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

© 2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware, the VMware "boxes" logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

**REVIEWING THE VMWARE CHANNEL STATUS** .............................................................. 87
**CONFIGURING PUBLIC NETWORK CONNECTION CHECKS** .............................................. 88
**SETTING MAX SERVER TIME DIFFERENCE** ................................................................. 89

## 7 APPLICATION PROTECTION ................................................................. 90

**APPLICATIONS TAB** .................................................................................................. 90
  - Editing Individual Applications ................................................................................. 90
  - Configuring Applications .......................................................................................... 91
  - Reviewing the Status of an Application ..................................................................... 92
  - Reviewing the Applications Status Log ................................................................. 92
  - Filtering Application Log Entries ............................................................................. 93
  - Resetting the Application Health Status ............................................................... 94
  - Removing an Application......................................................................................... 94

**SERVICES TAB** ........................................................................................................... 95
  - Adding a Service ....................................................................................................... 95
  - Editing a Service ...................................................................................................... 96
  - Checking the Status of Services .............................................................................. 97
  - Unprotecting Services and Stopping Monitoring .................................................... 98
  - Removing a Service................................................................................................. 98

**TASKS TAB** ............................................................................................................... 99
  - Adding a Task .......................................................................................................... 99
  - Editing a Task .......................................................................................................... 100
  - Removing a Task...................................................................................................... 101
  - Starting a Task Manually ........................................................................................ 102

**PLUGINS TAB** ............................................................................................................ 102
  - Installing a Plugin .................................................................................................... 103
  - Editing a Plugin ........................................................................................................ 104
  - Uninstalling a Plugin ............................................................................................... 104

## 8 PERFORMANCE PROTECTION ................................................................. 106

**RULES TAB** .................................................................................................................. 106
  - Editing a Rule .......................................................................................................... 106
  - Rules Installed by vCenter Server Heartbeat Plugins ...................................... 107
  - Checking a Rule Condition .................................................................................... 108

## 9 DATA PROTECTION ......................................................................................... 110

**AUTOMATIC FILTER DISCOVERY** .............................................................................. 111
  - Adding a User-Defined Inclusion Filter ............................................................... 111
  - Adding a User-Defined Exclusion Filter ............................................................... 112
  - Removing User-Defined Inclusion/Exclusion Filters ......................................... 112

**CONFIGURING MAX DISK USAGE** ........................................................................... 113
**REVIEWING STATUS OF PROTECTED FILES** ..................................................... 113
**DETERMINING EFFECTIVE FILTERS** ........................................................................ 114
**INITIATING FILE SYNCHRONIZATION MANUALLY** ........................................... 115
  - Initiating Verify and Synchronize Manually ......................................................... 115

**INITIATING A FULL SYSTEM CHECK** ..................................................................... 116
**REVIEWING THE REGISTRY SYNCHRONIZATION STATUS** ................................. 117
**INITIATING A FULL REGISTRY CHECK** ..................................................................... 118

## 10 OTHER ADMINISTRATIVE TASKS ............................................................ 119
11 TROUBLESHOOTING .......................................................... 127

TWO ACTIVE SERVERS ........................................................................ 127
Symptoms .................................................................................................. 127
Causes ......................................................................................................... 127
Resolution .................................................................................................. 128

TWO PASSIVE SERVERS ........................................................................ 128
Symptom...................................................................................................... 129
Causes ......................................................................................................... 129
Resolution .................................................................................................. 129

SYNCHRONIZATION FAILURES .................................................................. 129
Services Running on the Passive Server ...................................................... 130
VMware Channel Incorrectly Configured.................................................... 130
Incorrect or Mismatched Disk Configuration ................................................ 131
Passive Server Has Less Available Space than Active Server ................... 131
Unprotected File System Features .............................................................. 132

REGISTRY STATUS IS OUT OF SYNCH .................................................. 132
Resource issues .......................................................................................... 132
Registry security issues ............................................................................. 133

CHANNEL DROPS .................................................................................... 133
Performance issues .................................................................................... 133
Passive server does not meet minimum hardware requirements ............. 134
Hardware or driver issues on VMware Channel NICs ................................ 134
Firewall connection ................................................................................... 134
Incorrect VMware Channel configuration ................................................ 135
VMware vCenter Server Packet Filter is enabled on the Channel NIC(s) .... 136

SUBNET OR ROUTING ISSUES .............................................................. 136
LAN deployment ........................................................................................ 136
WAN deployment ....................................................................................... 137

MAXDISKUSAGE ERRORS ....................................................................... 137
Active server (unsafe) queue ....................................................................... 137
Passive server (safe) queue ........................................................................ 137

