Installation on Windows Server 2008 When the Secondary Server is Virtual

vCenter Server Heartbeat 6.5

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-000944-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About This Book

The Installation Guide provides information about installing VMware vCenter Server Heartbeat, including implementation in a Local Area Network (LAN) or Wide Area Network (WAN). To help you protect your VMware vCenter Server, this book provides an overview of installation procedures and guidance for configuration of vCenter Server Heartbeat when the Secondary server is virtual.

Intended Audience

This guide assumes the reader has a working knowledge of networks including the configuration of TCP/IP protocols and domain administration, 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 the Switchover and Failover processes.
- Chapter 2 — *vCenter Server Heartbeat Implementation* discusses environmental prerequisites and pre-install requirements for installation, options for server architecture, 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 servers, and through post-installation configuration.
- Appendix A — *Setup Error Messages* lists error messages that may appear during setup and tests that will help you resolve the errors.

- Appendix B — *Installation Verification* provides a procedure to verify that vCenter Server Heartbeat is properly installed and initially configured.
- Appendix C — *Upgrading* provides the procedures necessary to upgrade vCenter Server Heartbeat and vCenter Server and its components from the previous version to the current version.

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

vCenter Server Heartbeat is a Windows based service specifically designed to provide High Availability or Disaster Recovery protection for vCenter Server configurations without requiring any specialized hardware.

This chapter includes the following topics:

vCenter Server Heartbeat Concepts

Architecture

vCenter Server Heartbeat software is installed on a "Primary" (production) server and a "Secondary" (ready-standby) server. These names refer to the Identity of the servers and never change throughout the life of the server.

Depending on the network environment, vCenter Server Heartbeat can be deployed in a Local Area Network (LAN) for High Availability or Wide Area Network (WAN) for Disaster Recovery, providing the flexibility necessary to address most network environments.

When deployed, one of the servers performs the "Role" of the "Active" server that is visible on the Public network while the other is "Passive" and hidden from the Public network but remains as a ready-standby server. The Secondary server has a different Fully Qualified Domain Name (FQDN) different than the Primary server but uses the same file and data structure, same Principal (Public) network address, and can run all the same applications and services as the Primary server. Only one server can display the Principal (Public) IP address and be visible on the Public network at any given time. vCenter Server Heartbeat software is symmetrical in almost all respects, and either the Primary server or the Secondary server can take the active role and provide protected applications to the user.

vCenter Server Heartbeat provides continuous access to the passive server simultaneously as the active server continues to service clients allowing the passive server to be easily accessed for maintenance purposes, updating anti-malware definition files, receiving operating system hot-fixes, updates and patches from third-party management software, and allows use of third-party monitoring tools.

Protection Levels

vCenter Server Heartbeat provides the following protection levels:

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

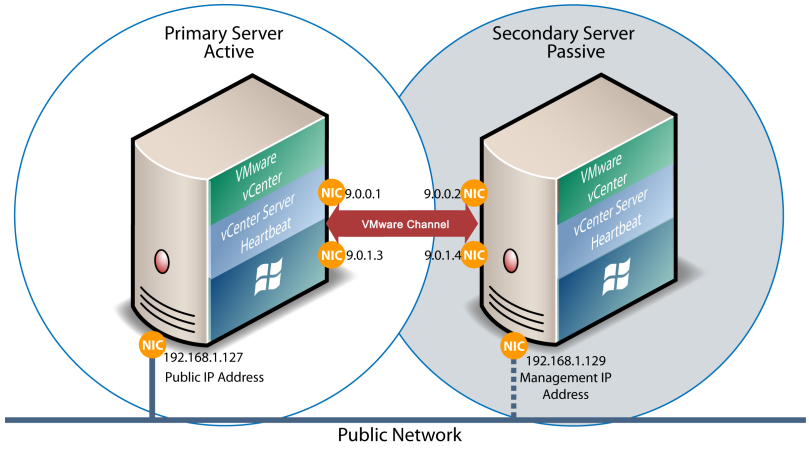
vCenter Server Heartbeat provides all five protection levels continuously, ensuring all facets of the user environment are maintained at all times, and that the Public network continues to operate through as many failure scenarios as possible.

Communications

vCenter Server Heartbeat communications consist of two crucial components, the VMware Channel and the Principal (Public) network.

To accommodate communications requirements, vCenter Server Heartbeat can be configured to use either multiple NICs (1 X Channel and 1 X Principal (Public) connection) on each server providing a separate dedicated VMware Channel network from the Principal (Public) network or a single NIC on each server to fulfill both the VMware Channel and Principal (Public) network connection requirements.

Figure 1- 1. Communications Between Primary and Secondary Servers



VMware Channel

The first component is the VMware Channel which provides communications between the active and passive servers. The VMware Channel is used for control and data transfer from the active server to the passive server and for monitoring of the active server's status by the passive server.

The NICs on the active and passive servers used for the VMware Channel are normally configured with IP addresses outside of the Principal (Public) network subnet range and are referred to as the VMware Channel addresses. During installation, setup will disable NetBIOS for the VMware Channel(s) on the active and passive servers to prevent server name conflicts.

