Installation and Upgrade on Windows Server 2008/2012 When the Secondary Server is Virtual

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-001235-02

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

The Installation Guide provides key 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, this book provides an overview of installation procedures and guidance for configuration of vCenter Server Heartbeat when the Secondary node is virtual.

Intended Audience

This guide is intended for IT Administrators with a working knowledge of networking to include configuration and domain administration on Windows™ 2008 and 2012 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 and configuration of 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 manual and automatic failover processes.
- Chapter 2 — *vCenter Server Heartbeat Implementation* discusses environmental prerequisites and pre-install requirements for installation, server architecture options, cloning technology, application components, and network configurations. It also gives guidance on anti-malware solutions and provides a convenient summary of supported configurations as you perform the installation.
- Chapter 3 — *Installing vCenter Server Heartbeat* describes the installation process, guides you through installation on the Primary and Secondary nodes, and through post-installation configuration.
- Chapter 4 — *Upgrading* provides the procedures necessary to upgrade vCenter Server Heartbeat and vCenter Server and its components from the previous version to the current version.

- Chapter 5 — *Uninstalling vCenter Server Heartbeat* describes the procedure to uninstall and remove vCenter Server Heartbeat from your vCenter Server installation.
- Chapter 6 — *Installation Verification* provides the procedure to verify vCenter Server Heartbeat is properly installed and initially configured.
- Appendix A — *Setup Error Messages* lists error messages that may appear during setup and tests that help you resolve the errors.
- Appendix B — *Setup Troubleshooting* describes common issues that may be encountered during installation and provides procedures to resolve them.

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

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.

Introduction 1

This chapter includes the following topics:

vCenter Server Heartbeat Concepts

vCenter Server Heartbeat is a Windows based service specifically designed to provide High Availability (HA) or Disaster Recovery (DR) protection for vCenter Server configurations.

Architecture Overview

vCenter Server Heartbeat is deployed in an "Active–Passive" architecture enabling configuration for either "High Availability (HA)" in a Local Area Network (LAN)/Metropolitan Area Network (MAN) or "Disaster Recovery (DR)" in a Wide Area Network (WAN) for vCenter Server, View Composer and/or SQL Server.

Server Identity

vCenter Server Heartbeat software is installed on an existing production server instance (virtual or physical) known as the "Primary" node which runs the protected applications (vCenter Server, View and/or SQL Server). An additional server instance (virtual or physical), known as the "Secondary" node, operates as a ready standby to provide service in the event of an application, system, or hardware failure. The terms Primary and Secondary refer to the "Identity" of each node and do not change over the life of the node.

Active / Passive Roles

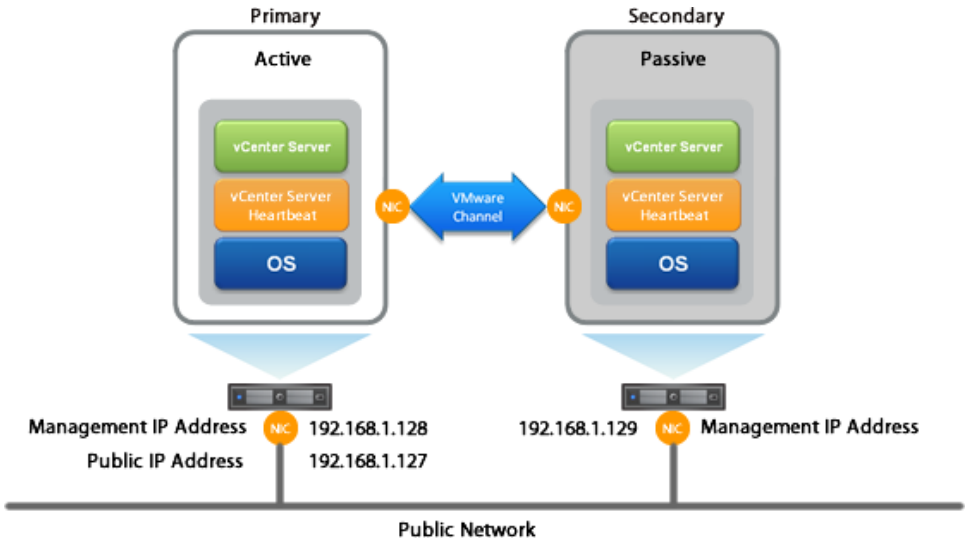
The "Role" of a node describes what the node is currently doing.

- Active Node – If the node is currently running protected applications, the node is said to be "Active". The active node will always host the running instance of protected applications. Only one node can be active at any one time.
- Passive Node – The "Passive" node acts as the ready standby for the active node. Protected applications are not running on the passive node.

IP Addressing

- "Public IP Address" – a static IP address used by clients to access protected applications hosted on the active node.
- "Management IP Address" – a unique permanent static IP address assigned to each node (Primary and Secondary) that is used for management of the node when the node is in the passive role.

Figure 1- 1. Architecture Overview



Managing the Primary and Secondary Servers

vCenter Server Heartbeat pairs are managed using standard network, domain policy, and domain management procedures with each node (both Primary and Secondary) assigned a unique domain name. Each domain name differs from the fully qualified domain name (FQDN) used by the original vCenter or SQL servers. Additionally, a Management IP address on each node ensures that the Administrator can access the node even when it is passive thereby allowing use of 3rd party monitoring tools and maintenance operations.

Failover Overview

The role of the nodes can be changed by a process known as "Failover" that is initiated automatically by vCenter Server Heartbeat or manually by the administrator.

vCenter Server Heartbeat uses failover to ensure that vCenter Server and its components are continuously available should a critical failure occur such as vSphere ESX host network failure. When a failover occurs, clients continue to connect to vCenter Server. View, or SQL Server using the vCenter Server service name which is the original and unique fully qualified domain name that was used previously by clients.

During installation, the service name is configured in vCenter Server Heartbeat which continues to resolve to the Public IP address in DNS regardless of which node is hosting the Public IP address.

- *Failover in a LAN* – When deployed in a LAN environment, the Public IP address is moved between the Primary and Secondary nodes as roles change from active to passive so that the protected applications are available to clients only when the node assumes the active role. When vCenter Server Heartbeat is started, the Public IP address is added to the active node. When a failover occurs, the Public IP address is removed from the active node as it becomes passive and then added to the passive node which is being made active. vCenter Server Heartbeat does not require updates to DNS during the failover; however, the DNS server must be preconfigured with the Management IP addresses.
- *Failover in a Stretched VLAN* – vCenter Server Heartbeat can also be deployed in a stretched VLAN using the same subnet for the production and the disaster recovery site.

  Similar to a LAN installation, this configuration requires that both the Primary and Secondary nodes share the Public IP address. The active node reveals the Public IP address while the passive node is hidden from the network resulting in vCenter Server Heartbeat being deployed without any changes to DNS during failover operations, just as in the LAN deployment.
- *Failover in a WAN* – vCenter Server Heartbeat can be deployed in a WAN where each site uses different subnets. When deployed in this manner, each site has a different Public IP address. When a failover occurs, vCenter Server Heartbeat automatically updates the DNS server with the Public IP address of the new site thereby allowing clients to connect to the new site.

vCenter Server Heartbeat Protection

vCenter Server Heartbeat provides the following protections:

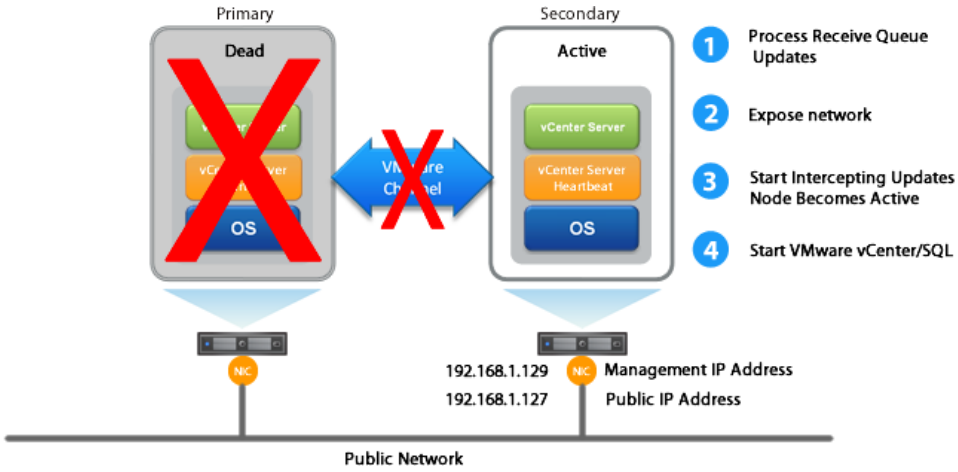
- *Server Protection* – provides continuous availability to end users through an operating system crash or hardware failure scenario ensuring that users are provided with a replica server instance and its IP address should the production node fail.
- *Network Protection* – proactively monitors the network by polling up to three predefined nodes to ensure that the active node is visible on the network.
- *Application Protection* – monitors the application environment ensuring that protected applications and services stay alive and are available on the network.
- *Performance Protection* – proactively monitors system performance attributes to ensure the system administrator is notified of problems and can take pre-emptive action to prevent an outage.
- *Data Protection* – intercepts all data written by users and applications, and maintains a copy of the data on the passive node 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 vCenter Server and its components continue to operate through as many failure scenarios as possible.

Server Protection

The Primary and Secondary nodes regularly send “I’m alive” messages to one another over a dedicated network connection referred to as the “VMware Channel” to detect interruptions in responsiveness. If the passive node detects that this monitoring process (referred to as the “Heartbeat”) has failed, it initiates an auto-failover as illustrated in Figure 1-2.

Figure 1- 2. vCenter Server Heartbeat Initiated Failover



An auto-failover occurs when the passive node detects that the active node is no longer responding. This can occur when the active node operating system crashes, loses its network connections, host hardware fails, or otherwise becomes unavailable. The failover process is discussed in detail later in this guide.

Network Protection

vCenter Server Heartbeat proactively monitors the network by polling up to three predefined IP addresses to ensure that the active node is visible on the network. vCenter Server Heartbeat polls by default the Primary DNS server, the Default Gateway, and the Global Catalog server at regular intervals. If all three nodes fail to respond, for example in the case of a network card or switch failure, vCenter Server Heartbeat can initiate a failover, allowing the Secondary node to assume the active role and service clients.

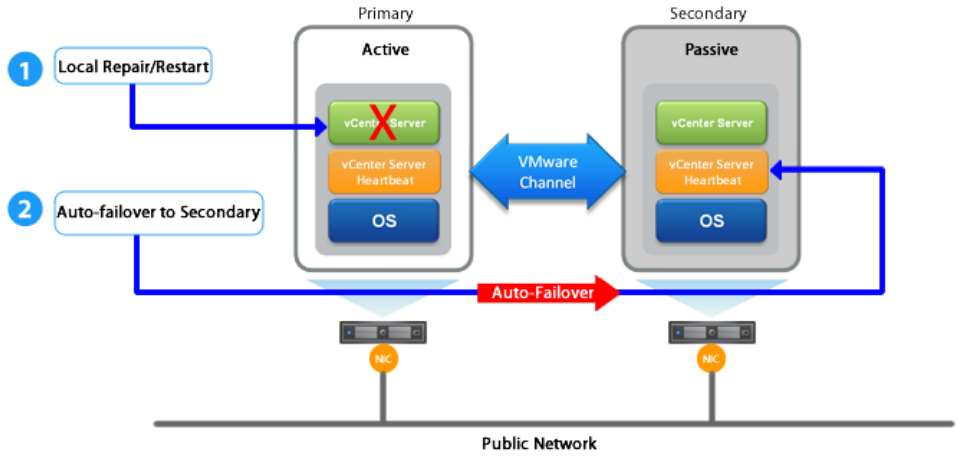
Application Protection

vCenter Server Heartbeat running on the active node locally monitors vCenter Server and its services to verify that vCenter Server is operational and not in an unresponsive or stopped state. This level of monitoring is fundamental in ensuring that vCenter Server remains available to users.

If vCenter Server should fail, vCenter Server Heartbeat first attempts to restart the application on the active node (1) in Figure 1-3.

If the application does not successfully restart, vCenter Server Heartbeat initiates an auto-failover (2) in Figure 1-3. Refer to “vCenter Server Heartbeat Failover Processes,” on page 16 for further information about the failover process.

Figure 1- 3. vCenter Server Heartbeat Initiated Failover



When vCenter Server Heartbeat initiates a failover as a result of a failed application or service, vCenter Server Heartbeat gracefully closes vCenter Server running on the active node and starts it on the passive node, including the component or service that caused the failure. For example, if the Primary is active and the Secondary is passive, the Primary is demoted to a passive role and is hidden from the network while the Secondary is promoted to an active role and is made visible to the network. The mechanics of a failover are discussed in more detail later in this guide.

Performance Protection

To ensure that vCenter Server is operational and providing service at an adequate level of performance to meet user demands, vCenter Server Heartbeat employs the vCenter Server Heartbeat Plug-in which provides performance monitoring and pre-emptive remediation capabilities. vCenter Server Heartbeat proactively monitors system performance attributes and can notify the system administrator in the event of a problem and can also be configured to take pre-emptive action to prevent an outage.

In addition to monitoring vCenter Server services, vCenter Server Heartbeat can monitor specific 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 ability 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

All data files that users or vCenter Server requires in the application environment are protected and 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 node by mirroring them in real time to the passive node. If a failover occurs, all files protected on the failed (Primary) node are available to users after the failover, hosted on the Secondary node.

vCenter Server Heartbeat intercepts all file system operations on the active node. Those write and update operations which are part of the protected set are placed in the “Send Queue” of the active node pending transmission to the passive node.

With the channel connected, the active node’s send queue is transferred to the passive node, which places all the requests in the passive node’s “Receive Queue”. The passive node confirms the changes were logged by sending the active node an acknowledgment. The active node then clears the data from its send queue. The apply process running on the passive node applies all updates thereby creating a duplicate identical set of file operations on the passive node.

vCenter Server Heartbeat Communications

The VMware Channel is a crucial component of vCenter Server Heartbeat and can be configured in a number of ways.