MAXDISKUSAGE ERROR MESSAGES ..................................................... 138
[L9] Exceeded the maximum disk usage (VCChannelExceededMaxDiskUsageException) ... 138
[L9] Exceeded the maximum disk usage on the ACTIVE server .................... 138
[L9] Exceeded the maximum disk usage on the PASSIVE server .................. 139
[L20] Out of disk space (VCChannelOutOfDiskSpaceException) .................. 140
Application Slowdown ............................................................................... 140
Poor application performance ................................................................... 140
Both servers can accommodate the initial load but the load has increased ... 141
One server is able to cope, but the other cannot ....................................... 141
Scheduled resource intensive tasks ......................................................... 141

GLOSSARY .............................................................................................. 143
About This Book

This Reference Guide provides an overview of the VMware® vCenter Server Heartbeat application. It describes how to install and configure the application, administer and maintain the day-to-day operations, and describes the levels and types of protection.

This manual provides information and instructions that are applicable to this specific version of vCenter Server Heartbeat and must not be applied to any other version of the software.

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>
<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 versions of this book and other books, go to http://www.vmware.com/support/pubs

Online and Telephone Support

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

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

Support Offerings

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

VMware Professional Services

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

This reference guide is designed to provide an understanding of vCenter Server Heartbeat concepts and on the installation of vCenter Server Heartbeat and its configuration.

Chapter 1 vCenter Server Heartbeat Concepts
vCenter Server Heartbeat provides four levels of protection out of the box with the topology and networking principles used by vCenter Server Heartbeat. The chapter also outlines the failover and switchover processes.

Chapter 2 Installing vCenter Server Heartbeat and Application Protection on Windows Server 2003
This chapter describes the installation used to deploy vCenter Server Heartbeat and Application Protection on the Primary and Secondary servers in a Windows 2003 environment.

Chapter 3 Configuring vCenter Server Heartbeat
This chapter discusses how to configure vCenter Server Heartbeat parameters and options to maximize use of vCenter Server Heartbeat.

Chapter 4 Status and Control
This chapter covers how to connect to vCenter Server Heartbeat using the vCenter Server Heartbeat Console and review the status of a server pair.

Chapter 5 Server Protection
vCenter Server Heartbeat protects from server system failure or server hardware crash.

Chapter 6 Network Protection
vCenter Server Heartbeat protects the network identity of the production server providing you with a replica server including server name, IP address shares on the failure of the production server.

Chapter 7 Application Protection
vCenter Server Heartbeat maintains any application environment ensuring that applications and services stay alive on the network.
Chapter 8 Performance Protection
vCenter Server Heartbeat monitors system and application attributes to prevent an unexpected failure of the system or application.

Chapter 9 Data Protection
vCenter Server Heartbeat intercepts all user-written data and applications, and maintains a copy of the data, which is used in case of a failure.

Chapter 10 Other Administrative Tasks
This chapter discusses additional administrative tasks to configure logging and alerting functions of the system.

Chapter 11 Troubleshooting
This chapter provides a list of the most common unexpected behaviors encountered in the day-to-day operations of vCenter Server Heartbeat.

Glossary
This section provides definitions of terms used in this document and in vCenter Server Heartbeat.
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, providing a replica server including server name and IP address shares on a 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 user-written data and applications, and maintains a copy of the data on the passive server used in the event of a failure.

vCenter Server Heartbeat provides all five protection levels contiguously, maintaining all facets of the user environment at all times, with continued network (Principal (Public) network) operation 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 has the same name, same file and data structure, same network address, and can run all the same applications and services as the Primary server.

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

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

**Server Protection**

vCenter Server Heartbeat protects the active server’s operating system or hardware from failing. Two instances of vCenter Server Heartbeat monitor each other by sending "I’m alive" messages and reciprocating with acknowledgments over a network connection termed the vCenter Server Heartbeat Channel. If the passive server detects that this process or heartbeat has failed, then a failover occurs as illustrated in Figure 1-1.
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 the default gateway, the primary DNS server, and the Global Catalog server at regular intervals. If all three nodes fail to respond, for example, in the case of a network card failure or a local switch failure, vCenter Server Heartbeat can initiate a switchover, allowing the secondary server to assume an identical network identity as the primary server.

**Application Protection**

vCenter Server Heartbeat running on the active server locally monitors the applications and services it has been configured to protect through the use of plugins. 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 the section on switchovers and failovers in this guide for further information about the switchover process.
A switchover gracefully closes any protected applications that are running on the active server and restarts them on the passive server with the application or service that caused the failure. 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

The protected applications must be operational and providing service, and that the performance of those applications must be adequate to be productive. The vCenter Server Heartbeat plugin provides 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.

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 you or the applications require in the application environment are made available in case of a failure. 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 protected on the failed server are available 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 vCenter Server Heartbeat Channel uses a separate NIC, a private connection between the servers used for control and data transfer between the pair of servers.