The NICs that support connectivity across the VMware Channel can be standard 100BaseT Ethernet cards providing a throughput of 100 Mbits per second across standard Cat-5 cabling. When using multiple NICs providing a separate dedicated VMware Channel, this channel requires no hubs or routers, but the direct connection does require crossover cabling.

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

Principal (Public) Network

The second component is the Principal (Public) network used by clients to connect to the active server. The Principal (Public) network provides access to the Principal (Public) IP address used by clients to connect to the active server and can be moved between the two Primary and Secondary servers to ensure clients can continue to connect to the active server in the event of a switchover or failover.

The Principal (Public) IP address is a static IP address that is only available on the currently active server and is the IP address a client uses to connect to the active server. It must be configured as a static IP address, that is, not DHCP (Dynamic Host Configuration Protocol) enabled. In the figure above, the IP address is configured as `192.168.1.127`. The Principal (Public) IP address is always assigned to the active server in the pair and in the event of a switchover or failover, will be removed from the previously active server and reassigned to the new active server. The passive server will always have the Management IP address (discussed below)available and therefore provide access to the passive server.

Management IP Address

Both the Primary and Secondary servers are configured with Management IP addresses that allow access to the server when the server is in the passive role. The Management IP address is a static IP address in the same subnet as the Principal (Public) IP address and is always available for administrators to access the server.

vCenter Server Heartbeat Switchover and Failover Processes

vCenter Server Heartbeat uses four different procedures – managed switchover, automatic switchover, automatic failover, and managed failover – to change the role of the active and passive servers depending on the status of the active server.

- *Managed Switchover* – You can click **Make Active** on the vCenter Server Heartbeat Console *Server: Summary* page to manually initiate a managed switchover. When a managed switchover is triggered, the running of protected applications is transferred from the active machine to the passive machine in the server pair. The server roles are reversed.
- *Automatic Switchover* – Automatic switchover (auto-switchover) is similar to failover (discussed in the next section) but is triggered automatically when system monitoring detects failure of a protected application.
- *Automatic Failover* – Automatic failover is similar to automatic switchover (discussed above) but is triggered when the passive server detects that the active server is no longer running properly and assumes the role of the active server.
- *Managed Failover* – Managed failover is similar to automatic failover in that the passive server automatically determines that the active server has failed and can warn the system administrator about the failure, but no failover actually occurs until the system administrator manually triggers this operation (the default configuration in a DR environment).

Implementation 2

This chapter discusses the deployment options and prerequisites to successfully implement vCenter Server Heartbeat and provides a step-by-step process to assist in selecting options required for installation. The deployment scenario table 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 can protect vCenter Server and SQL Server installed on the same server, or protect vCenter Server 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 server meets the minimum requirements for a successful installation. A critical stop or warning message appears if the server fails a check. Refer to the Appendix A, "Setup Error Messages," on page 41 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 will prompt 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 2008
  - Windows Server 2008 x86 Standard/Enterprise/Datacenter SP1 and SP2
  - Windows Server 2008 x64 Standard/Enterprise/Datacenter SP1 and SP2
  - Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1

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

- vCenter Server Heartbeat supports the following versions of vCenter Server
  - vCenter Server 4.0 Update 1
  - vCenter Server 4.0 Update 2
  - vCenter Server 4.0 Update 3
  - vCenter Server 4.0 Update 4
  - vCenter Server 4.1
  - vCenter Server 4.1 Update 1
  - vCenter Server 4.1 Update 2
  - vCenter Server 5.0
  - vCenter Server 5.0 Update 1
  - vCenter Server 5.1

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

- vCenter Server Heartbeat supports the following versions of SQL Server on Windows Server 2008 Platforms

  x86 Platform (32-bit hardware)

  - SQL Server 2012 Standard, Enterprise, and Express Editions on
    - Windows Server 2008 SP2 Standard and Enterprise
  - SQL Server 2008 R2 Standard, Enterprise, and Express Editions on
    - Windows Server 2008 SP2 Standard and Enterprise
  - SQL Server 2008 Standard, Enterprise and Express Editions up to SP2 on
    - Windows Server 2008 SP2 Standard and Enterprise
  - SQL Server 2005 up to SP4 Standard, Enterprise, and Express Editions
    - Windows Server 2008 SP2

  x64 / 64 Platform (64-bit hardware)

  - SQL Server 2012 Standard, Enterprise, and Express Editions on
    - Windows Server 2008 R2 SP1 Standard and Enterprise
    - Windows Server 2008 SP2 Standard and Enterprise
  - SQL Server 2008 R2 Standard, Enterprise, and Express Editions on
    - Windows Server 2008 R2 Standard and Enterprise
    - Windows Server 2008 SP2 Standard and Enterprise
  - SQL Server 2008 Standard, Enterprise and Express Editions up to SP2 on
    - Windows Server 2008 R2 Standard and Enterprise
    - Windows Server 2008 SP2 Standard and Enterprise
  - SQL Server 2005 up to SP4 Standard, Enterprise, and Express Editions
    - Windows Server 2008 SP2

Note This version of vCenter Server Heartbeat supports 32 bit versions of SQL Server 2005/2008 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

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 and SQL Server.

