vCenter Server Heartbeat Administrator's Guide

VMware vCenter Server Heartbeat 6.6 Update 2

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001239-02

vmware

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About This Book

To help you protect your VMware vCenter Server installation, the vCenter Server Heartbeat Administrator Guide provides information about monitoring, managing, maintaining, and diagnosing issues along with the architecture, configuration, and protection offered by vCenter Server Heartbeat.

Intended Audience

This guide is intended for IT Administrators with a working knowledge of networking to include configuration and domain administration on Windows™ 2008 and 2012 platforms, notably in Active Directory and DNS.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation go to www.vmware.com/support/pubs.

Overview of Content

This book is designed to provide guidance on the configuration and administration of vCenter Server Heartbeat, and is organized into the following sections:

- Preface — *About This Book* (this chapter) provides an overview of this guide and the conventions used throughout.
- Chapter 1 — *Introduction* presents an overview of vCenter Server Heartbeat concepts including the architecture, communications, and failover processes.
- Chapter 2 — *vCenter Server Heartbeat Monitoring* describes monitoring operations and how to view the operational status of vCenter Server Heartbeat and protected vCenter Server components.
- Chapter 3 — *Managing vCenter Server Heartbeat* provides instructions and procedures to configure vCenter Server Heartbeat to provide protection to vCenter Server and its components and services.
- Chapter 4 — *Maintaining vCenter Server Heartbeat* discusses common procedures to perform the day-to-day operations such as applying updates, hotfixes, and patches to your vCenter Server Heartbeat installation.
- Chapter 5 — *vCenter Server Heartbeat Diagnostics* identifies techniques to diagnose common issues and unexpected behaviors.

Document Feedback

VMware welcomes your suggestions for improving our documentation and invites you to send your feedback to docfeedback@vmware.com.

Abbreviations Used in Figures

Abbreviation	Description
Channel	VMware Channel
NIC	Network Interface Card
P2P	Physical to Physical
P2V	Physical to Virtual
V2V	Virtual to Virtual

Technical Support and Educational Resources

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

Online and Telephone Support

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

Go to www.vmware.com/support/phone_support.html to find out how to use telephone support for the fastest response on priority 1 issues (applies to customers with appropriate support contracts).

Support Offerings

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

VMware Professional Services

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

Introduction 1

This chapter includes the following topics:

vCenter Server Heartbeat Concepts

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

Architecture Overview

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

Server Identity

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

Active / Passive Roles

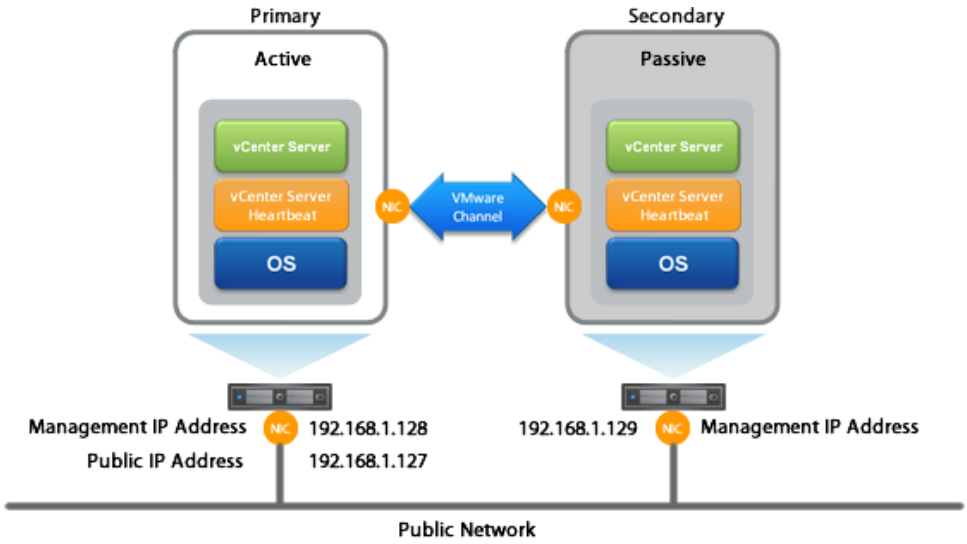
The "Role" of a node describes what the node is currently doing.

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

IP Addressing

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

Figure 1- 1. Architecture Overview



Managing the Primary and Secondary Servers

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

Failover Overview

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

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

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

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

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

vCenter Server Heartbeat Protection

vCenter Server Heartbeat provides the following protections:

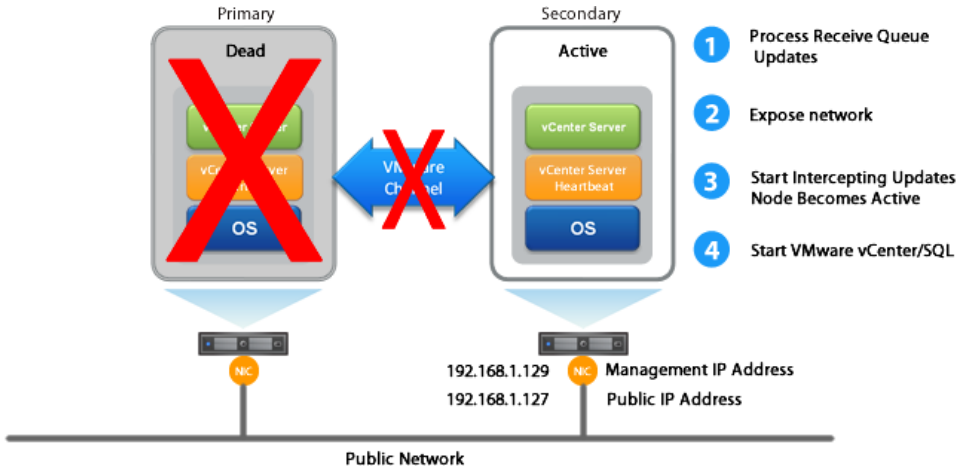
- *Server Protection* – provides continuous availability to end users through an operating system crash or hardware failure scenario ensuring that users are provided with a replica server instance and its IP address should the production node fail.
- *Network Protection* – proactively monitors the network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

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

Server Protection

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

Figure 1- 2. vCenter Server Heartbeat Initiated Failover



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

Network Protection

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

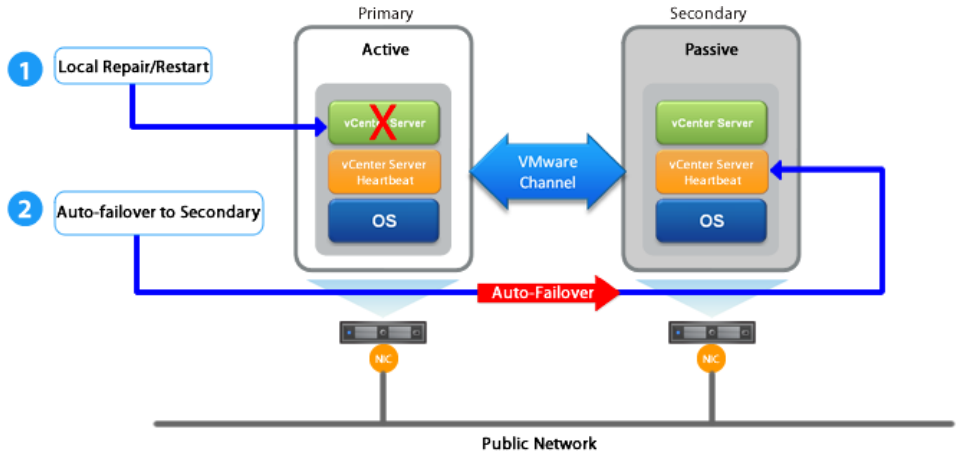
Application Protection

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

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

If the application does not successfully restart, vCenter Server Heartbeat initiates an auto-failover (2) in Figure 1-3. Refer to “vCenter Server Heartbeat Failover Processes,” on page 14 for further information about the failover process.

Figure 1- 3. vCenter Server Heartbeat Initiated Failover



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

Performance Protection

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

In addition to monitoring vCenter Server services, vCenter Server Heartbeat can monitor specific attributes to ensure that they remain within normal operating ranges. Similar to application monitoring, various rules can be configured to trigger specific corrective actions whenever these attributes fall outside of their respective ranges. vCenter Server Heartbeat provides the ability to define and perform multiple corrective actions in the event of problems on a service-by- service or even attribute-by-attribute basis.

Data Protection

All data files that users or vCenter Server requires in the application environment are protected and made available should a failure occur. After installation, vCenter Server Heartbeat configures itself to protect files, folders, and registry settings for vCenter Server on the active node by mirroring them in real time to the passive node. If a failover occurs, all files protected on the failed (Primary) node are available to users after the failover, hosted on the Secondary node.

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

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

vCenter Server Heartbeat Communications

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

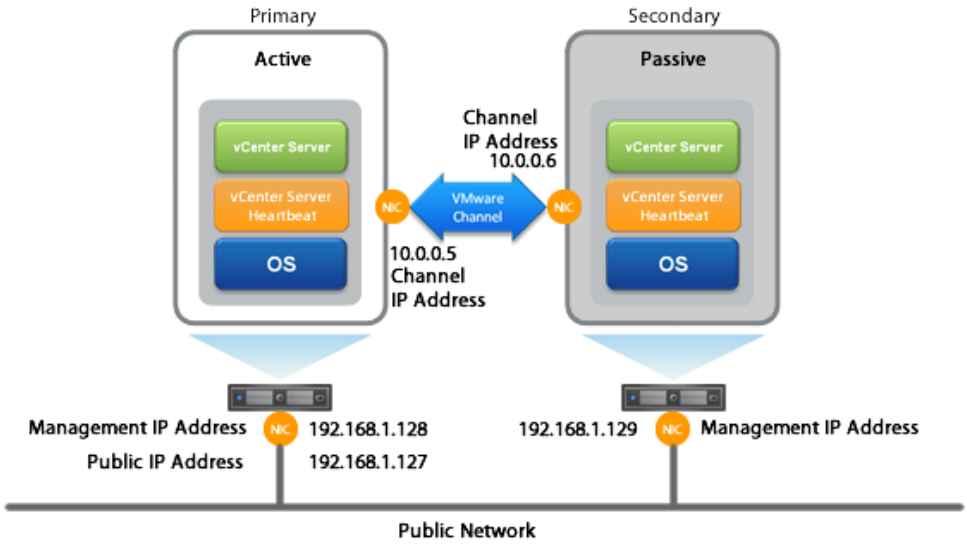
vCenter Server Heartbeat supports use of either multiple NICs or a single NIC. Both the Primary and Secondary must have the same number of NICs. The Public IP address provides client access and the Management IP address provides administrative access, while the VMware Channel provides for data transfer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

Multi-NIC Configuration

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

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

Figure 1- 4. Multi-NIC Configuration

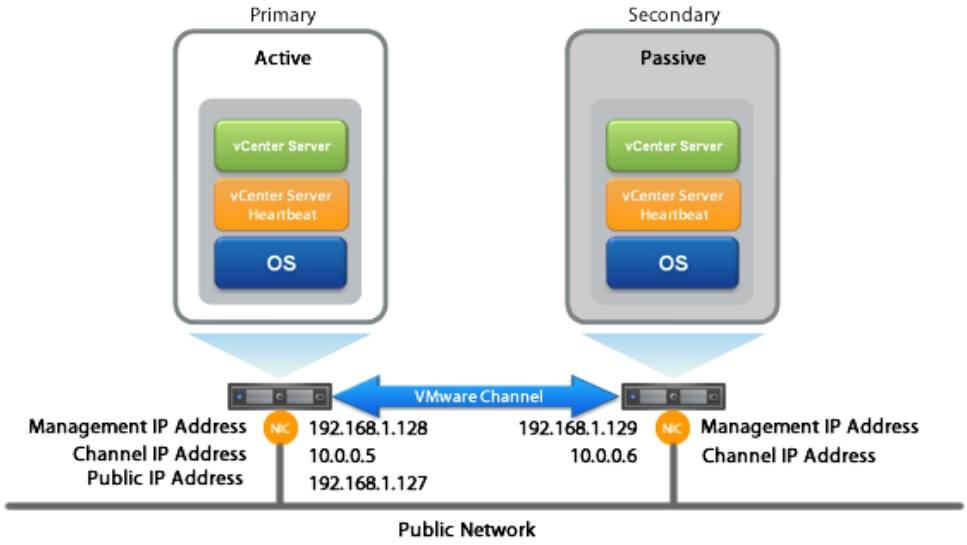


Single NIC Configuration

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

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

Figure 1- 5. Single NIC Configuration



LAN and Stretched vLAN Deployment

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

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

DNS in a LAN or Stretched vLAN

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

WAN Deployment

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

DNS in a WAN Deployment

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

vCenter Server Heartbeat Failover Processes

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

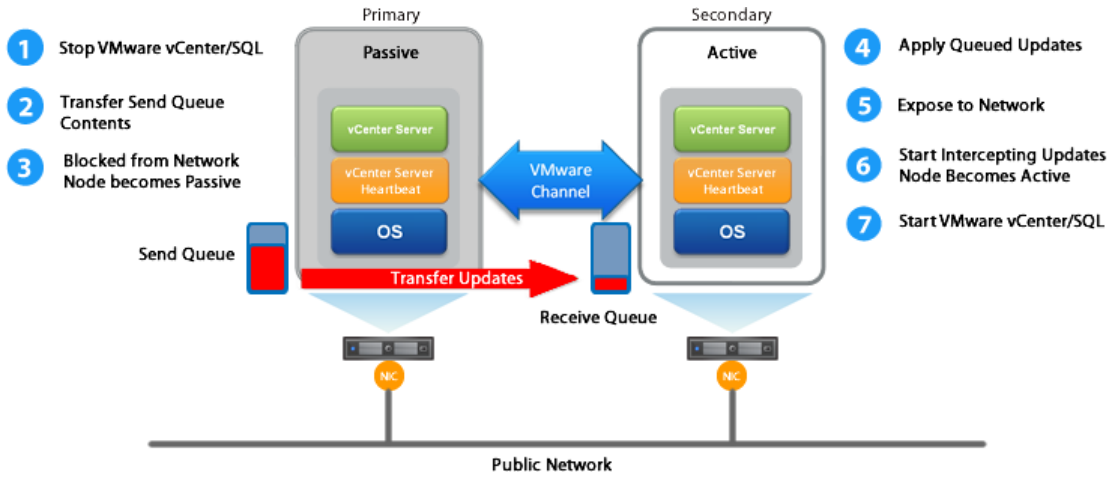
vCenter Server Heartbeat failovers are categorized by how the failover is initiated.

