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
Contents

About This Book  7

Getting Started

1 Introduction  11
   vCenter Server Heartbeat Concepts  11
   Server Protection  12
   Network Protection  12
   Application Protection  12
   Performance Protection  13
   Data Protection  13
   Communications  14
   Switchover Process  15
      Auto-Switchovers  16
   Failover Process  17
      Recovery from a Failover  18

Installation

2 vCenter Server Heartbeat Implementation  21
   Overview  21
   Environmental Prerequisites  22
   Common Requirements  22
   Server Architecture Options  22
      Virtual to Virtual (V2V)  22
      Physical to Virtual (P2V)  23
      Physical to Physical (P2P)  23
   Cloning Technology Options  24
      Supported Pre-Clone Technologies  24
      Supported Install Clone Technologies  24
   Application Component Options  24
      vCenter Server with SQL Server on the Same Host  24
      vCenter Server with SQL Server on a Separate Host  25
      vCenter Server Only  25
   Network Options  25
      LAN  25
      WAN  26
   Anti Virus Recommendations  27
   Deployment Options Summary  28
   Installation Process  28
      Installation Options Checklist  28
   Primary Server  29
   Secondary Server  50
Post Installation Configuration 66
vCenter Server 2.5 66
vCenter Server 4.0 66

3 Configuring vCenter Server Heartbeat 69
   Configuring Server Wizard 70
   Configuring the Machine Identity 71
   Configuring the Server Role 71
   Configuring the Client Connection Port 71
   Configuring Channel IP Routing 71
   Configuring the Default Channel Port 72
   Configuring Low Bandwidth Module 72
   Configuring Public IP Addressing 73
   Enabling Network Monitoring 73
   Configuring Split-Brain Avoidance 74
   Configuring Message Queue Logs 75
   Configuring the Maximum Disk Usage 75

System Administration and Management

4 Status and Control 79
   vCenter Server Heartbeat Console 79
   Logging into vCenter Server Heartbeat 79
      Connecting to a Pair of Servers 81
      Reviewing the Status of a Server Pair 81
   Configuring the Look and Feel of the vCenter Server Heartbeat Console 82
      Changing vCenter Server Heartbeat Console Screens 83
   Logging Out of the vCenter Server Heartbeat Console 83

5 Server Protection 85
   Server Protection Overview 85
   Checking the Server Pair Status 86
   Configuring Heartbeat Settings 87
   Configuring vCenter Server Heartbeat Shutdown Options 88
      Starting, Stopping, and Shutting Down vCenter Server Heartbeat 88
      Forcing a Switchover 90
      Recovering from a Failover 91
   Configuring Split-Brain Avoidance 92

6 Network Protection 93
   Communication Status 93
   Reviewing the VMware Channel Status 94
   Configuring Public Network Connection Checks 94
   Setting Max Server Time Difference 95

7 Application Protection 97
   Application Protection Overview 97
   Applications Tab 97
      Editing Individual Applications 98
      Configuring Applications 99
      Reviewing the Status of an Application 100
      Reviewing the Applications Status Log 101
Filtering Application Log Entries 101
Resetting the Application Health Status 102
Removing an Application 103

Services Tab 103
Adding a Service 104
Editing a Service 105
Checking the Status of Services 106
Unprotecting Services and Stopping Monitoring 106
Removing a Service 107

Tasks Tab 107
Adding a Task 108
Editing a Task 109
Removing a Task 110
Starting a Task Manually 111

Plug-Ins Tab 112
Installing a Plug-In 113
Editing a Plug-In 114
Uninstalling a Plug-In 115

Performance Protection 117
Rules Tab 117
Editing a Rule 118
Rules Installed by vCenter Server Heartbeat Plug-Ins 118
Checking a Rule Condition 120

Data Protection 121
Data Protection Overview 122
Automatic Filter Discovery 122
Adding a User-Defined Inclusion Filter 123
Adding a User-Defined Exclusion Filter 124
Removing User-Defined Inclusion/Exclusion Filters 125
Configuring Max Disk Usage 125
Reviewing Status of Protected Files 126
Determining Effective Filters 127
Initiating File Synchronization Manually 127
Initiating Verify and Synchronize Manually 128
Initiating a Full System Check 128
Reviewing the Registry Synchronization Status 130
Initiating a Full Registry Check 131

Other Administrative Tasks 133
Configuring Alerts 133
Configuring Alert Reporting 134
Test Alert Reporting 137
Configuring Event Log Files 138
Configuring Log File Email Recipients 138
Reviewing Event Logs 139

Troubleshooting 143
Troubleshooting Unexpected Behaviors 143
Two Active Servers 143
Symptoms 143
Causes 144
Resolution 144
Two Passive Servers 145
  Symptom 145
  Causes 145
  Resolution 145

Synchronization Failures 146
  Services Running on the Passive Server 146
  VMware Channel Incorrectly Configured 146
  Incorrect or Mismatched Disk Configuration 147
  Passive Server Has Less Available Space than Active Server 147

Registry Status is Out of Synch 148
  Resource Issues 148
  Registry Security Issues 148

Channel Drops 148
  Performance Issues 148
  Passive Server Does Not Meet Minimum Hardware Requirements 149
  Hardware or Driver Issues on VMware Channel NICS 149
  Firewall Connection 150
  Incorrect VMware Channel Configuration 150
  VMware vCenter Server Heartbeat Packet Filter Is Enabled on the Channel NIC(s) 151

Subnet or Routing Issues 152
  LAN Deployment 152
  WAN Deployment 152

MaxDiskUsage Errors 152
  Active Server (Unsafe) Queue 153
  Passive Server (Safe) Queue 153

MaxDiskUsage Error Messages 153
  [L9] Exceeded the Maximum Disk Usage (VCChannelExceededMaxDiskUsageException) 153
  [L9] Exceeded the Maximum Disk Usage on the ACTIVE Server 154
  [L9] Exceeded the Maximum Disk Usage on the PASSIVE Server 154
  [L20] Out of Disk Space (VCChannelOutOfDiskSpaceException) 155

Application Slowdown 155
  Poor Application Performance 156
  Both Servers Can Accommodate the Initial Load but the Load Has Increased 156
  One Server Is Able to Cope, but the Other Cannot 156
  Scheduled Resource Intensive Tasks 157

Appendix: Setup Error Messages 159

Glossary 161
About This Book

The Reference Guide provides information about installing and configuring VMware vCenter Server Heartbeat, including implementation in a Local Area Network (LAN) or Wide Area Network (WAN), how to configure network protection, application protection, data protection, Split-brain Avoidance, and so on. To help you protect your VMware vCenter Server, the book provides an overview of the protection offered by vCenter Server Heartbeat and the actions that vCenter Server Heartbeat can take in the event of a network, hardware, or application failure.

Intended Audience

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

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

Abbreviations Used in Figures

The figures in this book use the abbreviations listed in Table 1.

Table 1. Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>VMware Channel</td>
</tr>
<tr>
<td>NIC</td>
<td>Network interface card</td>
</tr>
<tr>
<td>P2P</td>
<td>Physical to physical</td>
</tr>
<tr>
<td>P2V</td>
<td>Physical to virtual</td>
</tr>
<tr>
<td>V2V</td>
<td>Virtual to virtual</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage area network type datastore</td>
</tr>
</tbody>
</table>

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

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

**Support Offerings**

To find out how VMware support offerings can help meet your business needs, go to www.vmware.com/support/services.

**VMware Professional Services**

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to www.vmware.com/services.
Getting Started
Introduction

This chapter includes the following topics:

- “vCenter Server Heartbeat Concepts” on page 11
- “Switchover Process” on page 15
- “Failover Process” on page 17

vCenter Server Heartbeat Concepts

vCenter Server Heartbeat is a Windows-based system that has been specifically designed to provide high availability to server configurations in one product without requiring any specialized hardware.

vCenter Server Heartbeat provides the following protection levels:

- **Server Protection** — vCenter Server Heartbeat continues to provide availability to end user clients through a hardware failure scenario or operating system crash. Additionally, vCenter Server Heartbeat protects the network identity of the production server, ensuring users are provided with a replica server including server name and IP address shares on the failure of the production server.

- **Network Protection** — vCenter Server Heartbeat proactively monitors the network by polling up to three nodes to ensure that the active server is visible on the network.

- **Application Protection** — vCenter Server Heartbeat maintains the application environment ensuring that applications and services stay alive on the network.

- **Performance Protection** — vCenter Server Heartbeat proactively monitors performance attributes of the system to ensure that the administrator of the system is notified of problems and can take pre-emptive action to prevent an outage.

- **Data Protection** — vCenter Server Heartbeat intercepts all data written by users and applications, and maintains a copy of the data on the passive server which can be used in the event of a failure.

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

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

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

Since only have one server name and network address visible on the same network at any one time, one of the two servers is live on the Principal (Public) network and serves the protected applications. This is the active server. The other server is hidden from the Principal (Public) network, remains as a ready standby server, and is the passive server.
The vCenter Server Heartbeat software is symmetrical in almost all respects, and either the Primary Server or the Secondary server can take the active role and provide the protected application to the user.

**Server Protection**

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

**Figure 1-1. Failover**

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

**Network Protection**

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

**Application Protection**

vCenter Server Heartbeat running on the active server locally monitors the applications and services it has been configured to protect through the use of plug-ins. vCenter Server Heartbeat protects the following components:

- VMware vCenter Server
- VMware Capacity Planner
- VMware Converter Enterprise
- VMware Update Manager
- VMware License Server
If a protected application fails, vCenter Server Heartbeat first tries to restart the application on the active server (1) in Figure 1-2.

If the restart of the application fails, then vCenter Server Heartbeat initiates a switchover (2) in Figure 1-2. Refer to “Switchover Process” on page 15 and “Failover Process” on page 17 for further information about the switchover process.

**Figure 1-2. Switchover**

A switchover gracefully closes any protected applications that are running on the active server and restarts them on the passive server along with the application or service that caused the failure. In the example where the Primary server is active and the Secondary server is passive, the Primary server is demoted to a passive role and is hidden from the network when the Secondary server is promoted to an active role and is made visible to the network. The mechanics of switchovers are discussed in more detail later in this guide.

**Performance Protection**

It is important to ensure that your protected applications are actually operational and providing service to your end users and that the performance of those applications is adequate for user to be productive. The vCenter Server Heartbeat plug-in provides these monitoring and pre-emptive repair capabilities.

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

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

Furthermore, vCenter Server Heartbeat provides the same level of flexibility to define and perform multiple corrective actions in the event of problems on a service-by-service or even attribute-by-attribute basis.

**Data Protection**

You can configure vCenter Server Heartbeat to protect the application environment. All data files that users or the applications require in the application environment are made available should a failure occur. Once installed, vCenter Server Heartbeat configures itself automatically to protect files, folders, and registry settings for vCenter Server on the active server by mirroring them in real-time to the passive server. This means that if a failover occurs, all the files that were protected on the failed server are available to users after the failover, hosted on the Secondary server.
vCenter Server Heartbeat intercepts all file system I/O operations on the active server. If the intercepted write and update operations are within the protected set, they are placed in a queue on the active server termed the active server (unsafe) queue pending transmission to the passive server. Each request is numbered to maintain its order in the queue.

With the request in the active server (unsafe) queue, vCenter Server Heartbeat then allows the disk I/O to continue with the requested disk operation.

If the channel is connected, the active server (unsafe) queue is transferred to the passive server, which places all the requests in the passive server (safe) queue. The passive server then confirms the changes have been logged by sending the active server an acknowledgement. The active server then clears the data from its queue.

**Figure 1-3. Apply Process**

The apply process running on the passive server (safe) queue applies all of the updates in strict sequence, duplicating an identical set of file operations on the passive server as illustrated in Figure 1-3.

**Communications**

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

Both the Primary and Secondary servers must have two or more network interface connections (NICs).

The Principal (Public) network requires one NIC. The VMware Channel uses a separate NIC for the private connection between the servers used for control and data transfer between the pair of servers.

A second pair of NICs may be used for the VMware Channel to provide a degree of redundancy. In this case, the VMware Channel has a Dual Channel if more than one dedicated NIC is provided for the VMware Channel on each server. To provide added resilience, the communications for the second channel must be completely independent from the first channel—they must not share any switches, virtual switches, routers or the same WAN connection.
The IP address used by a client to connect to the active server (the Principal (Public) IP address) must be configured to use a static IP address (Not DHCP enabled). In the example in Figure 1-4, the IP address is configured as 192.168.1.127.

**NOTE** Obtain the IP address: type ipconfig at the prompt in a DOS shell. For additional information about the IP configuration, type /A11.

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

The NICs on the active and passive servers used for the VMware Channel must be configured so that they have IP addresses outside of the Principal (Public) networks subnet range. These addresses are termed the VMware Channel addresses.

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

The NICs that allow the connectivity across the VMware Channel can be standard 100BaseT Ethernet cards providing a throughput of 100Mbits per second across standard Cat-5 cabling. In its simplest form, a dedicated channel needs no hubs or routers, but the direct connection requires the cabling to be cross-wired.

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.

**Switchover Process**

You can trigger a switchover manually from vCenter Server Heartbeat Console Status & Control screen by clicking the **Switchover** button or automatically if a protected application which the system has been monitoring has failed, has performance degradation, or a network failure prevented the active server from being visible to the network.

When a 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 switched.
Figure 1-5. Switchover

The automatic procedure executed during a switchover operation involves the following steps:

1. Stop the protected applications on the active server. Once the protected applications stop, no more disk updates are generated.
2. Send all updates that are still queued on the active server to the passive server. After this step, all updates are available on the passive server.
3. Change the status of the active server to switching to passive. The server is now no longer visible from the network.
4. Apply all queued updates on the passive server.
5. Change the status of the passive server to active. The new active server starts intercepting disk I/Os and queues them for the new passive server. The new active server is now visible on the network with the same identity as the old active server.
6. Change the status of the old active server from switching to passive to passive. The new passive server will now accept updates from the active server.
7. Start the same protected applications on the new active server. The protected applications now start and are accessible to users, generating disk updates.

The switchover is complete.

Auto-Switchovers

An auto-switchover is triggered automatically if a protected application or other system-monitored component such as networking fails.

An auto-switchover is different than a manual switchover in that although the roles of the servers are changed, replication stops to allow the administrator to investigate and rectify the cause of the auto-switchover.

Auto-switchovers are similar to a failover but caused by a failed monitored application or system component. Once you determine the cause for the auto-switchover, restore the server with the failed application or other system-monitored component to the active role as follows:

1. Correct the incident that caused the failover.
2. Verify the integrity of the disk data on the failed server.
3. Reboot the failed server.
4. Start vCenter Server Heartbeat on the failed server.
5. Allow vCenter Server Heartbeat to synchronize fully.
Failover Process

Figure 1-6. Failover

When the passive server detects the active server is no longer running properly, it assumes the role of the active server by taking the following steps.

1. The server applies any intercepted updates that are currently saved in the passive server (safe) update queue, that is, the log of update records saved on the passive server but not yet applied to the replicated files.

   The length of the passive server (safe) queue affects the time the failover process takes to complete. If the passive server queue is long, the system must wait for all the passive server updates to be applied before the rest of the process can take place.

   When there are no more update records that can be applied, the server discards any update records that it has been unable to apply. An update record can only be applied if all earlier update records were applied and the completion status for the update is in the passive server (safe) update queue.

2. The server switches its role from passive to active.

   The server enables the server’s public identity. The active and passive servers both have the same system name and same Principal (Public) IP address. This Principal (Public) IP address can only be enabled on one of the two systems at any time. When the public identity is enabled, any clients connected to the server before the failover can now reconnect.

3. The server starts intercepting updates to the protected data. Updates to the protected data are saved in the local server’s active server (unsafe) update queue.

4. The server starts all the protected applications. The applications will use the replicated application data to recover and then accept re-connections from any clients. Any updates that the applications make to the protected data are intercepted and logged.

At this stage, the originally active server is off the air, and the originally passive server has taken over the role of the active server and is running the protected applications. Because the originally active server stopped abruptly, the protected applications may have lost some data, but the no synch-mode update that completed before the failover is lost. The application clients can reconnect to the application and continue running as before.

Note that during a failover, the data in the active server (unsafe) queue is lost.
Recovery from a Failover

Assuming that the active server before the failover was the Primary server, and the Secondary server has assumed the active role following a failover, you can reinstate the Primary server to an active role after rectifying the problem that initiated the failover.

When vCenter Server Heartbeat starts on the failed Primary server, it detects that it did not stop cleanly the previous time. It disables the public identity by deploying the IP packet filter at boot time, and halts vCenter Server Heartbeat so that the issues that caused the failure can be resolved. The following steps restore the previously failed server to the active role:

1. Correct the incident that caused the failover.
2. Verify the integrity of the disk data on the failed server.
3. Reboot the failed server.
4. Start vCenter Server Heartbeat on the failed server.
5. Allow vCenter Server Heartbeat to synchronize fully.