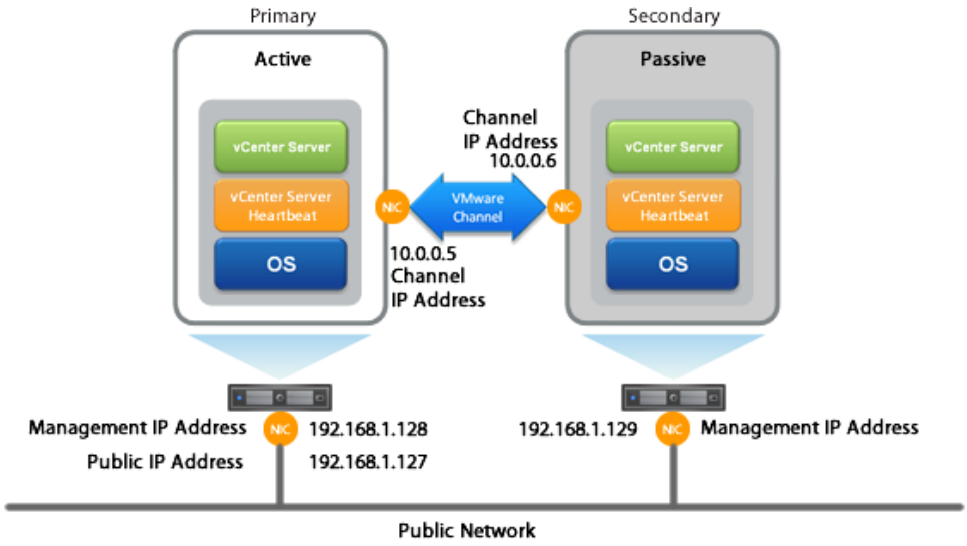
vCenter Server Heartbeat supports use of either multiple NICs or a single NIC. Both the Primary and Secondary must have the same number of NICs. The Public IP address provides client access and the Management IP address provides administrative access, while the VMware Channel provides for data transfer and control.

Multi-NIC Configuration

When installed using multiple NICs, a second pair of NICs can be configured for the VMware Channel to provide a degree of redundancy. To provide added resilience, the communications for the second channel should be completely independent from the first channel. They should not share any switches, routers, or the same WAN connection.

Configuring vCenter Server Heartbeat using multiple NICs (1 for the Public and Management IP and 1 for the VMware Channel IP) prevents a single point of failure in the system. Additionally, it allows vCenter Server Heartbeat to monitor availability of the nodes independently via the Public network and the VMware Channel network.

Figure 1- 4. Multi-NIC Configuration

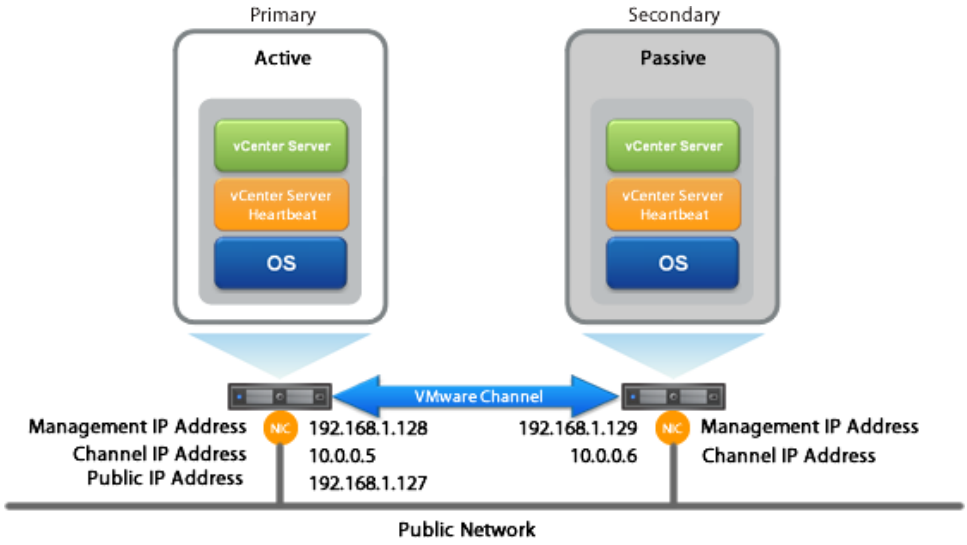


Single NIC Configuration

When installing using a single NIC, the Public IP, the Management IP, and the VMware Channel IP addresses are all configured on the same NIC.

Configuring vCenter Server Heartbeat with a single NIC on each node creates a network environment with a single point of failure where a malfunction of the NIC on either node can cause protection failure.

Figure 1- 5. Single NIC Configuration



LAN and Stretched vLAN Deployment

When deployed in a LAN, the Public NIC on the active node is configured with both a unique permanently assigned Management IP address for administrative access and the Public IP address which allows traffic from clients. The Public NIC on the passive node is configured to use its unique permanently assigned Management IP address. When a failover occurs, the Public IP address assigned to the currently active node is removed and reassigned to the new active node. The new passive node remains accessible to administrators via the Management IP address but is not visible to clients. The newly active node then starts accepting traffic from clients.

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

DNS in a LAN or Stretched vLAN

When deployed in a LAN or stretched vLAN configuration, should a failover occur, the Public IP address is simply removed from the currently active server and reassigned to the currently passive server without a need to update DNS. Clients continue to communicate to the same Public IP address that was used before the failover.

WAN Deployment

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.

DNS in a WAN Deployment

When deployed in a WAN configuration, should a failover occur, vCenter Server Heartbeat automatically updates DNS with the IP address of the new active server using vCenter Server Heartbeat's own DNSUpdate.exe utility.

vCenter Server Heartbeat Failover Processes

vCenter Server Heartbeat provides for failover from one node to the other node when initiated manually by the administrator or automatically as a result of hardware, operating system, network communications, protected applications, or services failure. Failover changes the role of the active and passive nodes depending on the status of the active node.

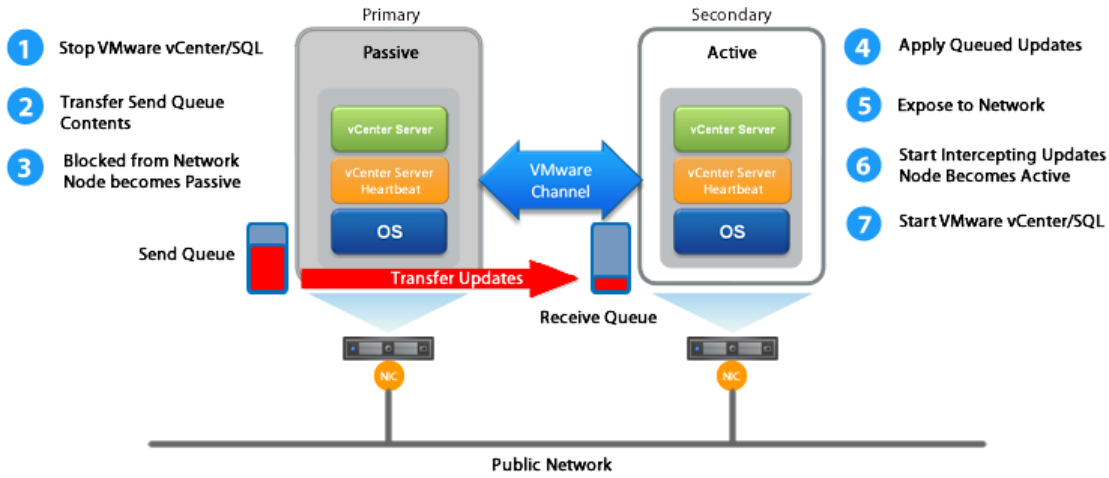
vCenter Server Heartbeat failovers are categorized by how the failover is initiated.

- When a failover is initiated manually by an administrator, the failover gracefully changes the roles between the active node and the passive node. This type of failover is frequently used to perform maintenance on the node or its software.
- If a failover is initiated automatically due to hardware, operating system, or network communications rendering the active node unavailable, vCenter Server Heartbeat considers the active node has failed and immediately initiates the process to change the role of the passive node to active.
- Should vCenter Server Heartbeat detect that the active node is alive but that a protected application or service has failed, it can first attempt to restart the application or service to correct the problem and if unsuccessful, initiate a failover causing the active and passive nodes to change roles making the passive node active and the active node passive.

Failover - Manually Initiated by an Administrator

You can click **Make Active** on the Heartbeat tab of the vSphere Web Client or the *Server: Summary* page of the vCenter Server Heartbeat Console to manually initiate a failover. When a failover is triggered, the running of protected applications is gracefully transferred from the active node to the passive node in the pair. The roles of the nodes are reversed.

Figure 1- 6. Failover



A manually initiated failover performs the following steps:

1 Stop the protected applications on the active node. After the protected applications stop, no more disk updates are generated.

2 Send all updates that are still queued on the active node to the passive node. After this step, all updates are available on the passive node.

3 Re-designate the Secondary as the new active node. After this step, vCenter Server Heartbeat:

- Reassigns the Public IP address to the Secondary in a LAN or updates DNS in a WAN.
- Makes the newly active node visible on the network. The newly active node begins to intercept and queue disk I/O operations for the newly passive node.

4 vCenter Server Heartbeat causes the newly passive node to begin accepting updates from the active node.

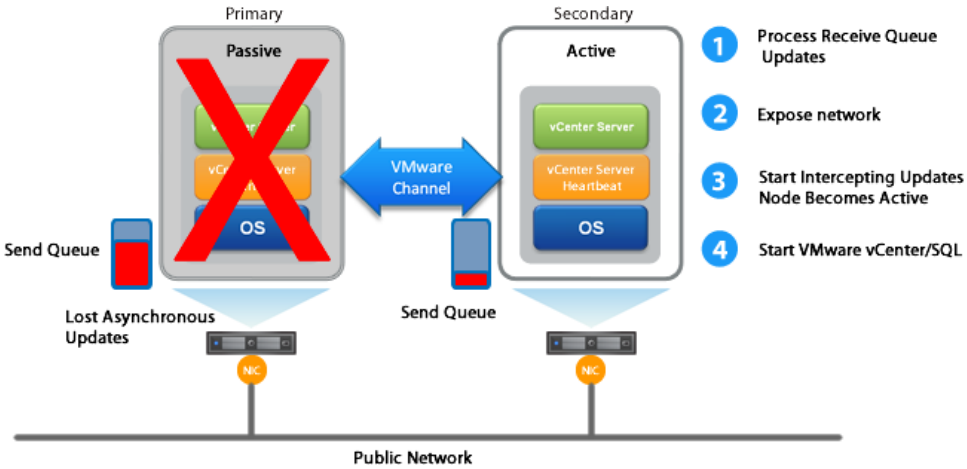
5 vCenter Server Heartbeat starts the same protected applications on the new active node. The protected applications become accessible to users. The failover is complete

Failover - Automatically Initiated by vCenter Server Heartbeat

Automatic failover (auto-failover) is triggered when system monitoring detects failure of a protected application or when the passive node detects that the active node is no longer running properly and assumes the role of the active node.

Resulting from a hardware, operating system, or network communications failure

Figure 1- 7. Automatic Failover (failed node)



During the auto-failover, the passive node performs the following steps:

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

The amount of data in the passive node's receive queue affects the time required to complete the failover process. If the passive node's receive queue is long, the system must wait for all updates to the passive node 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 node's receive queue. Update records that cannot be applied are discarded.

2 Switch mode of operation from passive to active.

This enables the public identity of the new active node. The shared Public IP address is assigned to the new active node and the node becomes available to clients that were connected to the previously active node before the auto-failover and clients are able to reconnect.

3 Start intercepting updates to protected data and store the updates in the send queue of the local node.

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.

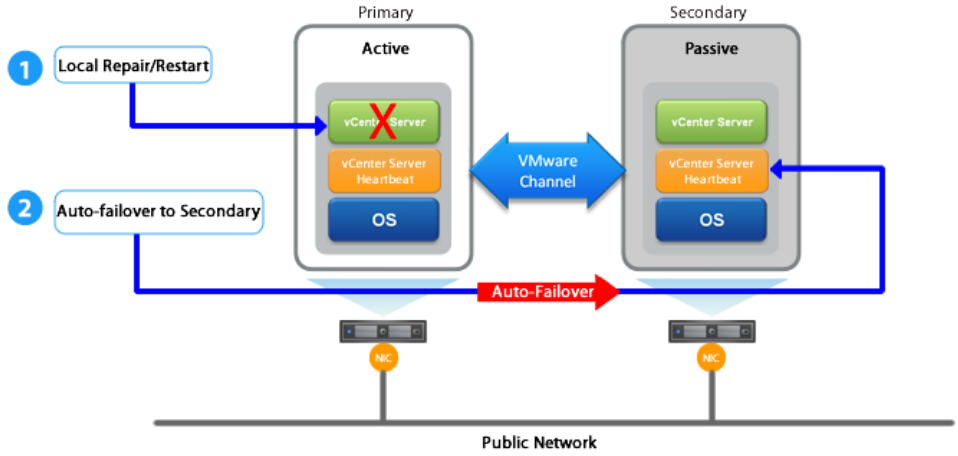
At this point, the originally active node is offline and the originally passive node is filling the active role and running the protected applications. Any updates completed before the auto-failover are retained. Application clients can reconnect to the application and continue running as before.

Resulting from a failed application or service

When an auto-failover occurs as the result of a failed protected application, auto-failover changes the roles of the nodes but then stops vCenter Server Heartbeat on the previously active node to allow the administrator to investigate the cause of the auto-failover and verify the integrity of the data.

After the cause of the auto-failover is determined and problems are corrected, the administrator can use the Heartbeat tab of the vSphere Web Client or the vCenter Server Heartbeat Console to return the node roles to their original state.

Figure 1- 8. Auto-Failover (protected application failure)



1 Stop the protected applications on the active node. After the protected applications stop, no more disk updates are generated.

2 Send all updates that are still queued on the active node to the passive node. After this step, all updates are available on the passive node.

3 Re-designate the Secondary as the new active node. After this step, vCenter Server Heartbeat:

- Reassigns the Public IP address to the Secondary in a LAN or updates DNS in a WAN.
- Makes the newly active node visible on the network. The newly active node begins to intercept and queue disk I/O operations for the newly passive node.

4 vCenter Server Heartbeat causes the newly passive node to begin accepting updates from the active node.

5 vCenter Server Heartbeat starts the same protected applications on the new active node. The protected applications become accessible to users.

Failover in a WAN Environment

Failover in a WAN environment differs from Failover in a LAN environment due to the nature of the WAN connection. In a WAN environment, auto-failover is disabled by default in the event that the WAN connection is lost.

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

Implementation 2

This chapter discusses 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 at the end of this chapter provides a visual reference to configuration options supported by vCenter Server Heartbeat.

This chapter includes the following topics:

vCenter Server Heartbeat Implementation

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 protects vCenter Server and SQL Server installed on the same node or in a distributed configuration. This flexibility enables vCenter Server Heartbeat to protect vCenter Server when using remote databases other than SQL Server.

During the installation process, vCenter Server Heartbeat performs a variety of checks to ensure the node meets the minimum requirements for a successful installation. A critical stop or warning message appears if the node fails a check. Refer to the Appendix B, "Setup Error Messages," on page 75 in this guide for a list of the checks and an explanation of the messages. 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 supports multiple versions of vCenter Server and its services.

Supported Environments

- vCenter Server Heartbeat is supported on the following versions of Windows Server
  - Windows Server 2012 R2 Standard/Datacenter
  - Windows Server 2012 Standard/Datacenter up to SP1
  - Windows Server 2008 R2 Standard/Enterprise/Datacenter up to SP1
  - Windows Server 2008 x64 Standard/Enterprise/Datacenter up to SP2
  - Windows Server 2008 x86 Standard/Enterprise/Datacenter up to SP2 (supporting SQL Server only)

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

- vCenter Server Heartbeat supports the following versions of vCenter Server
  - vCenter Server 5.0 and its updates
  - vCenter Server 5.1 and its updates
  - vCenter Server 5.5 and its updates

  Important Ensure that all VMware services are bound to the Public IP address on the Public network adapter.