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

Failover - Manually Initiated by an Administrator

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

Figure 1- 6. Failover



A manually initiated failover performs the following steps:

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

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

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

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

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

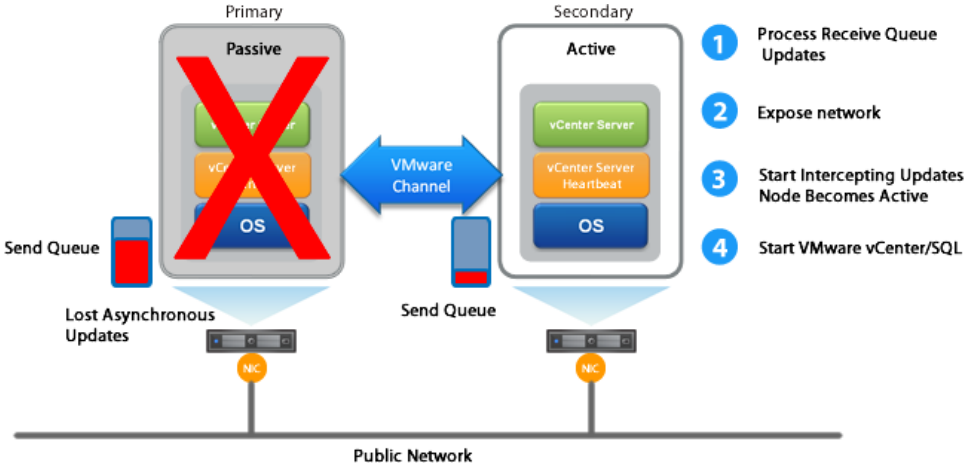
5 vCenter Server Heartbeat starts the same protected applications on the new active node. The protected applications become accessible to users. The failover is complete

Failover - Automatically Initiated by vCenter Server Heartbeat

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

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

Figure 1- 7. Automatic Failover (failed node)



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

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

The amount of data in the passive node's receive queue affects the time required to complete the failover process. If the passive node's receive queue is long, the system must wait for all updates to the passive node to complete before the rest of the process can take place. An update record can be applied only if all earlier update records are applied, and the completion status for the update is in the passive node's receive queue. Update records that cannot be applied are discarded.

2 Switch mode of operation from passive to active.

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

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

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

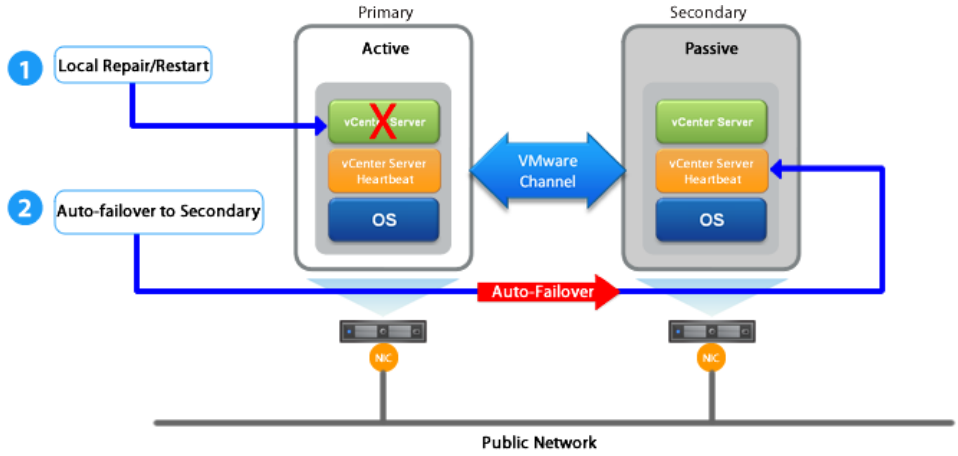
At this point, the originally active node is offline and the originally passive node is filling the active role and running the protected applications. Any updates completed before the auto-failover are retained. Application clients can reconnect to the application and continue running as before.

Resulting from a failed application or service

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

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

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



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

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

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

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

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

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

Failover in a WAN Environment

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

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

vCenter Server Heartbeat Monitoring 2

After installation of vCenter Server Heartbeat, initial operational configuration and day-to-day operations are performed using the vCenter Server Heartbeat Console. vCenter Server Heartbeat operates over a Pair of vCenter Server Heartbeat nodes and is administered in these Pairs. The vCenter Server Heartbeat Console is used to administer one or more Pairs.

This chapter includes the following topics:

Supported vCenter Server Heartbeat Clients

vCenter Server Heartbeat allows the use of multiple clients to provide basic management of vCenter Server Heartbeat pairs. vCenter Server Heartbeat communicates with the following clients:

Note Each client permits differing levels of permissions based upon either vCenter Server role or user account permissions as indicated below.

Available Clients:

- vSphere Web Client (NGC)
- vSphere Client (C#)
- vCenter Server Heartbeat Console (local or remote)
- NFCMD (command line)

The following (table 2-1) provides the level of permissions for each client based upon user role.

Table 2- 1. VMware vCenter Server Heartbeat Account Permissions

Client	vSphere Web Client		vSphere Client		vCSHB Console	NFCMD
vCenter Server role	Administrator	User	Administrator	User	N/A	N/A
Windows role	N/A	N/A	N/A	N/A	Local System Administrators Group	Local System Administrators Group
View	Yes	Yes	Yes	Yes	Yes	Yes
Make Active	Yes	No	Yes	No	Yes	Yes
Start/Stop Applications	Yes	No	Yes	No	Yes	Yes
Start/Stop Replication	Yes	No	Yes	No	Yes	Yes
Shutdown	Yes	No	Yes	No	Yes	Yes
Comments	Permissions derived from vSphere Client login		Permissions derived from vSphere Client login		Permissions derived from vCSHB Console login account[1, 2]	Permissions derived from the permissions of the currently logged in user[3]

Notes:

1 Only the Administrator or members of the Administrator Group can login to the vCenter Server Heartbeat Console. User level accounts are not permitted. The account used to login will be validated against the virtual machine where vCenter Server Heartbeat is installed. If the user account is validated as a member of the Administrator Group, login can proceed. If the user account is not a member of the Administrator Group, login will fail.

2 Once an Administrator has logged in to a vCenter Server Heartbeat pair using the vCenter Server Heartbeat Console, they are not prompted for username and password during subsequent logons to that specific pair.

3 The NFCMD utility connects to the vCenter Server Heartbeat instance and logs in using the credentials of the currently logged in user. The vCenter Server Heartbeat service allows administrators on the local node to log on using NFCMD and execute commands. If you are running NFCMD on another node, then you must setup a TrustedClient relationship for the hostname and user name you want to use by connecting first using the vCenter Server Heartbeat Console.

vCenter Server Heartbeat Console

The vCenter Server Heartbeat Console runs from either of the two nodes in the Pair or remotely from another node in the same subnet that has vCenter Server Heartbeat or the vCenter Server Heartbeat Client Tools installed.

Note You can install vCenter Server Heartbeat on a Windows XP and Windows Vista SP1 or later workstation to act as a client to the Pair or on Windows Server 2003. Download and run Setup similar to vCenter Server Heartbeat installation on the workstation and select *Install Client Tools Only* on the *Setup Type* page.

Starting vCenter Server Heartbeat Console

Start vCenter Server Heartbeat Console from any node of the vCenter Server Heartbeat Pair.

Procedure

1 Right-click the VMware vCenter Server Heartbeat interactive status icon on the Windows tool tray (located on the right side of the Windows tool bar). The vCenter Server Heartbeat quick access menu opens.

2 Select *Manage Server*.

The vCenter Server Heartbeat Console opens in a window and displays the *Heartbeat Servers* (overview) pane.

Note Alternatively you can start vCenter Server Heartbeat Console from the VMware program group on the Windows Start menu. This is the only method supported if vCenter Server Heartbeat Console has been installed on a workstation that is not part of the Pair.

Navigate vCenter Server Heartbeat Console

After vCenter Server Heartbeat Console is running, use the navigation panel on the left of the vCenter Server Heartbeat Console window to view and select Groups and Pair connections you can manage with vCenter Server Heartbeat Console.

Note A *Group* is an arbitrary collection of vCenter Server Heartbeat Pairs used for organization.

A *Connection*, or *Pair Connection* allows vCenter Server Heartbeat Console to communicate with a vCenter Server Heartbeat Pair either on the same machine or remotely.

See “Adding a vCenter Server Group,” on page 22 and “Adding a New Connection,” on page 23 for information on how to add Groups and Pair Connections to vCenter Server Heartbeat Console.

The selection of the Group or Pair you make in the navigation panel provides information related to only the selected Group or Pair. To avoid confusion, pay particular attention to the selection in the navigation panel when managing more than one Group or Pair.

Note Groups and Pairs are not automatically detected by vCenter Server Heartbeat Console. Each Group or Pair you intend to manage must be added to vCenter Server Heartbeat Console before you can use it to view status or change settings for that Group or Pair Connection.

Select a Pair in the navigation panel of vCenter Server Heartbeat to show a set of tabs and sub-tabs that offer detailed status and control of the associated vCenter Server Heartbeat node in the Pair.

Changing the Font for vCenter Server Heartbeat Console

You can change the font used in the vCenter Server Heartbeat Console interface.

Procedure

1 Select *Font Selection* from the *Preferences* menu. The *Font Selection* dialog opens.

2 In the *Style* pane, scroll to and click to select a font.

3 In the *Size:* text box, type a new numeric (point) size or use the arrow buttons to change the font size.

4 Click **OK**.

A confirmation message appears.

5 Click **Yes** to confirm the changes and restart vCenter Server Heartbeat Console to apply the new font settings. Click **No** to restart later; the changes will be applied the next time vCenter Server Heartbeat Console is started.

Working with Groups

vCenter Server Heartbeat allows you to Group pairs based upon logical organization such as business function or category.

Adding a vCenter Server Group

The *Add Group* feature in vCenter Server Heartbeat Console allows you to add new vCenter Server Heartbeat Groups to manage.

Procedure

1 Open vCenter Server Heartbeat Console and click **Add Group** in the tool bar, select *Add Group* from the *File* menu, or right-click an existing group in the navigation panel and select *Add Group* from the menu.

2 Type the name for the new group into the text box and click **OK**.

The newly created group appears in the navigation panel on the left of the vCenter Server Center Heartbeat window.

Removing a vCenter Server Heartbeat Group

The *Remove Group* feature in vCenter Server Heartbeat allows you to remove existing vCenter Server Heartbeat Groups from management.

Procedure

1 Select the Group to be removed in the navigation panel of vCenter Server Heartbeat Console. Click **Remove Group** in the tool bar or select *Remove Group* from the *File* menu.

A confirmation message appears.

2 Click **Yes**.

Working with Pairs in vCenter Server Heartbeat Groups

When you created a vCenter Server Heartbeat Group using the instructions in “Adding a vCenter Server Group,” on page 22, you created an empty container. You must add connections to the Pair or Pairs that make up your new vCenter Server Heartbeat Group to enable management of them.

Adding a New Connection

The *Add Connection* feature in the vCenter Server Heartbeat Console allows you to add a new Pair Connection to an existing vCenter Server Heartbeat Group.

Procedure

1 In the navigation panel, select the vCenter Server Heartbeat Group to receive the new connection. Click **Add Connection** in the tool bar, select *Add Connection* from the *File* menu, or right-click an existing group in the navigation panel and select *Add Connection* to invoke the *Add Connection* dialog.

2 Type the *Host Name* or *IP address* for the new connection into the text box, select the *Port Number* (if different from the default value of 52267), and select a group from the *Add to Group* drop-down list (to add the connection to a Group other than the one currently selected).

3 Click the **Alternate IPs** button to add additional IPs for the node. Click **OK**.

Note The *Add Connection* dialog allows you to add additional Management IP addresses to the connection for the node. In the event that the main IP address becomes unavailable, the vCenter Server Heartbeat Console will attempt to use the alternate IP addresses to connect to vCenter Server Heartbeat.

The newly created connection appears in the navigation panel on the left of the vCenter Server Heartbeat Console window and vCenter Server Heartbeat Console attempts to connect to the node. You may be prompted to accept a secure connection certificate from the node. This allows communications between vCenter Server Heartbeat Console and the node to be encrypted. To accept the certificate, click **OK**.

4 You may be prompted for credentials that allow you to have access to the node. Typically you will be asked for these credentials the first time you connect from a particular client system. If so, enter a *Username* that has administrator rights on the node that you are connecting to, enter the *Password*, and click **OK.**

Once you have connected to a particular node and have a valid secure connection certificate, the next time you use vCenter Server Heartbeat Console on this client system it will automatically connect to the node. If the certificate expires or becomes invalid, the connection may be removed from vCenter Server Heartbeat Console requiring you to reconnect and accept the new certificate. If the IP address of the client system changes, you may have to re-enter the username and password credentials.

Note The *Server: Summary* page updates to represent any existing network relationships of the added node.

---

5 Enter the remaining connections necessary to define the new vCenter Server Heartbeat Group.

Editing a Connection

The *Edit Connection* feature in the vCenter Server Heartbeat Console allows you to change the *Port Number* for existing connections.

Procedure

1 In the navigation panel, select the connection you want to change and select *Edit Connection* from the *File* menu or right-click an existing connection in the navigation panel and select *Edit Connection* from the menu to display the *Edit Connection* dialog.

Note When a configured connection is not found, an error message may be displayed. Click **Edit Connection** to reconfigure the connection.

2 Type the new value for the *Port Number* into the text box, or use the **Up** or **Down** arrow controls to the right of the text box to select a new value.

3 Click **OK**.

Moving a Connection

The *Move Connection* feature in vCenter Server Heartbeat Console allows you to reassign an existing Pair to a different Group.

Procedure

1 Select the Pair in the navigation panel and click **Move Connection** in the tool bar, select *Move Connection* from the *File* menu, or right-click on the Connection in the navigation panel and select *Move Connection* from the menu to display the *Move Connection* dialog.

2 Select the destination Group to receive the Connection from the drop-down list.

3 click **OK**.

Removing a Connection

The *Remove Connection* feature in vCenter Server Heartbeat allows you to remove an existing Connection.

Procedure

1 Select the Connection in the navigation panel and click **Remove Connection** in the tool bar, select *Remove Connection* from the *File* menu, or right-click on the connection in the navigation panel and select *Remove Connection* from the menu.

A confirmation dialog appears.

2 Click **Yes**.

Editing User Name and Password Settings

Use the *Edit User Name and Password* feature in vCenter Server Heartbeat Console to change the *User Name* and *Password* settings used to connect to a given Pair.

Procedure

1 Select a connection in the navigation panel and select *Edit User Name and Password* from the *File* menu or right-click on the Connection in the navigation panel and select *Edit User Name and Password* from the menu to display the *Edit User Name and Password* dialog.

2 Type new values for *User Name* and *Password* into the corresponding text boxes.

3 Click **OK**.

Reviewing the Status of Groups and Pairs

Click on the top level of the *Heartbeat Servers* page in the vCenter Server Heartbeat Console to view a list of all managed Pairs and a quick status of protected applications, network, files system, and registry settings for each Group. The status hyperlinks in the overview window links to pages that provide more specific related information and management controls.

- The *Server connection* name to view the *Server: Summary* page
- The *Applications status* to view the *Applications: Summary* page
- The *Network status* to view the *Network Monitoring* page
- The *File System or Registry status* to view the *Data: Replication* page

Exiting vCenter Server Heartbeat Console

Procedure

1 Click **Exit** on the *File* menu.

The *Confirm Exit* message appears.

2 Click **Yes**.

vSphere Web Client Plug-in

During installation of vCenter Server Heartbeat, Setup installs a plug-in for vSphere Web Client that allows you to view or manage vCenter Server Heartbeat, depending on your user account permissions, from the integrated vSphere Web Client. The *Heartbeat* tab of the vSphere Web Client provides the status of vCenter Server Heartbeat and provides administrators the ability to perform basic vCenter Server Heartbeat management functions such as perform a failover or stop and start replication.

Note Use of vCenter Server Heartbeat Plug-in for vSphere Web Client requires that Adobe Flash Player 11.4 or later is installed. If Adobe Flash Player 11.4 or later is not installed prior to installation of vCenter Server Heartbeat, selecting the *Heartbeat* tab in vSphere Web Client for the first time will provide an opportunity to download Adobe Flash Player 11.4 from the internet and install it.