After resolving these issues, you can start vCenter Server Heartbeat on the failed, now passive, server. At this stage, the vCenter Server Heartbeat software running on the pair of servers connects and starts to re-synchronize the data on the Primary server. When the re-synchronization is complete, you can continue operating with this configuration (for example, the Secondary server is the active server and the Primary server is the passive server), or perform a switchover to reverse the roles of the two servers in the vCenter Server Heartbeat pair (for example, assigning the Primary and Secondary the same roles that they had before the failover).
Installation
This chapter includes the following topics:

- “Overview” on page 21
- “Environmental Prerequisites” on page 22
- “Common Requirements” on page 22
- “Server Architecture Options” on page 22
- “Cloning Technology Options” on page 24
- “Application Component Options” on page 24
- “Network Options” on page 25
- “Anti Virus Recommendations” on page 27
- “Deployment Options Summary” on page 28
- “Installation Process” on page 28
- “Primary Server” on page 29
- “Secondary Server” on page 50
- “Post Installation Configuration” on page 66

Overview

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

This chapter discusses the deployment options and prerequisites necessary to successfully implement vCenter Server Heartbeat and provides a step-by-step process to assist in selecting options required for installation. The deployment scenario table provides a visual reference to configuration options supported by vCenter Server Heartbeat.

During the installation process, vCenter Server Heartbeat performs a variety of checks to ensure the server meets the minimum requirements for a successful installation. Should the server fail one of the checks, a Critical Stop or Warning message is displayed. Refer to the Appendix: Setup Error Messages of this guide for a list of the checks and an explanation of the message. You must resolve Critical Stops before you can proceed with setup.

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

The server protected by vCenter Server Heartbeat can NOT be configured as a domain controller / global catalog or DNS. It must be rebuilt beforehand if necessary.

Common Requirements

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

- Supported vCenter Server Versions 2.5.0, 2.5.1, 2.5.2, 2.5.3, 2.5.4, 4.0
- Operating System Windows Server 2003 x86 Sp1 or SP2
- During the setup process, vCenter Server Heartbeat will check for a minimum of 1GB RAM. To ensure proper operation, vCenter Server Heartbeat itself requires a minimum of 1GB RAM (2GB recommended) in addition to any other memory requirement for the Operating System or vCenter Server.
- 2 GB of disk space available on the drive where vCenter Server Heartbeat is to be installed
- Local administrator rights for installation vCenter Server Heartbeat installation
- Latest Microsoft security updates
- All applications to be protected by vCenter Server Heartbeat must be installed and configured on the Primary server prior to installing vCenter Server Heartbeat.
- The Primary and Secondary servers must be set to identical System Date / Time and Time Zone. Once configured, do not change the Time Zone.
- Verify that the Principle (Public) network adapter is listed as the first network adapter in the Network Connections Bind Order. (Network Connections > Advanced > Advanced Settings).
- Verify that the Managed IP setting in the Virtual Infrastructure Client is the same IP address used for the vCenter Server Heartbeat Principal (Public) IP address.

Server Architecture Options

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

Virtual to Virtual (V2V)

V2V is the supported architecture if vCenter Server is already installed on the production (Primary) server running on a virtual machine. 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 as follows.

- The specifications of the Secondary virtual machine should match the Primary virtual machine as follows:
  - Similar CPU (including resource management settings)
  - Memory configuration (including resource management settings)
  - Appropriate resource pool priorities
  - Each virtual machine used in the V2V pair must be on a separate ESX host to guard against failure at the host level.
  - Each virtual NIC must use a separate virtual switch.
Physical to Virtual (P2V)

P2V architecture is used when the environment requires a mix of physical and virtual machines, such as when vCenter Server is installed on a physical server in an environment where available hardware is limited. This architecture is appropriate if you need to avoid adding more physical servers or migrate to virtual technologies over a period of time. The P2V architecture allows you to test vCenter Server running in a virtual environment or migrate from Physical to Virtual without any downtime. The Secondary Virtual Machine must meet the minimum requirements as follows:

- The specifications of the Secondary virtual machine must match the Primary physical server as follows:
  - Similar CPU
  - Memory
- The Secondary Virtual Machine must have enough priority in resource management settings so that other virtual machines do not impact its performance.
- Each virtual NIC must use a separate virtual switch.

Physical to Physical (P2P)

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

Primary Server

The Primary server must meet the following requirements:

- Hardware as specified in “Common Requirements” on page 22.
- Software as specified in “Common Requirements” on page 22.

Secondary Server

The Secondary server must meet the following requirements:

Hardware

- Hardware should be equivalent to the Primary server to ensure adequate performance when the server is in the active role:
  - Similar CPU
  - Memory
- Identical number of NICs to the Primary server.
- Drive letters must match the Primary server.
- Available disk space must be greater than or equal to the Primary server.
- ACPI compliance must match the Primary server. The vCenter Server Heartbeat Standard implementation process assumes that the Advanced Configuration and Power Interface (or ACPI) compliance of both machines are the same. If this is not the case, contact VMware Support at www.vmware.com/support for further information.

Software

- OS version and Service Pack version must match the Primary server.
- OS must be installed to same driver letter and directory as on the Primary server.
- Machine name must be different from the Primary server prior to installing vCenter Server Heartbeat.
- Set up in a Workgroup prior to installing vCenter Server Heartbeat.
- System Date / Time and Time Zone must be consistent with Primary server.

**Cloning Technology Options**

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

**Supported Pre-Clone Technologies**

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

- VMware Converter for “Physical to Virtual (P2V)” on page 23
- VMware vCenter virtual machine cloning for “Virtual to Virtual (V2V)” on page 22

**Supported Install Clone Technologies**

Installation of vCenter Server Heartbeat provides support for NTBackup on Windows 2003 for automated Install Cloning. This process is automated but requires meeting all prerequisites for the Secondary server specified in “Physical to Physical (P2P)” on page 23.

**Application Component Options**

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

- vCenter Server Versions 2.5.0, 2.5.1, 2.5.2, 2.5.3, 2.5.4
  - VMware vCenter Server
  - VMware Capacity Planner
  - VMware Converter Enterprise
  - VMware Update Manager
  - VMware License Server
- vCenter Server Version 4.0
  - VMware vCenter Server
  - VMware License Server
  - VMware ADAM
  - VMware vCenter Management Web Server
  - VMware Update Manager
  - VMware Converter Enterprise
  - Guided Consolidation Service
  - VMware Orchestrator
  - VMware vSphere Host Update Utility

**NOTE** It is important to ensure that all VMware components are bound to the Principal (Public) IP address on the Principal (Public) network adapter and that the Principal (Public) network adapter is listed first in the bind order of the Network Connections > Advanced > Advanced Settings dialog.

**vCenter Server with SQL Server on the Same Host**

To ensure adequate performance in 20+ host or 200+ virtual machine environments, VMware recommends that SQL Server and vCenter Server be installed on separate physical disk drives. VMDKs must be on separate datastores to avoid potential disk bottlenecks.
**vCenter Server with SQL Server on a Separate Host**

When installing vCenter Server Heartbeat in an environment where SQL Server is on a separate host from vCenter Server, repeat the installation process for the Primary and Secondary server specifically for the SQL Server.

**vCenter Server Only**

The vCenter Server Only option requires a single iteration of the installation process because the database is not protected.

**Network Options**

Networking requirements are contingent based upon how vCenter Server Heartbeat is deployed. If deployed as a High Availability solution then a LAN configuration is required. If vCenter Server Heartbeat is deployed for Disaster Recovery, then a WAN configuration is required. Each network configuration has specific configuration requirements to ensure proper operation.

**LAN**

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

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

**Primary Server**

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

- Principal (Public) Network connection configured with the following:
  - Static IP address
  - Correct Network Mask
  - Correct Gateway address
  - Correct Preferred and Secondary (if applicable) DNS Server address
  - NetBIOS enabled

- Channel Network connection(s) configured with the following:
  - Static IP address (in a different subnet than the Principal (Public) network with a different IP address than the Secondary server channel NIC)
  - Correct Network Mask
  - No Gateway IP address
  - No DNS Server address
  - NetBIOS enabled
**Secondary Server**

The Secondary server must meet the following requirements:

- Same number of NICs as the Primary Server
- Principal (Public) Network connection configured with temporary network settings
- Channel Network connection(s) configured with the following:
  - Static IP address (in a different subnet than the Principal (Public) network with a different IP address than the Primary server channel NIC)
  - Correct Network Mask
  - No Gateway IP address
  - No DNS IP address
  - NetBIOS enabled
  - File and Print Sharing enabled

**WAN**

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

**WAN Requirements**

WAN deployments require the following.

- A persistent static route configured to the channel connection on the Secondary server where routing is required
- Two NICs (1 x Public; 1 x Channel) recommended
- At least one Domain Controller at the Disaster Recovery site

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

- During install, follow the steps for a LAN / VLAN (same subnet).
- Each server within the vCenter Server Heartbeat pair uses the same Public IP address.

If the Primary and DR site use different subnets:

- During install, follow the steps for a WAN.
- Each server within the vCenter Server Heartbeat pair requires its own separate Principal (Public) IP address as well as a VMware Channel IP address in a separate dedicated subnet.
- Provide a user account with rights to update DNS using the DNSUpdate utility provided as a component of vCenter Server Heartbeat.
- Recommend Microsoft DNS integrated into AD so that DNSUpdate automatically identifies all DNS Server that require updating.
- Refer to the following articles in the Knowledge Base:
  - KB 1008571 — Configuring DNS in a WAN Environment
  - KB 1008605 — Configuring vCenter Server Heartbeat to Update BIND9 DNS Servers Deployed in a WAN
Bandwidth

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

vCenter Server Heartbeat includes a Low Bandwidth Module for use in WAN environments. When enabled, the VMware Channel compresses the data, optimizing the traffic for low bandwidth connections causing some additional CPU load on the active server.

Latency

Latency has a direct effect on data throughput. Latency on the link 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.

Anti Virus Recommendations

Consult and implement the Anti-Virus manufacturer’s advice, as VMware guidelines often follow these recommendations. Consult the VMware Knowledge Base for up to date information on specific Anti-Virus products.

Do not use File Level AV to protect application server databases, such as MS SQL Server databases. The nature of database contents can cause false positives in virus detection, leading to failed database applications, data integrity errors, and performance degradation.

VMware recommends that when implementing vCenter Server Heartbeat, do not replicate File Level AV temp files by vCenter Server Heartbeat.

The File Level AV software running on the Primary server must be the same as the software that runs on the Secondary server. In addition, the same File Level AV must run during both active and passive roles.

Configure File Level AV to use the management IP address on the passive server for Virus Definition updates. If this is not possible, you might have to update Virus Definitions manually on the passive server.

Exclude the following VMware directories from File Level AV Scans (C:\Program Files\VMware\VMware vCenter Server Heartbeat\ is the default installation directory):

- C:\Program Files\VMware\VMware vCenter Server Heartbeat\r2\logs
- C:\Program Files\VMware\VMware vCenter Server Heartbeat\r2\log

Any configuration changes made to a file-level AV product on one server (exclusions etc.) must be made on the other server as well. vCenter Server Heartbeat does not replicate this information.
Deployment Options Summary

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

Table 2-1. Installation Options

<table>
<thead>
<tr>
<th>Network</th>
<th>Clone Technique</th>
<th>vCenter Server w/SQL</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LAN</td>
<td>WAN</td>
<td>Pre-Clone</td>
</tr>
<tr>
<td>V2V</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>P2V</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>P2P</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
</tbody>
</table>

Installation Process

After selecting implementation options, begin the installation process. The installation process for all scenarios follows the same basic procedure. Links to specific installation scenarios describing differences are identified by the blue hyperlinked text.

Installation Options Checklist

Verify the prerequisites:

Server architecture:
__ P2P
__ P2V
__ V2V

Cloning technology option:
__ Pre-Clone Install
__ Install Clone

Application components to protect:
__ vCenter Server with SQL Server on same host
__ vCenter Server with SQL Server on separate host
__ vCenter Server only

Network environment type:
__ LAN
__ WAN

Is the subnet the same at the Secondary site?
- If Yes, you need an IP address for this subnet.
- Active Directory Integrated DNS?
  - If Yes, then you need a Domain Account with rights to update DNS.
  - If No, then refer to the Knowledge Base articles in “Network Options” on page 25.
Primary Server

Installation of vCenter Server Heartbeat begins on the Primary Server.

1. Having verified all of the environmental prerequisites have been met, download vCenter Server Heartbeat software to the Primary server (either Physical or Virtual) and unpack the software from the distribution .zip file into an appropriate folder.

   You have the following options:
   - For P2P, go to Step 2 to continue the installation
   - For V2V or P2V Installations with the Pre-Clone technique selected, follow Step a of Step 1 to configure the network settings on the Secondary server.

   a. Clone the Primary server using either the VMware vCenter Converter for P2V, vCenter virtual machine cloning for V2V, or another third party utility to create a cloned image of the Primary server. The clone must be 100% with no changes to the Name, SID, or domain membership.
   b. Once the cloned image has been created, and before powering on the cloned image, edit the image settings.
c Select the Public virtual network adapter and clear the **Connected** and **Connect at power on** check boxes.

![Virtual network adapter configuration](image)

d Repeat the process on the Channel virtual network Adapter.

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

f Once started, open Network Connections, right-click the VMware Channel network connection and select **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**.

![Internet Protocol (TCP/IP) Properties](image)
g Configure the appropriate VMware Channel IP address and Subnet mask. Click Advanced.

h Select the DNS tab, clear the Register this connection's addresses in DNS check box, and click OK.

i In the WINS tab, select Disable NetBIOS over TCP/IP, then click OK twice.

j Select the Principal (Public) network connection, right-click and select Properties. Select Internet Protocol (TCP/IP) and click Properties. Set the appropriate IP address (same as the Primary server for LAN installations), Subnet Mask, and Default Gateway, then click OK.

k In Network Connections, click Advanced and select Advanced Settings. Verify that the Principal (Public) NIC IP address is listed first in the Bind Order, and click OK.
1 Right-click the Secondary (cloned) server image and select **Edit Settings**.

- Select the VMware Channel virtual network adapter and select the **Connected** and **Connect at power on** check boxes. At this point, you have IP communications with the Secondary server via the VMware Channel.

**NOTE** Do not connect the Principal (Public) virtual network adapter at this time as it will cause an IP address conflict on the network.

2 After unpacking the installation files on the Primary server, run **Setup.exe** to start the installation process.

**NOTE** If you click **Exit** any time after Setup has started, you are prompted to save the current settings. When you run **Setup.exe** later, you will be asked if you want to use the previously saved configuration.

3 The first screen in the installation setup prompts you to install vCenter Server Heartbeat or Client Tools Only. Assuming this is a new installation of vCenter Server Heartbeat software, select **Install VMware vCenter Server Heartbeat**, and then click **Next**.

![Setup Type](image)

**NOTE** The left panel of each screen in the setup wizard provides information about the setup process.
4. The **Physical Hardware Identity** screen allows you to select the identity of the server. Select **Primary** as the server identity, and then click **Next**.

![Physical Hardware Identity Screen]

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

Select the cloning options. If using the Install Clone technique, go to step 5. If using the Pre-Clone technique, click the link below to jump to the Pre-Clone technique instructions.

You have the following options:

- For installation using the Install Clone technique, continue with **Step 5**.
- For installation using the Pre-Clone technique, continue with **Step 5**.
5 Select **Secondary server is not a clone of the Primary server** and click **Next**.

After selecting **Secondary is not a clone of the Primary Server**, go to Step 6. If a virtual Secondary server has been created using either VMware Converter or a third party utility, select **Secondary server was pre-cloned**.
6 Read the license agreement carefully, and then select I accept the terms of the License Agreement. Click Next.
Configure the installation paths. The default installation location is C:\Program Files\VMware\VMware vCenter Server Heartbeat, but you can change it by manually typing a path to the desired install location.

![Installation Paths](image)

**NOTE** The path of the VMware installation folder cannot contain Unicode characters. If vCenter Server Heartbeat is installed in a folder that has a path containing Unicode characters, the Neverfail R2 Server service will fail to start. The path of the VMware installation folder can only contain lower and upper case letters A to Z, digits from 0 to 9, and the following special characters: space \ _ - ( ) : .

Alternatively, use the **Browse** button to select one of these locations. Select the option to create icons on Desktop, and then click **Next**.
8 The **Channel Adapter Identification** screen allows you to identify the network adapter(s) for use in the VMware Channel. Select the network adapters (NICs) that are to be used for the VMware Channel from the list. Click the adapter name to display the selected NIC properties in the lower panel. You must select at least one NIC to proceed with the installation.

![Channel Adapter Identification](image)

9 If no NICs are available then click **Open Network Connections** to review the network configuration of your machine and verify that you have the correct number of NICs installed.

   Only one channel can be configured for each NIC. To configure more than one channel you must identify more than one NIC.

10 A disabled NIC does not appear in this list. Enable the NIC to display it. If a NIC is disconnected, then its IP addresses are not displayed in the lower panel. Click **Next**.
11 The VMware Channel IP Configuration screen prompts you to configure the VMware Channel(s) IP network addresses. Click Add for each available channel connection. Enter the VMware Channel IP addresses for both the Primary and Secondary servers. Since this is the Primary server, a drop box displays all local IP addresses. Manually enter the reciprocal IP address on the Secondary server. You must specify all VMware Channel IP addresses in subnets outside of the normal Principal (Public) IP addressing schema so that VMware Channel traffic routing uses the VMware Channel network card rather than the Principal (Public) network card. Click OK. Repeat this step for additional NICs.

12 Review and adjust, if necessary, the default channel port. When the implementation spans multiple sites and there are firewalls between the servers, configure the firewalls to allow traffic to pass through the default channel port or the manually configured channel port. Consult the VMware Knowledge Base for additional information. Click Next.
13 Select the Principal (Public) NIC(s). The IP address information displays for each NIC.

vCenter Server Heartbeat software may be deployed in a configuration where both servers have the same Principal (Public) IP address, for instance, in a standard Local Area Network (LAN) deployment where both machines are co-located in the same subnet.