- Verify that the Primary server is a member of the domain. The Domain for the Primary server will not change throughout the installation process although the Primary and Secondary server names will be changed as part of the installation procedure.
- 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 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.
- 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 that will be protected by vCenter Server Heartbeat must be installed and configured on the Primary server prior to installing vCenter Server Heartbeat.
- Verify that both Primary and Secondary servers have identical system date, time, and time Zone settings.
- Verify that the Managed IP setting displayed in the Virtual Infrastructure Client is the same IP address used for the vCenter Server Heartbeat Principal (Public) IP address.
- Verify that Windows Server Backup Feature and Command Line Tools have been installed on the Primary and Secondary servers prior to installing vCenter Server Heartbeat. Installation of Windows Server Backup Feature and Command Line Tools will also install Windows PowerShell.
- 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 role of the server. The target state of the services is normally running on the active server and stopped on the passive.
- Configure Management IP addresses on the Principal (Public) NIC on both the Primary and Secondary servers.

Important Adjacent IP addresses should be reserved and used for the Principal (Public) IP address and the Management IP addresses for the Primary and Secondary Servers.

Server Deployment Architecture Options

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

Virtual to Virtual

Virtual to Virtual is the supported architecture if vCenter Server is already installed on the production (Primary) server running on a virtual machine. Benefits to this architecture include reduced hardware cost, shorter installation time, and use of the Pre-Clone technique for installation.

The Secondary virtual machine must meet the minimum requirements.

- The specifications of the Secondary virtual machine must match the specifications of the Primary virtual machine as follows:
  - Similar CPU (including resource management settings)
  - Memory configuration (including resource management settings)
  - Appropriate resource pool priorities
- Each virtual machine used in the Virtual to Virtual pair must be on a separate ESX host to guard against failure at the host level.

  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 servers 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 server as follows:
  - Similar CPU
  - Identical Memory
- The Secondary virtual machine must have sufficient priority in resource management settings so that other virtual machines do not impact its performance.
- Each virtual NIC must use a separate virtual switch.

Cloning Technology Options

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

Cloning Prior to Installation

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

- 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 server during the vCenter Server Heartbeat installation process. If VMware Tools are currently installed on the Secondary server, you must fully uninstall VMware Tools prior to initiation of the Setup process. Once the installation of vCenter Server Heartbeat has completed, you may reinstall VMware Tools.

- 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 server before starting the vCenter Server Heartbeat installation process.

Application Component Options

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

Supported vCenter Services

- vCenter Server Version 4.0
  - VMware vCenter Server
  - VMware Guided Consolidation Service
  - VMware License Server
  - VMware ADAM
  - VMware vCenter Management Web Server
  - VMware vCenter Update Manager
  - VMware vCenter Converter
  - VMware vCenter Orchestrator Configuration
  - VMware vCenter Orchestrator Server
  - VMware vSphere Host Update Utility
  - VMware vSphere Client
  - VMware Mount Service for VirtualCenter
- vCenter Server Version 4.1
  - VMware vCenter Server
  - VMware Guided Consolidation Service
  - VMware License Sever
  - VMware ADAM
  - VMware vCenter Management Web Server
  - VMware vCenter Update Manager
  - VMware vCenter Converter
  - VMware vCenter Orchestrator Configuration
  - VMware vCenter Orchestrator Server
  - VMware vSphere Host Update Utility
  - VMware vSphere Client
  - VMware Mount Service for VirtualCenter

- vCenter Server Version 5.0
  - VMware vCenter Server
  - VMware ADAM
  - VMware vCenter Management Web Server
  - VMware vCenter Update Manager
  - VMware vCenter Orchestrator Configuration
  - VMware vCenter Orchestrator Server
  - VMware vSphere Host Update Utility
  - VMware vSphere Client
  - VMware Inventory Service
  - VMware USB Arbitration Service
  - VMware vSphere Web Client
  - VMware vSphere ESXi Dump Collector
  - VMware vSphere ESXi Dump Collector Web Server
  - VMware vSphere Auto Deploy Waiter
  - VMware vSphere Authentication Proxy
  - VMware vSphere Authentication Proxy Adapter
  - VMware Syslog Collector
  - VMware vSphere Profile-Driven Storage Service

- vCenter Server Versions 5.1
  - VMware vCenter Inventory Service
  - VMware ADAM
  - VMware USB Arbitration Service
  - VMware vCenter Server
  - VMware vSphere Client
  - VMware vSphere Web Client
  - VMware vCenter Update Manager
  - VMware vSphere Update Manager Download Service
  - VMware vCenter Orchestrator Configuration
  - VMware vCenter Orchestrator Server
  - VMware vSphere ESXi Dump Collector
  - VMware Syslog Collector
  - VMware vSphere Auto Deploy
  - VMware vSphere Authentication Proxy
  - VMware vCenter Host Agent Pre-Upgrade Checker
  - VMware vCenter Single Sign On
  - VMware vSphere Profile-Driven Storage Service
  - RSA SSPI Service
- View Composer 1.1, 2.0, 2.7, and 3.0

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

  - VMware View Composer
  - VMware Universal File Access
  - vCenter Converter Enterprise

Important Ensure that all VMware services are bound to the Principal (Public) IP address on the Principal (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 separate host from vCenter Server, you must repeat the installation process for the Primary and Secondary server specifically for the SQL Server.

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 configuration has specific configuration requirements to ensure proper operation.