Launching the Heartbeat Plug-in for vSphere Web Client

The Heartbeat Plug-in is integrated with vSphere Web Client and allows you to administer your Pair.

Procedure

1 Login to vSphere Web Client.

2 Select *vCenter* in the navigation pane of vSphere Web Client.

The vCenter pane is displayed.

3 Under the Inventory Lists, select *vCenter Servers*.

A list of manageable vCenter Servers is displayed by Fully Qualified Domain Names (FQDN).

4 Select the FQDN of the vCenter Server to be managed.

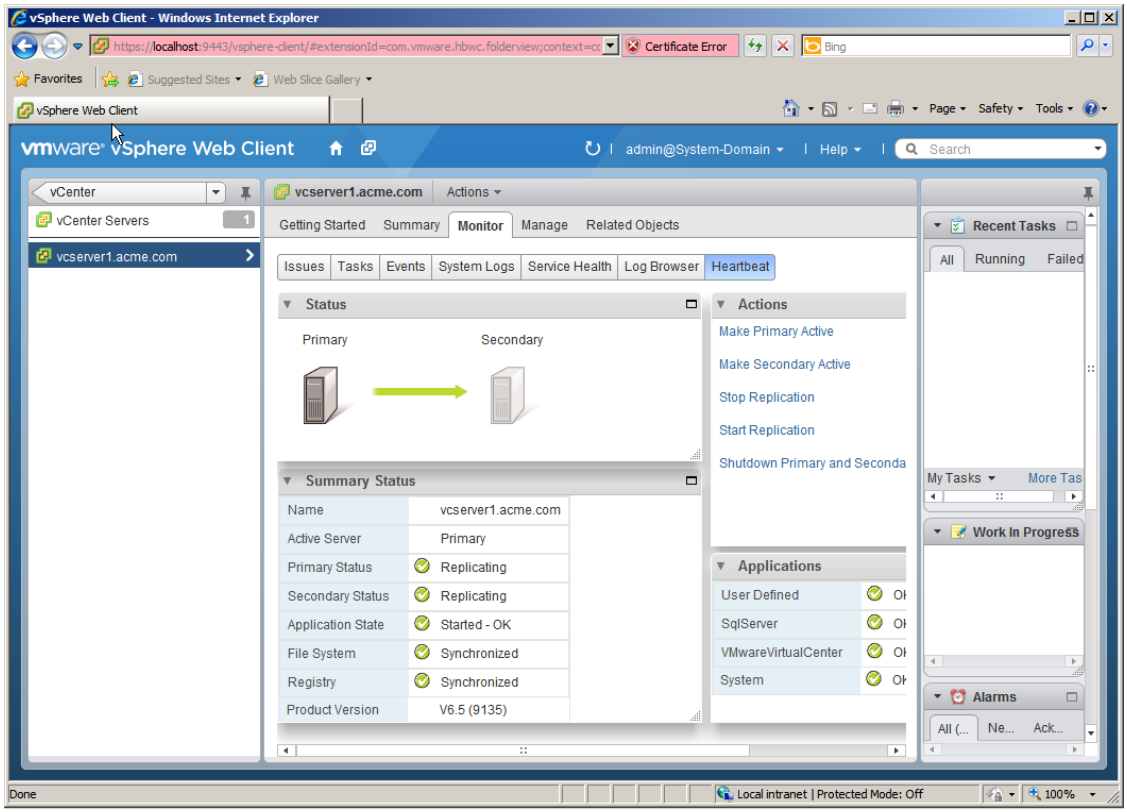
5 Select the *Monitor* tab of the vSphere Client.

The Monitor sub-tabs are displayed.

6 Select the *Heartbeat* sub-tab of vSphere Web Client.

The Heartbeat Plug-in content is displayed.

Figure 2- 1. vSphere Web Client Heartbeat Plug-in



Performing a Failover Using vSphere Web Client

Procedure

1 Navigate to the *Heartbeat* sub-tab in the vSphere Web Client.

2 Click either **Make Primary Active** or **Make Secondary Active** as appropriate.

A confirmation dialog is displayed.

3 Click **Yes** to confirm your action.

vCenter Server Heartbeat performs a failover.

Note After performing a *Make Active* operation, the *Heartbeat* tab may fail to display properly. To update the *Heartbeat* tab, refresh vSphere Web Client browser.

Starting or Stopping Replication Using vSphere Web Client

Procedure

1 Select the *Heartbeat* tab of vSphere Web Client.

2 Click either **Stop Replication** or **Start Replication** as appropriate.

vSphere Client Plug-in

During installation of vCenter Server Heartbeat, Setup installs a plug-in for vSphere Client that allows you to manage vCenter Server Heartbeat from the integrated vSphere Client. The *Heartbeat* tab of the vSphere Client provides the status of vCenter Server Heartbeat and the ability to perform basic vCenter Server Heartbeat management functions such as perform a failover or stop and start replication.

Note Use of vCenter Server Heartbeat Plug-in for vSphere Client requires that Adobe Flash Player 11.4 or later is installed. If Adobe Flash Player 11.4 or later is not installed prior to installation of vCenter Server Heartbeat, selecting the *Heartbeat* tab in vSphere Client for the first time will provide an opportunity to download Adobe Flash Player 11.4 from the internet and install it.

When using the Heartbeat Plug-in for the first time (selecting the *Heartbeat* tab), you must be connected to the internet.

Launching the Heartbeat Plug-in for vSphere Client

The Heartbeat Plug-in is integrated with vSphere Client and allows you to administer your Pair.

Procedure

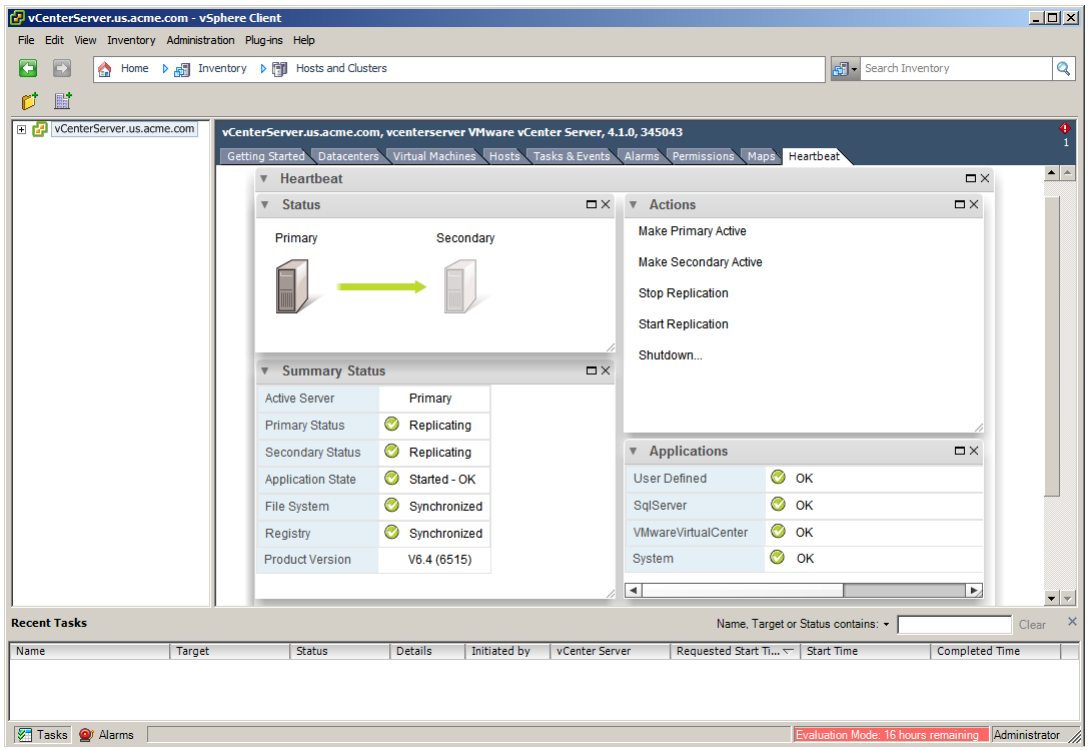
1 Login to vSphere Client.

2 A security certificate is presented. Select the check box to install the security certificate.

3 Select the *Heartbeat* tab of vSphere Client.

4 When prompted to acknowledge the Security Alert, click **Yes** to proceed. The Heartbeat Plug-in is displayed.

Figure 2- 2. vSphere Client Heartbeat Plug-in



Performing a Failover Using vSphere Client

Procedure

1 Select the *Heartbeat* tab of vSphere Client.

2 Click either **Make Primary Active** or **Make Secondary Active** as appropriate.

3 When prompted accept the security certificate to complete the operation.

Note Each time you perform a *Make Active* operation from the vSphere Client you must accept the security certificate. After performing a *Make Active* operation, the *Heartbeat* tab may fail to display properly. To update the *Heartbeat* tab, restart vSphere Client.

After a failover, should vSphere Client fail to authenticate when it attempts to connect, select the use *Windows Credentials* checkbox.

Starting or Stopping Replication Using vSphere Client

Procedure

1 Select the *Heartbeat* tab of vSphere Client.

2 Click either **Stop Replication** or **Start Replication** as appropriate.

Server Monitoring

Protection against operating system or hardware failure affecting the active node is accomplished using two instances of the vCenter Server Heartbeat that monitor one another by sending “I’m alive” messages over the VMware Channel. If the passive node detects that this process (the heartbeat) has failed, a failover is initiated.

Checking the vCenter Server Heartbeat Pair Status

The *Server: Summary* page is the default page that opens when administering the vCenter Server Heartbeat pair. The *Server: Summary* page allows you to view the roles that nodes are performing (active or passive), actions that each node is currently performing, and summary information on communications status and data replication between nodes. The lower pane displays status information for each node in the pair.

Note To change the currently displayed node (active or passive), click the node graphical representation in the upper pane, or select the *Identity* tab (Primary or Secondary) in the bottom pane.

The following (table 2-2) lists the possible system statuses and their meanings.

Table 2- 2. System Status

Status	Icon	Description
Heartbeat service shutdown		Heartbeat service is shut down.
Initializing		Heartbeat service is starting up.
Replicating		(Normal status) File and registry changes on the active node are intercepted and replicated to the passive node. Protected applications are monitored.
Not replicating		File and registry replication is stopping and all protected applications may be closing down.
Switching active server		The system is performing a failover.
Connecting to peer server		VMware Channel connections have been established between the two nodes.
Disconnecting from peer server		VMware Channel connections have been lost between the two nodes.
Stopping replication		File replication is stopping and, optionally, all protected applications may be closing down.
Starting replication		Replication is starting and protected applications are optionally starting.
Starting as active server		Heartbeat is initializing on the active node and starting protected applications.
Heartbeat service shutting down		Heartbeat is stopping. The Heartbeat service is shutting down, and will no longer participate in replication. Optionally, protected applications may be stopped.
Lost active server		The passive node has lost connection to the active node. If this condition persists for the failover timeout, and failover is permitted between the pair of nodes, then a failover will occur.
Active following failover		A failover has occurred,
Server not responding		The Heartbeat service cannot be contacted on the node.

When viewing the passive node status, the file system and registry status are displayed graphically. The following (table 2-3) lists possible synchronization statuses and their meanings.

Table 2- 3. File System and Registry Status

Status	Icon	Description
Synchronized		Fully synchronized.
Unchecked		There are files that are currently unchecked. A full system check did not complete.
Out-of-Sync		Not synchronized.
Uninitialized		Displayed when the Heartbeat service is starting up or shutting down.
Checking		The registry is currently in the process of synchronization.
Error		Not synchronized.

When vCenter Server Heartbeat establishes a connection, it triggers a file synchronization and verification process to ensure all protected files on both nodes are identical. The process checks each 64K block of the protected file and performs a checksum to determine whether blocks differ. If blocks are the same, it is marked as synchronized. If blocks differ, then it is replicated to the passive node and then marked as synchronized. The file verification and synchronization process is finished after all blocks of the stipulated files are marked as synchronized.

Monitoring the Status of the Active and Passive Nodes

The *Server: Monitoring* page provides additional information about the status of communications between nodes within the pair. Graphical representation provides an overview of communications status between nodes. A green channel icon indicates the channel is connected and healthy while a yellow dashed channel icon indicates that communications are not operational between indicated nodes. In addition to the heartbeat sent between nodes, vCenter Server Heartbeat also sends a ping to ensure the nodes remain visible to one another.

Network Monitoring

vCenter Server Heartbeat proactively monitors the network by polling up to three predefined nodes to ensure that the active node is visible on the network.

vCenter Server Heartbeat also proactively monitors the capability of the active and passive nodes to communicate with the rest of the network by polling the Primary DNS server, Default Gateway, and the Global Catalog server at regular intervals. If all three nodes fail to respond, for example, due to a network card or local switch failure, vCenter Server Heartbeat can initiate a failover, allowing the passive node to assume the role of the active node.

Communications Status

Use the *Data: Traffic/Queues* page to check the status of the VMware Channel, the active node's send, and passive node's receive queues.

Reviewing the VMware Channel Status

The *Data: Traffic/Queues* page displays the VMware Channel status.

VMware Channel status can be displayed as:

- Connected – A green solid arrow icon
- Waiting – A solid orange icon is displayed when the channel has just disconnected. vCenter Server Heartbeat will wait for a configured amount of time before deciding the channel is disconnected
- Not connected – A red broken line icon

Statistics of the connection with regards to the data sent by either node, and the size and age of the oldest entry in the active node's send queue and passive node's receive queue are displayed on this page.

The *Channel Connection* tab in the lower pane displays the IP addresses used by the VMware Channel for Primary to Secondary connections and the port that communications are using.

Network Isolation Protection

vCenter Server Heartbeat monitors the network to identify when a network failure has occurred and takes the appropriate action to maintain communications and prevent the occurrence of two active nodes.

Typical Failover and Active Node Isolation Scenarios

Failover

The following scenario assumes that vCenter Server Heartbeat is deployed in a LAN and the active node has failed and is no longer available.

Upon detection of missed heartbeats, vCenter Server Heartbeat on the passive node performs the following steps:

1 As soon as the passive node detects that the VMware Channel is experiencing missed heartbeats, it attempts to ping the active node's Management IP address via the Public network using the passive node's NIC configured with the Management IP address. If the ping is successful, the passive node will veto the failover. If the ping is unsuccessful, it will continue to the next step.

Note Since the passive node assumes that active node has failed, the passive node will not attempt to verify synchronization with the active node.

2 At this point, the passive node checks the configured value of the *Failover timeout* and starts a "Heartbeat lost" countdown. The passive node continues with the next step.

3 The passive node attempts to ping the configured waypoints on the Public network to determine if it is still visible on the Public network. If pings to the waypoints on the Public network are unsuccessful, the passive node remains passive and takes no action. If pings to the waypoints on the Public network are successful, the passive node continues to the next step.