The vCenter Server Heartbeat Channel might use a second pair of NICs to provide a degree of redundancy. In this case, the VMware Channel has a Dual Channel if more than one dedicated NIC is provided for the vCenter Server Heartbeat Channel on each server. To provide added resilience, the communications for the second channel must be completely independent from the first channel – they must not share any switches, virtual switches, routers or the same WAN connection.
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 `/All`.

The passive server’s Principal (Public) NICs 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 vCenter Server Heartbeat Channel must be configured so that they have IP addresses outside of the Principal (Public) networks subnet range. These addresses are termed the vCenter Server Heartbeat Channel addresses.

Switch off NetBIOS for the vCenter Server Heartbeat Channel(s) on the active and passive servers as this connection remains live and both the passive and active machines have the same NetBIOS name. After restore and after the vCenter Server Heartbeat installation 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 vCenter Server Heartbeat 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 vCenter Server Heartbeat Channel using 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 by clicking Switchover. An automatic switchover occurs 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, protected applications transfer 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 occur.
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 now accepts updates from the active server.
7. Start the same protected applications on the new active server. The protected applications now start and are accessible, generating disk updates.

The switchover is complete.

**Auto-Switchovers**

An auto-switchover occurs 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**

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.

![Figure 1-6 Failover](image)

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, 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 mode of operation 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 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 is the active server and the primary 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
vCenter Server Heartbeat provides a versatile solution that deploys multiple configurations in both a LAN and a 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 provide a step-by-step process to select options required for installation. The deployment scenario table provides a visual reference to configuration options supported by vCenter Server Heartbeat.

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
- Operating System Windows Server 2003 x86 Sp1 or SP2
- Additional 512 MB (minimum), 1 GB RAM (recommended)
- 2 GB of disk space available on the drive where vCenter Server Heartbeat is installed
- Local administrator rights for vCenter Server Heartbeat installation
- Latest Microsoft security updates
- All applications to be protected by vCenter Server Heartbeat must be installed and configured on the primary server prior to installing vCenter Server Heartbeat.
The primary and secondary servers must be set to identical System Date / Time and Time Zone. Once configured, do not change the Time Zone.

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 must 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

- Hardware as specified in the Common Requirements section.
- Software as specified in the Common Requirements section.

Secondary Server

Hardware

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

Software

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

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

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 the Physical to Physical (P2P) section.
Application Component Options

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

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

vCenter Server with SQL Server on the Same Host

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

vCenter Server with SQL Server on a Separate Host

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

To ensure proper failover, increase the default Heartbeat interval for the vCenter Server from 20 to 30 seconds. For information on configuring the Heartbeat interval, see Step 31 later in this guide.

vCenter Server Only

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

To ensure proper failover, increase the default interval from 20 to 30 seconds on the server running vCenter Server. For information on configuring the Heartbeat Interval, see Step 31 later in this guide. This configuration is required when SQL Server is not on the same host as vCenter Server.

Network Options

Networking requirements are contingent based upon how vCenter Server Heartbeat is deployed. If deployed as a High Availability solution then a LAN configuration is required. If vCenter Server Heartbeat is deployed for Disaster Recovery, then a WAN configuration is required. 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 used by both servers. Additionally, each server requires a separate VMware Channel IP address on a separate dedicated subnet.

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

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

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

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

Secondary Server

- Same number of NICs as the Primary Server

- Principal (Public) Network connection configured with temporary network settings

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

WAN

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

WAN Requirements

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

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

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

- VMware Knowledge Base article 1008571
- VMware Knowledge Base article 1008605

At least one Domain Controller at the Disaster Recovery site

Bandwidth

Determine the available bandwidth and estimate the volume of data for which throughput is required to determine acceptable latency for the throughput. Additionally, the bandwidth may affect the required queue size to accommodate the estimated volume of data.

VMware recommends a minimum of 1Mb of spare bandwidth be available for vCenter Server Heartbeat.

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

Latency

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

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.

When implementing vCenter Server Heartbeat, do not replicate File Level AV temp files with 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:\VMware\VMware vCenter Server Heartbeat\ is the default installation directory):

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

Make any configuration changes to a file-level AV product on one server (exclusions etc) on the other server as well. vCenter Server Heartbeat does not replicate this information.

### Deployment Options Summary

Table 3 provides all possible deployment options described in this section.

<table>
<thead>
<tr>
<th>Table 3 Installation Options</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>Clone Technique</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
<td>Pre-Clone</td>
<td>vCenter Server w/SQL Local</td>
</tr>
<tr>
<td>WAN</td>
<td>Install Clone</td>
<td>vCenter Server w/SQL Remote</td>
</tr>
</tbody>
</table>

- **V2V**
  - X
  - X
  - X
  - X
  - X
  - X

- **P2V**
  - X
  - X
  - X
  - X
  - X

- **P2P**
  - X
  - X
  - X
  - X
  - X
  - X
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 ___

Install in network environment type:
- LAN___
- WAN___

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

1. 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.