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

Multiple NICs

vCenter Server Heartbeat supports use of multiple NICs on each server pair. When using multiple NICs, one NIC is configured with the Principal (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 single point of failure that exists in single NIC configurations. To configure using multiple NICs on each server, see "Multi-NIC Configuration," on page 23.

Note vCenter Server Heartbeat does NOT out-of-the-box support teams of NICs but can be configured to support teamed NICs with additional configuration steps when installing with teamed NICs present. See knowledge base article 1027288 for more information about teamed NICs.

Single NIC

vCenter Server Heartbeat also supports use of a single NIC configured to perform all three functions, providing the Principal (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 server, see "Single NIC Configuration," on page 24.

Local Area Network (LAN)

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

Wide Area Network (WAN)

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

vCenter Server Heartbeat also supports sites with the same subnet. In this scenario the vCenter Server Heartbeat shares a single Principal (Public) IP address between the Primary and Secondary server assigning it to the active server. Although 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 *Principal (Public) IP Address Configuration* page and specify the IP address to be shared by both servers.

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 servers in the vCenter Server Heartbeat pair use the same Public IP address
- If the Primary and DR site use different subnets:
  - During install, follow the steps for a WAN
  - Both servers in the vCenter Server Heartbeat pair require a separate Principal (Public) IP address and a VMware Channel IP address
  - 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 server.

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

Latency

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

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

Network Interface Card (NIC) Configuration

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

Important The Primary and Secondary servers 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 Server

The Primary server is configured with the following connections:

- A Principal (Public) network connection configured with a static Principal (Public) IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.
- A Management IP connection using the same subnet and NIC as the Principal (Public) IP address, configured with a static IP address in the same subnet as the Principal (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 Principal (Public) IP address or Management IP address with a different IP address than the Secondary server channel NIC, and network mask. No gateway or DNS server address is configured. NetBIOS will be disabled during the installation process to prevent server 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 Server

The Secondary server must have the same number of NICs as the Primary server and is configured as follows:

- A Principal (Public) 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 Principal (Public) IP address of the Secondary server may be in a different subnet than the Primary server.

- A Management IP connection using the same subnet as the Secondary server's Principal (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 network connection(s) configured on a separate dedicated NIC with a static IP address in a different subnet than the Secondary Principal (Public) IP address or Management IP address and with a different IP address than the Primary server's VMware Channel NIC and a network mask. No gateway address or DNS server address is configured. NetBIOS will be disabled during the installation process to prevent server 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 Server

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

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

Secondary Server

The Secondary server must have the same number of NICs as the Primary server 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 Principal (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 will be disabled during the installation process to prevent server name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared prior to installing vCenter Server Heartbeat.

Firewall Configuration Requirements

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

Important When installing on Windows Server 2008, 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 servers, 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.

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 anit-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 server must be the same as the software that runs on the Secondary server. 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 server for malware definition updates. If this is not possible, manually update malware definitions on the passive server.

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 server (such as exclusions) must be made on the other server as well. vCenter Server Heartbeat does not replicate this information.

Deployment Options Summary

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

Table 2- 1. 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 server 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.

After selecting implementation options, begin the installation process. During the installation process, vCenter Server Heartbeat performs a variety of checks to ensure the server meets the minimum requirements for a successful installation. Should the server fail one of the checks, a critical stop or warning message appears. Refer to the Appendix A, "Setup Error Messages," on page 41 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 Server

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 server.

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. If using multiple NICs click **OK** three times to close the dialogs and continue with Step 5. If using a single NIC, go to Step 8.

5 Right-click the *Principal (Public)* network connection and select *Properties*.

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

7 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.

8 Configure the Management IP address on the Principal (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, and enter the Management IP address. Click **OK** three times to close the dialogs.

9 You have the following options:

   - If protecting vCenter Server 5.0 continue with Step 10.
   - If protecting vCenter Server 4.0, 4.1, or 5.1, go to Step 12.

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

11 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.

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

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

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

   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.

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

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

   The *Server Identity* page is displayed.

   Note The left pane of each page in the *Setup* wizard provides information about the setup process.

16 Select the identity of the server on the *Server Identity* page. Select *Primary* as the server identity and click **Next**.

   The *VMware End User License Agreement* page is displayed.

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

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 Server is Virtual* , then click **Next**.

The *Installation Paths* 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 " ".

If using a single NIC, go to Step 23. If using multiple NICs, continue with Step 22.

The *Channel Adapter Identification* page is displayed.

22 Identify the network adapter(s) for use in the VMware Channel on the *Channel Adapter Identification* page. Select the network adapters (NICs) for the VMware Channel from the list. Click the adapter name to display the selected NIC properties in the lower pane. You must select at least one NIC to proceed with the installation. If no NICs are available, click **Open Network Connections** to review the network configuration of your machine and verify that you have the correct number of NICs installed. After selecting the appropriate NIC, click **Next**.

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 *VMware Channel IP Configuration* page is displayed.

23 The *VMware Channel IP Configuration* page prompts you to configure the VMware Channel(s) IP network addresses. Click **Add** for each available channel connection. For the Primary server, select from a drop-down menu that lists all local IP addresses. Type the reciprocal IP address on the Secondary server into the *IP Address On Secondary* text box. 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 Principal (Public) IP addressing schema so that VMware Channel traffic routing uses the VMware Channel network card rather than the Principal (Public) network card.