4 At this point, failover to the passive node is postponed until the value of the *Failover timeout* has elapsed.

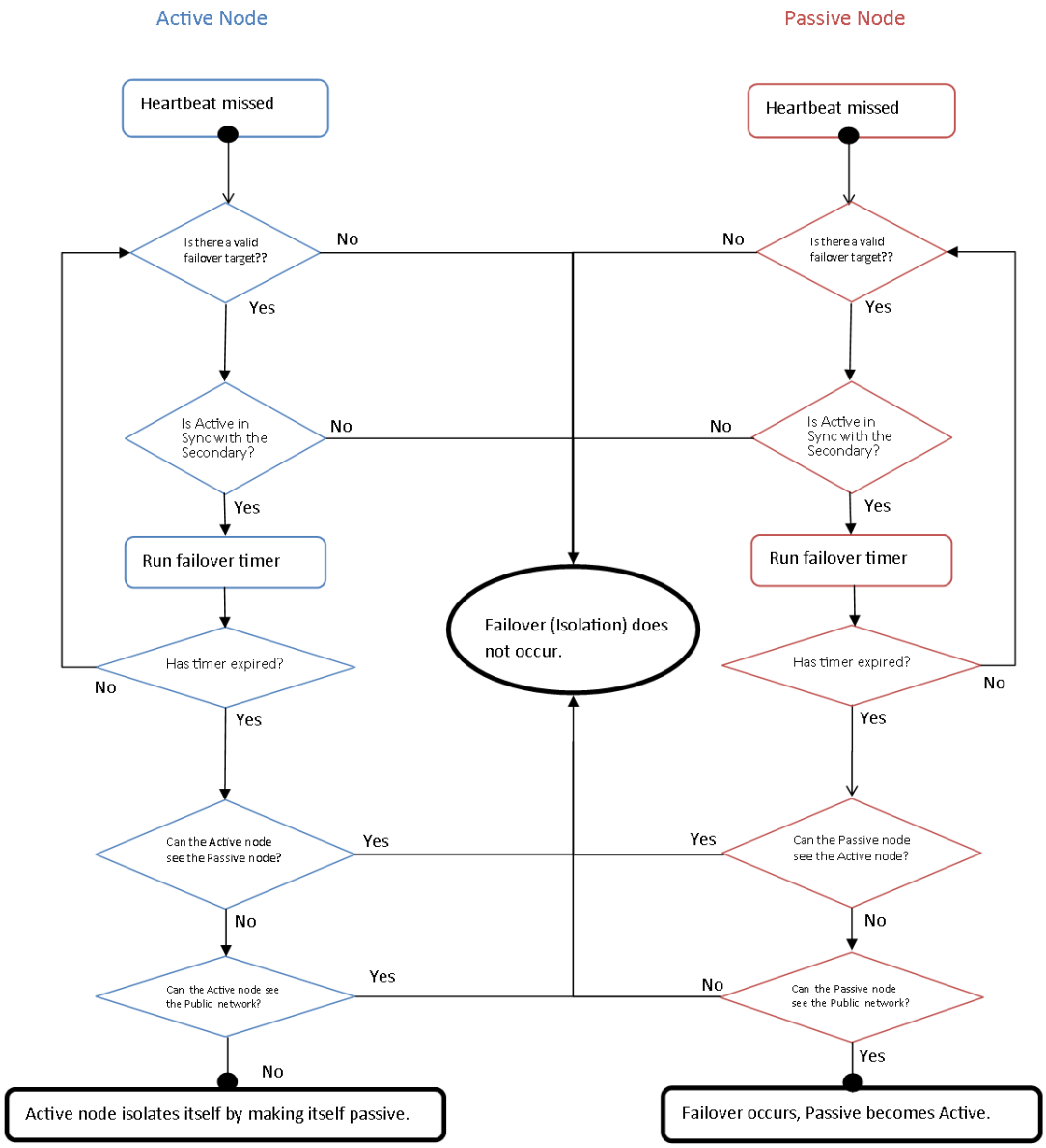
5 The passive node changes its role to active, assumes the Public IP address, and starts all services.

6 As the new active node, it will begin accepting traffic from clients.

Active node Isolation

Figure 2-3 illustrates a scenario where the active node has lost connection with the passive node via the VMware Channel.

Figure 2- 3. Network Isolation Workflow Diagram



Upon detection of missed heartbeats vCenter Server Heartbeat performs the following steps:

1 As soon as the active node detects that the VMware Channel is experiencing missed heartbeats, it determines *if a valid failover target (the passive node) is present*.

Simultaneously, once the passive node detects missed heartbeats, it determines *if it is a valid failover target*.

2 Next, the active node determines if it is synchronized with the failover target (the passive node). If synchronized, it continues to the next step. If it is not synchronized, it vetos a failover.

Simultaneously, the passive node checks to see if it is synchronized with the active node. If synchronized, it continues to the next step. If it is not synchronized, it vetos a failover.

3 At this point, both the active and passive nodes check the configured value of the *Failover timeout* and start a "Heartbeat lost" countdown. Both nodes start the countdown at approximately the same time.

4 Failover or isolation of the active node is postponed until the configured *Failover timeout* value (in seconds) has elapsed and it is during this period that both nodes accomplish steps 1 & 2.

5 Once the configured *Failover timeout* period has elapsed, the active node assumes the VMware Channel is lost and attempts to ping the failover target (passive node) via the Public network. If the ping is successful, active node isolation is vetoed. If the attempt to ping the failover target is unsuccessful, the active node proceeds to the next step.

Simultaneously, the passive node assumes the VMware Channel is lost and attempts to ping the active node via the Public network. If the ping is successful, failover is vetoed. If the ping attempt is unsuccessful, the passive node proceeds to the next step.

Note If the nodes have reached this point, then neither node can see the other node.

6 Both the active and passive nodes check their connectivity to the Public network. If the active node has lost connectivity to the Public network, it isolates itself by making itself passive (potential active).

Should the active node reconnect with the passive, it becomes active again. Otherwise, it remains passive. If the passive node has lost connectivity to the Public network, it vetos a failover.

Application Monitoring

vCenter Server Heartbeat monitors protected applications and services to ensure that applications are available to clients by monitoring application and service status.

The Applications: Summary page displays the active node identity, application state and health, details of application types, and their corresponding running status and health. The lower pane provides an *Applications Log* that allows viewing of application events as they occur. This page also provides controls to edit, remove, start, and stop applications, and to configure and edit the configuration of all protected applications.

Viewing Application Status

After an application successfully starts and is running, you can view application status in the *Applications* pane of the *Applications: Summary* page. If an application fails, right-click the event in the *Applications Log* and click on **Properties** to invoke the *Event Properties* dialog and investigate the failure.

Checking the Status of Services

The *Applications: Services* page displays services that either you or plug-ins specify and services related to them by dependency (either as dependents or depends-on). Target states of protected services for the Primary and Secondary can be specified and are typically *Running* on the active and *Stopped* on the passive nodes. Services are protected if they are set to *Running* or *Automatic*, and are otherwise logged as unprotected. The status shows both the target and actual state for both Primary and Secondary nodes and *Failure Counts* for both nodes.

Performance Monitoring

Performance Monitoring describes how vCenter Server Heartbeat monitors system and application attributes to prevent an unexpected system or application failure.

vCenter Server Heartbeat monitors select application attributes to ensure that the application is performing as it should within configured thresholds. vCenter Server Heartbeat uses *Rules* that were automatically configured during Setup to monitor those attributes. Should an attribute exceed predefined thresholds, vCenter Server Heartbeat can take pre-emptive action to restart the application, restart the service, or initiate a failover.

Rules

The *Applications: Rules* page provides a list of rules with their current status and the ability to edit and check rules.

The following plug-ins implement the rules listed.

vCenter Server Plug-in

- Check health of Tomcat server
- Check vCenter License Check Connection to vCenter

vCenter SQL Server Plug-in

- DiskAvgSecsPerRead
- DiskAvgSecsPerWrite
- DiskIO
- DiskQueueLength
- DiskReadsPerSec
- DiskWritesPerSec
- DiskWriteable
- FreeDiskSpace
- FreeDiskSpaceOnDrive
- MemoryCommittedBytes
- MemoryCommittedBytesPercent

- MemoryFreePTEs
- MemoryPageReadsPerSec
- MemoryPageWritesPerSec
- MemoryPagesPerSec
- MemoryPagingFileUseage
- 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

vCenter Server Heartbeat allows you to check rule conditions of the current configuration against attributes of the system or application.

Procedure

- Right-click the intended rule and select *Check Now* from the menu or click **Check Now** at the top of the pane. The rule condition is displayed in the pane.

Monitoring Data Replication

vCenter Server Heartbeat monitors data replication by monitoring the replication and synchronization of protected files and provides a visual cue to replication and synchronization status of the nodes.

Two panes near the top of the *Data: Replication* page in vCenter Server Heartbeat Console, *File System Synchronization Status* and *Registry Synchronization Status*, provide graphical status information.

The synchronization status for each file or folder can read one of three different values depending on the verification and synchronization states as described in Table 2-4.

Table 2- 4. File and Registry Synchronization Status

Icon	Description
	The file is verified and successfully synchronized.
	The file is not synchronized on the active and passive node. This state often follows a failover and requires manual synchronization and verification.
	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.

Managing vCenter Server Heartbeat 3

vCenter Server Heartbeat provides the tools to customize configuration parameters to protect vCenter Server, View Composer, and SQL Server in the event of hardware, operating system, network communications, applications, or services failure.

This chapter includes the following topics:

Server Configuration Wizard

vCenter Server Heartbeat's *Server Configuration* wizard (*Configure Server* wizard) configures and maintains communications between vCenter Server Heartbeat nodes. After a system is set up and functioning correctly, reconfiguration is not normally needed.

Launching the Configure Server Wizard

Use the *Configure Server* wizard to modify communications between the Primary and Secondary nodes and reconfigure other components of vCenter Server Heartbeat when necessary. When using the *Configure Server* wizard to make modifications, ensure vCenter Server Heartbeat is stopped.

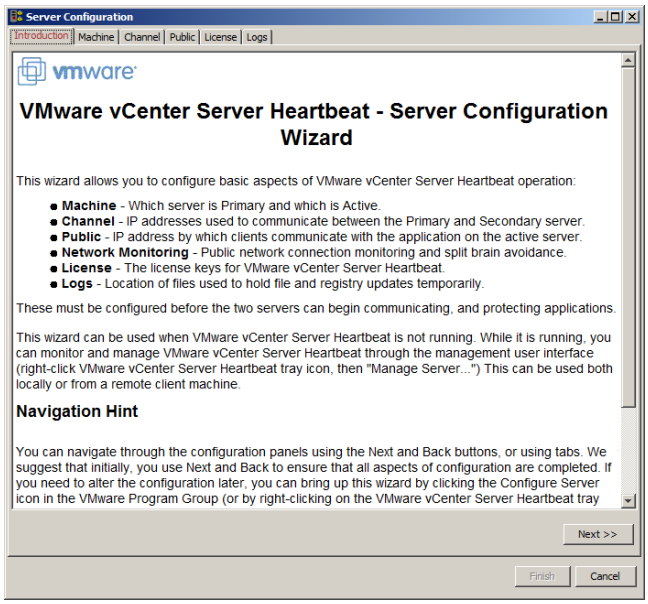
Procedure

1 Stop vCenter Server Heartbeat.

2 Click **Configure Server** on the desktop or navigate to **Start > All Programs > VMware > VMware vCenter Server Heartbeat > Configure Server** to launch the *Configure Server* wizard.

Note If vCenter Server Heartbeat was not stopped before launching the *Configure Server* wizard, a message displays stating that changes made in the *Configure Server* wizard will not be saved.

Figure 3- 1. Configure Server Wizard Introduction



Configuring the Machine

The *Machine* tab is used to set the *Server Identity*, identify the *Active Server*, and configure the *Client Connection Port*.

Configuring the Machine Identity

The identity is either Primary or Secondary and once assigned does not change during the life of the node.

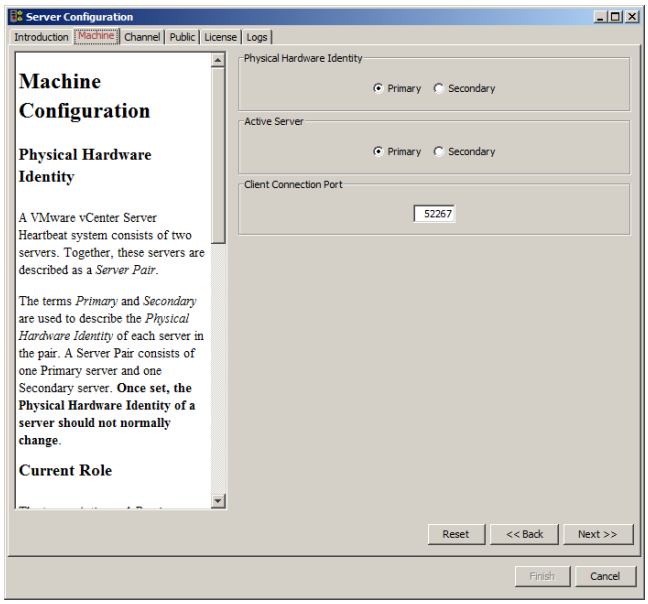
Caution The Identity should only be changed when directed to do so by VMware Support or by a knowledge base article.

Procedure

1 Click the **Machine** tab and select the *Physical Hardware Identity* for the local machine.

2 Click either **Next** or **Finish**.

Figure 3- 2. Configure Server wizard Machine Tab



Configuring the Role

Note Before changing the role of the local node, verify that the other (remote) node is not already performing the same role. vCenter Server Heartbeat is designed to prevent two passive or two active nodes from connecting.

Procedure

- To change the role, click the **Machine** tab, select the currently active node (Primary or Secondary), and click **Next** or **Finish**.

Configuring the Client Connection Port

Clients such as the vSphere Web Client or vCenter Server Heartbeat Console connect to vCenter Server Heartbeat using the *Client Connection Port*. Do not change this port unless another application is using it.

Procedure

- To change the *Client Connection Port*, click the **Machine** tab, edit the default entry (52267) and click **Next** or **Finish**.

Configuring the VMware Channel

Use the *Configure Server* wizard **Channel** tab to configure *Channel Routing*, *Default Channel Port*, and *Low Bandwidth Optimization*.

Configuring Channel Routing

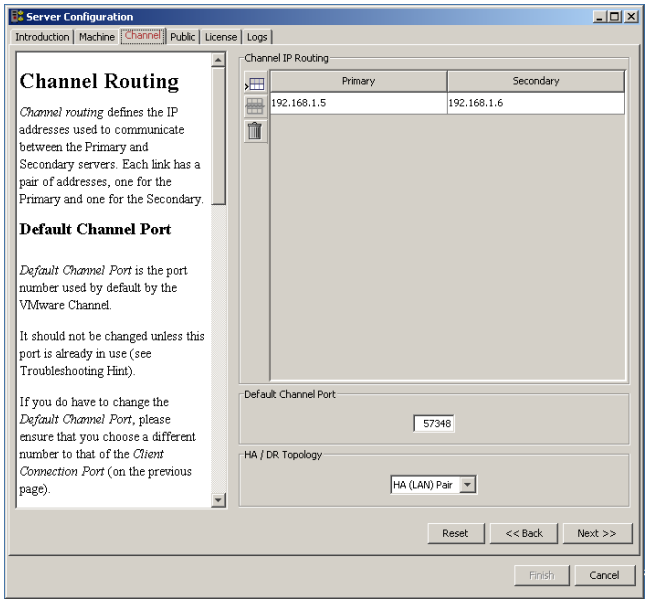
Channel IP Routing defines the IP addresses used to communicate between the Primary and Secondary nodes. Each link has a pair of IP addresses, one for the Primary and one for the Secondary.