For P2P, go to Step 2 to continue the installation.

For V2V or P2V Installations with the Pre-Clone technique selected, follow Step 1a 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.
d. Repeat the process on the Channel Virtual Network Adapter.

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

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

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 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.
l. Right click the Secondary (cloned) server image and select **Edit Settings**.

m. Select the VMware Channel virtual network adapter and select the **Connected** and **Connect at power on** check boxes. 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**.

**Note:** The left panel of each screen in the setup wizard provides information about the setup process.

4. Select **Primary** as the server identity, and then click **Next**.
Chapter 2 vCenter Server Heartbeat Implementation

**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.

---

**For installation using the Install Clone technique, continue with Step 5.**

**For installation using the Pre-Clone technique, go to Step 5a.**

---

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.

Since 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**.
7. 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.

**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 select the network adapter(s) for use in the VMware Channel. Select the network adapters (NICs) from the list that are used for the VMware Channel. 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.

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 VMware Channel(s) IP network addresses. Click **Add** for each available channel connection. Enter 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.

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.

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 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.

19. 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.

20. 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 the 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.

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.
For installation using the Pre-Clone technique, go to Step 26a.
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 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 protected applications 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, consider including application data and location of the backup folder.
Continue with Step 27.

a. When selecting the Pre-Clone technique, back up two 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 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.

27. Review the summary of options and configuration information for the installation. Click Next.
28. 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.

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

30. If the pre-install checks are successful, click **Next**.
31. 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 extranet.

32. Click Next after vCenter Server Heartbeat components are complete. If using the Pre-Clone installation technique, go to Step 35. If using the Install Clone installation technique, continue to Step 33.

33. The next screen displays Microsoft Windows Backup. Click Proceed. The automated backup is saved in the previously defined location.
34. A summary screen displays the results of the backup operation. Review the backup report and click **Next**.

35. The vCenter Server 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 will see multiple warnings. The lower pane displays the results of the process. Click **Next**.
By default, the vCenter Server Packet Filter Driver is applied to all Principle (Public) network cards present on the machine. The vCenter Server 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.

36. When the setup wizard confirms the successful completion of the installation, click Finish.
Secondary 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 Primary 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](image)

   **Physical Hardware Identity**
   
   A VMware vCenter Server Heartbeat system consists of two servers. Together, these servers are described as a "Server Pair".

   The terms Primary and Secondary are used to describe the Physical Hardware Identity of each server in the pair. A Server Pair consists of one Primary server and one Secondary server. Once set, the Physical Hardware Identity of a server should not normally change.

   Select Primary if you want this server to be your Primary server.

   Select Secondary if you want this server to be your Secondary server.

   ![VMware](image)

   **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.
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**.

![Installation progress](image1)

9. The progress of the VMware vCenter Server Packet Filter installation displays. Click **Next**.

![Packet Filter installation](image2)
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, go to Step 9a.

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**.
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**.
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, you 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 VMware vCenter Server 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:

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

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.

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

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

24. Log into the Secondary server domain with the domain administrator’s account.

25. Plug and Play re-identifies the actual hardware makeup of the Secondary server to distinguish from the restored backup file of the Primary server and might require you to reboot the server a few times.

   **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**.
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 remote SQL Server.

If vCenter Server only was installed and you want to install a remote 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 the beginning of the installation process.

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

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

c. Click **Add Pair**.

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.

f. Click Close to return to the login screen.

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

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.

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

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

j. 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 checkbox next to the server name.
When a pair is selected, the **Open**, **Clear Event**, and **Remove** buttons become active.  

k. **Open** displays the pair of servers for administration and configuration and displays the **System -> Status and Control** page. 

l. Click **Advanced -> Application -> Plugins**.
m. Select the vCenter Server plugin.

n. Click **Edit**.

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

p. Click **OK**.

32. If vCenter Server is installed either alone or with a remote SQL Server, configure the Heartbeat Interval.

   a. Navigate to **Start -> All Programs -> VMware -> VMware vCenter Server Heartbeat -> Manage Servers**.

   b. Click **Advanced -> Communication -> Configuration**.
c. Change the Heartbeat Interval setting to 30 secs.
d. Click **Apply**.
3 Configuring vCenter Server Heartbeat

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.

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

To change the machine identity, go to the Machine tab and select the Physical Hardware Identity of the local machine. Click Next or Finish.

Configuring the Server Role

To change the server role, go to 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, 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. Use the dropdown to display a list of available IP addresses on the local server. Manually enter the remote server IP address.
To change the VMware Channel IP addresses, select the entry in the table and edit the entry. 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 on memory and is essential for WAN installations or when bandwidth is limited.

Low Bandwidth Optimization is only available if it was included in the vCenter Server Heartbeat License key or separately licensed. If included, 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. In LAN implementation where the throughput is much higher, this feature might not improve performance.