Alternatively vCenter Server Heartbeat may be deployed where the Principal (Public) IP addresses differ, for instance, in a Wide Area Network (WAN) deployment where the Primary and Secondary servers are located in different sites and subnets where client access is therefore bound by the standard network routing to allow the correct connectivity to the server according to its locale.

14 Select LAN: Configure Primary and Secondary servers with the same Public IP addresses or WAN: Configure Primary and Secondary servers with different Public IP addresses.

You have the following options:

- For a WAN installation with different subnets, go to Step 16.
- For LAN installation or same subnet WAN installs, continue with Step 15.
15 For a LAN environment, click Add to specify the IP address.

If installing in a LAN or when the WAN uses the same subnet, go to Step 19.

16 For a WAN environment, specify IP addresses of the Secondary server as well as the Primary server.
17 Add each Principal (Public) network address until all addresses are present. Click Next.

18 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 credentials for Domain Administrators (or an account with equivalent rights). Enter the domain name, domain administrators account name and password and click Next.

The vCenter Server Heartbeat server pair may be administered remotely on client machines using the vCenter Server Heartbeat Console.
The vCenter Server Heartbeat Console connects to an IP address of the active server using the default client connection port of 52267. If this port is already in use, enter an available client connection port. Click Next.

Select the desired applications to protect. All licensed vCenter Server Heartbeat features are listed.

If installing vCenter Server only, or vCenter Server locally and the SQL Server on a separate server, select **Protect Virtual Center only**.

If installing SQL Server remotely, upon completion of the vCenter Server installation locally, repeat the installation procedure at the remote SQL Server location and select **Protect SQL Server only**.

If installing both vCenter Server and SQL server locally, select **Protect Virtual Center and SQL Server**.
Select the applications to protect. If installing in a WAN, enable the Low Bandwidth Module by selecting **Enable LBM**. Click **Next**.

**CAUTION**  Do not enable the Low Bandwidth Module (LBM) for a LAN install.

21 Configure Microsoft Windows Backup options.

To facilitate the clone of the Primary server onto the Secondary server, you must back up pertinent components of the Primary server for restoration on to the Secondary server.
You have the following options:

- For installation using the Pre-Clone technique, go to Step a of Step 26 on page 44.
- For installation using the Install Clone technique, continue with Step 22.

22 Where VMware Channel communications are fast and reliable, for instance in a LAN topology, you can directly create the backup files over the VMware Channel connections to a partition on the Secondary server. To perform this direct backup, click **Map Network Drive** and specify a network mapping to the Secondary server. Enter the path to the desired storage location of the backup file.

23 Choose an appropriate drive letter for the mapping and specify the required share on the Secondary server using the channel address of the Secondary server as the server name, Example: \\192.168.1.6\VM_BU. Verify that the partition to which you create the mapping has enough free space, a minimum of 2GB, to accommodate the backup file.

24 Where the VMware Channel connection is less than 10 Mbit or risks an interruption in connection, for example in a WAN topology, save the backup file locally and manually port the file to the Secondary server.

25 In either case, specify the path where the backup file is stored by either manually typing the path into **Backup File Folder** or click **Browse** to locate the folder or network mapping.

26 Depending on the network topology between the servers, backup files might either include or exclude application data. Application data included in the backup file decreases the time to initially verify and synchronize the applications data on first start up of vCenter Server Heartbeat software and is useful where the VMware Channel connections are slower than LAN speed, such as during a WAN implementation. With Windows 2003, vCenter Server Heartbeat takes the backup using the Windows Volume Shadow Service and does not stop services, thereby preventing downtime. Including the applications protected data vastly increases the backup file size and therefore increases the time of the backup. Due to the potentially large size of the backup file, care consideration is required when including application data and specifying the backup folder location.
Continue with Step a.

a. When selecting the Pre-Clone technique, Setup will backup two small files, nfsetup.dat and primary.csv, from the Primary server and restore them to the Secondary server for proper configuration.

b. Where VMware Channel communications are fast and reliable, for instance in a LAN topology, you can directly create the backup files over the VMware Channel connections to a partition on the Secondary server. To perform this direct backup, click Map Network Drive and specify a network mapping to the Secondary server. Enter the path to the desired storage location of the backup file.

c. Choose an appropriate drive letter for the mapping and specify the required share on the Secondary server using the channel address of the Secondary server as the server name, example: \192.168.1.6\VM_BU.

d. Where the VMware Channel connection is less than 10 Mbit or risks an interruption in connection, for example in a WAN topology, save the backup file locally and manually port the file to the Secondary server.

e. In either case, specify the path where the backup file is stored by either manually typing the path into Backup File Folder or click Browse to locate the folder or network mapping.

With Windows 2003, vCenter Server Heartbeat takes the backup using the Windows Volume Shadow Service and does not stop services, thereby preventing downtime. Click Next.
Review the summary of options and configuration information for the installation. Click Next.

Pre-install checks automatically run to ensure that the installation can continue. Setup checks the available disk space, system memory, operating system compatibility, and dependencies between modules. In the lower pane of the dialog, a report displays the results of the pre-install checks.

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

If the pre-install checks are successful, click Next.
The next screen displays the progress of the installation. During this process, Setup installs the necessary files and folders onto your system and applies the configuration you specified. Setup also installs Heartbeat Diagnostics and automatically configures it with the default settings. If a previous version of Heartbeat Diagnostics is detected, vCenter Server Heartbeat Setup updates it to the current version. To learn more about Heartbeat Diagnostics, see Getting Started with Heartbeat Diagnostics on the VMware Web site.

Click Next after vCenter Server Heartbeat components are complete. You have the following options:

- If using the Pre-Clone installation technique, go to Step 35.
- If using the Install Clone installation technique, continue to Step 33.
The next screen displays Microsoft Windows Backup. Click **Proceed**. The automated backup is saved in the previously defined location.

A summary screen displays the results of the backup operation. Review the backup report and click **Next**.
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, select the Continue Anyway option. If Windows is configured to display Signed Driver warnings, you may see multiple warnings. The lower pane displays the results of the process. 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. vCenter Server Heartbeat also disables NetBIOS on the Channel NIC(s) to prevent Domain Name conflicts on the subnet.
When the setup wizard confirms the successful completion of the installation, click **Finish**.

### Secondary Server

Installation of the Secondary server begins using the same process as the Primary server.

**To install the Secondary server**

1. Installing vCenter Server Heartbeat software on the Secondary server is a similar process to installing the software on the Primary server. Download vCenter Server Heartbeat software to the Secondary server (either Physical or Virtual) and unpack the software from the distribution .zip file into an appropriate folder.

2. As with the installation on the Primary server, select **Install VMware vCenter Server Heartbeat**, and then click **Next**.
3 Select **Secondary** as the server identity, and then click **Next**.

![Physical Hardware Identity](image1)

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

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

![Identify Microsoft Windows Backup Folder](image2)
5 The Pre-Install checks automatically run. Click Next.

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

6 If the pre-install checks are successful, click Next.

7 The next screen displays the progress of the installation. During this process, Setup installs the necessary files and folders onto your system and applies the configuration you specified. Setup also installs Heartbeat Diagnostics and automatically configures it with the default settings. To learn more about Heartbeat Diagnostics see Getting Started with Heartbeat Diagnostics.
8 The lower pane displays the results of the installation. Click **Next**.

9 The progress of the VMware vCenter Server Heartbeat Packet Filter installation displays. Click **Next**.
You have the following options:

- If the Secondary server is Physical such as in P2P, go to Step 10.
- If the Secondary server is Virtual such as in P2V or V2V, continue with Step a.

a At this point the Packet Filter has been 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 and then select the Connected and Connect at power on check boxes. Click OK.

10 In the Channel Adapter Identification screen, select the appropriate adapter and review the IP address configuration in the lower pane. Click Next.
You have the following options:

- If using the Install Clone installation technique, continue to Step 11.
- If using the Pre-Clone installation technique, go to Step 14.

11 The **Public Adapter Identification** screen allows you to configure the Principal (Public) adapter on the Secondary server. 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).
12 Click **OK**, then click **Open Network Connections** to change the static IP address of the Principal (Public) adapter to match that of the Primary server (LAN configuration only).

13 If in a WAN environment, verify the Secondary Principal (Public) adapter IP address configuration. Click **Next**.

You have the following options:

- If using the Install Clone installation technique, go to **Step 15**.
- If using the Pre-Clone installation technique, go to **Step 28**.
14 When using the Pre-Clone installation technique, although you previously configured the IP address of the Principal (Public) network connections, vCenter Server Heartbeat allows you to make any last minute changes on the Secondary server. Click Next.

15 The Microsoft Windows Backup Restore screen shows the process of unbinding the vCenter Server Heartbeat Packet Filter and disabling NetBIOS from the VMware Channel NIC(s). A Caution message displays, advising you that the restore process is about to begin and upon completion, the server must be restarted. After restarting, Plug and Play might require you to restart the machine again. Click Next.
16 The NTBackup wizard launches. If NTBackup has never run before, the software searches for backup devices. Close any wizards that display and click **Restore Wizard** on the welcome page.

![NTBackup wizard](image1)

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

![Browse](image2)

18 Navigate to the partition and select the appropriate folder in which the backup file was created, select the backup file, click **Open** and then **OK**.

![Select file to catalog](image3)
19 Expand the file tree structure to see the System State file in the left pane. Click OK to build indexes where required. Select all items listed under the media created tree and click Next.

20 With Where to restore at the default Original location, click Next. Click Finish.
21 A warning message alerts you that the restore process will overwrite the existing System State files. Click **OK** to allow the restore process to continue.

![Restore Progress](image)

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

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

24 Following the restart of the server, log into the Secondary server using the domain administrator’s account.

25 Plug and Play may require multiple restarts of the server as it re-identifies the actual hardware makeup of the Secondary server as opposed to that restored from the backup file of the Primary server.

**NOTE** vCenter Server Heartbeat starts each time the Secondary server reboots. Before a new reboot, manually stop vCenter Server Heartbeat.

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

27 When all Plug and Play cycles complete, the vCenter Server Heartbeat Setup is complete, and vCenter Server Heartbeat starts on the Secondary server.
28 Select **Start VMware vCenter Server Heartbeat after clicking Finish** and click **Finish**.

![Screenshot of VMware vCenter Server Heartbeat Setup]

29 Before starting vCenter Server Heartbeat, verify the time synchronization between the Primary and Secondary servers. If there is a difference, synchronize the Secondary (passive) server to the Primary (active) server across the VMware Channel. Type the following command at the command prompt:

```
net time \<Primary_Channel_IP_address> /set
```

Start vCenter Server Heartbeat on the Primary server; Right-click the vCenter Server Heartbeat System Tray icon and choose **Start VMware vCenter Server Heartbeat**. The icons change from a double dash to a **P**, indicating the server is the Primary server and an **A** indicating the server is acting in an active role.

30 The Primary and Secondary servers then establish a handshake and commence replication.

**NOTE** The installation is complete if vCenter Server was installed with a local SQL server or only vCenter Server was installed with no separate SQL Server.

If vCenter Server only was installed and you want to install a separate SQL server, repeat the installation process for the Primary and Secondary server at the remote site and selecting **SQL Server only**.

To install the SQL Server on a separate host from the vCenter Server, go to “**Primary Server**” on page 29.
31 Configure the appropriate username and password in the vCenter Server Heartbeat Console:

   a  Start vCenter Server Heartbeat Console from the desktop shortcut or go to **Start > All Programs > VMware > VMware vCenter Server Heartbeat >Manage Server**. The login page displays.

![Image of vCenter Server Heartbeat Login](image.png)

   b  Before you log in, you must identify the pair of servers to administer. Click **Servers**.

   **NOTE**  Enter the IP address of one of the server pairs for the VMware Channel to locally administer pairs of servers.

c  Click **Add Pair**.

![Image of Add Server Pair](image.png)

d  Enter the IP address of the Primary server of any NIC on the active server or the NetBIOS name of the server pair and click **OK**.
e The server pair appears in the list. If more than one server pairs exist within the organization, add them sequentially to the list by repeating the procedure.

To edit or delete server pairs from the list, click the entry in the list and select the relevant button.

f Click Close to return to the login screen.

To administer a pair of servers you must connect to them via the vCenter Server Heartbeat Console. vCenter Server Heartbeat Console does not connect until vCenter Server Heartbeat initializes. Wait 10 seconds after starting vCenter Server Heartbeat before attempting to connect.

g Select a server pair displayed in the Server box.

h Enter the username and password with valid Windows credentials. In a domain environment, enter the username in the format domainname\username.
The **Server Pairs Overview** screen lists the selected pair of servers with other server pairs that have historically been administered. The Primary server name is displayed with the roles that Primary and Secondary servers are currently performing.

Additionally, the Last event, Importance, and Time also display. These events are discussed later in this guide.

To add additional pairs of servers, click **Add** and follow the previously described procedure.

To select a pair listed in the main data grid, select the check box next to the server name.

When a pair is selected, the **Open**, **Clear Event**, and **Remove** buttons become active.
Open displays the pair of servers for administration and configuration and displays the System > Status and Control page.

k  Click Advanced > Application > Plugins.

l  Select the vCenter Server plug-in.

m  Click Edit.

n  Enter the username and password for an account with rights to the Virtual Infrastructure.

o  Click OK.
Post Installation Configuration

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

vCenter Server 2.5

The post installation configuration tasks are determined by the type of network environment.

LAN

For LAN deployments, perform the following:

1. If a Management IP address is configured, no additional tasks are needed.
2. If a Management IP address has not been configured, configure a VMware Managed IP address using the Virtual Infrastructure Client.
   a. Launch the Virtual Infrastructure Client.
   b. In the Virtual Infrastructure Client, navigate to Administration > VirtualCenter Management Server Configuration > Runtime Settings.
   c. In the Managed IP field, enter the Principal (Public) IP address.
   d. Click OK and close the dialog.

WAN

For WAN deployments, regardless of whether a Management IP address exists, vCenter Server Heartbeat provides a task that can be configured to update the ESX hosts with the new Managed IP address during a switchover or failover. The task requires the Managed IP to be set either in the vpxd.cfg file or the registry.

To configure the Managed IP in the Vpxd file

1. The vpxd.cfg files is located at C:\Documents and Settings\All Users\Application Data\VMware\VMware Virtual Center server.
2. On the active server, locate the <vpxd> element in the vpxd.cfg file and add a new element <managedIP> that contains the Principal (Public) IP address of the vCenter server.

To configure the Managed IP in the registry

At HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VirtualCenter, create a new string value called <managedIP> and set it with the Public (Principal) IP address of the currently active server.

IMPORTANT  Do not configure the VMware Managed IP address using the Virtual Infrastructure Client. The Managed IP field from Administration > VirtualCenter Management Server Configuration > Runtime Settings must be clear.

vCenter Server 4.0

The post installation configuration tasks are determined by the type of network environment.

LAN

With or without a Management IP address configured, no additional tasks are required.
WAN

With or without a Management IP address configured, disable the VMware VirtualCenter PostStart task via the vCenter Server Heartbeat Console using the following procedure.

1. Launch the vCenter Server Heartbeat Console.
2. Click Application.
3. Select the Tasks tab.
4. Select VMware VirtualCenter PostStart task.
5. Click Edit.
6. Clear the Enabled check box.
7. Click OK.

IMPORTANT Do not configure the Managed IP address using the vSphere Client. The vCenter Server Managed IP field from Administration > vCenter Server Settings > Runtime Settings must be clear.
This chapter includes the following topics:

- “Configuring Server Wizard” on page 70
- “Configuring the Machine Identity” on page 71
- “Configuring the Server Role” on page 71
- “Configuring the Client Connection Port” on page 71
- “Configuring Channel IP Routing” on page 71
- “Configuring the Default Channel Port” on page 72
- “Configuring Low Bandwidth Module” on page 72
- “Configuring Public IP Addressing” on page 73
- “Enabling Network Monitoring” on page 73
- “Configuring Split-Brain Avoidance” on page 74
- “Configuring Message Queue Logs” on page 75
- “Configuring the Maximum Disk Usage” on page 75


Configuring Server Wizard

The vCenter Server Heartbeat Server Pair Configuration Wizard (Configure Server wizard) sets up and maintains communications between the vCenter Server Heartbeat servers. Configuration information includes the IP address for the VMware Channel(s) and Principal (Public) addresses on both servers.

Once the system is set up and is functioning correctly, you do not need to reconfigure the system. The Configure Server wizard becomes redundant during day-to-day operations of the software.

1 Before launching the Configure Server wizard to change the vCenter Server Heartbeat configuration, you must stop vCenter Server Heartbeat.

2 Then click the Configure Server icon on the desktop or go to Start > All Programs > VMware > VMware vCenter Server Heartbeat > Configure Server to launch the Configure Server wizard.
Configuring the Machine Identity

**CAUTION** The machine Identity should only be changed when directed to do so by VMware Support or when instructed to by a Knowledge Base article. vCenter Server Heartbeat is designed not to allow two passive or two active servers to connect.

To change the machine identity

1. Go to the **Machine** tab and select the desired Physical Hardware Identity of the local machine.
2. Click **Next** or **Finish**.

Configuring the Server Role

To change the server role, go to the **Machine** tab and select the Current Role of the local machine. Once complete, click on **Next** or **Finish**.

**NOTE** Before changing the role of the local server, verify that the other (remote) server in the pair is not already performing the same role.

Configuring the Client Connection Port

Clients such as the vCenter Server Heartbeat Console use the Client Connection Port to connect to vCenter Server Heartbeat. Do not change this port unless another application is using it. To change the Client Connection Port, go to the **Machine** tab and edit the default entry (52267). Click **Next** or **Finish**.