- vCenter Server Heartbeat supports the following versions of SQL Server Database on Windows Server x64 Platforms

Table 2- 1. SQL Server Support on x64 Platforms

SQL Version	Edition			Service Pack	Windows Version	Edition			Service Pack
	Std	Ent	DC			Std	Ent	DC	
2014	X	X	NA		2012 R2	X	NA	X	
	X	X	NA		2012	X	NA	X	up to SP1
	X	X	NA		2008 R2	X	X	X	up to SP1
2012	X	X	NA		2012	X	NA	X	
	X	X	NA		2008 R2	X	X	X	up to SP1
	X	X	NA		2008	X	X	X	up to SP2
2008 R2	X	X	X	up to SP2	2012	X	NA	X	
	X	X	X	up to SP2	2008 R2	X	X	X	up to SP1
	X	X	X	up to SP2	2008	X	X	X	up to SP2

Table 2- 1. SQL Server Support on x64 Platforms

SQL Version	Edition			Service Pack	Windows Version	Edition			Service Pack
	Std	Ent	DC			Std	Ent	DC	
2008	X	X	NA	SP2 & SP3	2012	X	NA	X	
	X	X	NA	SP2 & SP3	2008 R2	X	X	X	up to SP1
	X	X	NA	SP2 & SP3	2008	X	X	X	up to SP2
2005	X	X	NA	SP4	2008	X	X	X	up to SP2

Note This version of vCenter Server Heartbeat also supports 32 bit versions of SQL Server 2005/2008/2012 installed on x64 Operating Systems.

Unsupported Environments

- The following environments are not supported by vCenter Server Heartbeat
  - On a server deployed as a "Domain Controller (DC)"
  - On a server deployed as a "Global Catalog Server" Server
  - On a server deployed as a "DNS (Domain Name System) Server"
  - On an IA-64 Itanium Platform

User Account Control (UAC)

VMware recommends that User Account Control (UAC) be disabled on both the Primary and Secondary nodes prior to initiating installation of vCenter Server Heartbeat on Windows Server 2008, 2008R2, 2012, and 2012R2. Once installation is complete, UAC may be re-enabled.

Attempting to install vCenter Server Heartbeat with UAC enabled may cause multiple issues during Setup thus preventing vCenter Server Heartbeat from installing properly.

Pre-Install Requirements

Prior to installing vCenter Server Heartbeat, the following requirements must be met and are in addition to those required for vCenter Server, SQL Server, and their components.

- Verify that the Primary node is a member of the domain. The Domain for the Primary node does not change throughout the installation process although the Primary and Secondary node names change as part of the installation procedure.
- Verify that User Account Control (UAC) has been disabled on both the Primary and Secondary nodes before initiating installation of vCenter Server Heartbeat.
- vCenter Server Heartbeat only protects the vCenter Server and its components and SQL Server applications. Verify no other critical business applications are installed on the node.
- Verify that vCenter Guided Consolidation, vCenter Update Manager, vCenter Converter, ESXi Dump Collector, Syslog Collector, Auto Deploy, and Authentication Proxy are configured using Fully Qualified Domain Names (FQDN) rather than IP addresses.

- Verify that there is a minimum of 1GB of available RAM (2GB recommended) in addition to any other memory requirements for the Operating System or vCenter Server.
- Verify that a minimum 2GB of free disk space is available on the installation drive for vCenter Server Heartbeat.
- Obtain and use local administrator rights to perform vCenter Server Heartbeat installation. See knowledge base article 2017529 - *Performing a Least Privilege Installation of vCenter Server Heartbeat*.
- Apply the latest Microsoft security updates.
- All applications to be protected by vCenter Server Heartbeat must be installed and configured on the Primary node prior to installing vCenter Server Heartbeat.
- Verify that both Primary and Secondary nodes have identical system date, time, and time Zone settings.
- Verify that the Managed IP setting displayed in the Virtual Infrastructure Client is the same IP address used for the vCenter Server Heartbeat Public IP address.
- Verify that Windows Server Backup Feature and Command Line Tools are installed on the Primary and Secondary nodes prior to installing vCenter Server Heartbeat. Installation of Windows Server Backup Feature and Command Line Tools also installs Windows PowerShell.
- Verify that all services to be protected are running or set to *Automatic* prior to installation. During installation, protected services are set to manual to allow vCenter Server Heartbeat to start and stop services depending on the node's role. The target state of the services is normally running on the active node and stopped on the passive.
- Configure Management IP addresses on the Public NIC on both the Primary and Secondary nodes.

  Important Use adjacent IP addresses for the Public IP address and the Management IP address for the Primary and Secondary Servers when installing vCenter Server Heartbeat on servers running Windows 2008.

- Configure any firewalls to allow traffic to pass through both the *Client Connection port* (52267) and the *Default Channel port* (57348).

Server Deployment Architecture Options

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

Virtual to Virtual

Virtual to Virtual is the supported architecture if vCenter Server is already installed on the production (Primary) node 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 node must meet the minimum requirements.

- The specifications of the Secondary node must match the specifications of the Primary node 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.

  Important In a vSphere HA and DRS enabled cluster, set VM anti-affinity rules on the pair to ensure the VM's aren't placed on the same host to guard against failure at the host level.

- If using more than one NIC, 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. This architecture is appropriate to avoid adding more physical nodes or if you plan to migrate to virtual technologies over a period of time.

The Secondary virtual machine must meet the minimum requirements.

- The specifications of the Secondary virtual machine must match the Primary physical node 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.

Cloning Technology Options

Cloning the Primary node to create a nearly identical Secondary node 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 node before you begin installing vCenter Server Heartbeat:

- Use VMware vCenter Converter when cloning in a Physical to Virtual environment.

  Important When installing in a Physical to Virtual architecture, VMware Tools must not be installed on the Secondary node during the vCenter Server Heartbeat installation process. If VMware Tools are currently installed on the Secondary node, you must fully uninstall VMware Tools prior to initiation of the Setup process. Once the installation of vCenter Server Heartbeat has completed, you may reinstall VMware Tools.

- Use VMware vCenter virtual machine cloning when cloning in a Virtual to Virtual environment.

  Important When installing in a Virtual to Virtual architecture, VMware Tools must be installed and running on the Primary node before starting the vCenter Server Heartbeat installation process.

Application Component Options

vCenter Server Heartbeat supports the following additional VMware vCenter Server components:

- VMware View Composer 2.7, 5.0, 5.2, and 5.3

  Note Remote deployment of View Composer is supported starting with View Composer 3.0

- VMware Universal File Access
- vCenter Converter Enterprise

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

Table 2- 2. vCenter Server Heartbeat Protected Services

Service	Version 5.0	Version 5.1	Version 5.5
VMware vCenter Inventory Service	X	X	X
VMware ADAM	X	X	NA
VMWare VCMSDS	NA	NA	X
VMware USB Arbitration Service	X	X	X
VMware vCenter Server	X	X	NA
VMware VirtualCenter Server	NA	NA	X
VMware vSphere Client	X	X	NA

Table 2- 2. vCenter Server Heartbeat Protected Services

Service	Version 5.0	Version 5.1	Version 5.5
VMware vSphere Web Client	X	X	X
VMware vCenter Update Manager	X	X	NA
VMware vSphere Update Manager Service	NA	NA	X
VMware vSphere Update Manager Download Service	NA	X	X
VMware vSphere Update Manager UFA Service	NA	NA	X
VMware vCenter Orchestrator Configuration	X	X	X
VMware vCenter Orchestrator Server	X	X	X
VMware vSphere ESXi Dump Collector	X	X	X
VMware vSphere ESXi Dump Collector Web Server	X	NA	X
VMware Syslog Collector	X	X	X
VMware vSphere Syslog Collector	NA	NA	X
VMware vSphere Auto Deploy	NA	X	NA
VMware vSphere Auto Deploy Waiter	X	NA	X
VMware vSphere Authentication Proxy	X	X	X
VMware vSphere Authentication Proxy Adapter	X	NA	X
VMware vCenter Management Web Server	X	NA	NA
VMware VirtualCenter Management Webservices	NA	NA	X
VMware vSphere Host Update Utility	X	NA	NA
VMware vCenter Host Agent Pre-Upgrade Checker	NA	X	X
VMware vCenter Single Sign-On	NA	X	NA
vCenter Single Sign-On	NA	NA	X
VMware Log Browser	NA	NA	X
VMware vSphere Profile-Driven Storage Service	X	X	X
RSA SSPI Service	NA	X	X

Important Ensure that all VMware services are bound to the Public IP address on the Public network adapter.

vCenter Deployment Models

vCenter Server Heartbeat supports protection of vCenter Server in the following deployment models.

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 in a Distributed Environment

In a distributed environment with remote services to be protected, vCenter Server Heartbeat must be installed for each distributed service at the service site. For example, when installing vCenter Server Heartbeat in an environment where SQL Server is on a host, separate from vCenter Server, you must repeat the installation process on the SQL Server's Primary and Secondary nodes.

vCenter Server Heartbeat Interoperability

vCenter Server Heartbeat supports interoperability with multiple VMware technologies as indicated below.

- Linked Mode - vCenter Server Heartbeat supports protection of both Standalone instances of vCenter Server and Linked Mode groups. For more information about Linked Mode groups, see knowledge base article 1022869 - *Joining or isolating a vCenter Server instance from a Linked Mode Group when protected by vCenter Server Heartbeat*.
- vSphere HA/DR - vCenter Server Heartbeat supports High Availability for vCenter Server. For more information about configuring vSphere HA/DR, see the VMware vSphere Availability Guide.
- Site Recovery Manager (SRM) - Site Recovery Manager supports use of vCenter Server Heartbeat. For more information, see knowledge base article 1014266 - *Using vCenter Heartbeat With SRM*.

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 type has specific configuration requirements to ensure proper operation.

vCenter Server Heartbeat can be configured to run using either multiple NICs (recommended) or a single NIC.

Multiple NICs

vCenter Server Heartbeat supports use of multiple NICs on each node in the pair. When using multiple NICs, one NIC is configured with the Public IP address for client access and a Management IP address for administrator access while a second dedicated NIC is configured with the VMware Channel IP address. Deploying with multiple NICs provides the advantage of redundancy and also removes the risk of a single point of failure that exists in single NIC configurations. To configure using multiple NICs on each node, see “Multi-NIC Configuration,” on page 31.

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 - *Installing the Packet Filter Driver while recreating a NIC team with Intel drivers* for more information about teamed NICs.

Single NIC

vCenter Server Heartbeat also supports use of a single NIC configured to perform all three functions, providing the Public IP address to users, the Management IP address, and the VMware Channel for data transfer and control. To configure using a single NIC on each node, see “Single NIC Configuration,” on page 32.

Local Area Network (LAN)

When deployed in a LAN environment, vCenter Server Heartbeat requires that both nodes use the same Public IP address. Each node also requires a VMware Channel IP address and a Management IP address.

Important 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 after installation is complete.

Wide Area Network (WAN)

vCenter Server Heartbeat supports sites with different subnets. In this scenario, the Primary and Secondary nodes in the vCenter Server Heartbeat Pair require unique Public IP addresses, unique VMware Channel IP addresses for each node in a different subnet, and unique Management IP addresses for each node in the same subnets as the Public IP addresses. During Setup, select the *Use different IP addresses for Secondary (Recommended for DR secondary)* and specify the Public IP addresses of both the Secondary node and the Primary node.

Note vCenter Server Heartbeat requires automatic DNS registration of network connections to be *disabled*. If the *Register this connection's addresses in DNS* checkbox is selected, the resulting configuration may cause unexpected results during reverse DNS lookup operations, since the Public address would be registered twice in DNS, first by the network adapter on the currently active server against its machine name, and second via the static records added manually for the Public Service Name, resulting in an conflict when performing a Reverse DNS Lookup on the Public address. As a result, Reverse DNS Lookup may not provide the expected name.

For example, if a component were to communicate with vCenter Server via the Public Service Name, vCenter Server would respond via the Public IP address. If the component then performed a Reverse DNS Lookup on the Public IP address to identify the name of the responder, the reverse lookup may provide the active server machine name rather than the expected Public Service Name.

vCenter Server Heartbeat also supports sites with the same subnet. In this scenario, vCenter Server Heartbeat shares a single Public IP address between the Primary and Secondary nodes assigning it to the active node. When configured in this manner, the VMware Channel addresses should be unique within the same subnet. During Setup, select the *Use same IP addresses for Secondary (Recommended for HA secondary)* on the *Public IP Address* page and specify the IP address to be shared by both nodes.

WAN Requirements

WAN deployments require the following:

- Persistent static routing configured for the channel connection(s) where routing is required
- One NIC minimum, 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 uses the same subnet:
  - During install, follow the steps for a LAN or VLAN on the same subnet
  - Both nodes 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 nodes in the vCenter Server Heartbeat pair require a separate Public IP address and a VMware Channel IP address
  - Provide a user account with rights to update DNS using the DNSUpdate.exe 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.exe 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:
    - Knowledge base article 1008571 - *Configuring DNS with VMware vCenter Server Heartbeat in a WAN Environment*
    - Knowledge base article 1008605 - *Configuring vCenter Server Heartbeat to Update BIND9 DNS Servers Deployed in a WAN*

Bandwidth

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 node.

Determine the available bandwidth and estimate the required volume of data throughput to determine acceptable latency for the throughput. Bandwidth can affect the queue size required to accommodate the estimated volume of data. VMware recommends making a minimum of 1Mbit of spare bandwidth available to vCenter Server Heartbeat.

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 node workload. For more information about Heartbeat Diagnostics, contact VMware Professional Services.

Network Interface Card (NIC) Configuration

vCenter Server Heartbeat supports the use of both a single NIC or multiple NIC configuration on Primary and Secondary nodes. The number of NICs present will determine how the NICs are configured.

Important The Primary and Secondary nodes must have the same number of NICs.

Multi-NIC Configuration

When using multiple NICs, one NIC functions for client and management access while a second NIC functions as a dedicated VMware Channel.

Primary Node

The Primary node is configured with the following connections:

- *Public* - network connection configured with a static Public IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.
- *Management IP* - connection using the same subnet and NIC as the Public IP address, configured with a static IP address in the same subnet as the Public IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.
- *VMware Channel* - connection(s) configured with a static IP address in a different subnet than the Public IP address or Management IP address with a different IP address than the Secondary node channel NIC, and network mask. No gateway or DNS server address is configured. NetBIOS is disabled during the installation process to prevent node name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared on all connections prior to installing vCenter Server Heartbeat.

Secondary Node

The Secondary node must have the same number of NICs as the Primary node and is configured with the following connections:

- *Public* - network connection configured with a static IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.

  Note If deploying in a WAN, the Public IP address of the Secondary node may be in a different subnet than the Primary node.