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 maintains so no IP address conflicts occur between the two servers.

To configure Principal (Public) IP address, 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.

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. Click **Next** or **Finish**.

### Enabling Network Monitoring

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

Monitor the network by pinging a set of machines on the Principal (Public) network. If enabled, the system pings a set of addresses automatically. Use the vCenter Server Heartbeat Console to change the configuration after installation.
To enable this feature, go to the Network Monitoring tab. Select **Enable public network monitoring using automatic configuration**. 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 fail over, 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 called the passive server (safe) queue and the replication data waiting to be sent called 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, go to the Logs tab. Click **Browse** to navigate to the folder to store the message queue logs. Select the folder, then click **Next** or **Finish**.

**Configuring the Maximum Disk Usage**

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

Replication stops. The system is no longer protected when the disk reaches quota.
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 has 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
vCenter Server Heartbeat operates over a pair of vCenter Server Heartbeat servers and is administered in these pairs.

The vCenter Server Heartbeat Console operates 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 the setup.exe from the setup CD/folder on the workstation and choose **Install Client Tools** 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.**

Before you log in, you must identify the pair of servers to administer. Click **Servers.**
**Note:** Enter the IP address at one of the server pairs for the VMware Channel to locally administer pairs of servers.

**Adding or Removing a Pair of vCenter Server Heartbeat Servers**

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

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**.

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. 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.

Select a server pair displayed in the Server box.

Enter the 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 been administered. The Primary server name is displayed with the roles that Primary and Secondary servers are currently performing.
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, click **Add** and follow the previously described procedure. **Exit** closes the interface but does not affect the vCenter Server Heartbeat Server service.

To select a pair listed in the main data grid, select the checkbox 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 launch the vCenter Server Heartbeat Console from the desktop shortcut or go to **Start -> All Programs -> VMware -> VMware vCenter Server Heartbeat ->Manage Server**.

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.

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

Click **Close** to log out of administering the current server pair.

![Confirmation Dialog]

A confirmation dialog asks for confirmation of the logout request.
Click **OK** to close the client.
5 Server Protection

Protection against the active server 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 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 administers a pair of servers. The System screen reviews 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.
The system status in the central grid for each server indicates procedures being executed. Table 4 lists each status with a description:

### Table 4 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) respectively before moving to the passive server (safe) queue or committed to disk. Above the data grid, a graph represents the connection status and speed. The Server Pair pane graphically displays the file and registry synchronization status with icons described in Table 5:
Table 5 File and Registry Status

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Synchronized The files or registry are fully synchronized.</td>
</tr>
<tr>
<td>☞</td>
<td>Unchecked There are files present that are currently unchecked, a full system check has not completed.</td>
</tr>
<tr>
<td>✔️</td>
<td>Synchronized and Busy Processing The registry is currently in the process of being synchronized.</td>
</tr>
<tr>
<td>(?)</td>
<td>Checking The differences in the registry are currently being checked to see if they are synchronized.</td>
</tr>
<tr>
<td>❌</td>
<td>Out of Synch 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 the passive server sends Heartbeat packets to the active server across the VMware Channel connections. Max Heartbeats Missed Before Failover determines the missed number of packets before initiating a failover.

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

![vCenter Server Heartbeat Console](image)

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.
Chapter 5 Server Protection

The default option, **Stop VMware vCenter Server Heartbeat but leave protected applications running** stops the protection (synchronization) of data files but does not stop protected applications.

**Stop VMware vCenter Server 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.

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:

---

**Shutdown**

**Shutdown** is similar to **Stop Replicating** and stops all protection of data and 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, which involves rebooting the server.

To trigger a switchover, click Switchover in the System Screen, which reverses the roles of the servers: the active server becomes passive and vice versa. You can work continuously even when the Primary server is offline.

Once the Primary server is back up and running, you can trigger 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 must 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.

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 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 executes 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.
Chapter 5 Server Protection

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. Use the Log Collector tool to collect information and send the output to VMware Support.

2. Do not perform a switchover 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 – Replace disk.
   - 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 for analysis.

3. Run the Configure Server wizard and set the server 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.


      **Note:** The data on this server is 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. 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 failover 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.

Configure IP addresses for **Split-Brain Avoidance** as required from those set at install time for both the Primary and Secondary servers.
6 Network Protection

The Communication screen displays communications status of vCenter Server Heartbeat. The **Status** tab allows you to check the status of the VMware Channel, the active server (unsafe) and passive server (safe) queues, and the Principal (Public) network.

### Reviewing the VMware Channel Status

The status displays connected or not connected, statistics of the connection with 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 Configuration tab.