To add an additional VMware Channel:

Procedure

1. Install and configure the additional NICs.
2. Launch the *Configure Server* wizard and click the **Channel** tab.
3. Click **Add Row** to add new IP addresses for both the Primary and Secondary nodes to the *VMware Channel IP Routing* table.
4. Use the drop-down menu to view a list of available IP addresses on the local node.
5. Type the remote node's IP address.

Figure 3- 3. Configure Server wizard — Channel Tab



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

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

Configuring the Default Channel Port

The VMware Channel uses the *Default Channel Port* to communicate between the Primary and Secondary nodes. Do not change this port unless another application is using it.

Procedure

- To change the *Default Channel Port*, click the **Channel** tab, edit the default entry (57348), and click **Next** or **Finish**.

Configure Low Bandwidth Optimization

Low Bandwidth Optimization is configured automatically during installation based upon configuration options selected during Setup. Low Bandwidth Optimization can be configured for: High Availability (HA) when deployed in a Local Area Network (LAN) or Disaster Recovery (DR) when deployed over a Wide Area Network (WAN).

In an HA configuration, queues and buffers are optimized for a high-speed LAN connection, compression is disabled, and failover between nodes is enabled.

In a DR configuration, queues and buffers are optimized for a low-bandwidth WAN connection, compression may be used, and failover between nodes is disabled.

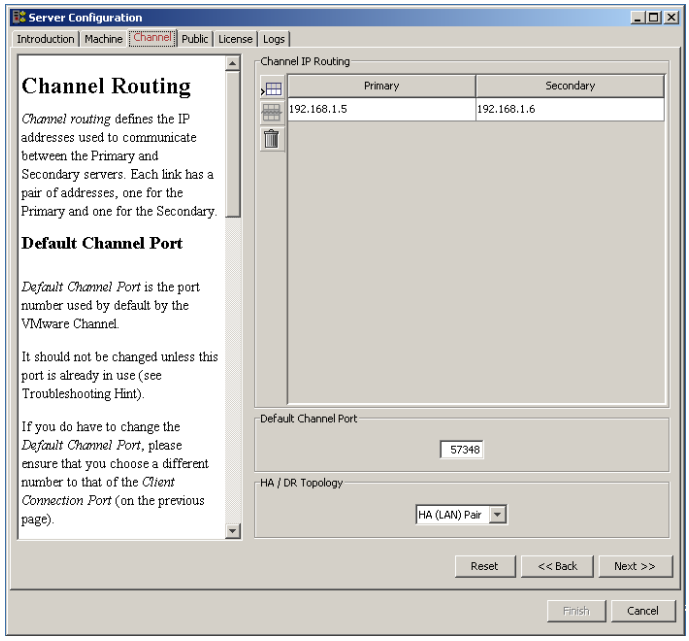
In the *Configure Server* wizard you can choose the HA or DR topology. However, if you have manually configured a non-standard topology, for example, by changing the failover settings, then *Non-Standard* will appear in the menu. You can choose to leave the non-standard topology option as it is, or reset it to one of the standard topologies.

Important The HA/DR Topology setting must be identical on both nodes in the pair.

Procedure

- To change Low Bandwidth Optimization after installation, select the **Channel** tab in the *Configure Server* wizard and click the *HA/DR Topology* drop-down to select the appropriate topology. Click **Next** or **Finish** to accept changes.

Figure 3- 4. Configure Server wizard - Channel tab



Configuring Public IP Addressing

During installation, vCenter Server Heartbeat configures the Public IP address(es). Depending on the deployment, vCenter Server Heartbeat nodes are configured with either one shared Public IP address in a LAN or two Public IP addresses in a WAN. The Public IP address(es) are used by clients to connect to protected applications.

Configuring Public IP Addressing

Should you need to add a Management IP address or additional Public IP address to your environment (for example when stretching from LAN to WAN), use the *Configure Server* wizard *Public* tab to add it.

Procedure

1. Select the **Public** tab of the *Configure Server* wizard and verify that *Non-Identical* is selected in the *Public Identity Mode* pane.

   Note This version of vCenter Server Heartbeat only supports *Non-Identical* Public Identity Mode. *Identical* Public Identity Mode is not supported.

2. Verify the vCenter Server or SQL Server Public name in the *Name used to connect to vCenter or SQL Server* field.
3. In the *NIC* field, select the Public network connection in the drop-down.
4. Enter the Public IP address in the *Public* IP field.

5 Enter the Public IP address Subnet Mask in the first *Mask* field.

6 Enter the reserved Management IP address in the *Mgmt IP* field.

7 Enter the reserved Management IP address Subnet Mask in the second *Mask* field.

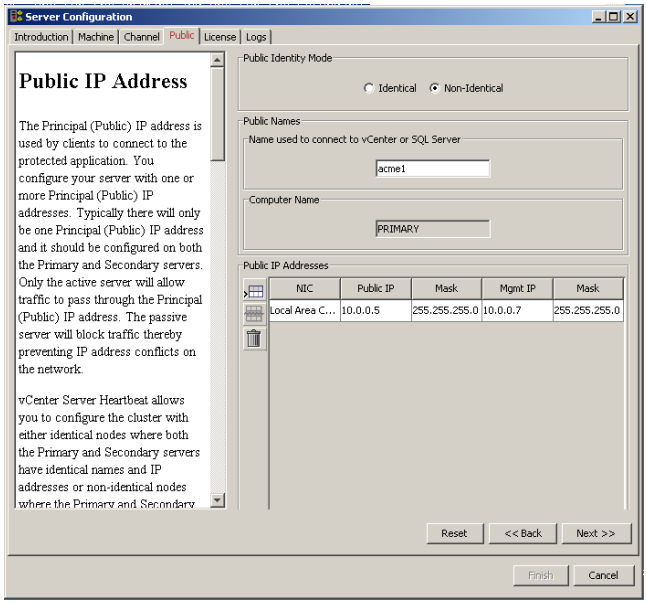
Note The *Public IP Addresses* table allows multiple entries. The table also allows you to configure Public IPs and Management IPs for the same network adapter on separate lines. This ability accommodates multiple Public IPs in the same or different subnets and multiple Management IPs in the same or different subnets. The following rules apply to the table:

- Each row must identify a network adapter
- Each row must identify either a Public IP/subnet mask or Mgmt IP/subnet mask
- For each network adapter listed, you must have at least 1 Public IP/subnet and 1 Mgmt IP/subnet, however these may be configured on separate rows

---

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

Figure 3- 5. Configure Server wizard — Public tab



Managing vCenter Server Heartbeat License Keys

To manage vCenter Server Heartbeat license keys, select the **License** tab of the *Configure Server* wizard.

Adding an Entry to the License Keys Table

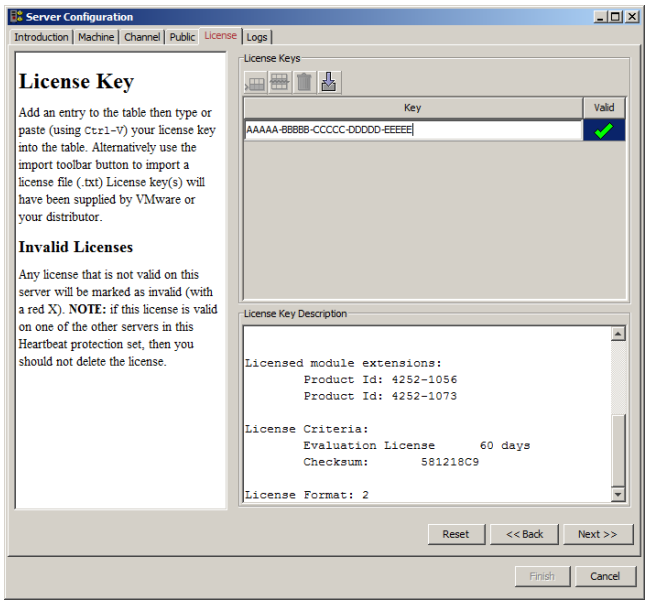
Procedure

1 Click the **Add Row** icon and enter your VMware vCenter Server Heartbeat serial number.

2 Manually type or paste (using **Ctrl**-**V**) your serial number into the table.

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

Figure 3- 6. Configure Server wizard — License tab



Configuring Logs

vCenter Server Heartbeat allows you to change the default location of logs used for storing data in the queue.

Configuring Message Queue Logs

Replication data received from the active node is temporarily stored in the passive node's receive queue. Replication data from the active node waiting to be sent across the VMware Channel is temporarily stored in the active node's send queue in message queue logs. When configuring the Message Queue Logs Location for each node, the setting only affects the local node. Logs can be in different locations on each node.

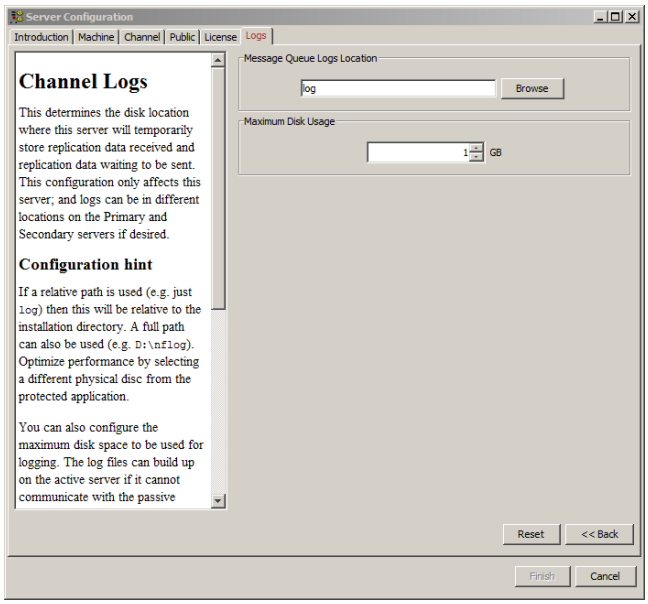
Procedure

1 Click the **Logs** tab.

2 Click **Browse** and navigate to the folder to store the message queue logs.

3 Select the folder and click **Next** or **Finish**.

Figure 3- 7. Configure Server Wizard — Logs



Configuring the Maximum Disk Usage

The *Configure Server* wizard allows you to configure the maximum disk space allocated for logging.

Log files can increase in size on the active node under the following conditions:

- If the active node cannot communicate with the passive node
- During certain operations on the passive node
- If the node is under heavy load

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

If vCenter Server Heartbeat runs out of disk space, it must be shut down before it can resume replication. Set the quota with sufficient overflow space so vCenter Server Heartbeat can stop replicating gracefully.

Note If using a dedicated disk for log files, consider setting the quota to zero to disable the quota.

Procedure

- To configure *Maximum Disk Usage*, click the **Logs** tab of the Configure Server wizard (Figure 3-7), type the maximum dedicated disk space allocated for message queue log files, and click **Finish**.

Managing Heartbeat Settings

The *Server: Monitoring* page provides three features to manage server monitoring operations: *Configure Pings*, *Configure Failover*, and *Configure Response Times*.

Configuring Pings

During startup of vCenter Server Heartbeat, the IP addresses of all NICs configured for the VMware Channel and Management IP addresses are automatically added to the server monitoring ping configuration. Use the *Server: Monitoring Ping Configuration* dialog to add additional ping targets. Server Monitoring ping configuration allows vCenter Server Heartbeat to send pings across the VMware Channel in addition to heartbeat ("I'm alive" messages). Additionally, it allows vCenter Server Heartbeat to ping the other node in the pair over the Public network via the Management IP address to confirm that the node is still operational and providing service.

To add additional ping targets:

Procedure

1. Click **Configure Pings** to open the *Server Monitoring: Ping Configuration* dialog.
2. Select the *Ping Settings* tab to configure the *Ping Interval*.
3. Select the *Ping Routing* tab to add additional ping targets.
4. Click **OK**.

Managing Public Network Connection Checks

The *Network Monitoring* page allows you to make adjustments to IP addresses used to ping multiple nodes within the network and view the status of the network.

The Public network monitoring feature is enabled by default during the installation of VMware vCenter Server Heartbeat. This feature integrates the polling of designated waypoints around the network through the active node's Public connection to ensure connectivity to the Public network is operational. By default, the Primary DNS server, Default Gateway, and Global Catalog server IP addresses are all selected. When one or more of the automatically discovered waypoints are co-located on a single node (leading to duplication of IP addresses), the ability to override existing settings and specify additional waypoints manually becomes an advantage.

Procedure

1. To manually specify a ping target for Public network checking, click **Configure Pings**.
2. When the *Ping Configuration* dialog is displayed, select the *Ping Routing* tab.

3 Modify the existing target IP addresses for each node to ping.

Note If IP address values are added to the **Network Monitoring** > **Ping Configuration** > **Ping Routing** dialog, the new values added will replace the default ping targets of the Global catalog, Primary DNS server, and Default Gateway.

In a WAN environment, the target addresses for Public network monitoring on the Secondary node may be different to those automatically selected on the Primary. Again, the ability to override automatically discovered selections is provided by manually specifying a new target address.

Public Network Monitoring is carried out by the active node effectively pinging the target addresses at regular time intervals. The time interval is set by default to every 10 seconds but the frequency may be increased or decreased as required. Each target is allowed 5 seconds (default) to respond. On slower networks where latency and network collisions are high, increase this interval by changing the *Ping echo timeout* value.

The failure of all three targets to respond is allowed up to the *Auto-switchover if client network is lost for* threshold value. If the failure count of all three targets exceeds this value, vCenter Server Heartbeat initiates a failover.

4 Click **OK**.

Managing Failover and Active Node Isolation

vCenter Server Heartbeat continuously monitors nodes in the pair and network to ensure availability and uses native logic combining elapsed time, administrator configured rules, current node network status, and configured ping routing to determine if failover or isolation of the active node is warranted should the nodes experience missed heartbeats.

vCenter Server Heartbeat can be configured to failover automatically if the active node becomes unavailable for more than the *Failover timeout*. It can also be configured to failover automatically if there is a failure of the Public network or one of the application monitoring rules.

Using this dialog, the automatic failover behavior can be overridden so that the user is instead alerted and has the opportunity to check the system before deciding to make the passive node active.

To configure failover:

Note For information on configuring ping routing, see “Configuring Pings,” on page 48 and “Managing Public Network Connection Checks,” on page 48.

Procedure

1 Navigate to **Server: Monitoring** > **Configure Failover** to open the *Server Monitoring: Failover Configuration* dialog.

2 *Failover timeout* can be customized by changing the default value (60 seconds) to a custom value. Enter a new value (seconds) in the *Failover timeout* field or use the arrow buttons to configure how long vCenter Server Heartbeat waits for a missed heartbeat before it takes a pre-configured action to failover or isolate the active node from the network.

3 Select or clear check boxes for each of the following items to select actions to take if the configured *Failover timeout* is exceeded.

Note If the first two check boxes are not selected, failover will not occur in a LAN.

When the configured *Failover timeout* value has elapsed, vCenter Server Heartbeat will evaluate, in order, the following pre-configured rules before taking action:

Important Options selected when configuring failover via the *Configure Failover* dialog work in concert with Failure actions for Rules and Services. For example, if you disable failover by clearing the first two check boxes but set Failure actions to Switchover, failover will be prevented.

If either *Server: Monitoring Ping Routing* or *Network Monitoring Ping Routing* is misconfigured, unpredictable behavior can occur.

- Failover from Primary server to Secondary server if channel heartbeat is lost for failover timeout

  If the heartbeat is lost for the configured *Failover timeout*, failover from the Primary node to the Secondary node.