Configuring Channel IP Routing

Channel IP routing defines the IP addresses used to communicate between the Primary and Secondary servers. Each link has a pair of addresses, one for the Primary, and one for the Secondary.
To add an additional VMware Channel after installing the NICs and configuring them

1. Go to the Channel tab. Click Add Row to add the new IP addresses for both the Primary and Secondary server to the VMware Channel IP Routing table.

2. Use the drop-down to display a list of available IP addresses on the local server.

3. Manually enter the remote server IP address.

4. To change the VMware Channel IP addresses, select the entry in the table and edit the entry.

5. Click Next or Finish.

Configuring the Default Channel Port

VMware Channel uses the Default Channel Port to communicate between the Primary and Secondary server. Do not change this port unless another application is using it. To change the Default Channel Port, go to the Channel tab and edit the default entry (57348). Click Next or Finish.

Configuring Low Bandwidth Module

This feature is enabled during installation. To disable this feature, go to the Channel tab and clear the Low Bandwidth Optimization check box. If selected, then the VMware Channel optimizes communications for low bandwidth connections. Low Bandwidth Optimization (LBO) stores data on disk rather than in memory and is essential for WAN installations or when bandwidth is limited.

To enable LBO, go to the Channel tab and select the check box to enable the feature. Click Next or Finish.

NOTE  This feature is designed for implementations where the available throughput on the VMware Channel is less than 10Mbit/s. Do not enable the Low Bandwidth Module in a LAN, this feature is not designed to work in a LAN where the throughput is much higher.
Configuring Public IP Addressing

vCenter Server Heartbeat servers are configured with one or more Principal (Public) IP addresses. These are the addresses by which clients of the protected application connect to the application. Typically, there is one Principal (Public) IP address.

You must configure all of the Principal (Public) IP addresses on both Primary and Secondary servers. On the passive server, all traffic to and from these Principal (Public) IP addresses is blocked. On the active server, all traffic passes through. When the server roles switch, the IP filtering mode also switches, so client systems always connect to the Principal (Public) IP addresses on the server that is currently active. When the vCenter Server Heartbeat service shuts down, the filtering remains in place so no IP address conflicts occur between the two servers.

To configure Principal (Public) IP address

1. Go to the Public tab and list all the addresses used as Principal (Public) IP addresses.
   - An address must not appear more than once. The Principal (Public) IP addresses listed cannot be the same as any of the IP addresses listed in the Channel tab.
2. To add an address, double-click a row and then either type in the address or select it from a list of currently defined addresses.
3. Click Next or Finish.

Enabling Network Monitoring

vCenter Server Heartbeat can monitor the connection between the active server and the Principal (Public) network. VMware recommends that you enable this feature.

The network is monitored by pinging a set of machines on the Principal (Public) network. If enabled, the system pings a set of default set of addresses automatically. Use the vCenter Server Heartbeat Console to change the configuration after installation.
To enable Network Monitoring

1. Go to the Network Monitoring tab.
2. Select Enable public network monitoring using automatic configuration.
3. Click Next or Finish.

Configuring Split-Brain Avoidance

Split-brain Avoidance is used in WAN installations to ensure that only one server becomes active if the VMware Channel connection is lost, but both servers are still connected to the Principal (Public) network.

Split-brain Avoidance works by pinging from the passive server to the active server across the Principal (Public) network. If the active server responds, the passive does not failover, even if the VMware Channel connection is lost. This feature requires that the active and passive servers have different IP addresses on the Principal (Public) network, which is typically the case for WAN installations.

To enable this feature, go to the Network Monitoring tab and select Enable split brain avoidance (Recommended for WAN). Enter the Principal (Public) IP address used by each server.

You must configure auxiliary IP addresses on both Principal (Public) network cards to allow the passive server to send a ping and send email alerts. Auxiliary IP addresses are additional IP addresses assigned to the network card, which is connected to the Principal (Public) network. They allow the passive server to communicate because unlike the Principal (Public) network address they are not filtered.

To configure an auxiliary IP address

1. Open the network properties for the Principal (Public) network connection.
2. Double-click Internet Protocol (TCP/IP) to display the properties.
3. Click Advanced.
4. Enter an additional (currently unused) IP address in the table.
5. Reposition the IP addresses in the list so that the additional (auxiliary) IP address appears first and the Principal (Public) network address that clients use to connect to the server appears second.

**NOTE** You can reposition the IP addresses by deleting it at the top of the list and adding it at the bottom.
6   Click **OK** three times.
7   Click **Next** or **Finish**.

**Configuring Message Queue Logs**

The server temporarily stores replication data received in the passive server (safe) queue and the replication data waiting to be sent in the active server (unsafe) queue in message queue logs.

This configuration only affects the local server. Logs can be in different locations on the Primary and Secondary servers.

**To configure the location of the message queue logs**

1   Go to the **Logs** tab.
2   Click **Browse** to navigate to the folder to store the message queue logs.
3   Select the folder, then click **Next** or **Finish**.

![Configuration screen](image)

**Configuring the Maximum Disk Usage**

You can configure the maximum disk space allocated for logging. Log files increase in size on the active server under the following conditions:

- If the active server cannot communicate with the passive server
- Certain operations on the passive server
- If the server is under heavy load

When the disk reaches quota, replication stops and the system is no longer protected.

If using a dedicated disk for log files, consider disabling the quota. To do this, set the quota to zero. If vCenter Server Heartbeat runs out of physical disk space, then it must be shut down before it can resume replication. Set the quota with overflow space to enable vCenter Server Heartbeat to stop replicating gracefully.

To configure Maximum Disk Usage, go to the **Logs** tab and enter the maximum dedicated disk space allocated for message queue log files. Click **Finish**.
System Administration and Management
This chapter includes the following topics:

- “vCenter Server Heartbeat Console” on page 79
- “Logging into vCenter Server Heartbeat” on page 79
- “Configuring the Look and Feel of the vCenter Server Heartbeat Console” on page 82
- “Logging Out of the vCenter Server Heartbeat Console” on page 83

**vCenter Server Heartbeat Console**

vCenter Server Heartbeat operates over a pair of vCenter Server Heartbeat servers and is administered in these pairs.

The vCenter Server Heartbeat Console is used to carry out the day-to-day administration of one or more pairs of servers.

The vCenter Server Heartbeat Console runs from either of the two servers in the pair or remotely from another machine in the same subnet, which has vCenter Server Heartbeat or the vCenter Server Heartbeat Client Tools installed.

**NOTE** You can install vCenter Server Heartbeat on a workstation to act as a client to the server pair. Run setup.exe from the setup CD folder on the workstation and choose the Install Client Tools option under the installation set.

**Logging into vCenter Server Heartbeat**

To access vCenter Server Heartbeat, launch the vCenter Server Heartbeat Console from the desktop shortcut or go to Start > All Programs > VMware > VMware vCenter Server Heartbeat > Manage Server.

**Figure 4-1. VMware vCenter Server Heartbeat Login**
Before you log in, you must identify the pair of servers to administer. Click **Servers**.

**NOTE**  Enter the IP address of one of the server pairs for the VMware Channel to locally administer pairs of servers.

**To add or remove a pair of vCenter Server Heartbeat servers**

1. A Server Pairs window displays no servers. To add a server pair, click **Add Pair**.

   ![Add Pair](image1)

2. Enter the IP address of the Primary server of any NIC on the active server or the NetBIOS name of the server pair and click **OK**.

   ![Add Server Pair](image2)

3. The server pair appears in the list. If more than one server pairs exist within the organization, add them sequentially to the list by repeating the procedure.

   ![Server Pairs](image3)
Chapter 4  Status and Control

4 To edit or delete server pairs from the list, click the entry in the list and select the relevant button.

5 Click Close button to return to the login screen.

Connecting to a Pair of Servers

To administer a pair of servers you must connect to them via the vCenter Server Heartbeat Console. vCenter Server Heartbeat Console does not connect until vCenter Server Heartbeat initializes. Wait 10 seconds after starting vCenter Server Heartbeat before attempting to connect.

1 Select a server pair displayed in the Server box.

2 Enter a username and password with valid Windows credentials. In a domain environment, enter the username in the format domainname\username.

Reviewing the Status of a Server Pair

The Server Pairs Overview screen lists the selected pair of servers with other server pairs that have historically been administered. The Primary server name is displayed with the roles that Primary and Secondary servers are currently performing.

Figure 4-2.  Server Pair Overview

Additional information about the communications between the servers displays: the length of the passive server (safe) and active server (unsafe) queues and the peak rate of data transfer over the VMware Channel. Last event, Importance, and Time also display. These events are discussed later in this guide.
To add additional pairs of servers

1. Click Add and follow the previously described procedure. Exit closes the interface but does not affect the vCenter Server Heartbeat Server service.

2. To select a pair listed in the main data grid, select the check box next to the server name.

When a pair is selected, the Open, Clear Event, and Remove buttons become active.
- **Clear Event** removes all events logged for that pair of servers and resets the log files for the pair of servers.
- **Remove** deletes the pair of servers from the vCenter Server Heartbeat Console.
- **Open** allows you to administer and configure the pair of servers.

### Configuring the Look and Feel of the vCenter Server Heartbeat Console

The vCenter Server Heartbeat Console graphical user interface allows you to change the style and color of the interface to suit your preferences.

### To change the style of the interface

1. Launch the vCenter Server Heartbeat Console from the desktop shortcut or go to **Start > All Programs > VMware > VMware vCenter Server Heartbeat > Manage Server.**

2. In the **Server Pairs Overview** screen, click Preferences and navigate to Look and Feel. Select a style to change the color and style of the interface automatically.
Changing vCenter Server Heartbeat Console Screens

The buttons on the left side of the screen allow navigation between the screens of the vCenter Server Heartbeat Console.

**Figure 4-3. Navigation Buttons**

The current screen is always visible as the text of the appropriate button turns a magenta color, as shown above on System.

Click Log to view the event log screen.

Logging Out of the vCenter Server Heartbeat Console

**To log out of the vCenter Server Heartbeat Console**

1. Click Close to log out of administering the current server pair.
   
   A confirmation dialog asks for confirmation of the logout request.

2. Click Yes to close the client and return to the Server Pairs Overview screen.
This chapter includes the following topics:

- “Server Protection Overview” on page 85
- “Checking the Server Pair Status” on page 86
- “Configuring Heartbeat Settings” on page 87
- “Configuring vCenter Server Heartbeat Shutdown Options” on page 88
- “Configuring Split-Brain Avoidance” on page 92

Server Protection Overview

Protection against the active server’s operating system or hardware failure is facilitated by the two instances of the vCenter Server Heartbeat software monitoring each other by sending “I’m alive” messages and reciprocating with acknowledgments over a network connection termed the VMware Channel. If the passive server detects that this process or heartbeat fails then a failover is initiated.

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

The System screen is the default screen opened when administering a pair of servers. The System screen displays the roles of the servers, active or passive, the actions that the servers are currently performing, and how well the system is coping with file and registry replication.

Figure 5-1. Status and Control

The system status in the central grid for each server indicates procedures being executed. Table 5-1 lists each status with a description:

Table 5-1. System Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Replicating</td>
<td>The file and registry replication has stopped and all protected applications may be stopped.</td>
</tr>
<tr>
<td>Stopping Replication</td>
<td>The file and registry replication is in the process of stopping and all protected applications may be closing down.</td>
</tr>
<tr>
<td>Replicating</td>
<td>File and registry changes on the active server are being intercepted and replicated to the passive server and protected applications are being monitored (This is the normal status).</td>
</tr>
<tr>
<td>Starting Replication</td>
<td>The replication process is in the process of starting and protected applications are being started.</td>
</tr>
<tr>
<td>Shutting Down</td>
<td>The vCenter Server Heartbeat file and registry interceptor has stopped. All protected applications may have stopped. The Neverfail Service is stopping.</td>
</tr>
<tr>
<td>Preparing to Switch</td>
<td>The system is performing ancillary operations prior to a switchover such as flushing the queues.</td>
</tr>
<tr>
<td>Switching</td>
<td>The system is in the process of performing a switchover.</td>
</tr>
</tbody>
</table>

The central grid also displays queue delays for each server. Queues show the time a specific piece of information resides in the passive server (safe) and active server (unsafe) queues respectively before moving to the passive server (safe) queue or committed to disk. Above the data grid, the connection status and speed are graphically represented. The Server Pair pane graphically displays the file and registry synchronization status with icons described in Table 5-2.
Table 5-2. File and Registry Status

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️ Synchronized</td>
<td>The files or registry are fully synchronized.</td>
</tr>
<tr>
<td>🔴 Unchecked</td>
<td>There are files present that are currently unchecked, a full system check has not completed.</td>
</tr>
<tr>
<td>✔️ Synchronized and Busy Processing</td>
<td>The registry is currently in the process of being synchronized.</td>
</tr>
<tr>
<td>❓ Checking</td>
<td>The differences in the registry are currently being checked to see if they are synchronized.</td>
</tr>
<tr>
<td>🔴 Out of Synch</td>
<td>The files or registry are not synchronized.</td>
</tr>
</tbody>
</table>

When the vCenter Server Heartbeat pair establishes a connection, it triggers a file synchronization and verification process to ensure all the files stipulated through file filters are mirror images of one another on their respective servers. The process works by checking each 64K block of each file configured to be protected and performing a checksum to determine differences in blocks. If the blocks are the same then the block is marked as in synch. If the blocks differ then the block is replicated to the passive server and marked as in synch. The file verification and synchronization process completes when all blocks of all files have been marked as in synch.

**Configuring Heartbeat Settings**

The Heartbeat interval dictates the time step at which the passive server sends Heartbeat packets to the active server across the VMware Channel connections. **Max Heartbeats Missed Before Failover** determines the number of missed packets before initiating a failover.

1. Click Advanced > Communication on the left navigation panel, and then click the Configuration tab.
2. Set Max Heartbeats Missed Before Failover and the Heartbeat Interval and click Apply.
Configuring vCenter Server Heartbeat Shutdown Options

vCenter Server Heartbeat allows you to select whether to leave protected applications running upon shutdown or to stop protected applications as part of the shutdown process.

1. To set this option, click **Advanced > System** on the left navigation panel, then the **Configuration** tab.
2. Select the option vCenter Server Heartbeat performs when it shuts down. Click **Apply**.

Starting, Stopping, and Shutting Down vCenter Server Heartbeat

**Start Replicating**, **Stop Replicating**, and **Shutdown** in the **System** screen allow you to configure the vCenter Server Heartbeat Server Service on both the servers synchronously.

**Start Replicating**

**Start Replicating** starts any application and data protection configured for the system. By default, all protection modes start when vCenter Server Heartbeat starts. Use **Start Replicating** only when the system has stopped activity with **Stop Replicating** or automatic stop.

**Stop Replicating**

**Stop Replicating** prompts you to stop parts of the system.

**Figure 5-2. Protected Application Stop Options**
The default option, **Stop Heartbeat but leave protected applications running** stops the protection (synchronization) of data files but does not stop protected applications.

**Stop Heartbeat and all protected applications** stops the protection (synchronization) of data files and stops all protected applications.

The vCenter Server Heartbeat service continues to run on both the Primary and Secondary servers, providing heartbeats and continuing to protect the system and network facets of the active server.

For example, use **Stop Replicating** when a virus has infected the Primary server or when upgrading the protected application.

Click **OK** to view the stop status of the various facets of the server.

**Figure 5-3. Replication Shutdown Status**

**Shutdown**

**Shutdown** is similar to **Stop Replicating** and stops all protection of data and when selected, protected applications. **Shutdown** also stops the vCenter Server Heartbeat Server service on both the active and passive machines. Use **Shutdown** when you need to reconfigure the server or upgrade vCenter Server Heartbeat.
Forcing a Switchover

After configuring vCenter Server Heartbeat to protect all the required applications and data, the Secondary server can take over from the Primary server in a managed and seamless way called a switchover.

This is particularly useful during any maintenance work on the Primary server that involves rebooting the server.

To initiate a switchover

Click Switchover in the System Screen, which reverses the roles of the servers: the active server becomes passive and vice versa. This allows users to work continuously even while the Primary server is offline.

Once the Primary server is back up and running, you can initiate the switchover again so that the Primary server becomes active and the Secondary server becomes passive.

NOTE You can perform a switchover any time provided that the systems are fully synchronized with respect to data files and registry replication. A switchover cannot occur if either server is in an unsynchronized or unknown state.

Before triggering a switchover, you should review the queue information. If the queues are large, file operations on the active server are high. You must clear the queues before triggering a switchover. Review the queue lengths in the vCenter Server Heartbeat Console in the list of administered server pairs.

Figure 5-4. Server Pair Queue Status
Recovering from a Failover

A failover differs from a switchover. A switchover is a controlled switch (initiated from the vCenter Server
Heartbeat Console or automatically when preconfigured) between the Primary and Secondary servers. A
failover happens when one or all of the following have experienced a failure on the active server: power,
hardware, or communications. The passive server counts a pre-configured number of missed Heartbeats
before beginning a failover, and when this happens, it automatically assumes the active role and start to
execute the protected applications.

The following recovery scenario is based on vCenter Server Heartbeat configuration with the Primary server
as active and the Secondary server as passive.

A failover has occurred and the Secondary server is now running as the active server.

1. Check event logs on both servers to determine the cause of the failover. If you are unsure how to do this,
   use the Log Collector tool to collect information and send the output to VMware Support.