## Configuring Public Network Connection Checks

![VMware vCenter Server Heartbeat Console](image)

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 with **Enable if Active Server’s Public Network Connection is Lost**. The feature polls 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 specifying additional waypoints. To specify a manual target for the Principal (Public) network checking, clear one **Auto Select** 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 **Auto Select** check box and manually specify the target address.

Principal (Public) Network Monitoring functions 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**:

![Max Server Time Difference](image)

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

vCenter Server Heartbeat incorporates an Application Management Framework (AMFx) to manage vCenter Server Heartbeat Plugins.

The AMFx provides additional functionality while maintaining the traditional stability of VMware. The AMFx allows plugins 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 plugins to share files or services while preventing removal of a shared file or service when one of the sponsoring plugins remain installed.

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

Applications Tab

The Application tab displays the current status of protected applications and application health. You can start, stop, and configure all protected applications. The Application Log allows you to view application events as they occur.

Log into the vCenter Server Heartbeat Console, click Application on the left navigation panel and select the Applications tab.

Editing Individual Applications

vCenter Server Heartbeat allows you to set 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 select the desired application and then click Edit. Enter the settings, and click OK.
Chapter 7 Application Protection

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. 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. 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.

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.
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 filters Application Log files to limit the events displayed. By default, all events display in the Application Log file. To filter the events displayed, click Filter in the Application panel titled Application Log. In the upper section, clear the event types you do not want to view. Configure a date and time range to limit the event to fit that date and time range. To limit the date and time range, select Events From and edit the date or time range. Click OK.
Reseting the Application Health Status

To reset the Application Health status, go to the Applications tab of the Applications screen. 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 plugin, then removing the application also removes the plugin. If the sponsor is not associated with a plugin then all sponsorship is removed from services, filters, and tasks.

**Services Tab**

The Services panel displays both services that you or plugins 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 are **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 depending on protected services (started and stopped) but not monitored (not restarted if stopped by some external agency). vCenter Server Heartbeat monitors protected services (i.e. restarted if stopped) but not managed (i.e. 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, add the service from the vCenter Server Heartbeat Console in a Running state. Click **Add** to see a list of the current running services under **Name**.
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.

If vCenter Server Heartbeat manages the start and stop of the service, select **Manage Starting and Stopping**. If vCenter Server Heartbeat monitors 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.

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, select the service and click **Edit**. Edit Service provides a subset of same options available when adding a new service. Make the modifications, and then click **OK**.
Chapter 7 Application Protection

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.
Unprotecting Services and Stopping Monitoring

To unprotect and stop monitoring the service, go to the Services tab. Select the service and click Edit.

Clear Manage Starting and Stopping and Monitor State. Click OK.

Services occur in an order, 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 plugins 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 (i.e. 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 service, select the service and 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, DNSUpdate. The task can launch a batch script containing multiple dnscmd. 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 plugins to define and implement tasks. An example of a plugin-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, click **Add**. Assign a name to the task and select the task type from the list. Enter the Interval setting and enter or browse for the script, .bat file, or command. Click **OK**.
If **Command** requires specific user credentials, click **User Accounts** in the upper right of the pane. 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, select the task and click **Edit**. You can edit the task interval or disable the task. Click **OK**.
Removing a Task

To remove a task, select the task and click **Remove**.
Starting a Task Manually

vCenter Server Heartbeat provides options to allow a designated period or event to occur before launching the task or launching the task immediately. To launch the task immediately, select the task and click Run Now. vCenter Server Heartbeat immediately launches the task.

Plugins Tab

Plugins support specific applications and contain all of the components to protect the designated application. Plugins 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.
Installing a Plugin

To install a new plugin, go to **Application** and select the Plugins tab. Click **Install** and browse for the plugin. The path statement is case-sensitive. Click **OK**.
Editing a Plugin

To edit the plugin configuration, select the plugin and click **Edit** to modify the default configuration. Review the configuration options before making modifications as they are specific to each plugin. Click **OK**.

Uninstalling a Plugin

You can uninstall a plugin when you need to upgrade or remove the application the plugin protects, or when directed by VMware Support. To uninstall a plugin, select the plugin and click **Uninstall**. The plugin is uninstalled and removed.
8 Performance Protection

Rules Tab

Rules are implemented by plugins 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.

![Rule Configuration Screen]

Editing a Rule

Each plugin contains a default set of rules with options you can modify. To edit a rule, go to Application and select the Rules tab. 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. Click OK.