- *Management IP* - connection using the same subnet as the Secondary node's Public IP address, configured using a static IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.
- *VMware Channel* - connection(s) configured on a separate dedicated NIC with a static IP address in a different subnet than the Secondary Public IP or Management IP address and with a different IP address than the Primary VMware Channel IP address and network mask. No default gateway or DNS server address is configured. NetBIOS is disabled during the installation process to prevent node name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared on all connections prior to installing vCenter Server Heartbeat.

Single NIC Configuration

Configuring vCenter Server Heartbeat using a single NIC requires that all three functions (Client access, Management access, and Channel operations) use the same physical or virtual NIC.

Primary Node

The Primary node requires a single NIC configured with the following IP addresses:

- *Public IP* address - configured using a static IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.
- *Management IP* address - configured on the same NIC as the Public IP address with a unique static IP address in the same subnet as the Public IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.
- *VMware Channel IP* address - configured on the same NIC as the Public IP address and Management IP address, configured with a static IP address in the same or different subnet than the Public IP address or Management IP address, and a network mask. No gateway address or DNS server address is configured. NetBIOS is disabled during the installation process to prevent node name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared prior to installing vCenter Server Heartbeat.

Secondary Node

The Secondary node must have the same number of NICs as the Primary node and be configured as follows:

- A *Management IP* address - configured on the same NIC as the VMware Channel address with a unique static IP address in the same subnet as the Public IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.
- A *VMware Channel IP* address - configured on the same NIC as the Management IP address with a static IP address in the same or different subnet than the Management IP address, and the network mask. No gateway or DNS server address is configured. NetBIOS is disabled during the installation process to prevent node name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared prior to installing vCenter Server Heartbeat.

Configure Firewalls

When firewalls are used to protect networks, you must configure them to allow traffic to pass through both the *Client Connection port* (52267) and the *Default Channel port (57348)*.

Important When installing on Windows Server 2008/2012, Microsoft Windows may change the connection type from a Private network to an Unidentified network after you have configured the firewall port to allow channel communications resulting in the previously configured firewall changes to be reset for the new network type (Unidentified).

The firewall rules must be recreated to allow traffic to pass through for the Client Connection port and the Default Channel port. VMware recommends that the firewall be configured to allow the Client to connect to the Client Connection port by process, nfgui.exe, rather than by a specific port. To enable Channel communications between nodes, change the Network List Manager Policy so that the VMware Channel network is identified as a Private Network, not the default Unidentified Network, and configure the firewall to allow traffic to pass through on Port 57348, the Default Channel port.

Anti-Malware Recommendations

Consult with and implement the advice of your anti-malware provider as VMware guidelines often follow these recommendations. Consult the VMware Knowledge Base for up-to-date information on specific anti-malware products.

Do not use file level anti-malware to protect application server databases, such as MS SQL Server databases. The nature of database contents can cause false positives in malware 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 anti-malware temp files using vCenter Server Heartbeat.

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

Configure file level anti-malware to use the Management IP address on the passive node for malware definition updates. If this is not possible, manually update malware definitions on the passive node.

Exclude the following VMware directories from file level anti-malware 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 anti-malware product on one node (such as exclusions) must be made on the other node as well. vCenter Server Heartbeat does not replicate this information.

Deployment Options Summary

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

Table 2- 3. Installation Options

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

Note Installation using the Install Clone technique is not supported when performing Unattended Installations.

Installing vCenter Server Heartbeat 3

This chapter discusses the installation process used to implement vCenter Server Heartbeat on Windows Server 2008 when the Secondary node is virtual. 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.

Important Before initiating the installation of vCenter Server Heartbeat, ensure that the Primary node is assigned the intended Public name.

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 node fail one of the checks, a critical stop or warning message appears. Refer to the Appendix B, "Setup Error Messages," on page 75 in this guide for a list of the checks and an explanation of the messages. You must resolve critical stops before you can proceed with setup.

This chapter includes the following topics:

Primary Node

Procedure

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 node.

2 Open *Network Connections*, right-click the VMware Channel network connection and select *Properties*.

3 Select *Internet Protocol (TCP/IP)* and click **Properties**.

4 Click **Advanced**, select the *DNS* tab and clear the *Register this connection's addresses in DNS* check box.

5 You have the following options:

- If using multiple NICs click **OK** three times to close the dialogs and continue with Step 6.
- If using a single NIC, go to Step 9.

6 Right-click the *Public* network connection and select *Properties*.

7 Select *Internet Protocol (TCP/IP)* and click **Properties**.

8 Click **Advanced**, select the *WINS* tab and select *Disable NetBIOS over TCP/IP*. Select the *DNS* tab, and clear the *Register this connection's addresses in DNS* check box. Click **OK** three times to close the dialogs.

9 Configure the Management IP address on the Public NIC.

   a Right-click the network connection and select *Properties*.

   b Select *Internet Protocol (TCP/IP)* and click **Properties**.

   c Click **Advanced**, select the *IP Settings* tab, and in the *IP addresses* pane, enter the Management IP address. Click **OK** three times to close the dialogs.

10 You have the following options:

   - If protecting vCenter Server 5.0 continue with Step 11.
   - If protecting vCenter Server 5.1 or 5.5, go to Step 13.

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

12 Select the following services and set them to *Manual*.

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

   Note During the installation process, vCenter Server Heartbeat will install its own instance of Tomcat Webservices independent from vCenter Server.

13 Clone the Primary node using either VMware vCenter Converter, vCenter virtual machine cloning, or another third-party utility to create a cloned image of the Primary node. VMware recommends that you rename the node during the cloning process if possible. Do not start the cloned node.

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

14 Double-click the self-extracting file to initiate the installation process on the Primary node. The *Setup Introduction* dialog appears. Review the information and click **OK**.

   Important 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.

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

   Note vCenter Server Heartbeat will check for the presence of an appropriate version of .Net and if required either install one or notify the user.

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

   The *End User License Agreement* page is displayed.

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

   The *License Configuration* page is displayed.

18 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.

The *Select Topology* page is displayed.

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

The *Deployment Option* page is displayed.

20 On the *Deployment Option* page, select *Secondary Node is Virtual* , then click **Next**.

The *Destination Folder* page is displayed.

21 Configure the installation paths. The default installation location is C:\Program Files\VMware\VMware vCenter Server Heartbeat, but can be changed by manually typing a path to another install location. Alternatively, click **Browse** to select a location. Select *Create icons on Desktop* and click **Next**.

Important 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, it will cause the VMware vCenter Server Heartbeat service to not 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 " ".

---

22 You have the following options:

- If using a single NIC, go to Step 24.
- If using multiple NICs, continue with Step 23.

23 The *Channel Adapter* page is displayed. Select the network adapters (NICs) to be used 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**.

Important 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.

The *Channel and Client Connection* page is displayed.

24 Click **Add** for each available channel connection. For the Primary node, select from a drop-down menu that lists all local IP addresses. Type the reciprocal IP address on the Secondary node into the *IP Address On Secondary* text box. Click **OK**. Repeat this step for additional NICs.

Important If using multiple NICs, you must specify all VMware Channel IP addresses in subnets outside of the normal Public IP addressing schema so that VMware Channel traffic routing uses the VMware Channel network card rather than the Public network card.

You will receive a warning message that the Secondary node cannot be contacted. Disregard the warning and click **No** to proceed.

25 The vCenter Server Heartbeat node pair can be administered remotely on client machines using the vCenter Server Heartbeat Console or the vSphere plug-in. The vCenter Server Heartbeat Console connects to the IP address of the active node using the Client Connection port of 52267. The VMware Channel connects using the Default Channel Port (57348). If these ports are already in use, type an available connection port in the appropriate text box. Review and adjust, if necessary, the Default Channel Port and Client Connection Port. Click **Next**.

- If using multiple NICs, continue with Step 26.
- If using a single NIC, go to Step 27.

Important When the implementation spans multiple sites with firewalls between the nodes, configure the firewalls to allow traffic to pass through the Default Channel Port or the manually configured channel port. See "Configure Firewalls," on page 44 for additional information. The *Public Adapter* page is displayed.

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

The *Public IP Address* page is displayed.

27 For LAN installation or same subnet WAN installs, select *Use same IP addresses for Secondary (Recommended for HA secondary)* or when installing in a WAN with different subnets, select *Use different IP addresses for Secondary (Recommended for DR secondary)*.

28 Click **Add** to specify the Public IP address in a LAN or same subnet WAN. When installing in a WAN with different subnets, specify the Public IP addresses of both the Primary and Secondary nodes. Click **Next**.

29 You have the following options:

- If you are deploying in a LAN or same subnet WAN, go to Step 31.
- If you are deploying in a WAN, go to Step 30.

30 When the Public address(es) on the Secondary node are different from those on the Primary node, vCenter Server Heartbeat must perform additional tasks during failover. These additional tasks require clients to change their resolution of the active node to a different IP address and requires that vCenter Server Heartbeat update the DNS entries for the active node 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**.

The *Management IP Address* page is displayed.

31 Using the **Add** buttons, add the previously configured Management IP addresses for the Primary and Secondary nodes and click **Next**.

If a message is displayed stating the Secondary IP address is not visible disregard and click **No** to proceed.

Note The Secondary node's Public NIC is disconnected and cannot be reached at this time.

The *Service and Node Name* page is displayed.

32 The *Service and Node Name* page identifies the Fully Qualified Domain Name (FQDN) of the protected application(s). It also allows you to specify new names for the Primary and Secondary nodes when they are renamed at the conclusion of installation. Enter the new non-FQDN node names for the Primary and Secondary nodes in the appropriate text box. If your Secondary node was renamed during the cloning process, enter the node's new name in the appropriate text field. Click **Next**.

The *Application Protection* page is displayed.

33 Setup will automatically select the applications that are installed on the node and require protection. The default selection should only be changed if an application is installed but services have been disabled because the application is no longer used on the node.

   a Confirm that the selection is correct and if appropriate, provide vCenter connections details (username and password).

   b Enter the Master Password for the Single Sign-on service in the *SSO Master Password* text box.

   c If the vCenter Server is remote, select the *Server is remote* check box and provide the Server Name or IP address for vCenter Server.

   Important If vCenter is local and is running on a custom port, you must use localhost for the node name and then add a colon and the custom port number.

   If vCenter is remote and is running on a custom port, you must use the IP address for the node name and then add a colon and the custom port number.

   Click **Next**. The *Save Data for use during Secondary Installation* page is displayed.

34 Setup backs up two small files, nfsetup.dat and primary.csv, from the Primary node and restores them to the Secondary node during the Secondary node installation for proper configuration. 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. Click **Next**.

   The *Installation Summary* page is displayed.

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

   The *Pre-Install Checks* page is displayed.

36 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.

   When finished, the *Report* pane displays the results.

37 Review the pre-install check results. 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**.

   The *Install* page is displayed.

38 The *Install* 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.

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

   The *Packet Filter Installation* page is displayed.

40 The vCenter Server Heartbeat Packet Filter driver installs on each network card of the production node. If you see 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 may see multiple warnings. The *Report* pane displays the results.

   By default, the vCenter Server Heartbeat Packet Filter driver is applied to all 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 node. Click **Next**.

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

41 Verify that the pre-populated management names and IP addresses to be used are configured and available in the DNS servers before proceeding to the next step.

42 If vCenter Server Heartbeat cannot use the current logon credentials to rename the node, a dialog prompts you for a *Username* and *Password* for an account with permissions to rename the node.

43 Enter a *Username* and *Password* to automatically rename the node with the previously provided new node name or click **Cancel** to manually perform a simple Windows rename of the node.

The system prompts you to restart the node.

44 Click **Yes** to restart the node.

Secondary Node

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

Procedure

1 You have the following options:

- If you are using a single NIC, continue with Step 2.
- If you are using multiple NICs, go to Step 3.

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

a Select the Public/VMware Channel virtual network adapter and clear the *Connected* and *Connect at power* on check boxes.

b Power on the Secondary (previously cloned) node image.

c On the Secondary node, open *Network Connections*, right-click the Public/VMware Channel network connection and select *Properties*. Select *Internet Protocol (TCP/IP)* and click **Properties**.

d Configure the appropriate VMware Channel IP address. Click **Advanced**.

e Click the *WINS* tab and select *Disable NetBIOS over TCP/IP* and clear the *Register this connection's addresses in DNS* check box.

f Configure the Management IP address (different than the Primary node), subnet mask, and default gateway.

g Click **OK** three times to close the dialogs.

h Right-click the Secondary (cloned) node image and select *Edit* Settings.

i Select the single virtual network adapter and select the *Connected* and *Connect at power on* check boxes. IP communications with the Secondary node go through the VMware Channel.

j Go to Step 4.

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

   a Select the 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) node image.

   d On the Secondary node, 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 and select *Disable NetBIOS over TCP/IP*. Select the *DNS* tab and clear the *Register this connection's addresses in DNS* check box. Click **OK** three times to close the dialogs.

   g Right-click the Public network connection and select *Properties*. Select *Internet Protocol (TCP/IP)* and click **Properties**. Configure the Public IP address, subnet mask, and default gateway. Click **Advanced**. Select the *DNS* tab and clear the *Register this connection's addresses in DNS* check box.

   h Configure the Management IP address (different than the Primary node), subnet mask, and default gateway.

   i Click **OK** three times to close the dialogs.

   j Right-click the Secondary (cloned) node image and select *Edit* Settings.

   k Select the VMware Channel virtual network adapter and select the *Connected* and *Connect at power on* check boxes. IP communications with the Secondary node go through the VMware Channel.

Important Do not connect the Public virtual network adapter at this time to prevent an IP address conflict on the network.

---

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

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

Note vCenter Server Heartbeat will check for the presence of an appropriate version of .Net and if required either install one or notify the user.

---

6 The *Setup Type* page appears. As with the installation on the Primary node, select *Install Secondary VMware vCenter Server Heartbeat* and click **Next**.

   The *Shared Install Data* page is displayed.

7 Identify the location of the folder containing the backup file from the Primary node. Manually type the location path in the text box. Click **Next**.

Note You must use the UNC path.

   The *Pre-Install Checks* page is displayed.

8 The pre-install checks run.

Important The pre-install checks will return the message that the Primary and Secondary node'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.
   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.

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

The *Packet Filter Installation* page is displayed.

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

a The Packet Filter is installed on the Public NIC and the Public network adapter can be reconnected. Right-click the Secondary node image name and select *Edit Settings*.

b Select the Public virtual network adapter, select the *Connected* and *Connect at power on* check boxes, and click **OK**.

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

The *Public Adapter* page is displayed.

13 Configure the Public adapter on the Secondary node through the *Public Adapter* page. When you select the Public adapter, a caution message notifies you that the IP address on the Public adapter does not match the IP address on the Primary node (LAN configuration only).

The *Configuring Node* page is displayed.

14 If vCenter Server Heartbeat cannot use the current logon credentials to rename the node, a dialog prompts you for a *Username* and *Password* for an account with permissions to rename the node. Enter a *Username* and *Password* to automatically rename the node with the previously provided new node name and click **OK** or click **Cancel** to manually perform a simple Windows rename of the node.

Click **Finish**. The system prompts you to restart the node.

15 Click **Yes** to restart the node.

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.