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

24 Review and adjust, if necessary, the default channel port. Click **Next**.

- If using multiple NICs, continue with Step 25.
- If using a single NIC, go to Step 26.

Important When the implementation spans multiple sites with firewalls between the servers, configure the firewalls to allow traffic to pass through the default channel port or the manually configured channel port. See "Firewall Configuration Requirements," on page 24 for additional information. The *Public Adapter Identification* page is displayed.

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

The *Principal (Public) IP Address Configuration* page is displayed.

26 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)*.

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

When the Principal (Public) addresses on the Secondary server are different from those on the Primary server, vCenter Server Heartbeat must perform additional tasks during failover or switchover. These additional tasks require clients to change their resolution of the active server to a different IP address and requires that vCenter Server Heartbeat update the DNS entries for the active server across the enterprise. Such updates require the credentials for domain administrators (or an account with equivalent rights). Type the *Domain Name*, a domain administrator *Username* and *Password* in the respective text boxes and click **Next**. The *Management IP Address Configuration* page is displayed.

28 Using the **Add** buttons, add the previously configured Management IP addresses for the Primary and Secondary servers 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 server's Principal (Public) NIC is disconnected and cannot be reached at this time.

The *Server Name Configuration* page is displayed.

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

The *Client Configuration* page is displayed.

30 The vCenter Server Heartbeat server 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 server using the default client connection port of `52267`. If this port is already in use, type an available client connection port in the text box. Click **Next**.

The *Application Protection* page is displayed.

31 *Setup* will automatically select the applications that are installed on the server and require protection. Confirm that the selection is correct and if appropriate, provide vCenter connections details (username and password). If the vCenter Server is remote, select the *Server is remote* check box and provide the Fully Qualified Domain Name for vCenter Server. The default selection should only be changed if the application is installed but services have been disabled because the application is no longer used on the server.

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

The *Installation Summary* page is displayed.

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

The *Pre-Install Checks* page is displayed.

33 Pre-install checks run to ensure that the installation can continue. *Setup* checks the available disk space, system memory, operating system compatibility, and dependencies between modules.

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

34 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.

35 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.

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

The *Microsoft Windows Backup Configuration* page is displayed.

37 *Setup* backs up two small files, `nfsetup.dat` and `primary.csv`, from the Primary server and restores them to the Secondary server during the Secondary server installation for proper configuration. 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 *Packet Filter Installation* page is displayed.

38 The vCenter Server Heartbeat Packet Filter driver installs on each network card of the production server. If you see warnings that the driver is unsigned or did not complete the Windows Logo tests, click **Install**. If Windows is configured to display Signed Driver warnings, you may see multiple warnings. The *Report* pane displays the results. Click **Next**.

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

The *Primary Installation Complete* page is displayed.

39 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.

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

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

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

The system prompts you to restart the server.

42 Click **Yes** to restart the server.

Secondary Server

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

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) server image, right-click the server image and select *Edit* Settings.

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

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

c On the Secondary server, open *Network Connections*, right-click the Principal (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 server), subnet mask, and default gateway.

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

h Right-click the Secondary (cloned) server 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 server go through the VMware Channel.

j Go to Step 4.

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

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

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

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

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

   e Configure the appropriate VMware Channel IP address and subnet mask. Click **Advanced**.

   f Click the *WINS* tab, select *Disable NetBIOS over TCP/IP*. 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 Principal (Public) network connection and select *Properties*. Select *Internet Protocol (TCP/IP)* and click **Properties**. Configure the Principal (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 server), subnet mask, and default gateway.

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

   j Right-click the Secondary (cloned) server 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 server go through the VMware Channel.

Important Do not connect the Principal (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 server, 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.

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

   The *Server Identity* page is displayed.

7 Select the identity of the server on the *Server Identity* page. Select *Secondary* as the server identity and click **Next**.

   The *Identify Microsoft Windows Backup Folder* page is displayed.

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

Note You must use the UNC path.

   The *Pre-Install Checks* page is displayed.

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

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

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

10 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.

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

The *Packet Filter Installation* page is displayed.

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

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

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

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

The *Public Adapter Identification* page is displayed.

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

The *Secondary Installation Complete* page is displayed.

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

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

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

The system prompts you to restart the server.

17 Click **Yes** to restart the server.

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 servers, the IP addressing configuration should reflect:

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

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

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

Procedure

- Verify that `Nslookup` resolves as shown below:
  1. Verify that `Nslookup` resolves Service Name to Public IP
  2. Verify that `Nslookup` resolves Primary Name to Primary Management IP
  3. 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.
5. Click **OK**.

Registering the Heartbeat Plug-in Manually in vCenter

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

Procedure

1 With the vCenter Server Heartbeat pair in sync, on the Primary/active server, 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 server 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 switchover to make the Secondary server active.

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

Configuring vCenter Server Heartbeat to Protect SQL Server

After successfully installing vCenter Server Heartbeat, the following tasks should be performed to configure vCenter Server Heartbeat to protect SQL Server.

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 Navigating 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 server 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 server, in the 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 server, in the 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 server 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 servers 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 servers at `Windows\System32`

This is normally present as a component of the Windows 2008 operating system.