2. Do not perform a switchback to the Primary server if the following issues occur on the Primary server.
   Resolve the following issues, then restart vCenter Server Heartbeat:
   - **Hard Disk Failure** — Disk might need replacing.
   - **Power Failure** — Restore power to the Primary server.
   - **Virus** — Clean the server of all viruses.
   - **Communications** — Replace physical network hardware.
   - **Blue Screen** — Determine cause and resolve. You might need to submit the dump file to VMware
     Support (www.vmware.com/support) for analysis.

3. Run the Configure Server wizard and verify the server is set to Primary and passive.

4. Disconnect the VMware Channel network cables or disable the network card.

5. Resolve the list of possible failures.

6. Reboot this server and reconnect or enable the network card again.

7. After reboot, check that the **Taskbar** icon now reflects the changes by showing P / - (Primary and passive).

8. On the Secondary active server or from a remote client, launch vCenter Server Heartbeat Console and
   confirm that the Secondary server as active.

If the Secondary server is not displaying as active, perform the following steps:

1. If the vCenter Server Heartbeat Console is unable to connect remotely, then try running it locally. If you
   are still unable to connect locally then check the service is running via the Service Control Manager. If it
   is not, check the event logs for a cause.

2. Run the Configure Server wizard and check that the server is set to Secondary and active.

3. Determine if the protected application is accessible from clients. If it is, then start vCenter Server
   Heartbeat on the Secondary server. If the application is not accessible, check the application logs to
determine why the application is not running.


5. **NOTE** The data on this server should be the most up to date and this server is the live server on the
   network. Once vCenter Server Heartbeat starts, it overwrites all the protected data (configured in the File
   Filter list) on the Primary passive server. If you are not sure that the data on the active server is up to date,
   contact VMware Support (www.vmware.com/support). Go on to the next step only if you are sure that
   you want to overwrite the protected data on the passive server.

5. Start vCenter Server Heartbeat on the Secondary active server and check that the **Taskbar** icon now
   reflects the correct status by showing S / A (Secondary and active).
Configuring Split-Brain Avoidance

You can enable or disable the Split-brain Avoidance feature by selecting or clearing **Prevent fail-over if heartbeat is lost but Active Server is visible via public network**.

The passive server polls the active servers Principal (Public) connection at the time interval specified in the ping interval text box. You can increase or decrease the interval from the default 10 seconds as required.

The active server must respond within the time period value specified in the **Time Out for Ping Echoes** text box to prevent a failover. If the active server responds in a timely manner, the failover mechanism ceases. If the active server does not respond, the failover occurs.

**Figure 5-5. Split-brain Avoidance Configuration**

Configure IP addresses for Split-brain Avoidance as required from those set at install time for both the Primary and Secondary servers.
This chapter includes the following topics:

- “Communication Status” on page 93
- “Reviewing the VMware Channel Status” on page 94
- “Configuring Public Network Connection Checks” on page 94
- “Setting Max Server Time Difference” on page 95

Communication Status

The Communication screen allows you to check the status of the VMware Channel, the active server (unsafe) and passive server (safe) queues, and the Principal (Public) network.

Figure 6-1. Communication Status
Reference Guide

Reviewing the VMware Channel Status

The status displays connected or not connected, statistics of the connection about the data sent by either server, and the size and age of the oldest entry in the active server (unsafe) and passive server (safe) queues. The link status displays the IP address used by the VMware Channel for the Primary and Secondary servers with the port used for communications.

Public Network Connectivity displays the status of Principal (Public) network monitoring and or Split-brain Avoidance if configured on the server pair.

To configure VMware Channel communications, click Advanced and select the Configuration tab.

Configuring Public Network Connection Checks

The Configuration tab allows you to make adjustments to the Principal (Public) network monitoring features, the VMware Channel heartbeat features, and the disk usage/max server time difference.

Enable or disable Principal (Public) network monitoring by either selecting or clearing the Failover if Active Server's Public Network Connection is Lost check box. This feature integrates the polling of particular waypoints around the network through the active server’s Principal (Public) connection to ensure connectivity with the Principal (Public) network. By default, it selects the IP addresses of the default gateway, the primary DNS server, and the Global Catalog server.

If one or more of the automatically discovered waypoints are co-located on a physical machine resulting in duplicate IP addresses, you can manually specify different waypoints. To specify a manual target for the Principal (Public) network checking, clear an Auto Select check box and manually overtype the IP address with the required target address.

In a WAN environment, the target addresses for Principal (Public) network monitoring on the Secondary server may be different from those automatically selected on the Primary server. To override automatically discovered selections, clear the Auto Select check box and manually specify the target address.
Principal (Public) Network Monitoring operates when the active server effectively pings the target addresses at regular time intervals. The time interval is set by default to every 20 seconds but you can increase or decrease the frequency as required.

Each target has by default 5 seconds to respond. On slower networks where latency and network collisions are high, you can increase the response time. Adjust the Timeout for Ping Echoes value.

If any target fails to respond within the stipulated timeout, increase the polling interval to the timeout value until you receive a response. Then decrease the polling interval to the default time interval specified.

If all three targets fail to respond by missing the maximum pinged echoes and exceed the failover threshold value, vCenter Server Heartbeat initiates a switchover.

To save changes to the configuration of the communications, click Apply. To reset all configuration settings to the last save or default settings, click Reset.

**Setting Max Server Time Difference**

vCenter Server Heartbeat generates a warning if the Primary and Secondary server system clocks are not synchronized. To override the warning, allow the servers a maximum time difference specified in the Max Server Time Difference.

**Figure 6-3. Server Time Difference**

To save configuration of the communications, click Apply. To reset all configuration settings to the last save or default settings, click Reset.
This chapter includes the following topics:

- “Application Protection Overview” on page 97
- “Applications Tab” on page 97
- “Services Tab” on page 103
- “Tasks Tab” on page 107
- “Plug-Ins Tab” on page 112

Application Protection Overview

vCenter Server Heartbeat incorporates an Application Management Framework (AMFx) to manage vCenter Server Heartbeat Plug-ins.

The AMFx provides additional functionality while maintaining the traditional stability of VMware. The AMFx allows plug-ins to be installed and removed on the fly while vCenter Server Heartbeat continues to provide protection to currently installed applications.

The AMFx also employs sponsorship for protected applications files and services. Sponsorship allows multiple plug-ins to share files or services while preventing removal of a shared file or service when one of the sponsoring plug-ins remain installed.

vCenter Server Heartbeat uses the System Plug-in to monitor the server performance. With vCenter Server Heartbeat, the System Plug-in allows the administrator to configure a variety of counters and to assign actions when associated rules are exceeded.

Applications Tab

The Applications tab displays the current status of protected applications and application health. From this screen, you can start, stop, and configure all protected applications. The lower pane provides the Application Log and allows you to view application events as they occur.

1. Log into the vCenter Server Heartbeat Console.
2. Click Application on the left navigation panel and select the Applications tab.
Editing Individual Applications

vCenter Server Heartbeat allows you to configure the amount of time to wait for an application to start or stop before taking action or reporting the failure.

To configure the timeout settings

1. Select the desired application and then click Edit.
2. Enter the settings, and click OK.
Configuring Applications

The **Applications** tab allows you to configure protected applications, enables and disables protection and monitoring. You can maintain applications without stopping vCenter Server Heartbeat or taking the full server offline. During installation, vCenter Server Heartbeat sets default settings for application configurations but allows for modifications to the configurations settings.

1. Click **Configure** in the **Applications** panel.

You can protect services and start monitoring applications or unprotect services and stop monitoring an application. You can also enable **Verbose Plugin logging**, **Discover protected data at startup**, **Discover protected services at startup**, and set the rule trigger count.

2. Click **OK**.
Reviewing the Status of an Application

Once an application has started and is running, you can view the status of the application in the Applications tab of the Application screen.

**Figure 7-1. Application Status**

If an application fails, right-click the Log and investigate the failure.
Reviewing the Applications Status Log

The Application Log helps troubleshoot the protected application environment.

**Figure 7-2. Application Log**

The Application Log provides information about the behavior of all protected applications and includes events such as Task status changes, Rule triggering, Task outputs, and Application warnings. Use this log to troubleshoot application errors.

Filtering Application Log Entries

vCenter Server Heartbeat can filters Application Log files to limit the events displayed. By default, all events display in the Application Log file.

**To filter the events displayed**

1. Click **Filter** in the **Application** panel titled **Application Log**.
2. In the upper section, clear the event types you do not want to view.
3. Configure a date and time range to limit the events to fit that date and time range. To limit the date and time range, select **Events From** and edit the date or time range.
Resetting the Application Health Status

To reset the Application Health status

1. Go to the Applications tab of the Applications screen.
2. On the upper right side, click Clear.
Removing an Application

To remove an application, select it and click Remove.

If the sponsor of the selected application is associated with a plug-in, then removing the application will have the same effect as removing the plug-in. If the sponsor is not associated with a plug-in then all sponsorship is removed from services, filters, and tasks.

Figure 7-3. Application Removal

Services Tab

The Services panel displays both services that you or plug-ins specify and the services related to them by dependency (either as dependents or depends-on). The target states of protected services for the active and passive server can be specified and are typically Running on the active and Stopped on the passive. Services are protected if they are Running or Automatic, and are otherwise logged as unprotected. vCenter Server Heartbeat manages services that depend on protected services (started and stopped) but not monitored (not restarted if stopped by some external agency). vCenter Server Heartbeat monitors protected services (restarted if stopped) but not managed (not stopped if protected applications are stopped).

Log into the vCenter Server Heartbeat Console, click Application on the left navigation panel and select the Services tab.
Adding a Service

To protect a service

1. Add the service from the vCenter Server Heartbeat Console in a Running state.

2. Click Add to see a list of the current running services under Name.

3. Select the service and set the values for **Target State on Active** and **Target State on Passive**. Normally the **Target State on Active** is set to **Running** and the **Target State on Passive** is set to **Stopped**.

   **NOTE** Setting the target state for both the active and passive server to **Running** can cause the service to place a lock on some files preventing synchronization from completing.

4. If vCenter Server Heartbeat is to manage the start and stop of the service, select **Manage Starting and Stopping**. If vCenter Server Heartbeat is to monitor the state of the service, select **Monitor State**.

   vCenter Server Heartbeat also assigns three sequential tasks to perform in the event of failure. Task options include **Recover Service**, **Application Restart**, **Log Warning**, and any additional user-defined tasks previously created.

   **NOTE** For dependent services, failure actions must match the protected service.

5. Assign a task to each of the three failure options, and then click **OK**.

   **NOTE** If an application with the failure option set to **Application Restart** fails, only the services that have failed will restart. Dependent services do not stop and restart as a result of the failure.
Editing a Service

To change the options of a protected service

1. Select the service and click **Edit**.

   Edit Service provides a subset of same options available when adding a new service.

2. Make the modifications, and then click **OK**.
Checking the Status of Services

The Services tab displays the status of all protected services. The status shows both the target and actual state for both the Primary and Secondary servers and the Failure Counts for both servers.

Figure 7-4. Application Service Status

Unprotecting Services and Stopping Monitoring

To unprotect and stop monitoring the service

1. Go to the Services tab. Select the service and click Edit.
2. Clear Manage Starting and Stopping and Monitor State. Click OK.
Services have an ordering, which can be modified using **Up** and **Down** arrows. The exact order in which services start and stop is influenced by a number of key factors:

The order of applications specified by plug-ins determines which services are started first.

Services can have dependencies, which must be respected. For example, if service B is listed after service A under the User-Defined group, and service A depends on Service B, then Service B starts first.

Multiple applications can use the same service (the same service can appear under more than one sponsor). The service starts when the first application to reference it starts.

The order of stopping services is the reverse for starting services.

### Removing a Service

To remove a service

1. Select the service.
2. Click **Remove**.

The service is removed from the protected list.

### Tasks Tab

Tasks are a generalization and extension of the start, stop, and monitor scripts. Task types are determined by when the tasks run, and include the following:

- **Network Configuration** — This is the first type of task that runs when applications start and is intended to launch `dnscmd` or `DNSUpdate`. The task can launch a batch script containing multiple `dnscmd` commands. Network Configuration tasks are the only types of task that can vary between Primary and Secondary servers.

- **Pre/Post Start** — These tasks run before and after services start on the active server.

- **Pre/Post Stop** — These tasks run before and after services stop on the active server.
Pre/Post Shadow — These tasks run before and after Data Rollback Module creates a shadow copy on the active server.

Rule Action — Configure these tasks to run in response to a triggered rule or when a service fails its check.

You can define and implement tasks at the command line, which can include launching a batch-script. Examples of built-in tasks include monitoring a protected service state on the active and passive servers. vCenter Server Heartbeat can use plug-ins to define and implement tasks. An example of a plug-in-defined task is the discovery of protected data and services for a particular application.

To navigate to the Tasks tab, click Application on the left navigation panel, and select the Tasks tab.

Adding a Task

To add a task

1. Click Add. Assign a name to the task and select the task type from the list.
2. Enter the Interval setting and enter or browse for the script, .bat file, or command.
3. Click OK.

4. If the Command requires specific user credentials, click User Accounts in the upper right of the pane.
5 Add user accounts to make them available as a selection in Run As when you add a task.

Editing a Task

To edit a task

1 Select the task and click Edit. You can edit the task interval or disable the task.

2 Click OK.
Removing a Task

To remove a task

1. Select the task.
2. Click Remove.
Starting a Task Manually

vCenter Server Heartbeat provides options to allow a designated time period or event to occur before launching the task or launching the task immediately.

To launch the task immediately

1. Select the task.
2. Click Run Now.

vCenter Server Heartbeat immediately launches the task.
Plug-Ins Tab

Plug-ins support specific applications and contain all of the components to protect the designated application. Plug-ins start and stop the application, monitor the application, and provide all rules necessary to ensure that application is available in the event of a failure by initiating a configured auto-switchover.

Figure 7-5. Application Plug-Ins
Installing a Plug-In

To install a new plug-in

1. Go to Application and select the Plugins tab.
2. Click Install and browse for the plug-in. The path statement is case-sensitive.
3. Click OK.
Editing a Plug-In

To edit the plug-in configuration

1. Select the plug-in and click Edit to modify the default configuration.
2. Review the configuration options before making modifications as they are specific to each plug-in.
3. Click OK.
Uninstalling a Plug-In

You can uninstall a plug-in when you need to upgrade or remove the application the plug-in protects, or when directed by VMware Support.

To uninstall a plug-in

1. Select the plug-in.
2. Click Uninstall.

The plug-in is uninstalled and removed.
This chapter covers the topic “Rules Tab” on page 117.

Rules Tab

Rules are implemented by plug-ins and there are no user-defined rules. Configure rule actions to trigger the rule that performs specific tasks. Rules have two trigger properties:

- **Timed** — They must evaluate as true continuously for the specified duration to trigger.
- **Latched** — They trigger as soon as they evaluate to true.

Figure 8-1. Application Rules
**Editing a Rule**

Each plug-in contains a default set of rules with options you can modify.

**To edit a rule**

1. Go to Application and select the Rules tab.
2. Select the rule and click Edit.

You can enable or disable a rule, set specific options, and assign tasks to be performed in the event of a first, second or third failure.

3. Click OK.

---

**Rules Installed by vCenter Server Heartbeat Plug-Ins**

The following plug-ins implement the rules listed.

**vCenter Server Plug-In**
- Check vCenter License
- Check Connection to vCenter

**vCenter SQL Server Plug-In**
- Default Instance Buffer Cache Hit Ratio
- Default Free Pages
- Default Instance Free Pages
- Named Instance Working Set
- Named Instance Buffer Cache Hit Ratio
- Named Instance Free Pages
- Named Instance Total Server Memory
vCenter Server Heartbeat System Plug-In

- DiskAvgSecsPerRead
- DiskAvgSecsPerWrite
- DiskIO
- DiskQueueLength
- DiskReadsPerSec
- DiskWritesPerSec
- DiskWriteable
- FreeDiskSpace
- FreeDiskSpaceOnDrive
- MemoryCommittedBytes
- MemoryCommittedBytesPercent
- MemoryFreePTEs
- MemoryPageReadsPerSec
- MemoryPageWritesPerSec
- MemoryPagesPerSec
- MemoryPagingFileUsage
- PageFaultsPerSec
- ProcessorIntsPerSec
- ProcessorLoad
- ProcessorQueueLength
- RedirectorBytesTotalPerSec
- RedirectorNetworkErrorsPerSec
- ServerBytesTotalPerSec
- ServerWorkItemShortages $\geq 3$ (if the rule for server work item shortages is triggered, consult Microsoft documentation on setting the registry values for InitWorkItems or MaxWorkItems accordingly).
- ServerWorkQueueLength
- SystemContextSwitches
Checking a Rule Condition

To check a rule condition

1. Select the rule.
2. Click Check Now.

vCenter Server Heartbeat immediately checks the rule conditions of the current configuration against the attributes of the system or application.
This chapter includes the following topics:

- “Data Protection Overview” on page 122
- “Automatic Filter Discovery” on page 122
- “Configuring Max Disk Usage” on page 125
- “Reviewing Status of Protected Files” on page 126
- “Determining Effective Filters” on page 127
- “Initiating File Synchronization Manually” on page 127
- “Initiating a Full System Check” on page 128
- “Reviewing the Registry Synchronization Status” on page 130
- “Initiating a Full Registry Check” on page 131
Data Protection Overview

The filter driver is responsible for dictating the files to be protected and the disk I/O operations that have been intercepted to be replicated on the passive server.

The filtering mechanism of this driver allows the inclusion and exclusion of files from the replication process.