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

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

Post Installation Configuration

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

Post Installation Tasks

Once installation of vCenter Server Heartbeat is complete, use Nslookup to verify configured name resolution.

Procedure

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

Configuring VirtualCenter Plug-in with the Correct Credentials

When protecting vCenter Server, after installation is complete you must enter the credentials for an account with rights to the Virtual Infrastructure to allow evaluation of rules.

To add the Virtual Infrastructure credentials:

Procedure

1. Using the vCenter Server Heartbeat Console, 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.

   Important If vCenter Server 5.1 is installed, you must also enter the *MasterPassword* for SSO.

5. Click **OK**.

Configure Firewalls

When firewalls are used to protect networks, you must configure them to allow traffic to pass through both the *Client Connection port* (52267) and the *Default Channel port (57348)*.

Important When installing on Windows Server 2008/2012, Microsoft Windows may change the connection type from a Private network to an Unidentified network after you have configured the firewall port to allow channel communications resulting in the previously configured firewall changes to be reset for the new network type (Unidentified).

The firewall rules must be recreated to allow traffic to pass through for the Client Connection port and the Default Channel port. VMware recommends that the firewall be configured to allow the Client to connect to the Client Connection port by process, nfgui.exe, rather than by a specific port. To enable Channel communications between nodes, change the Network List Manager Policy so that the VMware Channel network is identified as a Private Network, not the default Unidentified Network, and configure the firewall to allow traffic to pass through on Port 57348, the Default Channel port.

Registering the Heartbeat Plug-in Manually in vCenter

In the event that the Heartbeat Plug-in did not register successfully during Setup, perform the steps below to manually register Heartbeat Plug-in once Setup completes.

Procedure

1 With the vCenter Server Heartbeat pair in sync, on the Primary/active node, open an elevated command prompt and navigate to C:\Program Files\VMware\VMware vCenter Server Heartbeat\tomcat\apache-tomcat-6.0.32\bin

2 Run the following command: RegExt -register vchost[:port] username password hbconf.xml PublicServiceName

vchost – name/IP of the vCenter Server to which you want to register

port – https port on which vCenter is running

username – a valid username with administrator privileges on the vCenter Server

password – password of the user with administrator privileges on the vCenter Server

PublicServiceName – the public name of the vCenter Server Heartbeat pair

3 Copy the hbconf.xml file created at the previous step to C:\Program Files\VMware\VMware vCenter Server Heartbeat\tomcat\apache-tomcat-6.0.32\webapps\vcshb

4 Perform a manual failover to make the Secondary node active.

5 Repeat steps 1-3 on the Secondary/active node.

Configuring vCenter Server Heartbeat to Protect SQL Server

After successfully installing vCenter Server Heartbeat, perform the following tasks to configure vCenter Server Heartbeat to protect SQL Server.

Configuring SQL Server Plug-in

When protecting SQL Server 2012 or 2014, after installation is complete you must enter the credentials for an account with rights to SQL Server 2012 or 2014.

To add the SQL Server 2012 or 2014 credentials:

Procedure

1 Using the vCenter Server Heartbeat Console, navigate to the *Applications: Plug-ins* page.

2 Select the *SQLServer Plug-in*.

3 Click **Edit**.

4 Type the *Username* and *Password* for an account with rights to the SQL Server.

5 Click **OK**.

Configuring the SQL Server Instance Account

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.

Procedure

1 Navigate to **Start > Administrative Tools > Services**.

2 Select the SQL Service instance and click **Properties**.

3 Select the *Log On* tab and select *This account*.

4 Provide the new account credentials and click **OK**.

5 Once complete, restart the SQL Server instance service.

Configuring for SQL Server Running Under the LocalSystem Account

When SQL Server is run under the LocalSystem account, the following additional steps must be performed.

Procedure

1 On the Domain Controller, navigate to *Active Directory Users and Computers*.

2 Select the computer account of the node running vCenter Server Heartbeat.

3 On the Primary computer account (Primary Management Name):

   a Navigate to the *Security* tab and click **Advanced**.

   b On the *Permissions* tab click **Add**.

   c Select the user to run the SetSPN command (this can be the same user that runs SQL Server).

   d Assign the *Allow* permission for *Write all properties* and *Apply to this object and all child objects*.

   e Click **OK**.

4 On the Secondary computer account (Secondary Management Name):

   a Navigate to the *Security* tab and click **Advanced**.

   b On the *Permissions* tab click **Add**.

   c Select the user to run the SetSPN command (this can be the same user that runs SQL Server).

   d Assign the *Allow* permission for *Write all properties* and *Apply to this object and all child objects*.

   e Click **OK**.

   Important At this point, NFSetSPN will not operate properly as it requires SQL Server to be run with a domain user account. The following steps provide a workaround for this issue.

5 On the Primary node, using vCenter Server Heartbeat Console, navigate to the *Applications: Tasks* tab.

6 Click **User Accounts** and add the user you want to run the SetSPN command.

7 In the **Network Configuration** > **Sql Server** > **Set SPN (Primary)** click **Edit**.

8 For *Run As*, select the user added at Step 7 from the drop-down list and click **OK**.

9 On the Secondary node, using vCenter Server Heartbeat Console, navigate to the *Applications: Tasks* tab.

10 In the **Network Configuration** > **Sql Server** > **Set SPN (Secondary)** click **Edit**.

11 For *Run As*, select the user added at Step 7 from the drop-down list and click **OK**.

12 Select the task corresponding to the active node and click **Run Now** to test the task (The returned status should be: Completed with exit code 0)

Configure SetSPN.exe

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 nodes prior to starting vCenter Server Heartbeat for the first time.

Procedure

1 Verify that the SetSPN.exe tool is present on both the Primary and the Secondary nodes at Windows\System32.

   This is normally present as a component of the Windows 2008/2012 operating systems.

   Important 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 Public IP address and the Management IP address for the Primary and Secondary Servers.

2 Launch the vCenter Server Heartbeat Console and navigate to the *Applications: Tasks* page.

3 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 7.

4 In the *User Accounts* dialog, click **Add**.

5 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**.

6 Once the account has been successfully added to the list, click **Close**.

7 In the *Task* pane, select the Network Configuration task *Set SPN (Primary)*.

8 Click **Edit**.

9 In the *Edit Task* dialog, in the *Run As:* drop-down field, select an account with appropriate rights (the account previously added).

10 Click **OK**.

11 Repeat the procedure for the Network Configuration task *Set SPN (Secondary)*.

12 After successfully configuring the correct credentials, select the *Set SPN (Primary)* task and click **Run Now**.

Configuring 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 Server Heartbeat startup
- Shutdown with protected applications
- Manual Failover
- Automated Failover
- When the Administrator selects *Start Application*
- When the Administrator selects *Stop Application*

Note If there are multiple applications installed, vCenter Server Heartbeat totals the individual timeouts set for each application and issues a single *Application Timeout Exception* alert.

Configuring Timeout Settings

Procedure

1 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.

2 Enter new values into the *Stop Timeout* and *Start Timeout* text boxes or use the arrow buttons to adjust the values (seconds). Click **OK**.

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.

Configuring Orchestrator When Deployed in a WAN With Different Subnets.

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

Procedure

1 Launch vCenter Server Heartbeat Console.

2 Select *Data: File Filters*.

3 Click **Add Exclusion Filter**.

4 Browse to or enter the following path: $INSTALL_PATH_TO_ORCHESTRATOR/app-server/bin/boot.properties

5 Click **OK**.

6 Perform a manual failover so that the Secondary node becomes active.

7 Launch the vCenter Orchestrator Web Configuration wizard and select *Network*.

8 In the IP address field select the Public IP address of the Secondary node. Click **Apply changes**. If VMware Orchestrator Server is configured as a service, then proceed with following steps:

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

   b From vCenter Server Heartbeat Console, select *Applications: 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.

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:

Procedure

1 Ensure that View Composer has been installed on both the Primary and Secondary nodes 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.

Upgrading vCenter Components

Should vCenter Server or components of vCenter need to be upgraded when vCenter Server Heartbeat is installed, please refer to Chapter 4, “Upgrading,” on page 51.

vCenter Server with SQL Server on a Separate Host

It is not necessary to update ODBC connection information since the Public Service Name is used rather than the server name for ODBC calls.

Upgrading 4

This Appendix provides instructions to upgrade both vCenter Server Heartbeat and vCenter Server when vCenter Server Heartbeat is installed as indicated below.

- Upgrading vCenter Server when vCenter Server Heartbeat is installed
  - vCenter Server 5.0 to vCenter Server 5.5 Update 2
  - vCenter Server 5.1, 5.1 Update 1 or 5.1 Update 2 to vCenter Server 5.5 Update 2
  - vCenter Server 5.5 to vCenter Server 5.5 Update 2
- Upgrading vCenter Server Heartbeat
  - vCenter Server Heartbeat 6.5 to vCenter Server Heartbeat 6.6 Update 1 or Update 2
  - vCenter Server Heartbeat 6.5 Update 1 to vCenter Server Heartbeat 6.6 Update 1 or Update 2
  - vCenter Server Heartbeat 6.6 to vCenter Server Heartbeat 6.6 Update 1 or Update 2

Note vCenter Server Heartbeat must be upgraded prior to upgrading vCenter Server to allow vCenter Server Heartbeat to maintain protection of vCenter Server.

This chapter includes the following topics:

Upgrading vCenter Server Heartbeat 6.5, 6.5 Update 1, 6.6 or 6.6 Update 1 to vCenter Server Heartbeat 6.6 Update 2

The following procedure assumes that vCenter Server Heartbeat 6.5, 6.5 Update 1, 6.6, or 6.6 Update 1 is currently installed and provides step-by-step instructions to upgrade the currently installed version of vCenter Server Heartbeat to vCenter Server Heartbeat 6.6 Update 2. For information about upgrading from other versions of vCenter Server Heartbeat to vCenter Server Heartbeat 6.6 Update 1, see knowledge base article 1014435 - *Upgrading vCenter Server Heartbeat from an earlier version to a later version*.

Procedure

1 Download the new version of vCenter Server Heartbeat WinZip Self-Extracting file to a desired location on both the Primary and Secondary nodes.

2 On the Primary/active node, right-click on the *System Tray* icon and select to *Shutdown vCenter Server Heartbeat* opting to leaving protected applications running.

3 Navigate to **Start** > **Administrative Tools** > **Services** and set the *VMware vCenter Server Heartbeat* service to *Manual*.

4 On the Secondary/passive node, navigate to **Start** > **Administrative Tools** > **Services** and set the *VMware vCenter Server Heartbeat* service to *Manual*.

5 On the Secondary/passive node, right-click on the *System Tray* icon and select to *Shutdown vCenter Server Heartbeat*.

6 On the Secondary/passive node, disconnect the network cable from the Public NIC.

7 On the Primary/active node, double-click the WinZip Self-Extracting file. The *Setup Introduction* page is displayed. Click **OK**.

The *WinZip Self-Extractor* page is displayed.

8 Click **Setup** to open the *VMware vCenter Server Heartbeat Setup* window.

9 Select the option to *Install Update* when the *Setup Type* page is displayed.

10 Follow the on-screen instructions to install the ServicePack.nfs script. Click **Add** and use the default path to the Service Pack. When prompted, reboot the node.

Note During the Service Pack installation, the new vCenter Server Heartbeat plug-ins are copied to <Heartbeat install dir>\R2\<version> plug-ins\<plug-in name>

11 On the Secondary/passive node, double-click the WinZip Self-Extracting file. The *Setup Introduction* page is displayed. Click **OK**.

The *WinZip Self-Extractor* page is displayed.

12 Click **Setup** to open the *VMware vCenter Server Heartbeat Setup* window.

13 Select the option to *Install Update* when the *Setup Type* page is displayed.

14 Follow the on-screen instructions to install the ServicePack.nfs script. Click **Add** and use the default path to the Service Pack. When prompted, reboot the node.

Note During the Service Pack installation, the new vCenter Server Heartbeat plug-ins are copied to <Heartbeat install dir>\R2\<version> plug-ins\<plug-in name>

15 On both the Primary/active node and the Secondary/passive node, check the configuration of the NICs and make corrections if necessary (the packet filter should be selected on Public NICs and cleared on channel NICs).

16 On the Primary/active node, right-click on the *System Tray* icon and select to *Start VMware vCenter Server Heartbeat*.

17 Navigate to **Start** > **Administrative Tools** > **Services** and set the *VMware vCenter Server Heartbeat* service to *Automatic*.

18 On Secondary/passive node, right-click on the *System Tray* icon and select to *Start VMware vCenter Server Heartbeat* and then reconnect the network cable to the Public NIC.

19 On the Secondary/passive node, navigate to **Start** > **Administrative Tools** > **Services** and set the *VMware vCenter Server Heartbeat* service to *Automatic*.

20 Reconfigure the run-as account for the SetSPN tasks by performing the following:

a In the *Task* pane, select the Network Configuration Task *Set SPN (Primary).*

b Click **Edit**

c In the *Edit Task* dialog, in the *Run As:* drop-down list, select an account with the appropriate rights (the account previously added).

Click **OK.**

d Repeat the procedure for the Network Configuration Task *Set SPN (Secondary)*

Upgrading vCenter Server 5.0, 5.1 or 5.5 to vCenter Server 5.5 Update 2 when SQL Database is Remote and vCenter Server Heartbeat is Installed

The following procedure assumes that vCenter Server Heartbeat is installed and protecting vCenter Server 5.0, 5.1 or 5.5 using a remote SQL Database. This procedure provides step-by-step instructions to perform an upgrade of vCenter Server 5.0, 5.1 or 5.5 to vCenter Server 5.5 Update 2 with vCenter Server Heartbeat installed. For information about upgrading from other versions of vCenter Server with vCenter Server Heartbeat installed to vCenter Server 5.5, see knowledge base article 1010479 - *Upgrading or applying updates to vCenter Server and its components when protected by vCenter Server Heartbeat with a remote database*.

Upgrading the vCenter Server 5.0, 5.1 or 5.5 Secondary Node

Prerequisites

Before attempting to upgrade from vCenter Server 5.0 or vCenter Server 5.1 to vCenter Server 5.5 you must install the VMware vSphere Single Sign-On (SSO) 5.5 Update 2 component separately on a different machine (not on the Primary or Secondary node) and then protect SSO on the separate machine with vCenter Server Heartbeat. If upgrading from vCenter Server 5.5 to vCenter Server 5.5 Update 2, then proceed straight to the steps below.

Procedure

1 If the Primary node is active, use vCenter Server Heartbeat Console on the Secondary node to perform a manual failover to make the Secondary node active. If the Secondary node is currently active, go to Step 2.

2 Shutdown vCenter Server Heartbeat on both the Primary and Secondary nodes, leaving protected applications running on Secondary (active) node.

3 Using the Service Control Manager, configure *VMware vCenter Server Heartbeat* service *Startup Type* to *Manual* on both Primary and Secondary nodes.

4 Before proceeding with the upgrade procedure, perform a backup of the existing vCenter Server database, Single Sign-On database, VMware Update Manager database, and SSL certificates.

5 Upgrade VMware vSphere Web Client

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Web Client* from the list.

   b Proceed with the installation.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

6 Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vCenter Inventory Service* from the list.