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 Principal (Public) IP address and the Management IP address for the Primary and Secondary Servers when installing vCenter Server Heartbeat on servers running Windows 2008.

---

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
- Switchover
- Failover

- When the Administrator selects *Start Application*
- When the Administrator selects *Stop Application*

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

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.

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 servers with the same configuration settings.

2 Launch the vCenter Server Heartbeat Console.

3 Navigate to *Applications: Plug-ins* and click **Install**.

4 **Browse** to the plug-in file located at:
`<unzipped_folder>\<vCenterServerHeartbeatVersion-x86/x64>\plugins\ViewComposer\ViewComposerNFPlugin.dll`.

5 Click **OK** to install the View Composer Plug-in.

Upgrading vCenter Components

Should vCenter Server or components of vCenter need to be upgraded when vCenter Server Heartbeat is installed, please refer to Appendix C, “Upgrading,” on page 49.

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.

Setup Error Messages

A

Table A- 1. Setup Error Messages

Message	Pri	Sec	Level	Test
10 – 'The pre install check data file does not have the correct format. Setup cannot continue'.	No	Yes	Critical Stop	Check that the file adheres to the correct formatting and structure for use in analysis on the Secondary.
Setup has detected incompatible versions of the collector version $x and the analyzer version $y dll. This would suggest different versions of Setup have been run on the Primary and Secondary servers.	No	Yes	Critical Stop	Check that the analyzer and collector dlls are compatible.
File $x cannot be analyzed it may be corrupt Setup is unable to continue. If the file has been opened check that it has not been saved with Word Wrap.	–	Yes	Critical Stop	Check file format is correct.
190 – This server is a #1# domain controller. vCenter Server Heartbeat must not be installed on a domain controller.	Yes	Yes	Critical Stop	Test whether the server is a domain controller.
173 – vCenter Server Heartbeat does not support the '/3GB' switch on Windows 2000 Standard Edition.	Yes	Yes	Critical Stop	Test for /3GB on Windows 2000
175 – vCenter Server Heartbeat requires Windows 2003 Standard Edition SP1 or later if '/3GB' switch is on.	Yes	Yes	Critical Stop	
103 – vCenter Server Heartbeat does not support #1#. The following are supported Windows 2000 Server SP4 or greater; Windows Server 2003 SP1 or greater.	Yes	Yes	Warning	
200 – Your #1# server uses the Intel ICH7 chipset and Windows 2000 has been detected. This combination is incompatible with vCenter Server Heartbeat.	Yes	Yes	Critical Stop	
217 – vCenter Server Heartbeat is not supported on Windows Storage Server Edition.	Yes	Yes	Warning	

Table A- 1. Setup Error Messages

Message	Pri	Sec	Level	Test
106 – Primary and Secondary OS versions are not identical, #1# vs. #2#: and require the same Service Pack level.	–	Yes	Critical Stop	Compatibility check on secondary.
208 – You are running a 64-bit version of Windows on one of your servers and a 32-bit version of Windows on the other. This is not supported.	–	Yes	Critical Stop	Compatibility check on secondary.
111 – The system folders on primary and secondary system must be the same. Setup has detected that the secondary system folder is #2# and the primary was #1#.	–	Yes	Critical Stop	Compatibility check on secondary.
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 Verification Testing

B

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 controlled switchover in the event of an application failure and 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 63 for more information about vCenter Server Heartbeat Pairs.

This appendix includes the following topics:

Exercise 1 — Auto-switchover

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 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 switch to and make active the passive server in the Pair to 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 server is lost. VMware recommends that all actions intended to verify operation of the passive server be performed as a switchover rather than a failover.

Starting Configuration

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

- The Secondary server must be synchronized with the Primary server.
- 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 server exists and examine the Windows event logs for recent critical errors.

VMware provides an executable, `nfavt.exe`, to emulate conditions that result in auto-switchover 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-switchover) to return the Pair to its original operating configuration and state.

Table B- 1. Perform the following procedure to verify Auto-Switchover 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 server and vCenter Server Heartbeat shuts down on the Primary.
Secondary	Login to the vCenter Server Heartbeat Console.	
	In the *Servers* pane of the vCenter Server Heartbeat Console, select the server pair.	The *System Overview* screen indicates that the Secondary server 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 45.

Back-out Procedure (Auto-switchover)

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 servers.

2 Complete the following on both servers:

   a Open the *Configure Server* wizard.

   b Select the *Machine* tab.

   c Select the *Primary* server as active.

   d Click **Finish**.

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

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

5 On the Primary server, 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 server has resumed.

Exercise 2 - Data Verification

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

Starting Configuration

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

Steps to Perform

Table B- 2. Perform the following steps to verify that data is synchronized following Auto-switchover in a Pair configuration.

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 server 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 server to the Primary server.
	Select the *Data: Replication* tab and wait for both the *File System* and the *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 server back to the Primary server. 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 part of the Installation Verification process, detailed in "Exercise 3 - Switchover," on page 46.

Exercise 3 - Switchover

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

Starting Configuration

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

Steps to Perform

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

Machine ID	Activity	Results
Secondary	Launch vCenter Server Heartbeat Console and select the *Data: Replication* tab. Verify that both the *File System* and I status are *Synchronized*.	
	Select the *Server: Summary* tab. Select the Primary server icon and click **Make Active**.	The vCenter Server Heartbeat Console *Server: Summary* page displays the applications stopping on the active server. Once all applications are stopped, the active server becomes passive and the passive server becomes active. The Console shows the applications starting on the newly active server. 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 switchover process.	Services continue to be provided as before the switchover occurred. You may need to refresh or restart some client applications as a result of a switchover.