Rules Installed by vCenter Server Heartbeat Plugins

The following plugins implement the rules listed.

vCenter Server Plugin
- Check vCenter License
- Check Connection to vCenter

vCenter SQL Server Plugin
- 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 Plugin
- DiskAvgSecsPerRead
- DiskAvgSecsPerWrite
- DiskI/O
- DiskQueueLength
- DiskReadsPerSec
- DiskWritesPerSec
- DiskWriteable
- FreeDiskSpace
- FreeDiskSpaceOnDrive
- MemoryCommittedBytes
- MemoryCommittedBytesPercent
- MemoryFreePTEs
- MemoryPageReadsPerSec
- MemoryPageWritesPerSec
- MemoryPagesPerSec
- MemoryPagingFileUsage
- PageFaultsPerSec
- ProcessorIntsPerSec
- ProcessorLoad
- ProcessorQueueLength
- RedirectorBytesTotalPerSec
- RedirectorNetworkErrorsPerSec
- ServerBytesTotalPerSec
- ServerWorkItemShortages >= 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, select the rule and click **Check Now**. vCenter Server Heartbeat immediately checks the rule conditions of the current configuration against the attributes of the system or application.
### Rule Conditions

<table>
<thead>
<tr>
<th>Rule Description</th>
<th>Condition</th>
<th>Duration</th>
<th>Value</th>
<th>Last Triggered</th>
<th>Triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Disk Usage #1 (Free Disk Space)</td>
<td>Disk usage: Time &gt; 30% or ...</td>
<td>5000000000</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>High Disk Usage #2 (Free Disk Space)</td>
<td>Disk usage: Time &gt; 30% or ...</td>
<td>5000000000</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Advanced

- Processor Load: Processor Usage > 75%: 19
- Processor Queue Length: Processor Queue Length > 10: 1800000000
- Buffer View: Buffer Views Total/VM: 6000000000
- Network Error: Network Error/VM: 1000000000
- Server Buffer Total: Buffer Total/VM: 10000000000
- Server CPU: CPU Percentage/VM: 10000000000
- Server Memory: Memory Percentage/VM: 10000000000
- Server Network: Network Usage/VM: 10000000000
- Server Storage: Storage Usage/VM: 10000000000
- Server System: System Usage/VM: 10000000000

---

**Chapter 8 Performance Protection**

VMware, Inc.  109
9 Data Protection

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.

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 plugin provides database protection including changes or additions to the database and log files.

**Adding a User-Defined Inclusion Filter**

Click **Advanced -> Data** and 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 filter details. Effective – the filter has been properly configured and protects (replicate) the stipulated files to the passive server, Subset – contained within another filter, or Not Effective – not contained within another filter.

To define filters that protect user defined files and folders, 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. Click **OK**.

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 more Inclusion Filters.

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, 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. Click **OK**.

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.

To edit file filter definitions, select the filter and click **Edit**.

Removing User-Defined Inclusion/Exclusion Filters

To remove an Inclusion or Exclusion Filter, select the filter and 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. Go to Advanced -> Communications -> Configuration and select Max Disk Usage. 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.
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 node. 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 6:

Table 6 Synchronization Status

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>The file has been verified and synchronized successfully.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>The file is not synchronized on the active and passive servers. This state follows a failover and requires manual synchronization and verification.</td>
</tr>
<tr>
<td><img src="image" alt="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 plugin. 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. To manually synchronize the specified files, click **Synchronize**.

You can resynchronize files at any time. Select multiple files with the Shift or Ctrl keys and click **Synchronize**. 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, use **Verify & Synchronize** and select **Include Subdirectories** to ensure all underlying files and subfolders are included in the verification and synchronization operation. 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.
Reviewing the Registry Synchronization Status

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

The status of registry replication 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, go to **Data** and select **Registry Synch and Verify** tab. Click **Full Registry Check**.
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.

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, go to **Advanced -> System** and select the Configuration tab. Enter the outgoing SMTP server of both the Primary server (when active) and the Secondary server (when active) in the appropriate fields. Enter the fully qualified domain name of the mail server. Enter an email address that is authorized to send mail through the SMTP server.

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.

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.
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 of 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.

Another method to send an alert notification is to select **Run Command** under the pertinent alert state. **Browse** for a script to run or use a command line argument to run on the alert trigger.

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 7:
Table 7 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"
```

Click **Apply** to save the changes and enforce the defined notification rules.

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.
Configuring Event Log Files

To configure default settings for log files, select **Advanced ->Log**. The Configuration tab allows you to define the filename and path of the exported comma-separated variable file. You can manually type its path and file name or use **Browse** and navigate the file. Click **Apply**.

Configuring Log File Email Recipients

To configure vCenter Server Heartbeat to e-mail a copy of the log file, select **Mail Every**, and configure the day and time to send the log file.

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.

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

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

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 logs chronologically by default.

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, click the entry in the data grid.
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.

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.

Click Close to close the Event Properties.

Table 8 describes the four event categories:

Table 8 Log Events

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗</td>
<td>Errors within the underlying operation of vCenter Server Heartbeat are considered critical to the operation of the system.</td>
</tr>
<tr>
<td>!</td>
<td>Warnings generated for discrepancies within the vCenter Server Heartbeat operational environment are not deemed critical to the operation of the system.</td>
</tr>
<tr>
<td>📊</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>📱</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, select Events of at Least, select the importance level and click Apply. Logs above the selected severity are displayed.

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

To refresh the list of events, click **Refresh Event Log** at the bottom left of the Log Details data grid.

To clear the list, click **Remove all Entries** at the top left of the Log Details data grid.

To export the list to a comma separated variable file, click **Export event log** at the top left of the Log Details data grid. You can configure the file name and path to export the data in the Configuration tab.

To immediately email the list, click **E-mail**.
Troubleshooting

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 (e.g. 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, perform the following steps:

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 into 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

To resolve two passive servers, perform the following steps:

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

#### 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.
```