7 When prompted, select *Do not overwrite. Leave my existing database in place*.

8 Using the VMware vCenter Installer for the version you want to upgrade to, select *vCenter Server* from the list.

   ■ If applying an update, when prompted, select *Do not overwrite, leave the existing database in place*

   ■ If upgrading, when prompted, select *Upgrade existing vCenter Server database*

9 Continue with vCenter Server installation and record all configuration settings used.

Note On the vCenter Server service account information page, VMware recommends providing the same credentials used for the current service (open the Service Control Manager and check the *Logon As* account for VMware VirtualCenter Server service).

10 If asked, do not reboot the node.

11 You have the following options:

   ■ If the upgrade on the Secondary node is successful, go to Step 13.

   ■ If the upgrade on the Secondary node is not successful, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with Step 13, otherwise go to Step 12 to revert to a previous version.

12 To revert to a previous version:

   a Uninstall the upgraded components.

   b On the Secondary node, launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab. In the *Current Role* section, choose *Passive* and click **Finish**.

   c Reboot the node. vCenter Server Heartbeat starts and vCenter Server is stopped.

   d On the Primary node, launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab. In the *Current Role* section, choose *Active* and click **Finish**.

   e Restart vCenter Server Heartbeat on the Primary node and allow the system to synchronize.

   f Start the vCenter Server Heartbeat Console and check that the system completes the Full System Check.

13 Once the vCenter Server upgrade process ends successfully, VMware recommends that you upgrade the existing extensions on the node. Details for each component upgrade can be found below.

Important You must upgrade vCenter Server before upgrading vCenter Support Tools.

14 Upgrade VMware vSphere ESXi Dump Collector (Optional).

a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere ESXi Dump Collector* from the list.

b Provide vCenter Server, VMware vSphere ESXi Dump Collector information and record all configuration settings used.

c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

15 Upgrade VMware vSphere Syslog Collector (Optional).

a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Syslog Collector* from the list.

b Provide vCenter Server, VMware vSphere Syslog Collector information and record all configuration settings used.

c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

16 Upgrade VMware vSphere Auto Deploy (Optional).

a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Auto Deploy* from the list.

b Provide vCenter Server, VMware vSphere Auto Deploy information and record all configuration settings used.

c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

17 Upgrade VMware vSphere Authentication Proxy (Optional).

a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware Authentication Proxy* from the list.

b Provide vCenter Server, VMware Authentication Proxy information and record all configuration settings used.

c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

18 Upgrading Update Manager (Optional).

This procedure assumes you have already upgraded vCenter Server on Secondary node. During the vCenter Update Manager upgrade process, record all configuration settings used (vCenter Server information, Database information, port settings) as these will be required when upgrading the Primary node.

Note The VMware Update Manager database must be running before attempting to upgrade VMware Update Manager.

---

a Start VMware vCenter Installer for the version you want to upgrade to and select *vCenter Update Manager* from the list.

Important Perform a backup of the existing Update Manager database before proceeding with the next step.

---

b On the *Database Upgrade* page select the option *Yes, I want to upgrade the Update Manager database*.

c Continue with the install process.

d Once the upgrade is complete, verify that vCenter Update Manager is operational.

19 Verify that vCenter Server and all updated extensions are operational.

20 Change the node's role to Secondary/passive:

   a Launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab.

   b In the *Active Server* section, change the node's role for the Primary node to *Active* and click **Finish**.

21 Start VMware vCenter Server Heartbeat on the Secondary node only.

22 Reboot Secondary node.

   The upgrade process continues on the Primary node.

Upgrading the vCenter Server 5.0, 5.1 or 5.5 Primary Node

Continuation of the upgrade process assumes the upgrade of the Secondary node completed successfully.

Prerequisites

Before proceeding with the upgrade procedure, perform a restore of the vCenter Server database and SSL certificates that were backed up at Step 4 on the Secondary node.

Procedure

1 Change the node's role to Primary/active:

   a Launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab. Change the role for the current (Primary) node to *Active* and click **Finish**.

   b Using the Service Control Manager, start the *VMware vCenter Server Heartbeat* service.

   c Using the vCenter Server Heartbeat Console, verify that all status icons on the *Server: Summary* page are green indicating that the Start process has completed and all protected services are started.

   d Using the Service Control Manager, stop the *VMware vCenter Server Heartbeat* service.

2 Using VMware vCenter Installer for the version you want to upgrade to, select *VMware vCenter Inventory Service* from the list.

3 When prompted, select *Do not overwrite. Leave my existing database in place*.

4 From the VMware vCenter Installer for the version you want to upgrade to, select *vCenter Server* from the list.

   - If applying an update, on the *Database re-initialization warning* page, select the *Do not overwrite, leave my existing database in place* option and proceed with the installation process.
   - If applying an upgrade on the *Database Upgrade warning* page, select *Upgrade existing vCenter Server database* option and proceed with the installation process.

5 Continue with vCenter Server installation, using the identical configuration settings as used for installation on the Secondary node.

6 Once the vCenter Server upgrade process ends successfully, VMware recommends that you upgrade the existing extensions on the node. Details for each component upgrade can be found below.

Important You must upgrade vCenter Server before upgrading vCenter Support Tools.

7 Upgrade VMware vSphere ESXi Dump Collector (Optional).

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere ESXi Dump Collector* from the list.

   b Provide vCenter Server, VMware vSphere ESXi Dump Collector information and record all configuration settings used.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

8 Upgrade VMware vSphere Syslog Collector (Optional).

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Syslog Collector* from the list.

   b Provide vCenter Server, VMware vSphere Syslog Collector information and record all configuration settings used.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

9 Upgrade VMware vSphere Auto Deploy (Optional).

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Auto Deploy* from the list.

   b Provide vCenter Server, VMware vSphere Auto Deploy information and record all configuration settings used.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

10 Upgrade VMware vSphere Authentication Proxy (Optional).

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware Authentication Proxy* from the list.

   b Provide vCenter Server, VMware Authentication Proxy information and record all configuration settings used.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

11 Upgrade VMware vSphere Web Client (Optional)

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Web Client* from the list.

   b Proceed with the installation.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

12 Upgrading Update Manager (Optional)

Note The VMware Update Manager database must be running before attempting to upgrade VMware Update Manager.

a Using the Service Control Manager, start the VMware vCenter Server service.

b Start VMware vCenter Installer for the version you want to upgrade to and select *vCenter Update Manager* from the list.

c During the vCenter Update Manager upgrade, provide the same configuration settings used during the upgrade process on the Secondary node.

Important Before proceeding with the database upgrade, perform a backup of the existing vCenter Update Manager database.

d On the *Database re-initialization warning* page, select *Do not overwrite, leave my existing database in place* option and proceed with the installation process.

e Once the upgrade is complete, verify that vCenter Update Manager is operational.

13 Verify that vCenter Server and all updated extensions are operational.

14 Using the Service Control Manager, configure *VMware vCenter Server Heartbeat* service Startup Type to *Automatic* on both Primary and Secondary nodes.

15 Start vCenter Server Heartbeat on both nodes.

16 Launch the vCenter Server Heartbeat Console and connect to the node pair.

a Check that the system completes the Full System Check and is replicating.

b Navigate to the vCenter Server Heartbeat Console *Application: Tasks* page and manually run the Protected Service Discovery task.

Troubleshooting

If vCenter Server fails to start on the Secondary node following a manual failover, perform the following steps.

Procedure

1 Shutdown vCenter Server Heartbeat.

2 Launch the Configure Server wizard and set the Secondary node's role to *Passive*.

3 Start vCenter Server Heartbeat on the Secondary node.

4 Start the Configure Server wizard on the Primary node and set the node's role to *Active*.

5 Start vCenter Server Heartbeat on the Primary node.

6 Launch the vCenter Server Heartbeat Console and verify that the system completes the Full System Check.

7 Investigate the cause of the vCenter Server failure on the Secondary node.

Upgrading vCenter Server 5.0, 5.1 or 5.5 to vCenter Server 5.5 Update 2 when SQL Database is Local and vCenter Server Heartbeat is Installed

The following procedure assumes that vCenter Server Heartbeat is installed and protecting vCenter Server 5.0, 5.1 or 5.5 using a local SQL Database. This procedure provides step-by-step instructions to perform an upgrade of vCenter Server 5.0, 5.1 or 5.5 to vCenter Server 5.5 Update 2 with vCenter Server Heartbeat installed. For information about upgrading from other versions of vCenter Server with vCenter Server Heartbeat installed to vCenter Server 5.5 Update 2, see knowledge base article 1034131 - *Upgrading or applying updates to vCenter Server 4.0 and later when protected by vCenter Server Heartbeat local SQL database*.

Upgrading the vCenter Server 5.0, 5.1 or 5.5 Secondary Node

Prerequisites

Before attempting to upgrade from vCenter Server 5.0 or 5.1 to vCenter Server 5.5 you must install the VMware vSphere Single Sign-On (SSO) 5.5 Update 2 component separately on a different machine (not on the Primary or Secondary node) and then protect SSO on the separate machine with vCenter Server Heartbeat. If upgrading from vCenter Server 5.5 to vCenter Server 5.5 Update 2 then proceed straight to the steps below.

Procedure

1 If the Primary node is active, use vCenter Server Heartbeat Console on the Secondary node to perform a manual failover to make the Secondary node active. If the Secondary node is currently active, go to Step 2.

2 Shutdown vCenter Server Heartbeat on both the Primary and Secondary nodes, leaving the protected applications running on Secondary (active) node.

3 Using the Service Control Manager, configure *VMware vCenter Server Heartbeat* service *Startup Type* to *Manual* on both Primary and Secondary nodes.

4 Before proceeding with the upgrade procedure, perform a backup of the existing vCenter Server database and SSL certificates.

5 Upgrade VMware vSphere Web Client

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Web Client* from the list.

   b Proceed with the installation.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

6 Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vCenter Inventory Service* from the list.

Note If you attempt to upgrade vCenter Server before upgrading the Inventory Service, a warning is displayed and the upgrade will not be allowed to proceed.

7 Start VMware vCenter Installer for the version you want to upgrade to and select *vCenter Server* from the list.

8 Proceed with the setup, selecting the correct ODBC data source and database server credentials.

If other components are installed, vCenter Server Setup will warn about the need to upgrade them as well.

9 You have the following options: otherwise,

- If applying an update, when prompted, select the *Do not overwrite, leave my existing database in place* option and continue with the update procedure.
- If this is an upgrade, when prompted, select *Upgrade existing vCenter Server Database* and choose to *Automatically upgrade the vCenter Agent*. Continue with the upgrade procedure.

10 Once the vCenter Server upgrade process ends successfully, VMware recommends that you upgrade the existing extensions on the node. Details for each component upgrade can be found below.

Important You must upgrade vCenter Server before upgrading vCenter Support Tools. When upgrading components, you must use the Fully Qualified Domain Name (FQDN) and not the Public Service Name.

11 Upgrade VMware vSphere ESXi Dump Collector (Optional).

a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere ESXi Dump Collector* from the list.

b Provide vCenter Server, VMware vSphere ESXi Dump Collector information and record all configuration settings used.

c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

12 Upgrade VMware vSphere Syslog Collector (Optional).

a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Syslog Collector* from the list.

b Provide vCenter Server, VMware vSphere Syslog Collector information and record all configuration settings used.

c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

13 Upgrade VMware vSphere Auto Deploy (Optional).

a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Auto Deploy* from the list.

b Provide vCenter Server, VMware vSphere Auto Deploy information and record all configuration settings used.

c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

14 Upgrade VMware vSphere Authentication Proxy (Optional).

a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware Authentication Proxy* from the list.

b Provide vCenter Server, VMware Authentication Proxy information and record all configuration settings used.

Note If you encounter an Authentication proxy logon failure or a warning that the specified user doesn't exist, acknowledge and continue the upgrade procedure.

c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

15 Upgrading Update Manager (Optional).

This procedure assumes you have already upgraded vCenter Server on Secondary node. During the vCenter Update Manager upgrade process, record all configuration settings used (vCenter Server information, Database information, port settings) as these will be required when upgrading the Primary node.

Note The VMware Update Manager database must be running before attempting to upgrade VMware Update Manager.

a Start VMware vCenter Installer for the version you want to upgrade to (should be the same installer used for vCenter Server upgrade) and select *vCenter Update Manager* from the list.

Important Perform a backup of the existing Update Manager database before proceeding with the next step.

b Provide vCenter Server and database information, and record all configuration settings used.

c On the *Database Upgrade* page select the option *Yes, I want to upgrade the Update Manager database*.

d In the event errors are encountered during the installation, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure, otherwise revert to a previous version.

e Once the upgrade is complete, verify that vCenter Update Manager is operational.

16 Verify that vCenter Server and all updated extensions are operational

17 You have the following options:

- If the upgrade on the Secondary node is successful, go to Step 19.
- If the upgrade on the Secondary node was not successful, research the cause of the upgrade failure. If the issue can be resolved, then it is safe to proceed with Step 19, otherwise, go to Step 18 to revert to a previous version.

18 To revert to a previous version:

a Uninstall the upgraded components.

b On the Secondary node, launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab. Change the node's *Role* to Secondary/passive.

c Reboot the node. vCenter Server Heartbeat starts and vCenter Server is stopped

d On the Primary node, launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab. Change the node's *Role* to Primary/active.

e Restart vCenter Server Heartbeat on the Primary node and allow the system to synchronize.

f Start the vCenter Server Heartbeat Console and verify that the system completes the Full System Check.

19 Change the node's role to Secondary/passive:

a Launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab.

b Change the node's *Role* to Secondary/passive and click **Finish**.

20 Start VMware vCenter Server Heartbeat on the Secondary node only.

21 Reboot Secondary node. The upgrade process continues on the Primary node.

Upgrading the vCenter Server 5.0, 5.1 or 5.5 Primary Node

Continuation of the upgrade process assumes the upgrade of the Secondary node completed successfully.

Procedure

1 Change the node's role to Primary/active:

   a Launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab. Change the node's role for the current (Primary) node to *active* and click **Finish**.

   b Using the Service Control Manager, start the *VMware vCenter Server Heartbeat* service.

   c Using the vCenter Server Heartbeat Console, verify that all status icons on the *Server: Summary* page are green indicating that the Start process has completed.

   d Using the Service Control Manager, stop the *VMware vCenter Server Heartbeat* service.

2 Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vCenter Inventory Service* from the list.

   Note If you attempt to upgrade vCenter Server before upgrading the Inventory Service, a warning is displayed and the upgrade will not be allowed to proceed.

3 Using the VMware vCenter Installer for the version you want to upgrade to, select *vCenter Server* from the list.

4 Proceed with the setup, selecting the correct ODBC data source and database server credentials.

   If other components are installed, vCenter Server Setup warns about the need to upgrade them as well.

5 You have the following options:, otherwise

   - If applying an update, when prompted, select the *Do not overwrite, leave my existing database in place* and continue the update procedure.
   - If this is an upgrade, when prompted, select *Upgrade existing vCenter Server database* and choose to *Automatically upgrade the vCenter Agent*. Continue the upgrade procedure.