- Failover from Secondary server to Primary server if channel heartbeat is lost for failover timeout

  If the heartbeat is lost for the configured *Failover timeout*, failover from the Secondary node to the Primary node.

- Prevent failover or auto-switchover while not synchronized

  If the Primary and Secondary node's registry or protected files are not synchronized, do not allow to failover.

- Prevent Failover if channel heartbeat is lost but Active server is still visible to other servers

  If communications over the VMware Channel are lost for the configured *Failover timeout* but the node can successfully ping configured ping targets, failover is prevented.

- Make the server passive if the Channel and Public networks are lost for the configured failover timeout

  If communications over the VMware Channel are lost for the configured *Failover timeout* and the node's attempt to ping configured targets are unsuccessful for the *Failover timeout*, the node will become passive to prevent the possibility of split-brain.

Note If a rule is not selected, vCenter Server Heartbeat will skip the rule and move to the next rule in the list. After all rules have been evaluated vCenter Server Heartbeat will take action based upon the configured *Failover timeout*.

4 Click **OK**.

Managing Response Times

vCenter Server Heartbeat also allows you to configure the time to wait following a channel connection before starting replication and the time to wait following channel disconnection before stopping replication.

Procedure

1 Click **Configure Response Times** to open the *Server Monitoring: Response Times* dialog.

2 Type new values (seconds) into the fields or use the arrow buttons to select new values.

3 Click **OK**.

Enabling Failover in a WAN

By default, when deployed in a WAN environment, failover is disabled. To enable failover in a WAN environment, follow the steps below.

Procedure

1 Navigate to the *Network*: *Network Monitoring* page.

2 Click **Configure Auto-switchover**.

3 Select the *Auto-switchover if client network connectivity lost for* check box.

4 Configure the number of pings to wait before performing the failover.

5 Click **OK**.

Managing Split-brain Avoidance

Split-brain Avoidance ensures that only one node is active if the VMware Channel connection is lost, but both nodes remain connected to the Public network. Split-brain Avoidance works by pinging from the passive node to the active node across the Public network. If the active node responds, the passive node does not failover, even if the VMware Channel connection is lost.

Procedure

1 To enable Split-brain Avoidance, navigate to the *Server: Monitoring* page.

2 Click **Configure Failover**.

3 Select *Prevent failover if channel heartbeat is lost but Active server is still visible to other servers (recommended)*.

4 Click **OK**.

Managing Max Server Time Difference

vCenter Server Heartbeat generates a warning if the Primary and Secondary node's system clocks are not synchronized. The threshold for time difference is configured on the *Server: Summary* page.

Procedure

1 Select the *Server: Summary* tab and click **Configure** to display the *Server: Summary Configure* dialog.

2 Enter a value (seconds) or use the arrow buttons to select an alert threshold value for time difference between nodes, which is checked at handshake following startup.

3 Click **OK**.

Initiating a Failover

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

This is particularly useful when maintenance work performed on the Primary requires rebooting the node.

Since a failover cannot be performed during synchronization, it is important to review the queue information prior to attempting a failover. If the queues are large, file operations on the active node are high and it may be prudent to delay a failover due to the length of time required to completely clear the queue. Queue lengths can be viewed from the *Data: Traffic/Queues* page of the vCenter Server Heartbeat Console.

Prior to performing work on the Primary node, a failover can be triggered by selecting the Secondary node and clicking **Make Active** on the *Server: Summary* page. This changes the roles such that the active node becomes passive and the passive node becomes active. This allows users to continue to work while the Primary node is offline.

When the Primary node is back up and running, a failover can be triggered again so that the Primary node becomes active and the previously active (Secondary) node becomes passive.

Note The failover process may be performed at any time with the proviso that the systems are fully synchronized with respect to data files and registry replication. *Failovers cannot be performed if either node is in an unsynchronized or unknown state*.

Recovering From an Automatic Failover

A manually initiated failover is a controlled switch (initiated manually from the vSphere Web Client or vCenter Server Heartbeat Console) between the active and passive nodes. An auto-failover happens when any of the following fail on the active node: power, hardware, VMware Channel communications, or when preconfigured, a protected application or service. The passive node waits a preconfigured time after the first missed heartbeat before initiating failover. When this period expires, the passive node automatically assumes the active role and starts all protected applications.

The following recovery scenario assumes that initially the Primary node is active and the Secondary node is passive. A failover occurs and the Secondary node becomes the active node.

Note When failover conditions, such as a power failure, cause failures in both active and passive nodes, a condition may result that causes both nodes to restart in passive mode. In this situation, manual intervention is required. See “Two Passive Nodes,” on page 81.

Procedure

1 Review event logs on both nodes to determine the cause of the failover. For assistance, use the *Log Collector* (launched from the Taskbar icon) tool to collect information and send the output to VMware Support.

   If any of the following issues exist on the Primary node, performing a failback to the Primary node may not be possible until other important actions are carried out. **Do not** restart vCenter Server Heartbeat until the following issues have been resolved:

   - Hard Disk Failure – Replace the defective hard disk
   - Power Failure – Restore power to the Primary node
   - Malware – Clean the node of all malware
   - Communications – Replace or repair defective network hardware
   - Blue Screen – Determine the cause and resolve it. As required, submit the dump file to VMware Support (www.vmware.com/support) for analysis

2 On the Primary node, launch the *Configure Server* wizard and verify the node *Identity* is set to Primary and the *Active Server* is set to Secondary. Click **Finish** to accept the changes.

3 Disconnect the VMware Channel network cables or disable the virtual or physical NIC.

4 Resolve the list of possible failures.

5 Restart the Primary node and reconnect or enable the NIC.

6 After restart, check that the Taskbar icon now reflects the changes and displays **P** / **–** (Primary and passive).

7 On the Secondary active node or from a remote client, launch vCenter Server Heartbeat Console and confirm that the Secondary node is reporting as active.

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

a If the vCenter Server Heartbeat Console is unable to connect remotely, try running it locally. If you are still unable to connect locally, use the Service Control Manager (SCM) to verify that the service is running. If the service is not running, review the event logs for a cause.

b Run the *Configure Server* wizard and confirm that the node identity is set to Secondary and that the Active Server is set to Secondary.

Note If vCenter Server Heartbeat is running, you can run the *Configure Server* wizard but any changes made will not be saved.

c Verify that the protected application is accessible from clients. If accessible, start vCenter Server Heartbeat on the Secondary. If the application is not accessible, review the application logs to determine why the application is not running.

d Start vCenter Server Heartbeat on the Secondary active node.

Note At this point, the data on the Secondary (active) node should be the most up to date and this node should be the live node on your network. When vCenter Server Heartbeat starts, it overwrites all the protected data (configured in the File Filter list) on the Primary (passive) node. If you are not sure that the data on the active node is the most current and up to date, contact VMware Support (www.vmware.com/support). Go on to the next step only if you are sure that you want to overwrite the protected data on the passive node.

8 Start vCenter Server Heartbeat on the Secondary (active) node and check that the Taskbar icon now reflects the correct status by showing **S** / **A** (Secondary and active).

Managing Application Protection

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

The AMFx provides additional functions while maintaining the traditional stability of VMware software. Use the AMFx to install and remove plug-ins on the fly while vCenter Server Heartbeat continues to provide protection to currently installed applications.

The AMFx also employs sponsorship for protected application files and services. With sponsorship, multiple plug-ins can share files or services. When removing a plug-in, sponsorship prevents removal of a shared file or service that is still required by a remaining plug-in.

vCenter Server Heartbeat uses the *System plug-in* to monitor the node's performance. With the *System plug-in*, you can configure a variety of counters and assign actions when associated rules are exceeded.

Managing Applications

Use the *Applications: Summary* page to start, stop, and configure all protected applications and enable or disable protection and monitoring. Applications can be managed without needing to stop vCenter Server Heartbeat or taking the full server offline. During installation, vCenter Server Heartbeat configures default settings for application protection but accepts modifications to configurations settings.

To configure applications:

Procedure

1 Click **Configure** on the *Applications: Summary* page.

Within the *Applications Configuration* dialog, you can modify the following settings:

- Protect services and start monitoring applications
- Unprotect currently protected services and stop monitoring currently monitored applications
- Enable/disable *Verbose Plugin logging*
- Enable/disable *Discover protected data at startup*
- Configure the rule trigger count reset

2 After making modifications, click **OK**.

Remove an Application

Procedure

1 To remove an application, select the application in the *Applications* pane of the *Applications: Summary* page and click **Remove** at the top of the pane.

2 When the confirmation dialog is displayed, click **OK** to remove.

Manually Stop and Start Applications

Procedure

◆ To stop or start all protected applications, click the appropriate button at the top of the *Applications: Summary* page.

Option	Description
Stop Applications	The protected applications set stops. You can view the progress of the stopping in the *Applications Log* pane.
Start Applications	The applications start. You can view the progress of starting in the *Applications Log* pane.

Resetting the Application Health Status

If a problem occurs (for example, a failed service or rule), the *Application Health* status becomes *Degraded*. Even if vCenter Server Heartbeat corrects the problem (for example, restarts the failed service) or the user corrects the problem, the *Degraded* status remains until manually cleared by the Administrator. In this state, the Service Discovery Task will not run.

To reset the *Application Health* status

Procedure

- After acknowledging the problem and solving it, click **Clear** in the *Application Health* pane of the *Applications: Summary* page to reset the *Application Health* status.

  The status updates to provide the actual current *Application Health* status.

Setting the Application Timeout Exception

vCenter Server Heartbeat can alert the Administrator if the time taken to start or stop an entire application exceeds the expected time during the following operations:

- vCenter Heartbeat startup
- Shutdown with protected applications
- Failover
- When the Administrator selects **Start Application**
- When the Administrator selects **Stop Application**

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

Configuring Timeout Settings

Note The *Start Timeout* value should be configured according to vCenter inventory size and the *Stop Timeout* values according to inventory size and operational load. For example, if the inventory is large (more than 500 hosts and 15K virtual machines, the Start time can be 20-30 minutes. Use the resulting *Start Timeout* experienced as a guide to assist in determining the *Stop Timeout* value.

Procedure

1. Right-click the selected application and select *Edit* from the menu or select the application and click **Edit** at the top of the pane to invoke the *Edit Application* dialog.
2. Enter new values (seconds) into the *Stop Timeout* and *Start Timeout* text boxes or use the arrow buttons to adjust the values.
3. Click**OK**.

Reviewing the Applications Log

The *Applications Log* helps when troubleshooting the protected application environment. The *Applications 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. The order that entries are displayed can be sorted either ascending or descending by clicking the column title.

Filtering Application Log Entries

vCenter Server Heartbeat can filter *Applications Log* files to limit the events displayed. By default, all events are displayed in the *Applications Log* file.

Procedure

1 Right-click an event in the *Applications Log* and select *Filter* or click **Filter** in the *Applications Log* pane of the *Applications: Summary* page.

2 In the upper section, clear the event types you do not want to view.

3 To limit the date and time range, select *Only show events from* and edit the date or time range.

4 Click **OK**.

The *Application Log* events are filtered to meet the selected criteria.

Managing Services

The *Applications: Services* page displays all services that you or plug-ins specify and the services related to them by dependency. vCenter Server Heartbeat manages services that depend on protected services (started and stopped) but not monitored (not restarted if stopped by some external agency). vCenter Server Heartbeat monitors protected services (restarted if stopped) but not managed (not stopped if protected applications are stopped).

Adding a Service

To protect a service that was not automatically added by vCenter Server Heartbeat during installation, the service must be added via the vCenter Server Heartbeat Console and be in a *Running* state.

Procedure

1 Right-click on any service and select **Add** from the menu or click **Add** on the *Applications: Services* page to invoke the *Add Service* dialog. The *Name* drop-down list contains a list of all currently running unprotected services.

2 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 nodes to *Running* can cause the service to place a lock on some files preventing synchronization from completing.

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

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

4 Assign a task to each of the three failure options and click **OK**.

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

Editing a Protected Service

Once a protected service has been added and configured, you can change the action to take upon failure and other options using the *Edit Service* dialog.

Procedure

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

The *Edit Service* dialog opens to provide a subset of the same options available when adding a new service.

2 Make the modifications and click **OK**.

Editing All Protected Services

vCenter Server Heartbeat Console allows you to perform a single operation to configure the actions to take upon failure for all protected services.

Procedure

1 Click **Edit All**.

The *Edit Services* dialog opens to provide the actions to take upon failure for all three instances. Selections made in the *Edit Services* dialog will be applied to all protected services.

2 Select the action to take for First, Second, and Third failure and then click **OK**.

Unprotect and Stop Monitoring User Defined Services

To unprotect and stop monitoring user defined services:

Procedure

1 Navigate to the *Applications: Services* page and select the intended user defined service.

2 Click **Edit**.

3 Clear *Manage Starting and Stopping and Monitor State*.

4 Click **OK**.

Changing the Order of Services

The exact order in which services start and stop is influenced by a number of key factors:

- The order of applications specified by plug-ins determines which services are started first.
- Services can have dependencies which must be respected. For example, if service B is listed after service A under the *User-Defined* group, and service A depends on Service B, Service B starts first.
- Multiple applications using the same service (the same service can appear under more than one sponsor). The service starts when the first application to reference it starts.
- The order of stopping services is the reverse for starting services.

Procedure

- To modify the order in which the services start and stop, use the **Up** and **Down** arrows.

Remove a Service

Procedure

1. Select the service to remove in the *Applications: Services* page.
2. Click **Remove**.

   A confirmation message is displayed.
3. Click **Yes**.

   The service is removed from the protected list.

Managing Tasks

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

- *Network Configuration* – Run when applications start and is intended to launch dnscmd or DNSUpdate. This task can launch a batch script containing multiple dnscmd commands. Network Configuration tasks are the only types of task that can vary between the Primary and Secondary nodes.
- *Periodic* – Run at specific configurable intervals
- *Pre/Post Start* – Run before and after services start on the active node
- *Pre/Post Stop* – Run before and after services stop on the active node
- *Pre/Post Shadow* – Run before and after the Data Rollback Module creates a shadow copy on the active node (Not available in this release)
- *Rule Action* – A configurable task run in response to a triggered rule or when a service check fails

Tasks can be defined and implemented by plug-ins, users, or can be built-in tasks defined by vCenter Server Heartbeat. User defined tasks are implemented as command lines, which can include launching a batch script. Examples of built-in tasks include monitoring a protected service state on the active and passive nodes. An example of a plug-in-defined task is the discovery of protected data and services for a particular application.

The vCenter Server Heartbeat *Applications: Tasks* page provides a list of tasks and associated status information, and includes features to quickly manage tasks.

Adding a Task

To add a task:

Procedure

1 Click **Add** to invoke the *Add Task dialog*.

2 Assign a name to the task.

3 Select the task type from the *Task Type:* drop-down list.

Note If the *Task Type* is *Network Configuration*, you must select the identity of the node to run the task (Primary or Secondary).

4 In the *Command* text box, enter the path or **Browse** to the script, .bat file, or command for the task to perform.

Note When the *Command* entry requires specific user credentials, you must select that user from the *Run As* drop-down list. To add a user account, click **User Accounts** (near the top of the pane). See"Viewing, Adding, and Removing User Accounts," on page 59.

5 Click **OK**.

Editing a Task

You can edit the interval of a task or disable a task.

To edit a task:

Procedure

1 Right-click on an existing task and select **Edit** from the menu or select the task and click **Edit** at the top of the pane to invoke the *Edit Task* dialog.