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

Upgrading

C

This Appendix provides instructions to upgrade both vCenter Server Heartbeat 6.4 Update 1 to 6.5 and vCenter Server 5.0 to 5.1 when vCenter Server Heartbeat is installed.

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

This appendix includes the following topics:

Upgrading vCenter Server Heartbeat 6.4 Update 1 to 6.5

The following procedure assumes that vCenter Server Heartbeat 6.4 Update 1 is currently installed and provides step-by-step instructions to upgrade vCenter Server Heartbeat 6.4 Update 1 to vCenter Server Heartbeat 6.5. For information about upgrading from previous versions of vCenter Server Heartbeat to vCenter Server Heartbeat 6.5, see knowledge base article 1014435.

Procedure

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

2 On the Primary/active server, right-click on the *System Tray* icon and select to *Stop 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 server, navigate to **Start** > **Administrative Tools** > **Services** and set the *VMware vCenter Server Heartbeat* service to *manual*.

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

6 On the Secondary/passive server, disconnect the network cable from the Principal (Public) NIC.

7 On the Primary/active server, 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 Service Pack* 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 server.

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 server, 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 Service Pack* 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 server.

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 the Primary/active server, check the configuration of the NICs and make corrections if necessary (the packet filter should be selected on Principal (Public) NICs and cleared on channel NICs).

16 On the Secondary/passive server, check the configuration of NICs and make corrections if necessary (the packet filter should be selected on Principal (Public) NICs and cleared on channel NICs).

17 On the Primary/active server, right-click on the *System Tray* icon and select to *start vCenter Server Heartbeat*.

18 Using vCenter Server Heartbeat Console, navigate to *Applications: Services* and locate the VMware vCenter Server Heartbeat WebService in the Heartbeat section. Right-click on *VMware vCenter Server Heartbeat WebService* and select *Remove*.

19 Navigate to **Start** > **Administrative Tools** > **Services** and set the *VMware vCenter Server Heartbeat WebService* and *VMware vCenter Server Heartbeat* service to automatic.

20 On Secondary/passive server, start vCenter Server Heartbeat and then reconnect the network cable to the Principal (Public) NIC.

21 On the Secondary/passive server, navigate to **Start** > **Administrative Tools** > **Services** and set the *VMware vCenter Server Heartbeat WebService* and the *VMware vCenter Server Heartbeat* service to automatic.

22 On the Secondary/passive server, navigate to **Start** > **Administrative Tools** > **Services**. Right-click *VMware vCenter Server Heartbeat WebService* and select **Start**.

Upgrading vCenter Server 5.0 to 5.1 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 using a remote SQL Database. This procedure provides step-by-step instructions to perform an upgrade of vCenter Server 5.0 to 5.1 with vCenter Server Heartbeat installed. For information about upgrading from previous versions of vCenter Server with vCenter Server Heartbeat installed to vCenter Server 5.1, see knowledge base article 1010479.

Upgrading the Secondary Server

The following procedure assumes that vCenter Server 5.0 and vCenter Server Heartbeat are currently installed. For information about upgrading from previous versions of vCenter Server with vCenter Server Heartbeat installed to vCenter Server 5.1, see knowledge base article 1014435.

Procedure

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

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

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

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

Important Before attempting to upgrade to vCenter Server 5.1, you must separately install the VMware vSphere Single Sign-On (SSO) component.

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

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

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

8 If applying an update, when prompted, select *Do not overwrite, leave the existing database in place*, otherwise if there is an upgrade, 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 server.

11 If the upgrade on the Secondary server fails, research the cause of the upgrade failure. If the issue can be resolved then it is safe to proceed with upgrade procedure. Otherwise, revert to a previous version.

   a Uninstall the upgraded components.

   b On the Secondary server, 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 server. vCenter Server Heartbeat starts and vCenter Server is stopped.

   d On the Primary server, 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 Server and allow the system to synchronize.

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

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

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

13 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.

14 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.

15 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.

16 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.

17 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.

18 Upgrading Update Manager (Optional).

This procedure assumes you have already upgraded vCenter Server on Secondary server. 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 server.

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 server role to Secondary/passive:

a Launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab. In the *Active Server* section, change the server role for the Primary server to *Active* and click **Finish**.

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

22 Reboot Secondary server.

The upgrade process continues on the Primary server.

Upgrading the Primary Server

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

Procedure

1 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 Server.

2 Change the server role to Primary/active:

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

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

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

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

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

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

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

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

9 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.

10 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.

11 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.

12 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.

13 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.

14 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 server.

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.

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

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

17 Start vCenter Server Heartbeat on both servers.

18 Launch the vCenter Server Heartbeat Console and connect to the server 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 server following a switchover, perform the following steps.

Procedure

1 Shutdown vCenter Server Heartbeat.

2 Launch the Configure Server wizard and set the Secondary server role to *Passive*.

3 Start vCenter Server Heartbeat on the Secondary server.

4 Start the Configure Server wizard on the Primary server and set the server role to *Active*.

5 Start vCenter Server Heartbeat on the Primary server.

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 server.