6 Once the vCenter Server upgrade process ends successfully, VMware recommends that you upgrade the existing extensions on the node. Details for each component upgrade can be found below.

   Important You must upgrade vCenter Server before upgrading vCenter Support Tools. When upgrading components, you must use the Fully Qualified Domain Name (FQDN) and not the Public Service Name.

7 Upgrade VMware vSphere ESXi Dump Collector (Optional).

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere ESXi Dump Collector* from the list.

   b Provide vCenter Server, VMware vSphere ESXi Dump Collector information and record all configuration settings used.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

8 Upgrade VMware vSphere Syslog Collector (Optional).

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Syslog Collector* from the list.

   b Provide vCenter Server, VMware vSphere Syslog Collector information and record all configuration settings used.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

9 Upgrade VMware vSphere Auto Deploy (Optional).

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Auto Deploy* from the list.

   b Provide vCenter Server, VMware vSphere Auto Deploy information and record all configuration settings used.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

10 Upgrade VMware vSphere Authentication Proxy (Optional).

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware Authentication Proxy* from the list.

   b Provide vCenter Server, VMware Authentication Proxy information and record all configuration settings used.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

11 Upgrade VMware vSphere Web Client (Optional)

   a Start VMware vCenter Installer for the version you want to upgrade to and select *VMware vSphere Web Client* from the list.

   b Proceed with the installation.

   c In the event that errors are encountered during the upgrade process, research the cause of the upgrade. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

12 Upgrading Update Manager (Optional)

Note The VMware Update Manager database must be running before attempting to upgrade VMware Update Manager.

a Using the Service Control Manager, start the *VMware vCenter Server* service.

b Start VMware vCenter Installer for the version you want to upgrade to and select *vCenter Update Manager* from the list.

c During the vCenter Update Manager upgrade, provide the same configuration settings used during the upgrade process on the Secondary node.

d On the *Database re-initialization warning* page, select *Do not overwrite, leave my existing database in place* option and proceed with the installation process.

Important Before proceeding with the database upgrade, perform a backup of the existing vCenter Update Manager database.

e On the *Database Upgrade* page, select the option *Yes, I want to upgrade my Update Manager database*.

f In the event errors are encountered during the installation, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with the upgrade procedure.

g Once the upgrade is complete, verify that vCenter Update Manager is operational.

13 Verify that vCenter Server and all updated extensions are operational.

14 Using the Service Control Manager, configure *VMware vCenter Server Heartbeat* service Startup Type to *Automatic* on both Primary and Secondary nodes.

15 Start vCenter Server Heartbeat on both nodes.

16 Launch the vCenter Server Heartbeat Console and connect to the pair.

a Check that the system completes the Full System Check and is replicating.

b Navigate to the vCenter Server Heartbeat Console *Application: Tasks* page and manually run the Protected Service Discovery task.

Troubleshooting

If vCenter Server fails to start on the Secondary node following a manual failover, perform the following steps.

Procedure

1 Shutdown vCenter Server Heartbeat.

2 Launch the Configure Server wizard and set the Secondary node's role to *Passive*.

3 Start vCenter Server Heartbeat on the Secondary node.

4 Start the Configure Server wizard on the Primary node and set the node's role to *Active*.

5 Start vCenter Server Heartbeat on the Primary node.

6 Launch the vCenter Server Heartbeat Console and verify that the system completes the Full System Check.

7 Investigate the cause of the vCenter Server failure on the Secondary node.

Uninstalling vCenter Server Heartbeat 5

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.

Note To ensure that protected application(s) are available after VMware vCenter Server Heartbeat has been uninstalled, VMware strongly recommends that only one of the two nodes (the currently active node) is left on the network. If the passive node is a virtual machine, the image can be deleted and the uninstall procedure applied only to the active node.

Procedure

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 node on the network. In a typical uninstall process, the active node remains on the network to continue providing application services to end users, and the passive node is removed from the network.

7 Select whether to leave the node 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 node that will be renamed. Click **Next** to start the uninstall process.

Note After the uninstall process completes, you will be notified of any files that could not be removed and advised to delete them manually. The SupportLogs directory is also left behind. This is intentional and should not be deleted in the event you need to submit a support request.

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

11 Click **Content**.

12 Click **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.

A new window appears.

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 node in the pair to uninstall vCenter Server Heartbeat.

Installation Verification Testing 6

Important The following procedure provides information about performing Installation Verification testing on a vCenter Server Heartbeat Pair to ensure proper installation and configuration. Additionally, this procedure provides step-by-step procedures to perform a manual failover in the event of an application failure and automated failover in the event of network or hardware failure resulting in excessive missed heartbeats.

Note In this document, the term “Pair” refers to a vCenter Server Heartbeat Pair. Refer to the “Glossary,” on page 83 for more information about vCenter Server Heartbeat Pairs.

This chapter includes the following topics:

Exercise 1 — Auto-failover

VMware vCenter Server Heartbeat monitors vCenter Server services and the system environment to ensure that protected services are available for end users. To monitor services and the system environment, vCenter Server Heartbeat uses plug-ins which are designed specially for VMware services and the system.

If a protected service or the system begins to operate outside of preconfigured thresholds, vCenter Server Heartbeat can automatically failover to and make the passive node active to continuously provide services for end users.

Important These exercises are examples and should be performed in order. VMware recommends against attempting to test failover on a properly operating pair by methods such as unplugging a power cord. At the moment power is lost, any data not written to the passive node is lost. VMware recommends that all actions intended to verify operation of the passive node be performed as a manual failover rather than an automated failover.

Starting Configuration

Prior to initiating the Installation Verification process in a pair, vCenter Server Heartbeat must be configured with the Primary node as active and the Secondary node as passive. Additionally, the following prerequisites must be met:

- The Secondary node must be synchronized with the Primary node.
- All protected services must be operating normally.
- If installed in a LAN environment, verify that *Failover from Primary server to Secondary server if channel heartbeat is lost for failover timeout* is selected from the **Server: Monitoring** > **Configure Failover** dialog (default setting).
- If installed in a WAN environment, you must manually select *Failover from Primary server to Secondary server if channel heartbeat is lost for failover timeout* in the **Server: Monitoring** > **Configure Failover** dialog.

Important Prior to starting the Installation Verification process, ensure that a known good backup of the Primary node exists and examine the Windows event logs for recent critical errors.

VMware provides an executable, nfavt.exe, to emulate conditions that result in auto-failover so you can verify that your vCenter Server Heartbeat installation performs as expected. This section guides you through the steps necessary to perform this verification.

Steps to Perform

Important If you encounter errors and or find it necessary to back out the changes made by this exercise, you can stop at any point and perform the steps described in the Back-out Procedure (Auto-Failover) to return the pair to its original operating configuration and state.

Table 6- 1. Perform the following procedure to verify auto-failover in a pair configuration.

Machine ID	Activity	Results
Primary	Open a command prompt.	
	Change directory to C:\Program Files\VMware\VMware vCenter Server Heartbeat\R2\Bin	
	Execute nfavt.exe When prompted, "*Are you sure you wish to continue*", click **Continue**.	Service is switched to the Secondary node and vCenter Server Heartbeat shuts down on the Primary node.
Secondary	Login to the vCenter Server Heartbeat Console.	
	In the *Servers* pane of the vCenter Server Heartbeat Console, select the pair.	The *System Overview* screen indicates that the Secondary node is active.
	Verify all protected applications have started on the Secondary.	Services are running on the Secondary.
	Verify data is present.	Data is present.

Successful completion of this procedure leaves the vCenter Server Heartbeat pair in the state necessary to perform the second part of the Installation Verification process, detailed in "Exercise 2 - Data Verification," on page 69.

Back-out Procedure (Auto-Failover)

Important Do not perform this back-out procedure if you intend to continue the Installation Verification process.

If for any reason you find it necessary to back out of this exercise, you can stop at any point and return the pair to the state it was in at the beginning of this exercise by performing the following steps:

1 Shut down vCenter Server Heartbeat and protected services on all nodes.

2 Complete the following on both nodes:

   a Open the *Configure Server* wizard.

   b Select the *Machine* tab.

   c Select the *Primary* node as active.

   d Click **Finish**.

3 On the Secondary node, right-click the taskbar icon and select *Start vCenter Server Heartbeat*.

4 Verify that the Secondary node is passive (**S**/**–**).

5 On the Primary node, right-click the taskbar icon and select *Start vCenter Server Heartbeat*.

6 After vCenter Server Heartbeat starts, login to the vCenter Server Heartbeat Console.

7 Verify that applications have started and replication to the passive node has resumed.

Exercise 2 - Data Verification

The Data Verification exercise validates that data is synchronized between the nodes resulting in current data on the active node following the auto-failover exercise performed previously. The objective is to take a working active node (the Secondary node) and synchronize it with the passive (Primary node). This exercise also demonstrates that all the correct services stopped when the Primary node became passive.

Starting Configuration

vCenter Server Heartbeat is running on the Secondary active node. Using the *System Tray* icon, verify that the node status displays **S/A**. vCenter Server Heartbeat is not running on the Primary node which is set to passive. Using the *System Tray* icon, verify that the node status displays ***-/-*** to indicate that vCenter Server Heartbeat is not running.

Steps to Perform

Table 6- 2. Perform the following steps to verify that data is synchronized following an auto-failover in the pair.

Machine ID	Activity	Results
Primary	Right-click the taskbar icon and select *Start vCenter Server Heartbeat*.	vCenter Server Heartbeat successfully starts.
	Login to vCenter Server Heartbeat Console.	
	In the *Servers* pane of the vCenter Server Heartbeat Console, select the pair.	The *System Overview* screen is displayed.
	Navigate to the *Server: Summary* tab to show the connection from the Secondary (active) to Primary (passive).	The *Server: Summary* page shows a connection from the Secondary node to the Primary node.
	Select the *Data: Replication* tab and wait for both the File System and *Registry* status to display as *Synchronized*. Access the vCenter Server Heartbeat logs and confirm that no exception errors occurred during the synchronization process.	Data replication resumes from the Secondary node back to the Primary node. Both the *File System & Registry* status become *Synchronized*.

Successful completion of this procedure leaves the vCenter Server Heartbeat pair in the state necessary to perform the final component of the Installation Verification process, detailed in “Exercise 3 - Manual Failover,” on page 70.

Exercise 3 - Manual Failover

The Manual Failover exercise demonstrates the ability to switch the functionality and operations of the active node on command to the other node in the pair using the vCenter Server Heartbeat Console. Perform this exercise only after successfully completing the Auto-Failover and Data Verification Exercises.

Starting Configuration

vCenter Server Heartbeat is running on the Secondary active node. Using the *System Tray* icon, verify that the node status displays **S/A**. vCenter Server Heartbeat is running on the Primary node which is set to passive. Using the *System Tray* icon, verify that the node status displays **P/-** to indicate that vCenter Server Heartbeat is running on the Primary node and that the Primary node is passive

Steps to Perform

Table 6- 3. Perform the following steps to switch functionality and operations on command from the active node to the ready standby node.

Machine ID	Activity	Results
Secondary	Launch vCenter Server Heartbeat Console and select the *Data: Replication* tab. Verify that both the *File System* and status are *Synchronized*.	
	Select the *Server: Summary* tab. Select the Primary node icon and click **Make Active**.	The vCenter Server Heartbeat Console *Server: Summary* page displays the applications stopping on the active node. Once all applications are stopped, the active node becomes passive and the passive node becomes active. The Console shows the applications starting on the newly active node. Both the *File System* and *Registry* status are *Synchronized*.
	Confirm application performance and availability meets previously defined criteria. Verify that client applications are running as expected after the manual failover process.	Services continue to be provided as before the manual failover occurred. You may need to refresh or restart some client applications as a result of a manual failover.

Successful completion of this procedure indicates a successful outcome from the Installation Verification process.

Pre-Installation Checklist

A

The following checklist is provided to assist you in preparing for installation of vCenter Server Heartbeat.

- ☐ Verify that the Primary node is a member of the domain.
- ☐ Verify that the Primary node is assigned the name to be used for the vCenter Service name (Both the Primary and Secondary nodes will be renamed during installation).
- ☐ Verify that UAC has been disabled on both the Primary and Secondary nodes.
- ☐ Verify that other than vCenter Server, its components, and SQL server, no other business critical applications are installed on the Primary server.
- ☐ Verify that vCenter Guided Consolidation, vCenter Update Manager, vCenter Converter, ESXi Dump Collector, Syslog Collector, Auto Deploy, and Authentication Proxy are configured using Fully Qualified Domain Names (FQDN) rather than IP addresses
- ☐ Verify that there is a minimum of 1GB of available RAM (2GB recommended) in addition to any other memory requirements for the Operating System or vCenter Server
- ☐ Verify that a minimum 2GB of free disk space is available on the installation drive for vCenter Server Heartbeat.
- ☐ Verify that local administrator rights are being used to perform vCenter Server Heartbeat installation.
- ☐ Verify that the latest Microsoft security updates are installed.
- ☐ Verify that all applications/components to be protected by vCenter Server Heartbeat are installed and configured on the Primary node.
- ☐ Verify that both Primary and Secondary nodes have identical system date, time, and time zone settings.
- ☐ Verify that the VMware Channel IP addresses have been properly configured on the VMware Channel NICs.
  Primary Channel IP _____
  Secondary Channel IP _____
- ☐ Verify that the Public IP address has been configured on the Primary Public NICs (LAN) or Primary and Secondary Public NICs (WAN).
  Primary Public IP _____
  Secondary Public IP (WAN only) _____
- ☐ Verify that Management IP addresses have been configured on the Public NICs using the same subnet as the Public IP and adjacent to the Public IP.
  Primary Management IP _____
  Secondary Management IP _____
- ☐ Verify that the Managed IP setting displayed in the Virtual Infrastructure Client is the same IP address used for the vCenter Server Heartbeat Public IP address.

- [ ] Verify that Windows Server Backup Feature and Command Line Tools are installed on the Primary and Secondary nodes (V2V only).
- [ ] Verify that all services to be protected are running or set to *Automatic* prior to installation.
- [ ] Configure any firewalls to allow traffic to pass through both the *Client Connection port* (52267) and the *Default Channel port* (57348).

Setup Error Messages

B

Table B- 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 node 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.

Table B- 1. Setup Error Messages

Message	Pri	Sec	Level	Test
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.
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	

Installation Troubleshooting

C

This appendix includes the following topics:

Pre-Installation Troubleshooting

Display resolution

Problem

The Setup dialogs occupy the entire screen and prevent access to the dialog controls.

Cause

vCenter Server Heartbeat is designed to display at a minimum resolution of 1024 X 768. Lower resolutions will cause the dialogs to occupy the full screen of a monitor.

Solution

Prior to running Setup or launching vCenter Server Heartbeat Console, ensure that screen resolution is set to a minimum of 1024 X 768.

VMware Channel

Problem

Attempts to ping between the Primary and Secondary nodes fail.

