server
- VMware Capacity Planner
- VMware Converter Enterprise
- VMware Update Manager
- VMware License Server

vCenter Server with SQL Server on the Same Host

To ensure adequate performance in 20+ host or 200+ VM environments, VMware recommends installing SQL Server and vCenter Server 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 interval from 20 to 30 seconds on the server running vCenter Server. This configuration is required when SQL Server is not on the same host as vCenter Server.

Network Options

Networking requirements are contingent based upon how vCenter Server Heartbeat is deployed. If deployed as a High Availability solution then a LAN configuration is required. If vCenter Server Heartbeat is deployed for Disaster Recovery, then a WAN configuration is required.

LAN

vCenter Server Heartbeat deployed in a LAN environment requires the same Principal (Public) IP address used by both servers. Additionally, each server requires a separate VMware Channel IP address on a separate dedicated subnet.

Note: When installing vCenter Server Heartbeat in a LAN environment, do not enable the Low Bandwidth Module as this is designed for WAN deployments.

Primary Server

- Three NICs (1 x Public; 2 x Channel) 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. Configure split brain avoidance.

- 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

Secondary Server

- 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

o   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 as well as a VMware Channel IP address in a separate dedicated subnet.

WAN Requirements

- A persistent static route configured to the channel connection on the Secondary server where routing is required

- Two NICs (1 x Public; 1 x Channel) recommended

- If the Primary and Disaster Recovery (DR) site use the same subnet:

    o   During install, follow the steps for a LAN / VLAN (same subnet).

    o   Each server within the vCenter Server Heartbeat pair uses the same Public IP address.

- If the Primary and DR site use different subnets:

    o   During install, follow the steps for a WAN.

    o   Each server within the vCenter Server Heartbeat pair requires its own separate Principal (Public) IP address as well as a VMware Channel IP address in a separate dedicated subnet.

    o   Provide a user account with rights to update DNS using the DNSUpdate utility provided as a component of vCenter Server Heartbeat.

    o   Recommend Microsoft DNS to be integrated into AD so that DNSUpdate automatically identifies all DNS Servers that require updating.

    o   Refer to the following articles in the Knowledge base:

        ▪   VMware Knowledge Base article 1008571

        ▪   VMware Knowledge Base article 1008605

- At least one Domain Controller at the Disaster Recovery site

Bandwidth

Determine the available bandwidth and estimate the volume of data for which throughput is required to determine acceptable latency for the throughput. Additionally, the bandwidth may affect the required queue size to accommodate the estimated volume of data. VMware recommends a minimum of 1Mb of spare bandwidth be available for vCenter Server Heartbeat.

vCenter Server Heartbeat includes a Low Bandwidth Module for use in WAN environments. When enabled, the VMware Channel compresses the data, 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 ___

Install in network environment type:
- LAN ___
- WAN ___

Is the subnet the same at the Secondary site?
- If Yes, you need an IP address for this subnet ____
- Active Directory Integrated DNS? ____
  - If Yes, you need a Domain Account with rights to update DNS.
  - If No, then refer to the Knowledge Base articles in the Networking Section.

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.

1. Run setup.exe on the Primary server.

2. The first option is the Server Identity. Select Primary.

   Note: If you need help during the setup process, the left panel of the setup dialog explains each step or option.

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

4. 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, or SQL only)
   - The location to store the clone files

5. The setup process runs a Pre-Install Check to ensure that the server meets the appropriate requirements.

6. The setup installs vCenter Server Heartbeat.

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

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

Secondary Server

To set up the Secondary server, complete the following steps:

1. Run setup.exe to start the setup process for the Secondary server (physical or virtual).

2. The first option is the Server Identity. Select Secondary.

3. The setup identifies the backup file location and runs Pre-Install checks before installing vCenter Server Heartbeat on the Secondary server.

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

5. When using an Install Clone setup in a LAN environment, configure the Principal (Public) NIC to the same IP address as the Primary server.

6. After reconfiguring the Principal (Public) NIC (if necessary), initiate the restore process.

7. Once the restore is complete, if the secondary server is a physical server, Windows Plug and Play runs multiple times to detect hardware differences. Allow it to complete and if prompted, reboot.

8. When Plug and Play is complete, the setup process displays the Finish dialog.

9. Do **NOT** start vCenter Server Heartbeat on the Secondary server.

Post Installation Tasks

After installation and prior to starting vCenter Server Heartbeat, complete the following tasks:

1. Verify that the Date and Time and Time Zone on the Secondary server are identical to that of the Primary server.
2. Log in to the vCenter Server Heartbeat Console and add a Username and Password with rights to Virtual Infrastructure for the vCenter Plug-in.
3. If SQL Server is not installed on the same host as vCenter Server, in the Heartbeat Console, navigate to the **Advanced -> Communication -> Configuration** screen and configure the Heartbeat Interval from 20 secs to 30 secs.

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 location where SQL Server is hosted.

Installation Verification

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

Verifying vCenter Server Heartbeat

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 by methods such as unplugging a power cord. When power is lost, any data not written to the passive server is lost. VMware recommends a switchover rather than a failover to check 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 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 2 Exercise One Actions

Machine	Activity	Result
	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.
Primary	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	Check the Application functionality against the acceptance criteria.	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 demonstrates that all the correct services stop when the Primary server is 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 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).
	Check the vCenter Server Heartbeat logs to confirm no exception errors during the synchronization. Allow the Status of both the Registry and File System to become **Synchronized**.	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 4 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 functionality per previously defined acceptance criteria. Check the behavior of client applications 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.