Services that keep files locked on the passive server are:

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

#### 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 Sync** status, perform the following steps:

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

#### Symptom
If the VMware Channel is not properly configured, it cannot initiate the handshake to establish communications through the VMware Channel connection. Failure to establish the VMware Channel connection prevents a full system check, thereby leaving the File System Status and Registry Status as **Out of Sync**.

#### Causes
The most common VMware Channel configuration errors are as follows:
■ VMware vCenter Server 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

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

Incorrect or Mismatched Disk Configuration

Symptom

When vCenter Server Heartbeat starts, it checks the complete set of file filters for consistency. 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 VMware Knowledge Base article 1008458.

Passive Server Has Less Available Space than Active Server

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.
Reference Guide

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.

Unprotected File System Features

Symptom
The replication set contains unprotected file system features. vCenter Server Heartbeat detects Unprotected Features from category 2 (Extended Attributes and file encryption), logs an error, and sets the File System Status to Out Of Synch. If these types of files are present in the replication set, replication continues but the system remains Out of Synch.

Cause
vCenter Server Heartbeat does not synchronize if the replication set contains files with unprotected file system features. Unprotected file system features are described by category in VMware Knowledge Base article 1008444.

Resolution
Two methods of dealing with these Unprotected Features are described in VMware Knowledge Base article 1008444. If these features are not essential for the normal operation of the file system, zip and unzip the affected files within their parent directory to remove the unprotected features, allowing the vCenter Server Heartbeat to synchronize the file system.

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

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 correct the problem that the server does not have enough virtual memory.

Registry security issues

Symptom
vcCenter 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

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 VMware vCenter Server R2 service experiences problems, does not respond, or terminates unexpectedly.

Resolution

- 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 Channel hardware or driver issues for more information on this topic.
Passive server does not meet minimum hardware requirements

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. An upgraded Primary server might require a new vCenter Server Heartbeat license if the Hardware ID changes. Upgrading the Secondary server does not require a new license.

Hardware or driver issues on VMware Channel NICs

Symptom
The VMware Channel drops or disconnects and reconnects intermittently.

Causes
- 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
- 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 VMware Knowledge Base article 1008383.
- 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

Symptoms

- IP conflicts occur on one of the VMware Channel IP addresses.
- The VMware Channel does not connect, or connects and disconnects.

Causes

- 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 Packet Filter is enabled on the Channel NIC(s)**

**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 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 as part of the installation of vCenter Server Heartbeat. If the vCenter Server 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 the vCenter Server 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**

**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

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, the static route is not 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 traffics in the VMware Channel.

Resolution
Refer to VMware Knowledge Base article 1008451, 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 $<\text{VMware vCenter Server Heartbeat Install Directory}>\text{R2}\text{\textbackslash log}$, 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.
To set the queue size:

- Start vCenter Server Heartbeat, open the vCenter Server Heartbeat Console, and select **Advanced -> Communication -> Configuration**. Set **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**

[L9] Exceeded the maximum disk usage (VCChannelExceededMaxDiskUsageException)

**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.

[L9] Exceeded the maximum disk usage on the ACTIVE server

**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 VMware Knowledge Base article 1008551) 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

Symptom

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

Causes

- 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 eventually exceeds 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

- 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:
  1. Shut down vCenter Server Heartbeat.
  2. Open the Server Configuration wizard and select the Logs tab.
  3. Set the path for Message Queue Logs Location and click Finish.
  4. 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.
Out of disk space (VCChannelOutOfDiskSpaceException)

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
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. If the total resource requirements of these 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.

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

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 Heartbeat was installed.
Resolution
Heartbeat Diagnostics reports these conditions and issues warnings if CPU usage or memory usage exceed a certain percentage of the available resource. Minimize the risk of application slowdown by upgrading the recommended hardware on the Primary server.

Both servers can accommodate the initial load but the load has increased

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 Exchange 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

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

Symptom
Resource-intense scheduled tasks impact performance at certain times.
Cause

Two or more resource-hungry 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.
Glossary

**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 so you can 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 switchovers 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.

**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.

**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.
**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.

**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.

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

**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.

**Plugin** – 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 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.

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.

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.

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 Extranet - 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.