2 Edit the parameters of the task.

3 Click **OK**.

Viewing, Adding, and Removing User Accounts

vCenter Server Heartbeat Console allows you to view, add, and remove user accounts used to run tasks.

Viewing the User Accounts

Procedure

1 On the *Applications: Task* page, click **User Accounts** to invoke the *User Accounts* dialog and view the current *User accounts* used to run tasks.

2 Click **Close** to exit the dialog.

Adding a User Account

Procedure

1 On the *Applications: Tasks* page, click**User Accounts** to invoke the *User Accounts* dialog.

2 Click **Add** to invoke the *Add User* dialog.

3 Type the name of the User, the associated Domain, and a Password into the corresponding text boxes.

4 Click **OK**.

Removing a User Account

Procedure

1 To remove a user, click **User Accounts** on the *Applications: Tasks* page to invoke the *User Accounts* dialog.

2 Select the user account to remove from the list in the *User Accounts* dialog and click **Remove**.

A confirmation message appears.

3 Click **Yes**.

Removing a Task

Procedure

1 To remove a task, select the task to remove on the *Applications: Task* page and click **Remove**.

A confirmation message is displayed.

2 Click **Yes**.

Changing the Order of Tasks

Procedure

- To change the order of tasks, use the **Up** and **Down** arrows (near the top of the pane) to change the order in which the tasks appear in the tasks list.

Starting a Task Manually

vCenter Server Heartbeat provides options to launch a task immediately, after a designated time period elapses, or following the occurrence of a specified event.

To launch the task immediately:

Procedure

1 Select the task from the task list.

2 Right-click on the existing task and select **Run Now** from the menu or click **Run Now** at the top of the pane.

vCenter Server Heartbeat immediately launches the task.

Managing Rules

Rules are implemented by plug-ins (there are no user-defined rules). Rules can be configured with rule actions, which are tasks to be performed when a rule triggers. Rules have two trigger properties:

- *Timed* – They must evaluate as true continuously for the specified duration to trigger.

  The timed rule provides three recovery actions, labeled as *On First Failure*, *On Second Failure*, and *On Third Failure* in the vCenter Server Heartbeat Console.

  Timed rules are triggered when a specific condition registers as true for a specified length of time. Timed rules are normally used in conditions where immediate triggering is undesirable; for example, when the CPU is configured to trigger when it exceeds 90% for five minutes, the timed rule requires that the threshold must be exceeded for 5 minutes before it can trigger rather than the moment the CPU exceeds 90%.

- *Latched* – They trigger as soon as they evaluate to true.

  The latched rule provides only one recovery action, labeled as *On Failure* in the vCenter Server Heartbeat Console.

  Latched rules are triggered only once and then are disabled until they are re-enabled by manual intervention from the administrator. Usually latched rules should be used in situations where multiple triggering is undesirable or could cause problems. Latched rules provide the functionality to alert the administrator about a problem once and then stop triggering until the problem has been fixed.

Editing a Rule

Rules are implemented by plug-ins and cannot be created by users. Each plug-in contains a default set of rules with options that may be modified by the user.

Procedure

1 Right-click on the rule and select *Edit* from the menu or click **Edit** at the top of the pane.

The following parameters can be edited for each rule:

- *Condition* – the condition being evaluated
- *Duration* – the length of time the condition exists (if a timed rule)
- *Interval* – the length of time between rule checks
- *First Failure* – action to take upon first failure (default setting is Alert)
- *Second Failure* – action to take upon second failure (default setting is Alert)
- *Third Failure* – action to take upon third failure (default setting is Alert)

2 Edit the parameters of the rule and click **OK**.

Managing Plug-ins

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

Installing a Plug-in

vCenter Server Heartbeat allows you to install and upgrade plug-ins as needed to support applications without stopping vCenter Server Heartbeat.

Important Plug-ins should be installed only on the active node. Plug-ins will be replicated automatically to the passive node. Installation of a plug-in on a passive node may cause an Exception to occur.

Procedure

1 Navigate to the *Applications: Plug-ins* page.

2 Right-click any existing plug-in and select *Install* from the menu or click **Install** at the top of the pane to invoke the *Install Plugin* dialog.

3 Type a path to the plug-in location or click **Browse** to navigate to the plug-in location. The path statement is case-sensitive.

4 Select the plug-in <plug-in_name>.dll file at the plug-in location.

5 Click **OK**.

Editing a Plug-in

vCenter Server Heartbeat allows you to edit the configuration of user installed plug-ins.

Procedure

1 On the *Applications: Plug-ins* page, right-click on an existing plug-in from the *Plugins* list and select *Edit* from the menu or select the plug-in and click **Edit** at the top of the pane to invoke the *Edit Plugin* dialog.

2 Review the configuration options before making modifications as they are specific to each plug-in.

Note When configuring the SQL Server Plug-in, vCenter Server Heartbeat Console allows you to exclude specific databases from rule checks to prevent false alarm triggering when databases are intentionally taken offline.

3 Click **OK**.

Uninstalling a Plug-in

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

Procedure

1 On the *Applications: Plug-ins* page, right-click an existing plug-in and select *Uninstall* or select the plug-in and click **Uninstall** at the top of the pane.

A confirmation dialog appears.

2 Click **OK**.

Managing Data Protection

vCenter Server Heartbeat can protect many permutations or combinations of file structures on the active node by the use of custom Inclusion and Exclusion filters configured by the administrator.

The filter driver identifies files to protect and disk I/O operations to intercept and replicate to the passive node. Use this driver to filter files for inclusion in or exclusion from the replication process.

By default, vCenter Server Heartbeat automatically protects a folder called Protected on the system partition.

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

The VMware application folder contains the active node‘s send and passive node’s receive queues on the active and passive nodes. This folder must be explicitly excluded from file protection.

File Filters

File filters dictate which files are protected and replicated to the passive node.

The *File Filters* pane of the *Data: File Filters* page allows you to set up and manage Inclusion and Exclusion filters.

The *File Filters* pane contains three columns:

- *Filter* – Lists the pattern for protecting files and folders on the active node.
- *State* – Identifies the filter as *Effective, Subset (contained within another filter)*, or *Not Effective (not contained within another filter)*.

  An Effective filter is properly configured and functions to protect (replicate) the stipulated files to the passive node.
- *Detail* – Describes the file filter details based upon the state of the file filter.

Adding a User-Defined Inclusion Filter

Inclusion filters create a subset of files to include for protection.

Procedure

1 In the *Data: File Filters* pane, click **Add Inclusion Filter** to display the *Add Inclusion Filter* dialog.

2 Type the complete path and pattern, specify a pattern containing wildcards, or click **Browse** to locate the file or folder.

3 Click **OK**.

Note There are two forms of wildcards available, * which matches all files in the folder and **, which matches all files, subfolders, and the files in the subfolders of the folder. After defining the filter, you can add additional Inclusion Filters.

Adding a User-Defined Exclusion Filter

Exclusion filters create a subset of an Inclusion Filter to specify items to exclude from protection.

Procedure

1 In the *Data: File Filters* pane, click **Add Exclusion Filter** to display the *Add Exclusion Filter* dialog.

2 Type the complete path and pattern, specify a pattern containing wildcards, or click **Browse** to locate the file or folder.

3 Click **OK**.

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

Editing User Defined Inclusion/Exclusion Filters

Existing Inclusion and Exclusion Filters can be edited using the procedure below.

Procedure

1 Selecting the filter on the *Data: File Filters* page.

2 Click **Edit** at the top of the *File Filters* pane or right-click the filter and select *Edit* from the menu. Edit the value in the *Pattern:* text box by typing over the current file filter definition.

3 Click **OK**.

Determining Effective Filters

An *Effective Filter* is the result of the remainder of files and folders stipulated in the *Inclusion Filter* after removing the files and 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. This allows, for example, file servers with thousands of individual shares requested by a plug-in to use a single, more general, user configured filter.

Example: (Inclusion filter) - (Exclusion filter) = Effective filter

Removing User-Defined Filters

When necessary, user defined Inclusion Filters and Exclusion filters can be removed.

Procedure

1 Select the filter in the *Data: File Filters* list and click **Remove**, or right-click on the filter in the *Data: File Filters* list and select *Remove* from the menu.

A confirmation message appears.

2 Click **Yes** to remove the filter.

Automatic Filter Discovery

When Administrators make changes to the configuration, vCenter Server Heartbeat automatically adjusts file filter protection for protected locations. Additionally, the SQL Server plug-in provides database protection including changes or additions to the database and log files.

Replication

You can manage data replication and view replication status using the *Data: Replication* page.

Initiating a Full Registry Check

A Full Registry Check re-scans and synchronizes all registry keys specified in the built-in registry filters between the nodes.

Procedure

- Click **Full Registry Check** in the *Registry Synchronization* pane.

  A full registry check is performed with results of the check displayed in the *Registry Synchronization Status* pane.

Initiating a Full System Check

A Full System Check verifies and synchronizes the entire protected file set by performing the same block level check of all the files identified by file filters in the initial startup synchronization and verification.

Procedure

1 Click **Full System Check** in the *File Hierarchy* pane to initiate a Full System Check.

A confirmation dialog asks you to confirm the request and warns you that depending on the amount of data under protection, this task can take a long time to complete (possibly a number of hours).

Note While a Full System Check (FSC) is in progress, a manual failover cannot be initiated, and in this case the recovery point time simply shows the age of file updates which have not yet been applied on the passive node. When the FSC is complete, then the recovery point shows the age of the oldest file update on the active node which has not yet been transmitted to the passive.

2 Click **Yes** to perform the check.

Note VMware recommends that once an FSC is initiated, you allow it to run to its conclusion. Canceling the FSC leaves the file system status *Unchecked*. Depending on the amount of data, resynchronization may take substantial time to complete. A manually initiated failover is not permitted until after the task is complete and the File System Status is Synchronized.

Enabling Fast Check

Fast Check is a process used by vCenter Server Heartbeat to rapidly verify files between nodes prior to starting applications. Fast Check compares file time stamps and attributes rather than check sums of the data thereby accelerating startup and synchronization processes. If the time stamp or attribute check fails, than normal verification and synchronization processes will initiate. Fast Check allows you to configure the length of time to wait for Fast Check to complete before starting applications.

Fast Check is beneficial after a graceful shutdown where servers were synchronized before shutdown. Fast Check allows the node to check file synchronization rapidly and start to service clients. If Fast Check detects files that are out-of-sync, it initiates a full Verify and Synchronize process to resynchronize your data.

Procedure

1 Navigate to *Data: Replication*.

2 Click **Configure**.

3 Select the *Fast Check* tab.

4 Select the *Use Fast Check* check box.

5 Configure *Maximum Application Delay*. This is the length of time vCenter Server Heartbeat will delay the startup of the application while it attempts to establish replication between the active and passive nodes.

6 Click **OK**.

Note When Fast Check is configured in addition to Controlled Shutdown, vCenter Server Heartbeat can be configured to perform an unattended restart. For more information about Controlled Shutdown, see “Controlled Shutdown,” on page 72.

Initiating File Synchronization Manually

The *Data: Replication File Hierarchy* pane displays files that were detected as out of synchronization.

Procedure

- To initiate file synchronization manually, perform one of the following:
  - To synchronize the specified files, click **Synchronize**.
  - Select multiple files using the **Shift** or **Ctrl** keys and click **Synchronize**.
  - Select a folder and select *Including Subdirectories* to synchronize files within folders and then click **Synchronize**.

  A progress bar graphically displays the status of the verification or synchronization operation. When complete, the status displays a green *Synchronized* icon.

Initiating Verify and Synchronize Manually

A manual or scheduled synchronization and verification request is a task that is queued for processing after the running task completes.

Procedure

1. Select one or more files and folders from the *File Hierarchy* pane. Multiple files and folders can be selected from this file list using the standard Windows multiple selection techniques, **Shift** + click and **Ctrl** + click.

   Note You can also right-click on a folder in the tree view (in the left pane of the *File Hierarchy* pane) to quickly select *Verify and Synchronize* from a menu. This option automatically includes subdirectories.

2. When one or more folders are selected, also select the *Including Subdirectories* check box to ensure that all files within the folder(s) are also verified and synchronized.
3. Click **Verify and Synchronize**.

   As verify and synchronization runs, you may see its progress in the *Current Task* pane at the bottom left of the *Data: Replication* page. When the verify and synchronization process successfully completes, a green icon indicates the verified and synchronized status.

   Each verification and synchronization request (manually or automatically scheduled) is defined as a task with subsequent tasks queued for processing after the current task is completed. Each task is listed in the *Pending Tasks* list to the right of the *Current Tasks* frame.

   You can cancel individual tasks. If you cancel a scheduled task, you risk an unchecked system. Possible consequences of canceling tasks display in a warning message.

Alerts and Events

vCenter Server Heartbeat can notify Administrators of potential problems or when specific events occur by sending custom configured predefined alerts and route event logs to a remote Administrator as required.

Managing Alerts

vCenter Server Heartbeat can send predefined alerts to remote administrators via email when configured using the *Logs* page.

Procedure

1 Navigate to the *Logs* page and click **Configure Alerts**.

You can configure one of three alert states: *Red* alerts are critical, *Yellow* alerts are not as serious, and *Green* alerts are informational. Alerts are preconfigured with the recommended alerting levels.

2 To reconfigure each event to trigger Red, Yellow, Green, or to not alert, select the appropriate tab and select the check box(s).

3 Click **OK**.

Managing Alert Reporting

vCenter Server Heartbeat can alert the administrators or other personnel and route logs by email when an Alert condition exists.

Procedure

1 Navigate to the *Logs* page and click **Mail Settings** to open the *Mail Settings* dialog.

2 Type the Fully Qualified Domain Name (FQDN) of the outgoing SMTP server for both Primary (for when active) and Secondary (for when active) nodes in the appropriate fields.

3 Type an email address authorized to send mail through the SMTP server.

4 If SMTP servers require authentication to accept and forward SMTP messages, select *Mail Server requires authentication* and specify the credentials for an appropriate authenticated user account.

5 Click **OK**.

Managing Alert Email Triggers

vCenter Server Heartbeat allows you to configure email recipients using the *On Red Alert*, *On Yellow Alert*, and *On Green Alert* tabs of the *Configure Alerts* dialog after configuring trigger levels and the email servers.

Configuring Default Alert Email Triggers

Red, Yellow, or Green alert triggers can email to the same or different recipients. The process to add recipients is the same for all trigger levels.

Procedure

1 Click on the intended alert tab and select *Send mail*.

2 Select the frequency for the email to be sent.

3 Click **Add** and type a fully qualified email address for each recipient for the respective trigger level alert.

4 To delete a recipient, select the recipient's email address in the *Mail Recipients* pane and click **Remove**.

Use the preconfigured subject and content for alert emails for Red, Yellow, or Green alerts. You may add content as required. VMware recommends leaving the preconfigured subject and content and if necessary, add additional information.

Note In the *Configure Alerts* pane, *On Red Alert*, *On Yellow Alert* and *On Green Alert* tabs allow the frequency, recipient, and text of emails to be configured.

When *Send mail* is selected, three alternatives are available:

- Always – will always send an email if this alert type is triggered.
- Once – will send an email once for each triggered alert. An email will not be sent again for the same triggered alert, until vCenter Server Heartbeat is re-started
- Once per – within the time period selected, an email will only be sent once for the same triggered alert, subsequent emails for that trigger will be suppressed. Once the time period has expired, an email will be sent if the same alert is triggered

Note that *Once* and *Once Per* options will operate per individual triggered Alert. Multiple emails will be sent, but only if the event being alerted is different.