Figure 9-1. Data File Sync and Verify

vCenter Server Heartbeat protects a folder called Protected on the system partition.

You can configure the system to protect any permutation or combination of file structures on the active server by adding Inclusion Filters.

NOTE vCenter Server Heartbeat forbids replicating certain files and folders by using a veto. If an inclusion filter includes any of those files or folders, the entire filter is vetoed, even if an Exclusion Filter is used to prevent replication of those files and folders. Examples of folders are the vCenter Server Heartbeat installation directory or the system32 folder.

The VMware program folder contains the active server (unsafe) and passive server (safe) queues on the active and passive servers. This folder must be explicitly excluded from file protection.

Automatic Filter Discovery

When Administrators make changes to the configuration, vCenter Server Heartbeat adjusts file filter protection for protected locations. Additionally, the SQL Server Plug-in provides database protection including changes or additions to the database and log files.
Adding a User-Defined Inclusion Filter

To add a user-defined Inclusion Filter

1. Click Advanced > Data.
2. Select the Configuration tab.

You can specify the Inclusion Filter on the Data screen.

File Filters displays three columns: Filter, State, and Detail.

- **Filter** lists the pattern for protecting files and folders on the active server.
- **State** describes the filter state.
  - Effective — The filter has been properly configured and protects (replicates) the stipulated files to the passive server.
  - Subset — contained within another filter
  - Not Effective — not contained within another filter
- **Detail** describes file filter details based upon the state.

To define filters that protect user defined files and folders

1. Click Add Inclusion Filter and then either type the complete path and pattern, specify a pattern containing wildcards, or use Browse to locate the file or folder.
2. Click OK.

The two forms of wildcards available are * which matches all files in the current folder and ** which matches all files, subfolders and the files in the subfolders of the current folder.

After defining the filter, you can add additional Inclusion Filters.

3. To edit file filter definitions, select the filter and click Edit.
Adding a User-Defined Exclusion Filter

Exclusion Filters create a subset of an Inclusion Filter to be excluded from protection.

**To define filters that exclude files and folders from protection and replication**

1. Click **Add Exclusion Filter** and then type the complete path and pattern, specify a pattern containing wildcards, or use **Browse** to locate the file or folder.

2. Click **OK**.

The two forms of wildcards available are * which matches all files in the current folder and ** which matches all files, subfolders and the files in the subfolders of the current folder.

3. To edit file filter definitions, select the filter and click **Edit**.
Removing User-Defined Inclusion/Exclusion Filters

To remove an Inclusion or Exclusion Filter

1. Select the filter.
2. Click Remove.

Configuring Max Disk Usage

The active server (unsafe) and passive server (safe) queues are preconfigured to utilize a maximum space on disk of 1GB. If required, you can adjust the disk space.

1. Go to Advanced > Communications > Configuration and select Max Disk Usage.
2. You might need to increase disk space when queued data requires more space during slow connectivity on VMware Channel.
Reviewing Status of Protected Files

The File Synch and Verify tab allows you to review the status of protected files.

**Figure 9-2. Data Protected Files Status**

The Synchronization Status graphically displays the global status of the file synchronization and verification, with the same seven different states in the System screen.

A tree structure graphically represents the protected files and folders as defined by the file filters. Expand or collapse each level by double-clicking the appropriate folder. The + icon next to a folder indicates that there are subfolders.

The right side displays the subfolders, the protected files within folders and their synchronization status.

The synchronization status for each file may read three different values depending on the verification and synchronization states as described in Table 9-1.

**Table 9-1. Synchronization Status**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>The file has been verified and synchronized successfully.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>The file is not synchronized on the active and passive servers. This state often follows a failover and requires manual synchronization and verification.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>The file or folder has not been checked because a full system check has not been performed or the system check has not yet reached the file or folder.</td>
</tr>
</tbody>
</table>
Determining Effective Filters

An Effective Filter is the result of the remainder of the files/folders stipulated in the Inclusion Filter after removing the files/folders in the Exclusion Filter.

Filters are compared with each other, and if one filter is a superset of another, the superset filter is used. You can configure a single, general filter to replace file servers with 1000s of individual shares requested by a plug-in. The Configuration pane displays rejections after filters are validated before passing to the replication components.

Initiating File Synchronization Manually

The Data screen displays files that have been detected as out of synchronization.

1. To manually synchronize the specified files, click Synchronize.
2. You can resynchronize files at any time. Select multiple files with the Shift or Ctrl keys and click Synchronize.
3. Select Including Subdirectories to synchronize files within folders.

A progress graphic displays the status of the verification or synchronization operation. When complete, the status displays a green Synchronized icon.
Initiating Verify and Synchronize Manually

To verify and synchronize folders

1 Use Verify & Synchronize and select Include Subdirectories to ensure all underlying files and subfolders are included in the verification and synchronization operation.

2 Right-click a folder to access a popup menu to perform quick synchronization and verification of folders and subfolders.

A manually or automatically scheduled synchronization and verification request is defined as a task that is queued for processing after the current task completes. Tasks display in the Pending Tasks pane. You can cancel individual tasks. If you cancel an automatically triggered task, you risk an unchecked system. Possible consequences of canceling tasks display in a warning message.

Initiating a Full System Check

You can verify and synchronize the entire protected file set with Full System Check. A Full System Check performs the same block level check of all the files set by the file filters in the initial startup synchronization and verification.

When you click Full System Check, a window asks you to confirm the request and warns you that depending on the amount of data under protection, this task may take a long time to complete (for example, a number of hours). Click Yes to perform the check.

Switchover cannot occur until the full system check completes and the File System Status is Synchronized.
The File System Status is **Unchecked** when you cancel the task. Depending on the amount of data, resynchronization may take substantial time to complete.

**Figure 9-3. Data Initiate Full System Check**

![Data Initiate Full System Check](image)
Reviewing the Registry Synchronization Status

Registry Synch and Verify allows you to review the status of registry replication.

Figure 9-4. Data Review Registry Synchronization Status

The status of registry synchronization displays in Synchronization Status with the same icons displayed in System.

Full Registry Check rescans and synchronizes all the registry keys matching the built-in registry filters between the servers.
Initiating a Full Registry Check

To initiate a full registry check

1. Go to Data and select Registry Synch and Verify tab.
2. Click Full Registry Check.
This chapter includes the following topics:

- “Configuring Alerts” on page 133
- “Configuring Alert Reporting” on page 134
- “Test Alert Reporting” on page 137
- “Configuring Event Log Files” on page 138
- “Reviewing Event Logs” on page 139

**Configuring Alerts**

vCenter Server Heartbeat can send predefined alerts to remote administrators via email using Advanced > Alerts.

You can configure alerts on the Alerts screen in the Configuration tab.

**Figure 10-1. Alerts Configuration**
You can configure two alert states: Red alerts are critical and yellow alerts are less serious. These alerts are preconfigured with the recommended alerting levels.

To reconfigure each event to trigger red, yellow, or no alert, check the appropriate boxes and click Apply.

To reset the alerts to the last applied changes, click Reset.

### Configuring Alert Reporting

vCenter Server Heartbeat can alert the administrator and route logs via email when an Alert condition exists.

**To configure email alerts**

1. Go to Advanced > System and select the Configuration tab.
2. Enter the outgoing SMTP server of both the Primary server (when active) and the Secondary server (when active) in the appropriate fields.
3. Enter the fully qualified domain name of the mail server. Enter an email address that is authorized to send mail through the SMTP server.
4. If the SMTP servers require authentication to accept and forward SMTP messages, select Mail Server requires authentication and specify the credentials for an appropriate authenticated user account.
5 Click **Apply**. To restore the configuration to the last saved state, click **Reset**.

You can configure email recipients in the **Reporting** tab of the **Alerts** screen after configuring the trigger levels and the email server.

**Figure 10-2. Alerts Reporting**

Red or yellow alert triggers emails to the same or different recipients. The process to add recipients is the same for both trigger levels.

1 Select **Send mail on red alert** or **Send mail on yellow alert**.

2 Click **Add Row** and enter a fully qualified email address for each recipient in each row for the respective trigger level alert.

3 To delete a row, click **Delete row**. To clear a trigger level, click the **Trash can** icon.

Use the preconfigured subject and content of the alert emails for both Red or Yellow alerts. You can add content if necessary. VMware recommends leaving the preconfigured subject and content and if necessary, add additional information.
Another method to send an alert notification is:

1. Select **Run Command** under the pertinent alert state.
2. **Browse** for a script to run or use a command line argument to run on the alert trigger.

   ![Run Command](image)

The preconfigured WScript command creates an event in the Application Event Log and can be customized to include vCenter Server Heartbeat specific informational variables as detailed in **Table 10-1**.

**Table 10-1. Script Variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$EventId</td>
<td>Id of event as listed above</td>
</tr>
<tr>
<td>$EventName</td>
<td>Human-readable name of event</td>
</tr>
<tr>
<td>$EventDetail</td>
<td>Detail message for event</td>
</tr>
<tr>
<td>$EventTime</td>
<td>Time at which event occurred</td>
</tr>
</tbody>
</table>

The following command line argument creates an event in the Application Event Log listing the machine that caused the alert, the time the alert occurred, the name, and details of the alert:

```
WScript //T:10 $(installdir)\bin\alert.vbs "VMware vCenter Server Heartbeat alert on $EventHost at $EventTime because $EventName ($EventDetail). Event Id is $EventId"
```

3. Click **Apply** to save the changes and enforce the defined notification rules.
4. To restore the configuration to the last saved state, click **Reset**.
Test Alert Reporting

Click Test Alert Reporting to run a test alert email. This way you can avoid triggering an actual alert during the operation of the active server.

Figure 10-3. Alerts Testing
Configuring Event Log Files

To configure default settings for log files

1. Select Advanced > Log. The Configuration tab allows you to define the filename and path of the exported comma-separated variable file.

2. You can manually type its path and file name or use Browse and navigate the file. Click Apply.

Configuring Log File Email Recipients

vCenter Server Heartbeat allows you to email the log to specified personnel at predetermined intervals.

To configure logs to be sent via email

1. To configure vCenter Server Heartbeat to email a copy of the log file, select Mail Every, and configure the day and time to send the log file.

2. Specify the recipients. Click the Add Row icon on the top left of the email recipient data grid and type the email address in the row.

3. To remove a recipient, select the row and click the Delete selected row icon on the top left of the data grid.

4. To clear the entire data grid, click the Trash can icon.

5. You can configure additional features for event logs in the main Configuration screen.
To override multiple logs generating for a single event, select Ignore Repeated Events Within and set the time increment to ignore the duplication.

To adjust the length of the event log list, use Record At Most. The default is to record 100 events but you can change the value accordingly.

Click Apply to commit the changes.

Click Reset to restore the previously applied log configuration. Reset does not affect the logs already recorded in the list.

Reviewing Event Logs

The Log Details data grid lists events logged chronologically by default.

Figure 10-4. Log View Events

The logs show the time the event happened, its importance, the type of event that triggered the log, and its detail.

The data grid displays truncated information.
To review the details

1. Double-click the entry in the data grid.

![Event Properties](image)

**Event Properties** displays the full detail and trace of the log that caused the event and the source of the error to aid in troubleshooting.

2. Use the **Up** and **Down** arrows in this window to review other logs. This feature is useful where many logs have occurred simultaneously and helps to identify the source of the problem.

3. Click **Close** to close the **Event Properties**.

**Table 10-2. Log Events**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Error" /></td>
<td>Errors within the underlying operation of vCenter Server Heartbeat and can be considered critical to the operation of the system.</td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td>Warnings generated for discrepancies within the vCenter Server Heartbeat operational environment that are not deemed critical to the operation of the system.</td>
</tr>
<tr>
<td><img src="image" alt="System" /></td>
<td>System logs generated following normal vCenter Server Heartbeat operations allow you to check the success of processes such as file synchronization.</td>
</tr>
<tr>
<td><img src="image" alt="Information" /></td>
<td>Information on operations within the graphical user interface rather than operations on vCenter Server Heartbeat service, such as log in.</td>
</tr>
</tbody>
</table>

To display logs according to severity

1. Select **Events of at Least**.

2. Select the importance level and click **Apply**. Logs above the selected severity are displayed.

![Log Display](image)

You can filter logs to display a subset of logs between a specific date and time range.
3 Select **Events From**, adjust the start date, end date, and time, and then click **Apply**.

4 Click **Reset** to remove and reset the filter criteria.

<table>
<thead>
<tr>
<th>Table 10-3. Log Configuration Icons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Icon</strong></td>
</tr>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon" /></td>
</tr>
</tbody>
</table>
This chapter includes the following topics:

- “Troubleshooting Unexpected Behaviors” on page 143
- “Two Active Servers” on page 143
- “Two Passive Servers” on page 145
- “Synchronization Failures” on page 146
- “Registry Status is Out of Synch” on page 148
- “Channel Drops” on page 148
- “Subnet or Routing Issues” on page 152
- “MaxDiskUsage Errors” on page 152
- “MaxDiskUsage Error Messages” on page 153

Troubleshooting Unexpected Behaviors

The following unexpected behaviors illustrate symptoms, causes and resolution for a given scenario.

Two Active Servers

When two identical active servers are live on the same network, vCenter Server Heartbeat refers to the condition as Split-brain syndrome. Two active servers do not occur by design and when detected, must be resolved immediately.

Symptoms

Split-brain syndrome is identified by the following symptoms:

- Both servers in the pair are running and in an active state. The task bar icons display P / A (Primary and active) and S / A (Secondary and active).
- An IP address conflict occurs on a server pair running vCenter Server Heartbeat on the Principal (Public) IP address.
- A name conflict occurs on a server pair running vCenter Server Heartbeat. In a WAN environment the Primary and Secondary servers connect to the network using different IP addresses. However, if the servers are running with the same name and are visible to each other across the WAN, then a name conflict occurs.
- Clients (for example, Outlook) cannot connect to the server running vCenter Server Heartbeat.
Causes
The most common causes of two active servers (Split-brain syndrome) are as follows:
- Loss of the VMware Channel connection (most common in a WAN environment)
- The active server is too busy to respond to heartbeats.
- Misconfiguration of the vCenter Server Heartbeat software

You must determine the cause of the Split-brain syndrome and resolve the issue to prevent this condition from recurring.

Resolution
To resolve a Split-brain syndrome, identify the server with the most up-to-date data. If you identify the wrong server you risk losing data. You must reinstate the correct server.

To identify the server with the most up-to-date data
1. Check the date and time of files on both servers. Make the most up-to-date server the active server.
2. From a client PC on a LAN, run nbtstat –A 192.168.1.1 where the IP address is the Principal (Public) IP address of the server. This can help identify the MAC address of the server currently visible to client machines.

**NOTE** If the two active servers have both been servicing clients, perhaps at different WAN locations, you can make only one server active. Both servers contain recent data that cannot be merged using vCenter Server Heartbeat. To restart replication, make one server active and one server passive. When replication restarts, the active server overwrites all data on the passive server. You can manually extract the up-to-date data from the passive server prior to restarting replication. Consult the Microsoft knowledge Base for information on various tools for this purpose. For further information, contact your VMware support representative.

To resolve two active servers (Split-brain syndrome)
1. Identify the server with the most up-to-date data or the server to make active.
2. Shut down vCenter Server Heartbeat on both servers if it is running.
3. On the server to make passive, right-click the Task bar icon, and select the Server Configuration wizard.
4. Go to the Machine tab and set the server role to passive. Do not change the identity of the server, example, Primary/Secondary.
5. Click Finish to accept the changes.
6. Reboot this server.
7. Start vCenter Server Heartbeat, if required, and check that the Task bar icon now reflects the changes by showing P / - (Primary and Passive) or S / - (Secondary and Passive).
8. On the active server, right-click the Task bar icon and select the Server Configuration wizard.
9. Select the Machine tab and check the server role is set to active. Do not change the identity of the server, example, Primary/Secondary.
10. Click Finish to accept the changes.
11. Reboot this server. As the server restarts, it connects to the passive server and starts replication. The active server overwrites data on the passive server.
12. Start vCenter Server Heartbeat, if required, and check that the Task bar icon now reflects the changes by showing P / A (Primary and active) or S / A (Secondary and active).
13. Log in to the vCenter Server Heartbeat Console.
14. Check that the servers have connected and replication has started.
Two Passive Servers

Primary and Secondary servers are both passive at the same time. This situation is serious and must be resolved immediately.

Symptom

You are unable to connect to protected applications, and if you configured alerts, you receive notification that replication is not functioning properly.

Causes

The condition of two passive servers results from a sudden failure on the active server. Examples:

- An unexpected termination of the VMware vCenter Server R2 service
- A transient power failure
- A server reset triggered from the Power or Reset button
- An unclean shutdown. Following an unclean shutdown, an active server automatically assumes the passive role to isolate itself from the network until the failure is investigated.

- The active server fails before the handshake that establishes the VMware Channel connection. The passive server cannot detect that the active server is not responding when the failure occurs and cannot determine the condition of the active server. The active server suffers a transient failure and the passive server cannot respond by failing over into the active role, leaving both servers in the passive role.

- Both Primary and Secondary servers experience a power outage simultaneously, for example, they use the same power source and neither is attached to a UPS. A failover cannot occur and when the servers are rebooted, each displays the following error message:

  Cannot start replication because previous run did not shutdown properly. Check configuration.

NOTE If you attempt to start vCenter Server Heartbeat without reconfiguring one server in the pair as active, vCenter Server Heartbeat responds with the following warning:

[U16] Serious configuration mismatch between the two servers. Please reconfigure so there is one and only one Primary, and one and only one Active.