Cause

The most common VMware Channel configuration errors are as follows:

- VMware Channel IP addresses are configured in different subnets
- Firewalls are blocking traffic between the Primary and Secondary nodes
- In a WAN implementation, no static routes exist between the VMware Channel NICs

Solution

The VMware Channel configuration should be reviewed to verify proper configuration.

1. Configure the VMware Channel IP addresses properly.
2. Verify that firewalls are not blocking traffic on port 57348, the default channel port
3. In a WAN implementation, configure static routes between VMware Channel NICs properly.
4. Disable NetBIOS on the VMware Channel NICs.

Setup Troubleshooting

Setup permissions

Problem

When performing a restart during installation, Setup prompts for elevated permissions.

Cause

Attempting to run Setup without disabling UAC will result in permission elevation prompts anytime the node is restarted.

Solution

When installing on Windows Server 2012, 2008, or 2008 R2, VMware recommends that UAC be disabled on both the Primary and Secondary nodes. Once installation is complete, UAC can be re-enabled.

Setup fails to progress

Problem

VMware License Server is installed and Setup fails to progress.

Cause

The Web Client service is not set to either *Manual* or *Automatic*.

Solution

Before attempting to run vCenter Server Heartbeat Setup, set the Web Client service to either *Manual* or *Automatic*.

Packet filter fails to install

Problem

While attempting to install in a Physical to Virtual architecture using the Install Clone technique, the packet filter fails to install.

Cause

VMware Tools installed on the Secondary node during installation in a Physical to Virtual architecture using the Install Clone technique causes installation of the packet filter to fail.

Solution

Uninstall VMware Tools prior to starting the Setup process. Once vCenter Server Heartbeat is installed, you can reinstall VMware Tools.

During installation, node rename step fails to rename the node

Problem

During installation, the node rename of the Primary and Secondary nodes fail.

Cause

The domain controller for the domain was unable to process the rename request at time of the rename attempt.

Solution

The node rename process is the last step of vCenter Server Heartbeat installation. Should the node rename process fail to complete, manually rename the node to complete installation.

Post-Installation Troubleshooting

VMware Channel Fails to Connect After Configuring Firewall Ports

Problem

The VMware Channel fails to connect and does not allow traffic to pass between the Primary and Secondary nodes.

Cause

If Microsoft Windows changed the connection type from Private network to Unidentified network after the user has configured the firewall port to allow channel communications, this may cause the firewall changes to be reset for the new network type.

Solution

The firewall rules must be recreated to allow traffic to pass through for the Client Connection port and the Default Channel port. VMware recommends that the firewall be configured to allow the Client to connect to the Client Connection port by process, nfgui.exe, rather than by a specific port. To enable Channel communications between nodes, change the Network List Manager Policy so that the VMware Channel network is identified as a Private Network, and not the default Unidentified Network, and configure the firewall to allow traffic to pass through on Port 57348, the Default Channel port.

After installing vCenter Server Heartbeat, the packet filter fails to filter or an operating system failure (blue screen error) is experienced

Problem

After installing vCenter Server Heartbeat on a node with TCP Offload Engine (TOE) enabled NICs, the following symptoms are experienced:

- Operating system failure (blue screen error)
- Packet filter installs but cannot filter traffic
- Packet filter installs but the node is not visible on the network

Cause

vCenter Server Heartbeat is incompatible with TOE, a common feature of 10GB Ethernet cards. Some newer models of Ethernet cards offer a TOE to help manage TCP/IP communications. vCenter Server Heartbeat is intended to manage the passing or filtering of selected IP addresses, therefore the TOE function must be disabled to allow vCenter Server Heartbeat to exercise intelligent control of TCP/IP communications, depending on whether the node is the active or passive node.

Solution

If 10GB Mellanox network cards with TCP Offload Engine (TOE) enabled were present during installation, see VMware knowledge base article 1024066 - *TCP Offload features on all NICs must be disabled before installing vCenter Server Heartbeat* for instructions on how to resolve this problem.

vSphere Client Plug-in

Installing vCenter Plug-ins through the vSphere Client requires the vSphere Client to connect and download the plug-ins through the Public IP address. The Public network adapter must be first in the bind order. If vSphere Client is configured with any other IP address first in the bind order, the installation will fail.

Problem

Attempting to install the vSphere Client plug-in fails.

Cause

Installing vCenter Plug-ins through the vSphere Client requires the vSphere Client to connect and download the plug-ins through the Public IP address. To download the plug-in through the Public network adapter, it must be first in the bind order.

Solution

Reconfigure the network adapter/IP address bind order to show the Public IP address as first i the bind order.

DNS resolution

Problem

When deployed in a LAN, DNS fails to resolve the proper node management name and IP address.

Cause

Once installation has completed, vCenter Server Heartbeat nodes deployed in a LAN are assigned different node management names but must use the same Public IP address. If DNS has not been manually pre-populated with the new node management name and IP addresses, name resolution fails.

Solution

Pre-populate the DNS server with the new node management names and IP addresses to be used in the pair prior to starting vCenter Server Heartbeat to ensure proper resolution.

Glossary

Active
The functional state or role of a node when it is visible to clients through the network, running protected applications, and servicing client requests.

Alert
A notification provided by vCenter Server Heartbeat 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 between proprietary services. vCenter Server Heartbeat failovers require no changes to AD resulting in failover times typically measured in seconds.

Active–Passive
The coupling of two nodes with one node visible to clients on a network and providing application service while the other node is not visible and not providing application service to clients.

Advanced Configuration and Power Interface (ACPI)
A specification that dictates how the operating system can interact with the hardware especially where power saving schemes are used. The Primary and Secondary nodes must have identical ACPI compliance.

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

Basic Input/Output System (BIOS)

The program a personal computer's microprocessor uses to get the computer system started after you turn it on. It also manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse, and printer.

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

Channel Drop
An event in which the dedicated communications link between nodes fails, often resulting in the passive node becoming active and consequently creating a split-brain syndrome.

Channel NIC (Network Interface Card)
A dedicated NIC used by the VMware Channel.

Checked
The status reported for user account credential (username/password) validation.

Cloned Servers
Servers that have identical configuration settings, names, applications, Security Identifiers (SIDs) and IP addresses, following the installation of vCenter Server Heartbeat.

Cloning Process
The vCenter Server Heartbeat process whereby all installed programs, configuration settings, and the machine name, Security Identifier (SID), and IP address are copied to another node.

Cluster
A generic term for a vCenter Server Heartbeat Pair and the set of machines (physical or virtual) involved in supporting a single protected node.

Connection
Also referred to as Cluster Connection. Allows an administrator to communicate with a vCenter Server Heartbeat Cluster, either on the same machine or remotely.

Crossover Cable
A network cable that crosses the transmit and receive lines.

Data Replication
The transmission of protected data changes (files and registry) from the active to the passive node via the VMware Channel.

Degraded
The status reported for an application or service that has experienced an issue that triggered a Rule.

Device Driver
A program that controls a hardware device and links it to the operating system.

Disaster Recovery (DR)
A term indicating how you maintain and recover data with vCenter Server Heartbeat in event of a disaster such as a hurricane or fire. DR protection is achieved by placing the Secondary node (in a Pair) at an offsite facility, and replicating the data through a WAN link.

DNS (Domain Name System) Server
Provides a centralized resource for clients to resolve NetBIOS names to IP addresses.

Domain
A logical grouping of client server based machines where the administration of rights across the network are maintained in a centralized resource called a domain controller.

Domain Controller (DC)
The server responsible for maintaining privileges to domain resources; sometimes called AD controller in Windows 2003 and above domains.

Dualed
A way to provide higher reliability by dedicating more than one NIC for the VMware Channel on each node.

Failover
A process by which the role of the passive node is changed to active automatically in an "Failover (Automatic)", or the active node and the passive node switch roles in a "Failover (Manual)" failover.

Failover (Automatic)
Failover is the process by which the passive node assumes the active role when it no longer detects that the active node is alive as a result of a critical unexpected outage or crash of a node.

Failover (Manual)
The graceful transfer of control and application service to the passive node.

Full System Check (FSC)
The internal process automatically started at the initial connection or manually triggered through the vCenter Server Heartbeat Console to perform verification on the files and registry keys and then synchronize the differences.

Fully Qualified Domain Name (FQDN)
Also known as an absolute domain name, a FQDN specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain, relative to the root domain. Example: somehost.example.com., where the trailing dot indicates the root domain.

Global Catalog Server
A global catalog is a domain controller that stores a copy of all Active Directory objects in a forest. The global catalog stores a full copy of all objects in the directory for its host domain and a partial copy of all objects for all other domains in the forest.

Graceful (Clean) Shutdown
A shutdown of vCenter Server Heartbeat based upon completion of replication by use of the vCenter Server Heartbeat Console, resulting in no data loss.

Group
An arbitrary collection of vCenter Server Heartbeat Clusters used for organization.

Hardware Agnostic
A key vCenter Server Heartbeat feature allowing for the use of nodes with different manufacturers, models, and processing power in a single vCenter Server Heartbeat Cluster.

Heartbeat
The packet of information issued by the passive node across the Channel, which the active node responds to indicating its presence.

Heartbeat Diagnostics
The umbrella name for the vCenter Server Heartbeat process and tools used to verify the production nodes health and suitability for the implementation of a vCenter Server Heartbeat solution.

Heartbeat Diagnostics Report
A report provided upon the completion of the Heartbeat Diagnostics process that provides information about the node, system environment, and bandwidth.

High Availability (HA)
Keeping users seamlessly connected to their applications regardless of the nature of a failure. LAN environments are ideally suited for HA.

Hotfix
A single, cumulative package that includes one or more files that are used to address a problem in a product.

Identity
The position of a given node in the vCenter Server Heartbeat Cluster: Primary or Secondary.

Install Clone
The installation technique used by vCenter Server Heartbeat to create a replica of the Primary node using NTBackup or Wbadmin and to restore the replica to the Secondary node.

Low Bandwidth Module (LBM)
A module that compresses and optimizes data replicated between nodes over a WAN connection. This delivers maximum data throughput and improves application response time on congested WAN links.

Machine Name
The Windows or NETBIOS name of a computer.

Management IP Address
An additionally assigned unfiltered IP address used for node management purposes only.

Many-to-One
The ability of one physical node (hosting more than one virtual node) to protect multiple physical nodes.

Network Monitoring
Monitoring the ability of the active node to communicate with the rest of the network by polling defined nodes across the network at regular intervals.

Pair
See vCenter Server Heartbeat Pair above.

Passive
The functional state or role of a node when it is not delivering service to clients and is hidden from the rest of the network.

Pathping
A route-tracing tool that works by sending packets to each router on the way to a final destination and displays the results of each hop.

Plug-and-Play (PnP)
A standard for peripheral expansion on a PC. On starting the computer, PnP automatically configures the necessary IRQ, DMA and I/O address settings for the attached peripheral devices.

Plug-in
An application specific module that adds vCenter Server Heartbeat protection for the specific application.

Pre-Clone
An installation technique whereby the user creates an exact replica of the Primary node using VMware vCenter Converter or other 3rd party utility prior to the initiation of installation and uses the replica as a Secondary node.

Pre-Installation Checks
A set of system and environmental checks performed as a prerequisite to the installation of vCenter Server Heartbeat.

Primary
An identity assigned to a node during the vCenter Server Heartbeat installation process that normally does not change during the life of the node and usually represents the production node prior to installation of vCenter Server Heartbeat.

Protected Application
An application protected by the vCenter Server Heartbeat solution.

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

Public NIC
The network card which hosts the Public IP address.

Public Network
The network used by clients to connect to node applications protected by vCenter Server Heartbeat.

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 may have a higher priority than ICMP traffic, as the consequences of interrupting data replication are more obvious than slowing down ICMP traffic.

Receive Queue
The staging area on a node used to store changes received from another node in the replication chain before they are applied to the disk/registry on the passive node.

Remote Desktop Protocol (RDP)
A multi-channel protocol that allows a user to connect to a computer running Microsoft Terminal Services.

Replication
The generic term given to the process of intercepting changes to data files and registry keys, transporting the changed data across the Channel, and applying them to the passive node(s) so the nodes are maintained in a synchronized state.

Role
The functional state of a node in the vCenter Server Heartbeat Cluster: active or passive.

Rule
A set of actions performed by vCenter Server Heartbeat when defined conditions are met.

Secondary
An identity assigned to a node during the vCenter Server Heartbeat installation process that normally does not change during the life of the node and usually represents the standby node prior to installation of vCenter Server Heartbeat.

Security Identifier (SID)
A unique alphanumeric character string that identifies each operating system and each user in a network of 2008/2012 systems.

Send Queue
The staging area on a node used to store intercepted data changes before being transported across to a passive node in the replication chain.

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

Shared Nothing
A key feature of vCenter Server Heartbeat in which no hardware is shared between the Primary and Secondary nodes. This prevents a single point of failure.

SMTP
A TCP/IP protocol used in sending and receiving e-mail between nodes.

SNMP
Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks.

Split-Brain Avoidance
A unique feature of vCenter Server Heartbeat that prevents a scenario in which Primary and Secondary nodes attempt to become active at the same time leading to an active-active rather than an active-passive model.

Split-Brain Syndrome
A situation in which more than one node in a vCenter Server Heartbeat Cluster are operating in the active mode and attempting to service clients, resulting in the independent application of different data updates to each node.

Subnet
Division of a network into an interconnected but independent segment or domain, intended 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.

Synchronize
The internal process of transporting 64KB blocks of changed files or registry key data, through the VMware Channel, from the active node to the passive node to ensure the data on the passive node is a mirror image of the protected data on the active node.

System Center Operations Manager (SCOM)
System Center Operations Manager is a cross-platform data center management server for operating systems and hypervisors.

System State
Data that comprises the registry, COM+ Class Registration database, files under Windows File Protection, and system boot file; other data may be included in the system state data.

Task
An action performed by 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 your computer and a specified destination computer.

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 not monitored nor its data replicated by vCenter Server Heartbeat.

vCenter Server Heartbeat
The core replication and system monitoring component of the vCenter Server Heartbeat solution.

vCenter Server Heartbeat Packet Filter
The network component, installed on all nodes, that controls network visibility.

vCenter Server Heartbeat Pair
Describes the coupling of the Primary and Secondary node in a vCenter Server Heartbeat solution.

vCenter Server Heartbeat Plug-ins
Optional modules installed into a vCenter Server Heartbeat node to provide additional protection for specific applications.

vCenter Server Heartbeat Failover Process
A process unique to vCenter Server Heartbeat in which the passive node gracefully (manual) or unexpectedly (automatic) assumes the role of the active node providing application services to connected clients.

Virtual Private Network (VPN)
A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

VMware Channel
The IP communications link used by the vCenter Server Heartbeat system for the heartbeat and replication traffic.

VMware License Key
The key obtained from the VMware that allows the use of components in vCenter Server Heartbeat; entered at install time, or through the Configure Server Wizard.

Windows Management Instrumentation (WMI)
A management technology allowing scripts to monitor and control managed resources throughout the network. Resources include hard drives, file systems, operating system settings, processes, services, shares, registry settings, networking components, event logs, users, clusters, and groups.