Upgrading vCenter Server 5.0 to 5.1 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 using a local SQL Database. This procedure provides step-by-step instructions to perform an upgrade of vCenter Server 5.0 to 5.1 with vCenter Server Heartbeat installed. For information about upgrading from previous versions of vCenter Server with vCenter Server Heartbeat installed to vCenter Server 5.1, see knowledge base article 1034131.

Upgrading the Secondary Server

Procedure

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

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

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

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

5 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.

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

7 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.

8 If applying an update, when prompted, select the *Do not overwrite, leave my existing database in place* otherwise, if this is an upgrade, when prompted, select *Upgrade existing vCenter Server Database*. Additionally, choose to *Automatically upgrade the vCenter Agent*.

9 Once the vCenter Server upgrade process ends successfully, VMware recommends that you upgrade the existing extensions on the server. 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.

10 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.

11 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.

12 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.

13 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 during the upgrade, acknowledge and continue the upgrade procedure. If you encounter a warning that the specified user doesn't exist, acknowledge and continue with the upgrade process.

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 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.

15 Upgrading Update Manager (Optional).

This procedure assumes you have already upgraded vCenter Server on Secondary server. 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 server.

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 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 If the upgrade on the Secondary server fails, research the cause of the upgrade failure. If the issue can be resolved, then it is safe to proceed with upgrade procedure, otherwise, revert to a previous version. To revert to a previous version:

   a Uninstall the upgraded components.

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

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

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

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

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

18 Change the server role to Secondary/passive:

   a Launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab. Change the server *Role* to Secondary/passive and click **Finish**.

19 Start VMware vCenter Server Heartbeat on the Secondary server only.

20 Reboot Secondary server.

Note The upgrade process continues on the Primary server.

Upgrading the Primary Server

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

Procedure

1 Change the server role to Primary/active:

   a Launch the vCenter Server Heartbeat Configure Server wizard and click the **Machine** tab. Change the server role for the current (Primary) server 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 and 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 will warn about the need to upgrade them as well.

5 If applying an update, when prompted, select the *Do not overwrite, leave my existing database in place*, otherwise if this is an upgrade, when prompted, select *Upgrade existing vCenter Server database*. Additionally, choose to *Automatically upgrade the vCenter Agent*.

6 Once the vCenter Server upgrade process ends successfully, VMware recommends that you upgrade the existing extensions on the server. 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 server.

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 servers.

15 Start vCenter Server Heartbeat on both servers.

16 Launch the vCenter Server Heartbeat Console and connect to the server 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 server following a switchover, perform the following steps.

Procedure

1 Shutdown vCenter Server Heartbeat.

2 Launch the Configure Server wizard and set the Secondary server role to *Passive*.

3 Start vCenter Server Heartbeat on the Secondary server.

4 Start the Configure Server wizard on the Primary server and set the server role to *Active*.

5 Start vCenter Server Heartbeat on the Primary server.

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 server.

Glossary

Active
The functional state or role of a server 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 switchovers and failovers require no changes to AD resulting in switchover/failover times typically measured in seconds.

Active–Passive
The coupling of two servers with one server visible to clients on a network and providing application service while the other server 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 servers must have identical ACPI compliance.

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

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 servers fails, often resulting in the passive server 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 server.

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

Connection
Also referred to as Cluster Connection. Allows the 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 server 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 can be achieved by placing the Secondary server (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 server.

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

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 servers with different manufacturers, models, and processing power in a single vCenter Server Heartbeat Cluster.

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

Heartbeat Diagnostics
The umbrella name for the vCenter Server Heartbeat process and tools used to verify the production servers 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 server, 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 server 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 server using NTBackup or Wbadmin and to restore the replica to the Secondary server.

Low Bandwidth Module (LBM)
A module that compresses and optimizes data replicated between servers 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 server management purposes only.

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

Network Monitoring
Monitoring the ability of the active server 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 server 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 server using VMware vCenter Converter or other 3rd party utility prior to the initiation of installation and uses the replica as a Secondary server.

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 server during the vCenter Server Heartbeat installation process that normally does not change during the life of the server and usually represents the production server prior to installation of vCenter Server Heartbeat.

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

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

Principal (Public) Network
The network used by clients to connect to server applications protected by vCenter Server Heartbeat.

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

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 server used to store changes received from another server in the replication chain before they are applied to the disk/registry on the passive server.

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 server(s) so the servers are maintained in a synchronized state.

Role
The functional state of a server 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 server during the vCenter Server Heartbeat installation process that normally does not change during the life of the server and usually represents the standby server 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 2003/2008 systems.

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

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

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

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

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 servers attempt to become active at the same time leading to an active-active rather than an active-passive model.

Split-Brain Syndrome
A situation in which more than one server 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 server.

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.

Switchover
The graceful transfer of control and application service to the passive server.

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

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 servers, that controls network visibility.

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

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

vCenter Server Heartbeat Switchover/Failover Process
A process unique to vCenter Server Heartbeat in which the passive server gracefully (switchover) or unexpectedly (failover) assumes the role of the active server providing application services to connected clients.

Virtual Private Network (VPN)
A private data network that 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.