Resolution

Two passive servers prevent users from accessing the protected application and should be resolved immediately.

To resolve two passive servers

1. Determine the active server.
2. Shut down vCenter Server Heartbeat on both servers. Leave any protected applications running on the server to make active.
3. On the server to make active, start the Server Configuration wizard, and select the active role. Do not change the identity (Primary / Secondary).
4. On the server to make passive, start the Server Configuration wizard, and confirm the passive server. Do not change the identity (Primary / Secondary).
5. Reboot the passive server. All protected application services stop.
6. Start vCenter Server Heartbeat on both servers.
Synchronization Failures

When you start vCenter Server Heartbeat, a full system check occurs to verify the following:

- All protected registry keys and values from the active server are present on the passive server.
- All protected file and folder structures from the active server are present on the passive server.

After the full system check completes, the File System Status and the Registry Status display as **Synchronized**. However, the File System Status or the Registry Status can also display as **Out of synch** or **Synchronized and busy processing**. Some of the cases are described with possible causes and workarounds.

### Services Running on the Passive Server

Services running on a passive server is not normal behavior and can prevent synchronization.

**Symptom**

File System Status is **Out of synch** or **Synchronized and busy processing**.

**Cause**

A service running on the Passive server opens a protected file for exclusive access. If vCenter Server Heartbeat attempts to update this opened file, the Apply component logs the following error message:

[N29] The passive VMware vCenter Server Heartbeat server attempted to access the file: [filename]. This failed because the file was in use by another application. Please ensure that there are no applications which access protected files running on the passive.

**NOTE** This will occur if the Virtual Infrastructure Client is left running on the passive server.

Services that keep files locked on the passive server are:

- Protected application services
- File-level anti-virus tool services

**NOTE** vCenter Server Heartbeat will periodically check for and stop any services found to be running on the passive server.

**Resolution**

Until the file is closed on the passive server, vCenter Server Heartbeat reports the file status and the File System Status as **Out of synch**.

**To resolve the Out of synch status**

1. Set Protected Application services to **Manual** on both servers and verify that they are not running on the passive server.
2. Set Recovery Actions to **Take No Action**. You can set this from the Service Control Manager (SCM) for the Protected Application services. Otherwise, the SCM restarts the Protected Application services.
3. Verify that file-level anti-virus is not part of the protected set as the file-level anti-virus and the corresponding services are running on both machines.

### VMware Channel Incorrectly Configured

If the VMware Channel is not properly configured, it cannot initiate the handshake to establish communications through the VMware Channel connection.

**Symptom**

Failure to establish the VMware Channel connection prevents a full system check, thereby leaving the File System Status and Registry Status as Out of Synch.
Chapter 11 Troubleshooting

Causes
The most common VMware Channel configuration errors are as follows:

- VMware vCenter Server Heartbeat Packet Filter is enabled on one or more VMware Channel NICs.
- VMware Channel IP addresses are configured in different subnets.
- In a WAN implementation, no static routes exist between the VMware Channel NICs.

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

To resolve a VMware Channel configuration error
1. Disable the VMware vCenter Server Heartbeat Packet Filter on VMware Channel NICs.
2. Configure the VMware Channel IP addresses properly.
3. In a WAN implementation, configure static routes between VMware Channel NICs properly.
4. Disable NetBIOS on the VMware Channel NICs.

Incorrect or Mismatched Disk Configuration

When vCenter Server Heartbeat starts, it checks the complete set of file filters for consistency.

Symptom
If any of the entries points to a non-existent drive letter or to a non-NTFS partition, the list of file filters resets to the default value of C:\Protected\**. This is a safety measure as vCenter Server Heartbeat requires the same drive letter configuration on the Primary and the Secondary servers, and only supports protection of NTFS partitions.

Cause
Different partition structures on Primary and Secondary servers, such that one or more file filters point to drives which cannot be protected on both servers. For example:

- The Primary server has drive G, which is a valid NTFS partition. There is no corresponding drive on the Secondary server.
- The Primary server has drive G, which is a valid NTFS partition. The equivalent drive on the Secondary server is a CD / DVD drive or a FAT / FAT32 partition, which cannot be protected.

In either case, if you configure a file filter to protect a directory on drive G, the entire filter set is rejected and the filters are reset to the default value of <Windows drive>\Protected\**.

Resolution
Follow the steps documented in Knowledge Base article 1008458 (vCSHB-Ref-500) Troubleshooting a set of File Filters that is reset to C:\Protected\**.

 Passive Server Has Less Available Space than Active Server

Inadequate available disk space on the passive server can cause replication to cease.

Symptom
Replication stops with the following error:

[N27]Failed to write information for the file: [filename] to the disk. Either the disk is full or the quota (for the SYSTEM account) has been exceeded.
**Cause**
The passive server has less available disk space than the active server, preventing updates from being replicated to the passive server. The quantity of updates from the active server exceeds the passive server's available disk space.

**Resolution**
Free up some additional disk space on the passive server. Do not delete data from the protected set as you might lose data in the event of a switchover. You might need to update the disk subsystem on the passive server. After allocating space, start replication.

**Registry Status is Out of Synch**
The Registry may be reported as Out Of Synch when one or more Registry keys fail to synchronize.

**Resource Issues**
Inadequate resources can cause poor performance and prevent the registry from synchronizing.

**Symptom**
vCenter Server Heartbeat logs the following error message:

*Call to RegOpenKeyEx failed: on *<Reg_Key>*/: Insufficient system resources exist to complete the requested service.*

**Cause**
One or both of the servers are running low on virtual memory.

**Resolution**
Restart the server to free up virtual memory.

**Registry Security Issues**
Inability to access the registry will prevent replication of the registry.

**Symptom**
vCenter Server Heartbeat is unable to read, sync, or replicate the registry.

**Cause**
If a protected registry key has permissions that deny Write access to the System account, vCenter Server Heartbeat might be unable to synchronize or replicate it.

**Resolution**
Change the permissions on the affected registry key to grant the System account Full Control.

**Channel Drops**
When the VMware Channel loses connection between the servers, the following scenarios might occur.

**Performance Issues**
Poor performance may be experienced as a result of a channel loss.
Symptom
The message `java.io.IOException: An existing connection was forcibly closed by the remote host` appears in the active server’s NFLog.txt file, and the VMware Channel connection between the servers is lost.

Causes
This unusual condition points to an application or Windows experiencing a fault on the passive server. A sudden reboot of the passive server might occur due to the following causes:

- The server is configured for automatic software update management and some updates force a server reboot.
- A software or Operating System issue that occasionally fails and requires a system restart.
- The Neverfail Server R2 service experiences problems, does not respond, or terminates unexpectedly.

Resolution
To resolve the issue, make the following checks.

- Determine the likely source by examining the Windows event logs.
- If the server does not display evidence of a system restart or unresponsive application, one or both of the VMware Channel NICs might be forcing a channel disconnection. See “Hardware or Driver Issues on VMware Channel NICs” on page 149 for more information on this topic.

Passive Server Does Not Meet Minimum Hardware Requirements
Inadequate hardware can cause channel drops and result in poor performance.

Symptom
The data rate between the servers is very high during a Full System Check and the VMware Channel drops.

Cause
The passive server does not meet the recommended hardware requirements for vCenter Server Heartbeat or it meets the requirements, but is much less powerful than the active server. The underpowered server cannot apply the received replication data from the active server at the rate that the data is sent to the passive server.

Resolution
To avoid reinstalling vCenter Server Heartbeat, upgrade the hardware, such as memory or CPU, on the passive server. Establish the identity (Primary or Secondary) of the affected server before you perform the upgrade.

Hardware or Driver Issues on VMware Channel NICs
NIC malfunctions and old or incorrect drivers can cause channel drops resulting in poor performance.

Symptom
The VMware Channel drops or disconnects and reconnects intermittently.

Causes
The following are common causes of NIC problems.

- Old or incorrect VMware Channel NIC drivers
- Hardware failure of the hub or Ethernet switch used for the VMware Channel connection
- Defective Ethernet patch or crossover cables
Improper configuration of the NICs used for the VMware Channel connection

ISP problems in a WAN environment

Resolution
When a NIC problem is encountered, the following should be checked.

- Verify that VMware Channel NIC drivers are the correct and latest versions. Known issues are identified with HP/Compaq ProLiant NC67xx/NC77xx Gigabit Ethernet NICs. Check other NIC types. See Knowledge Base article 1008383 (vCSHB-Ref-116) – VMware vCenter Server Heartbeat and Gigabit Ethernet NIC drivers. (NC77XX).

- Verify hubs and Ethernet switches are operating properly. Identify and replace any defective components.

- Test for defective Ethernet patch or crossover cables and replace if defective.

- Correctly configure the NICs used for the VMware Channel connection.

- Check the physical link for ISP problems.

Firewall Connection
In a LAN or WAN deployment, the VMware Channel may be connected via one or more Internet firewalls. Since firewalls block unauthorized network traffic, configure firewalls on the route of the VMware Channel to allow channel traffic.

Symptoms
The VMware Channel cannot connect, or connects and disconnects continuously.

Causes
In a WAN deployment, port 57348 or any other port configured for the VMware Channel is closed on one or more firewalls on the route between the VMware Channel NIC on the Primary server and its counterpart on the Secondary server.

Resolution
Open port 57348 and any other port configured for the VMware Channel on all firewalls on the route between the VMware Channel NIC on the Primary server and its counterpart on the Secondary server.

Incorrect VMware Channel Configuration
An incorrectly configured channel connection can prevent proper communication and replication.

Symptoms
The following problems are experienced.

- IP conflicts occur on one of the VMware Channel IP addresses.

- The VMware Channel does not connect, or connects and disconnects.

Causes
The list below provides the most common misconfigurations.

- Identical IP addresses at each end of the VMware Channel

- IP addresses in different subnets without static routing at each end of the VMware Channel

- VMware Channel NIC configured for DHCP when a DHCP server is not available.
During installation, vCenter Server Heartbeat configures the VMware Channel NICs with user-provided information. Incorrect information or incorrectly modifying the VMware Channel NIC configuration after installation causes the VMware Channel to fail communicating.

On rare occasions, if the Primary and Secondary servers have NICs of the same type in a different order, both the name and IP address of a VMware Channel NIC on the Primary server might transfer to the Principal (Public) NIC on the Secondary or the name and IP address of the Principal (Public) NIC might transfer to a VMware Channel NIC. Similarly, the names of the VMware Channel NICs might reverse on the Secondary server. You must then reconcile the names of the NICs with their physical identities and assign the correct IP address to each NIC on the Secondary server.

**Resolutions**

The installation process manually assigns the correct IP addresses to each NIC on the Secondary server. If no VMware Channel connection occurs between the servers, verify the configuration of the IP addresses on the Secondary server's channel NICs. Check the settings for the Principal (Public) NIC. The configuration error might not be apparent until you perform a switchover or a failover occurs.

To capture the identities of all of the NICs on the Secondary server prior to installing vCenter Server Heartbeat, open a Windows Command Prompt on that server and execute the following command:

```
ipconfig /all > ipconfig.txt
```

The output of this command saves the current name, TCP/IP configuration, and MAC address of each NIC on the Secondary server to a file called ipconfig.txt, which is present on that server after the Plug and Play phase of the vCenter Server Heartbeat install completes. Compare the pre-install and post-install state of each NIC by running `ipconfig /all` from a Windows command prompt and compare the output of this command with the content of ipconfig.txt.

The MAC address of each NIC is connected to the physical identity of each card and never changes. You can identify each NIC by its MAC address and determine its original name and network configuration, even if they have been updated by the Plug and Play process.

**VMware vCenter Server Heartbeat Packet Filter Is Enabled on the Channel NIC(s)**

Proper configuration requires that the packet filter be disabled on the VMware Channel NIC. When the packet filter is enabled on the channel NICs, the following symptoms are encountered.

**Symptom**

Interference with network traffic across the VMware Channel results in an intermittent channel connection or no channel connection at all.

**Cause**

During installation, the VMware vCenter Server Heartbeat Packet Filter is automatically installed and enabled on all NICs on both the Primary and Secondary servers. The Packet Filter on the VMware Channel NICs on each server is disabled later in the installation of vCenter Server Heartbeat. If the vCenter Server Heartbeat Packet Filter is left enabled on one or more channel NICs after installation completes, it might interfere with network traffic across the VMware Channel.

**Resolution**

In the Properties tab for each Channel NIC on both servers, verify that the check box for vCenter Server Heartbeat Packet Filter is not selected, so that the Packet Filter is disabled on that NIC.
Subnet or Routing Issues

In a LAN or WAN deployment, the following connection problems might occur.

**LAN Deployment**

Incorrectly configured subnets or routing can cause channel problems resulting in poor performance or failure to connect.

**Symptom**

The Channel disconnects or fails to connect in a LAN deployment.

**Causes**

The Channel might disconnect or fail to connect due to the Principal (Public) NIC and/or one or more channels sharing the same subnet.

**Resolution**

If vCenter Server Heartbeat is deployed in a LAN environment, the Principal (Public) IP address and the Channel IP address on a server must be in separate subnets. If there are multiple redundant channels, each must have its own subnet. Check the network configuration for each NIC on both servers in the pair and correct any issues.

**WAN Deployment**

Incorrect routing can prevent the active and passive servers from connecting in a WAN environment.

**Symptom**

The VMware Channel disconnects or fails to connect in a WAN deployment.

**Cause**

When the VMware Channel disconnects or fails to connect in a WAN deployment, it might be due to not having a static route configured or configured incorrectly.

When vCenter Server Heartbeat is deployed in a WAN, the Principal (Public) IP address and the VMware Channel IP addresses cannot be in different subnets, since there is usually a single network path between the two servers. Configure a static route between the endpoints to route traffic in the VMware Channel.

**Resolution**

Refer to Knowledge Base article 1008451 (vCSHB-Ref-466) - Creating a static route for the VMware Channel Connection Where the Channel and Principal (Public) IP Addresses are on the Same Subnet in a WAN Environment for a detailed discussion about WAN channel routing issues, and for instructions on how to configure a static route for the VMware Channel.

**MaxDiskUsage Errors**

vCenter Server Heartbeat uses queues to buffer the flow of replication data from the active server to the passive server. This configuration provides resilience in the event of user activity spikes, VMware Channel bandwidth restrictions, or VMware Channel drops which might occur in a WAN deployment. Some types of file write activity may also require buffering as they may cause a sharp increase in the amount of channel traffic. The queues are called the active server (unsafe) queue or the passive server (safe) queue.
Active Server (Unsafe) Queue

vCenter Server Heartbeat considers the active server queue as unsafe because the data in this queue has not yet been replicated across the VMware Channel to the passive server and may therefore be lost in the event of a failover. As a result of failover, some data loss is inevitable, with the exact amount depending on the relationship between current VMware Channel bandwidth and the required data transmission rate. If the required data transmission rate exceeds current VMware Channel bandwidth, the active server queue fills; if the current VMware Channel bandwidth exceeds the required data transmission rate, the active server queue empties. This situation is most commonly seen in a WAN environment, where VMware Channel bandwidth may be restricted. In a LAN that normally has high bandwidth on a dedicated channel, the size of the active server queue is zero or near zero most of the time. On a server not protected with vCenter Server Heartbeat, all data is technically unsafe and it is possible to lose all data if the server fails.

Passive Server (Safe) Queue

The passive server queue is considered safe because the data in this queue has already been transmitted across the VMware Channel from the active server, and is not lost in the event of a failover, which applies all updates to the passive server as part of the process.

Both active and passive server queues are stored on disk by default in the <VMware vCenter Server Heartbeat Install Directory>\R2\log directory, with a quota configured for the maximum permitted queue size (by default, 1 GB on each server). You can configure both the queue location and the quota.

Two methods to set the queue size:

- Start vCenter Server Heartbeat, open the vCenter Server Heartbeat Console, and select Advanced > Communication > Configuration. Set the Max Disk Usage value and click Apply. Shut down and restart vCenter Server Heartbeat for the change to take effect. You do not need to stop protected applications.
- Open the Server Configuration wizard and select the Logs tab. Set the Maximum Disk Usage value and click Finish.

**NOTE** vCenter Server Heartbeat is a symmetrical system and can operate with either server in the active role. For this reason, the queue size is always set to the same value for both servers.

MaxDiskUsage Error Messages

The following error messages may be seen when available disk space on the servers is exceeded.

[L9]Exceeded the Maximum Disk Usage
(VCChannelExceededMaxDiskUsageException)

This message indicates that you have exceeded the amount of allocated disk space reserved for the queue.

**Symptom**

vCenter Server Heartbeat exceeds its preconfigured queue size.

**Causes**

On the active server, the size of the active server queue has exceeded the disk quota allocated for it. On the passive server, the size of the passive server queue has exceeded the disk quota allocated for it.

**Resolution**

While neither condition is critical, determine the sequence of events that led to the condition.
Exceeded the Maximum Disk Usage on the ACTIVE Server

This message indicates that you have exceeded the amount of allocated disk space reserved for the active server (unsafe) queue.

Symptom
Replication stops and the vCenter Server Heartbeat Event Log displays the error message originating from the active server.

Causes
A temporary interruption in the VMware Channel or insufficient VMware Channel bandwidth to cope with the current volume of replication traffic starts filling the active server queue. The size of the queue eventually exceeds the configured disk quota.

Resolution
Assuming there are no other channel connection issues (see Knowledge Base article 1008551 (vCSHB-Ref-992) - Troubleshooting VMware vCenter Server Channel Drops) you can increase the amount of disk space allotted to the queues. The default setting is 1 GB, which might be insufficient on servers with a large volume of replication traffic and limited VMware Channel bandwidth. If you have sufficient disk space, set the queue size to zero (unlimited). This allows vCenter Server Heartbeat to utilize any free disk space to store the queues.

Exceeded the Maximum Disk Usage on the PASSIVE Server

This message indicates that you have exceeded the amount of allocated disk space reserved for the passive server (safe) queue.

Symptom
Replication stops and the vCenter Server Heartbeat Event Log displays the error message originating from the passive server.

Causes
Two of the most common causes are shown below.

- The bottleneck lies between the VMware Channel NIC and the disk subsystem on the passive server. Replication traffic passes across the VMware Channel faster than it can be written to disk on the passive server. It is buffered temporarily in the passive server (safe) queue. The size of the queue can eventually exceed the allotted disk quota.

- If the passive server is much less powerful than the active server in terms of processor speed, RAM, or disk performance, it may lag behind the active server during periods of high replication activity. Monitor one or more Windows performance counters to determine the component experiencing sustained high activity. Intensive page file use or persistently large disk queue length might indicate a problem. Upgrade one or more physical components of the server.

Either server can be active or passive. If the Secondary server is more powerful than the Primary server, hardware-related issues might only occur while the Secondary server is in the active role.

Resolution
To resolve this issue:

- If you have multiple physical disks on each server, locate the vCenter Server Heartbeat active and passive server queues on a separate physical disk, away from the Windows directory, the Windows page file, and any protected files help to alleviate disk performance issues:
  a. Shut down vCenter Server Heartbeat.
  b. Open the Server Configuration wizard and select the Logs tab.
c  Set the path for **Message Queue Logs Location** and click **Finish**.

d  Start vCenter Server Heartbeat on both servers.

The selected path is applied to all vCenter Server Heartbeat queues on both servers.

- Increase the amount of disk space allotted to the queues. However, if a hardware issue is the root of the problem, correct that problem at the source.

- The size of the passive server queue can increase sharply in response to certain types of file write activity on the active server, such as when vCenter Server Heartbeat is replicating a large number of very small updates of a few bytes each. The volume of update traffic might be far greater than the physical size of the files on the disk, and the passive server queue might become disproportionately large. You can see this pattern of disk activity during the population of Full-Text Catalogs in Microsoft SQL Server. Increase the amount of disk space available for the queues. Move the queues to their own physical disk, upgrade the memory or the disk subsystem.

- vCenter Server Heartbeat requires a certain amount of system resource for its own basic operations and requires some additional resources for processing replication traffic. This is in addition to the resources used by Windows and other applications running on the server, including critical applications protected by Heartbeat. Allocate sufficient resources for all the applications and services running on such a server to provide maximum performance, stability, and resilience for changing client, server, and network activity.

[L20] **Out of Disk Space (VCChannelOutOfDiskSpaceException)**

This message indicates that one of the servers in the pair has run out of disk space without reaching its preset quota.

**Symptom**

Replication stops and the vCenter Server Heartbeat Event Log displays the error message originating from either server in the pair.

**Cause**

One of the queues has exceeded the amount of physical disk space available for it without reaching its quota limit. For example, if the maximum queue size is set to 5 GB, but only 3 GB of physical disk space remains, this error message is reported if one of the queues exceeds 3 GB in size.

**Resolution**

Free up more disk space or move the queues to a disk with sufficient free space to accommodate queue sizes up to the limit configured for Maximum Disk Usage.

**Application Slowdown**

Operations performed by the application might take longer to complete, and in turn, might affect the time required to log in to a remote client, or to open or save a file. This is true for both servers running vCenter Server Heartbeat and for servers running any other application. vCenter Server Heartbeat can monitor system performance counters and display warnings when predefined thresholds are exceeded, but it does not actively manage system resources for other applications. Like any other application, it also requires a finite amount of resources for its own operations in addition to the resources used by the operating system and the protected application.

The machines hosting vCenter Server Heartbeat must meet recommended hardware requirements and must be powerful enough to cope with the load, the protected applications, and any other critical applications running on the same server pair.
Poor Application Performance

When applications are competing for resources, one or more applications might perform poorly.

Symptom

Neither server in the pair can accommodate the load placed upon it during normal operation.

Cause

The Primary server’s resource usage in one or more areas reached close to the maximum before vCenter Server Heartbeat was installed.

Resolution

Heartbeat Diagnostics can report these conditions and issues warnings if CPU usage or memory usage exceed a certain percentage of the available resource. Information provided by Heartbeat Diagnostics can minimize the risk of application slowdown by identifying needed hardware upgrades on the Primary server.

Both Servers Can Accommodate the Initial Load but the Load Has Increased

Any software installed on a server or workstation consumes a finite amount of system resources when it runs and it must share the resources it uses with any other applications running at the same time. Higher demand caused by additional user activity can have an impact on the server performance.

Symptom

Increased user activity slows application response time.

Causes

The server pair might operate normally when vCenter Server Heartbeat is first installed, then decrease performance due to increased user activity. For example, users on the SQL Server system increase or the typical usage pattern becomes more intense. This might be a gradual and sustained increase over time, or it may be transient if a specific event triggers a temporary surge in user activity.

Resolution

If the situation is sporadic, it can correct itself when the load decreases. If the increase is sustained and permanent, upgrade the server hardware.

One Server is Able to Cope, but the Other Cannot

If the total resource requirements of the applications exceed the available physical resources, the operating system attempts to provide resources, but some applications might be under resourced—an application cannot obtain enough memory to operate normally, or a process needs to wait before accessing the hard disk

Symptom

Applications operate normally when the Primary server is active but operate slowly when the Secondary server is active or vice versa.

Cause

A large discrepancy occurs in the processing power between the Primary and Secondary servers. One server can handle the operational load while the other cannot. The load on a server is higher when it is in the active role when the protected application starts. Applications on the server pair run successfully when the Primary server is active, but might experience performance issues when the Secondary is active (or vice-versa). Problems might arise even when the more powerful server is active.
Resolution
Both servers must have approximately equivalent processing power, RAM and disk performance. Upgrade the hardware on one server in the pair so that the two servers have roughly the same performance.

Scheduled Resource Intensive Tasks
Scheduling multiple resource intensive tasks at the same time can adversely impact server performance and affect application performance.

Symptom
Resource‐intense scheduled tasks impact performance at certain times.

Cause
Two or more resource‐intense processes run simultaneously or one process may perform actions that increase the load on vCenter Server Heartbeat by triggering additional and sometimes unnecessary replication traffic. Examples: processes such as backups, database maintenance tasks, disk defragmentation, or scheduled virus scans.

Resolution
Schedule operations so that they do not overlap and schedule them outside regular working hours, when the load imposed on the server by users accessing the protected application is likely to be smaller.
## Appendix: Setup Error Messages

### Table A-1. Setup Error Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Pri</th>
<th>Sec</th>
<th>Level</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 – ‘The pre install check data file does not have the correct format. Setup cannot continue’.</td>
<td>No</td>
<td>Yes</td>
<td>Critical Stop</td>
<td>Check that the file adheres to the correct formatting / structure for use in analysis on the Secondary.</td>
</tr>
<tr>
<td>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.</td>
<td>No</td>
<td>Yes</td>
<td>Critical Stop</td>
<td>Check that the analyzer and collector dlls are compatible.</td>
</tr>
<tr>
<td>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.</td>
<td>-</td>
<td>Yes</td>
<td>Critical Stop</td>
<td>Check file format is correct.</td>
</tr>
<tr>
<td>190 - This server is a #1# domain controller. vCenter Server Heartbeat must not be installed on a domain controller.</td>
<td>Yes</td>
<td>Yes</td>
<td>Critical Stop</td>
<td>Test whether the server is a domain controller.</td>
</tr>
<tr>
<td>175 -- vCenter Server Heartbeat requires Windows 2003 Standard Edition SP1 or later if '/3GB' switch is on.</td>
<td>Yes</td>
<td>Yes</td>
<td>Critical Stop</td>
<td></td>
</tr>
<tr>
<td>103 - vCenter Server Heartbeat does not support #1#. The following are supported Windows 2000 Server SP4 or greater; Windows Server 2003 SP1 or greater.</td>
<td>Yes</td>
<td>Yes</td>
<td>Warning</td>
<td></td>
</tr>
<tr>
<td>200 - Your #1# server uses the Intel ICH7 chipset and Windows 2000 has been detected. This combination is incompatible with vCenter Server Heartbeat.</td>
<td>Yes</td>
<td>Yes</td>
<td>Critical Stop</td>
<td></td>
</tr>
<tr>
<td>217 - vCenter Server Heartbeat is not supported on Windows Storage Server Edition.</td>
<td>Yes</td>
<td>Yes</td>
<td>Warning</td>
<td></td>
</tr>
<tr>
<td>106 - Primary and Secondary OS versions are not identical, #1# vs. #2#: and require the same Service Pack level.</td>
<td>-</td>
<td>Yes</td>
<td>Critical Stop</td>
<td>Compatibility check on secondary.</td>
</tr>
<tr>
<td>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.</td>
<td>-</td>
<td>Yes</td>
<td>Critical Stop</td>
<td>Compatibility check on secondary.</td>
</tr>
<tr>
<td>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#.</td>
<td>-</td>
<td>Yes</td>
<td>Critical Stop</td>
<td>Compatibility check on secondary.</td>
</tr>
<tr>
<td>113 - You do not have enough total memory to install vCenter Server Heartbeat on your #1# server. You must have at least 1 GB.</td>
<td>Yes</td>
<td>Yes</td>
<td>Critical Stop</td>
<td></td>
</tr>
</tbody>
</table>
VMware recommend a minimum of 2 GB. Note actual memory requirements depend on the application load; and may require more memory.

Note actual memory requirements depend on the application load; and may require more memory.

<table>
<thead>
<tr>
<th>Message</th>
<th>Pri</th>
<th>Sec</th>
<th>Level</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>117 - You do not have enough free disk space to install vCenter Server Heartbeat. You must have at least 2 GB available.</td>
<td>Yes</td>
<td>Yes</td>
<td>Warning</td>
<td>Compatibility check on secondary.</td>
</tr>
<tr>
<td>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.</td>
<td>-</td>
<td>Yes</td>
<td>Warning</td>
<td>Compatibility check on secondary.</td>
</tr>
<tr>
<td>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'</td>
<td>Yes</td>
<td>Yes</td>
<td>Critical Stop</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>Yes</td>
<td>Yes</td>
<td>Critical Stop</td>
<td></td>
</tr>
<tr>
<td>201 - #1#: This service is incompatible with running vCenter Server Heartbeat and must be stopped before vCenter Server Heartbeat can be installed.</td>
<td>Yes</td>
<td>Yes</td>
<td>Warning</td>
<td></td>
</tr>
<tr>
<td>209 - Double-Take drivers have been detected on this server. To avoid compatibility problems please uninstall Double-Take before re-running setup.</td>
<td>Yes</td>
<td>Yes</td>
<td>Critical Stop</td>
<td></td>
</tr>
<tr>
<td>Oracle has been detected on this Server. vCenter Server Heartbeat does not support Oracle on the same server as VirtualCenter.</td>
<td>Yes</td>
<td>Yes</td>
<td>Critical Stop</td>
<td>It is recommended that you move Oracle to another server before attempting to re-run Setup, OR that you move VirtualCenter to another server and deploy vCenter Server Heartbeat there</td>
</tr>
</tbody>
</table>
Glossary

A

Active
The functional state or role of a server visible through the network by clients running protected applications and servicing client requests.

Alert
A notification sent to a user or entered into the system log indicating an exceeded threshold.

Active Directory (AD)
Presents applications with a single, simplified set of interfaces allowing users to locate and use directory resources from a variety of networks while bypassing differences among proprietary services. vCenter Server Heartbeat switchovers and failovers require no changes to AD, resulting in switchover and failover times measured in seconds.

Active – Passive
The coupling of two servers: one server visible to clients on a network and providing application service, the other server not visible and not providing application service.

Active Server Queue
The staging area of the active server used to store intercepted data changes before being transported across the VMware Channel to the passive server.

Advanced Configuration and Power Interface (ACPI)
A specification that dictates how the operating system can interact with hardware using power saving schemes. Primary and Secondary servers must have the same ACPI compliance.

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

B

Basic Input/Output System (BIOS)
The program a personal computer’s microprocessor uses to start the computer system after you turn it on. It also manages data flow between the computer’s operating system and attached devices such as the hard disk, video adapter, keyboard, mouse, and printer.

C

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

Channel Drop
An event in which the dedicated communications link between the Primary and Secondary server fails, often resulting in the passive server becoming active and consequently creating a split-brain syndrome.
Channel NIC (Network Interface Card)
A dedicated subnet used by the VMware Channel.

Cloned Servers
Two servers in a pair with the same configuration settings, names, applications, Security Identifiers (SIDs) and IP addresses, following the installation of vCenter Server Heartbeat.

Cloning Process
The vCenter Server Heartbeat process whereby all installed programs, configuration settings, the machine name, security identifier (SID), and IP address are copied to a second server.

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

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

Device Drivers
A program that controls a hardware device, linking it to the operating system.

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

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

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

Domain Controller (DC)
The server responsible for maintaining privileges to domain resources, sometimes called AD controller in Windows 2000 and above domains.

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

Full System Check (FSC)
The internal process automatically started at the initial connection of a server pair or manually triggered through the vCenter Server Heartbeat Console. The FSC verifies the files and registry keys, and then synchronizes the differences.

G Graceful (Clean) Shutdown
vCenter Server Heartbeat shuts down with no data loss after completing replication using the vCenter Server Heartbeat Console.

H Hardware Agnostic
A key vCenter Server Heartbeat feature allowing the use of servers from different manufacturers and/or models, and processing power in a single vCenter Server Heartbeat server pair.

Heartbeat
The packet of information issued by the passive server across the VMware Channel, which the active server responds to, indicating its presence.
Heartbeat Diagnostics
The umbrella name for the VMware process and tools used to check the production server health and applicability to the implementation of the vCenter Server Heartbeat solution.

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

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

Identity
The reference of a server’s position in the server pair based upon hardware, either the Primary server or the Secondary server.

Low Bandwidth Module (LBM)
A vCenter Server Heartbeat Module that compresses and optimizes data replicated between a Primary and Secondary server, thereby delivering maximum data throughput and improving application response time on congested WAN links.

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 Secondary server (hosting more than one virtual server) to protect multiple physical Primary servers.

Network Monitoring
Monitoring the active server’s ability to communicate with the rest of the network by polling defined nodes around the network at regular intervals.

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

Passive Server Queue
The staging area on the passive server used to store changes received from the active server before they are applied to the passive server’s disk/registry.

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

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

Plug-in
An optional module that can be installed into a vCenter Server Heartbeat server, which provides additional protection for a specific application.

Pre-Installation Checks
A list of system and environmental checks performed before the installation of vCenter Server Heartbeat.
Principal IP address
An IP address used by clients to contact the server through drive mappings, UNC paths, DNS resolved paths, to access the server's services and resources.

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

Protected Application
An application protected by vCenter Server Heartbeat.

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.

Remote Desktop Protocol (RDP)
A multi-channel protocol that allows you 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 VMware Channel, and applying them to the passive server so both servers are maintained in a synchronized state.

Role
The functional state of the server in the pair that can be either active or passive.

Rule
A set of actions to be performed by vCenter Server Heartbeat when defined conditions have been met.

Security Identifier (SID)
A unique alphanumeric character string that identifies each operating system and each user in a network of NT/2000/2003 systems.

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

Server Pair
The generic term used to describe the coupling of the Primary and Secondary server in vCenter Server Heartbeat.

Shared Nothing
A key vCenter Server Heartbeat feature whereby hardware is not shared between the Primary and Secondary servers, thus preventing a single point of failure.

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

Split-brain Avoidance
A unique feature of vCenter Server Heartbeat that uses various checks to overcome a scenario where both Primary and Secondary servers attempt to become active at the same time, leading to an active-active rather than an active-passive model.

Split-brain Syndrome
A situation where both the Primary and Secondary servers in a vCenter Server Heartbeat server pair are operating in the active mode and attempting to service clients, causing different data updates to be applied independently to each server.
Subnet
A division of a network into an interconnected but independent segment or domain, to improve performance and security.

Storage Area Network (SAN)
A high-speed special-purpose network or (sub-network) that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users.

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

Synchronize
The internal process of transporting 64KB blocks of changed files or registry key data, through the VMware Channel from the active server to the passive server. The data on the passive server is a mirror image of the protected data on the active server, a required condition for data replication on a vCenter Server Heartbeat server pair.

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

T
Task
An action to be performed by vCenter Server Heartbeat when defined conditions have been met.

Time-To-Live (TTL)
The length of time that a locally cached DNS resolution is valid. The DNS server must be re-queried after the TTL expires.

Traceroute
A utility that records the route through the Internet between the computer and a specified destination computer.

U
Ungraceful (Unclean) Shutdown
A shutdown of vCenter Server Heartbeat resulting from a critical failure or by shutting down Windows without first performing a proper shutdown of vCenter Server Heartbeat, resulting in possible data loss.

Unprotected Application
An application that is not monitored or its data replicated by vCenter Server Heartbeat.

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

VMware vCenter Server Heartbeat
The core replication and system monitoring component.

VMware vCenter Server Heartbeat Packet Filter
The network component installed on both servers that controls network visibility.

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

Virtual Private Network (VPN)
A private data network that uses the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.
VMware Web Site
The VMware web site dedicated to support partners and customers providing technical information, software updates, and license key generation.

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, and groups.