Configuring Alert Email Triggers (Alternate Method)

vCenter Server Heartbeat allows an alternate method to configure sending alert notifications that allow the Administrator to create an event in the Application Event Log which can be customized to include vCenter Server Heartbeat specific information variables.

Procedure

1 Select *Run Command* under the pertinent alert state.

2 **Browse** to the 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 shown in Table 9-1.

Table 3- 1. Customized Information Variables

Variable	Value
$EventId	Id of event as listed above
$EventName	Human-readable name of event
$EventDetail	Detail message for event
$EventTime	Time at which event occurred

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

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

3 Click **OK**.

Testing Alert Reporting

vCenter Server Heartbeat allows you to test alert reporting without triggering an actual alert during operations on the active node.

Procedure

1 Navigate to the *Logs* page.

2 Click **Test Alert Reporting**.

A *Test Alert* email is sent to the configured email recipients.

Managing Event Log Files

vCenter Server Heartbeat allows you to configure *Event Log* files to direct where the log file is stored and the number of events to be recorded.

Procedure

1 Navigate to the *Logs* page and click **Configure**.

2 Select the *General* tab to define the filename and path of the exported comma-separated variable (.CSV) file.

3 Type a path and filename or click **Browse** and navigate to the file.

4 Adjust the length of the event list to meet your needs by increasing or decreasing the value (the default is 300 events) in the *Record at most* field.

5 Click **OK**.

Managing Log File Email Recipients

Use vCenter Server Heartbeat to email logs to specified personnel at predetermined intervals.

Procedure

1 To configure vCenter Server Heartbeat to email a copy of the log file, select the *Mail Log File* tab.

2 Select the *Mail Every* check box and configure the day and time to send the log file.

3 To specify recipients, click **Add** on the top left of the email recipient field and type the email address in the *Add Mail Address* dialog.

4 To remove a recipient, select the recipient's email address in the *Mail Log File* pane and click **Remove**.

5 Click **OK**.

Maintaining vCenter Server Heartbeat 4

vCenter Server Heartbeat's unique architecture allows administrators to perform routine maintenance and, for most operations, prevents having to shutdown nodes to complete maintenance procedures.

This chapter includes the following topics:

Common Administrative Tasks in vCenter Server Heartbeat

vSphere Web Client and vCenter Server Heartbeat Console provide convenient controls that allow you to quickly perform common administrative tasks.

From the vSphere Web Client Heartbeat tab or vCenter Server Heartbeat Console *Server: Summary* page, the following controls are available.

- **Make Active** – Prompts you to verify that you want to make the passive node in the pair active. Click **Yes**.
- **Shutdown** – Prompts you to select the node(s) to shut down. If you select the active node, additional options to stop or not stop protected applications appear in the dialog. Click **OK**.
- **Start Replication** – Opens the *Start Replication Options* dialog. Select to start or not start the protected applications and click **OK**. By default, all protection modes start when vCenter Server Heartbeat is started and a manual start is not required unless the system was stopped in response to an automated stop.
- **Stop Replication** – Opens the *Stop Replication Options* dialog. Use this method to stop replication, such as to contain a malware infection or to upgrade a protected application. Select whether to stop or not stop protected applications and click **OK**. Replication of data files stops and if selected, protected applications also stop.

Note The vCenter Server Heartbeat service continues to run on the nodes providing heartbeats and protecting the system and network facets of the active node.

In additional to those listed above, vCenter Server Heartbeat *Server: Summary* page provides the following additional controls:

- **Start Applications** – Click to start protected applications on the active node.
- **Stop Applications** – Click to stop protected applications on the active node.
- **Configure** – Click to open the *Configure* dialog. Select the radio button corresponding to whether you want to stop or leave the protected applications running when vCenter Server Heartbeat is shut down. You can select whether to leave protected applications running upon shutdown when a net stop command is issued, and to start protected applications upon startup when a net start command is issued. Type a number (seconds) or use the arrow buttons to select an alert threshold value for time difference between nodes, which is checked at handshake following startup. Click **OK**.

Controlled Shutdown

A *Controlled Shutdown* is a process where vCenter Server Heartbeat service is able to delay system shutdown long enough to perform all necessary steps required to stop applications and replication in a synchronized state. Controlled Shutdown is intended for situations where an unattended planned shutdown of the node is necessary. When configured via the vCenter Server Heartbeat Console *Data: Replication* page, this feature allows vCenter Server Heartbeat to gracefully shutdown in the absence of the administrator.

Configuring Controlled Shutdown

Procedure

1 Navigate to vCenter Server Heartbeat Console's *Data: Replication* page.

2 Click **Configure**.

3 On the *Replication Configuration* dialog, select the *Controlled Shutdown* tab.

4 Select the nodes on which to enable Controlled Shutdown.

5 Select the days and hours parameters under which the node(s) will perform Controlled Shutdown.

6 Configure the length of time for node(s) to wait for Controlled Shutdown.

Note The ability to configure the length of time for the node(s) to wait for the Controlled Shutdown is configurable on Windows Server 2008 but is not configurable on Windows Server 2003.

When the Fast Check process is enabled in addition to Controlled Shutdown, vCenter Server Heartbeat can be scheduled to perform unattended restarts of the system while maintaining synchronization of data. For more information about Fast Check, see Configuring Fast Check .

Application Maintenance Mode

Use the *Applications: Summary* page to disable application protection and service monitoring for maintenance purposes.

To perform manual maintenance:

Procedure

1 On the *Applications: Summary* page, click **Configure**.

2 Select *Unprotect services and stop monitoring all applications (for manual application maintenance)* and click **OK**.

3 Perform the required maintenance.

4 When maintenance is complete, on the *Applications: Summary* page of vCenter Server Heartbeat Console, click **Configure**.

5 Select *Protect services and monitor all applications (recommended)* and click **OK**.

Reviewing Event Logs

The *Event Log* pane of the *Logs* page lists events logged chronologically by default and shows when an event happened, the event type, event source, its importance, and its detail. Display order for events can be sorted either descending or ascending by clicking on the column heading. Since detail in the data grid is truncated, it may be necessary to review the log in more detail.

Reviewing Event Log Details

Event Properties displays full detail and trace of an event that caused an error and its source to aid in troubleshooting.

Procedure

1 Select an event in the Event Log and double-click the entry in the data grid.

The *Event Properties* dialog is displayed.

2 Use the **Up** and **Down** arrows in this window to review other logs.

This feature is useful when many events have occurred simultaneously and helps to identify the source of the problem.

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

Table 4- 1. Log Events

Icon	Description
	Errors within the underlying operation of vCenter Server Heartbeat and can be considered critical to system operations.
	Warnings generated for discrepancies within vCenter Server Heartbeat's operational environment that are not deemed critical to the operation of the system.
	System log events are generated following normal vCenter Server Heartbeat operations. Use these logs to verify the success of processes such as file synchronization.
	Information on operations within the graphical user interface rather than operations on vCenter Server Heartbeat service, such as Test Alert Reporting.

Filtering log events by importance

Event lists displayed by that vCenter Server Heartbeat may be filtered to hide less important events and/or limit events displayed to a specific date and time range.

Procedure

1 Click **Filters** on the *Logs* page to invoke the *Event Log Filters* dialog.

2 Select *Events of at Least*.

3 Select the *Show events of at least* check box in the *Importance* group.

4 Select the importance level from the drop-down list and click **OK**.

Only logs equal to or above the selected severity are displayed.

Filtering log events by date and time range

Procedure

1 Select the *Only show events from* check box and adjust the start date, end date, and times.

2 Click **OK**.

Table 4- 2. Event Log Buttons

Icon	Purpose
	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 filename and path to export the data in the *Configuration* tab.
	To immediately email the list, click **E-mail**.
	To clear the list, click **Remove all Entries** at the top left of the *Log Details* data grid.

Checking for Orphaned Files

vCenter Server Heartbeat provides the opportunity to check for orphaned files and either notify the administrator or delete the orphaned files. Orphaned files are those files in a protected set that exist on the passive node but do not exist in the protected set on the active node.

Orphaned File Check can either delete or log the orphaned files on the passive node that exist within the protected set; they were *orphaned* because vCenter Server Heartbeat was not running when content changes were made on the active node.

Note Orphaned File Check does not delete files on the passive node if there is no file filter to include the content as this would be unsafe.

Special Cases

The following special cases apply to Orphaned File Check.

- *Folder root filters* - Orphaned File Check will manage the entire contents of that folder (for example, D:\folder**). This deletes all passive files within the folder that do not exist on the active node, and includes content created only on the passive node.
- Exclusion file filters - Orphaned File Check will not delete any files excluded from the protected set by Exclusion filters. This rule safeguards users and applications.
- Filters for files, file types, or other wildcards - Orphaned File Check is not managing the contents of the folder (for example, D:\database*.log), only the selected files. Orphaned File Check will only process files that match the filter and will not delete files with any other extension within the folder D:\database.

Configuring Orphaned Files Check Options

Prior to initiating an Orphaned Files Check, you must configure the actions to take in the event orphaned files are found. By default, Orphaned Files Check is configured to delete orphaned files. Should you want to log the files presence rather than delete, follow the steps below.

Procedure

1 Navigate to the *Data: Replication* page and click **Configure**.

2 Select the *Orphaned Files* tab.

3 Select the *Detect orphaned files* check box.

4 In the *On detection, take the following action* drop-down, select either *Delete* to automatically delete the orphaned files or *Log to file* to add the list of files to the log file.

5 After selecting options, click **OK** to close the dialog.

6 On the *Data: Replication* page, click **Orphaned Files Check**.

Orphaned Files Check runs.

Applying Patches with vCenter Server Heartbeat Installed

vCenter Server Heartbeat's unique architecture allows you to install updates to the operating system or apply hotfixes without interrupting end-users. The active/passive pair allows you to install an update or hotfix on one node and ensure functionality before installing on the other.

Applying Operating System Patches and Hotfixes

Before implementing this procedure, ensure that the Automatic Update feature supplied by Microsoft is configured so that Updates are NOT applied automatically. It is acceptable to allow updates to be downloaded automatically.

This procedure assumes that vCenter Server Heartbeat is configured with the Primary node as active and both File System Status and Registry Status are synchronized.

Procedure

1 On the Secondary (passive) node, launch Windows Update.

2 Download and install patches or hotfixes, but DO NOT reboot the node if instructed to do so.

3 Launch vCenter Server Heartbeat Console.

4 Shutdown vCenter Server Heartbeat selecting the option to Shutdown vCenter Server Heartbeat, but leave protected applications running.

5 Reboot the Secondary node if previously prompted at Step 2 to complete installation of OS patches or hotfixes.

6 Verify all patches or hotfixes are installed properly.

7 On the Secondary (passive) node, launch Windows Update again and check for any further updates that may be required. If additional updates are required, repeat Steps 2 to 6.

8 Start vCenter Server Heartbeat on the Primary node and also on the Secondary node if no reboot was required at Step 5 allowing the nodes to synchronize.

9 Launch vCenter Server Heartbeat Console.

10 Perform a manual failover using vCenter Server Heartbeat Console to make the Secondary node active. Note, at this point users may notice a slight interruption to the protected application.

11 When the failover is complete, launch Windows Update on the Primary (passive) node.

12 Download and install patches or hotfixes, but DO NOT reboot the node if instructed to do so.

13 Shutdown vCenter Server Heartbeat selecting the option to Shutdown vCenter Server Heartbeat, but leave protected applications running.

14 Reboot the Primary node if prompted at step 13 to complete installation of OS patches or hotfixes.

15 Verify all patches or hotfixes are installed properly.

16 On the Primary (passive) node, launch Windows Update again and check for any further updates that may be required. If additional updates are required, repeat Steps 11 to 15.

17 Start vCenter Server Heartbeat on the Secondary node and also on the Primary node if no reboot was required at step 14 allowing the nodes to synchronize.

18 Launch vCenter Server Heartbeat Console.

19 Perform a manual failover using the vCenter Server Heartbeat Console to make the Primary node active again. Note, at this point users may notice a slight interruption to the protected application.

Applying SQL Server Patches

Prior to upgrading SQL Server with vCenter Server Heartbeat installed, check with VMware for the latest version of vCenter Server Heartbeat and verify that it supports the new application version or Service Pack.

To upgrade SQL Server with vCenter Server Heartbeat installed:

Prerequisites

Prior to attempting this upgrade, read the entire procedure.

Procedure

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

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

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

Upgrade starts on the Secondary (active) server.

4 Upgrade the SQL Server or apply the Service Pack to the Secondary (active) server by running Setup.exe

5 Restart the Secondary server if requested.

- The SQL Server starts
- The SQL Server upgrade / Service Pack resumes

6 Allow the SQL Server upgrade/Service Pack to complete.

7 Once complete, start SQL Server services.

8 Verify that SQL Server is operational.

9 Change the server role to Secondary/passive.

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

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

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

11 Restart the Secondary server.

12 The upgrade process continues on the Primary (passive) server.

Important Use identical Setup program upgrade parameters on both the Primary and Secondary servers.

13 Change the server role to Primary/active:

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

   b Change the server role for the current (Primary) server to *Active* and click **Finish**.

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

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

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

14 Upgrade SQL Server on the Primary (active) server by running Setup.exe

15 Restart the Primary server if required.

   - The server returns as passive with vCenter Server Heartbeat in the stated state
   - The SQL Server services stop
   - The SQL Server upgrade resumes

16 If server was restarted in Step 15, allow the SQL Server upgrade to complete.

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

18 Finalize the installation and synchronize vCenter Server Heartbeat:

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

   b Start vCenter Server Heartbeat on both servers.

   c Launch the vCenter Server Heartbeat Console and connect to the server pair.

   d Verify that the system completes the Full System Check and is replicating.

   e Using the vCenter Server Heartbeat Console, navigate to the *Application: Tasks* page and manually run the *Protected Service Discovery* task.

Shutting Down Windows

Always stop vCenter Server Heartbeat before attempting to shut down Microsoft Windows. If an attempt is made to shut down Windows without stopping vCenter Server Heartbeat, a confirmation message is displayed. When the *Windows Shutdown* confirmation message is displayed, click **Cancel** and stop vCenter Server Heartbeat before attempting Windows shut down again.

vCenter Server Heartbeat Diagnostics 5

You can use a variety of procedures for diagnosing and fixing problems that you may encounter when using vCenter Server Heartbeat. You can use troubleshooting procedures to investigate the causes of such problems and attempt to correct them yourself, or you can obtain assistance from VMware Technical Support. The following unexpected behaviors illustrate Problems, Causes, and Solutions for a given scenario.

This chapter includes the following topics:

Collecting Diagnostic Logs

In the event that it is necessary to collect diagnostic logs for vCenter Server Heartbeat, launch the *LogCollector* tool to automatically collect all required diagnostic logs for forwarding to VMware support.

Procedure

1 Right-click the *vCenter Server Heartbeat* System tray icon.

2 Select *Collect Diagnostic Logs*.

The vCenter Server Heartbeat *LogCollector* is displayed.

3 Click either **Collect logs from all machines** or **Collect logs from this machine only**.

The LogCollector displays the progress of collecting logs and once complete, provides a .zip file containing the logs located in at <install_location>\VMware\vCenter Server Heartbeat\Log_<date>\<server>.zip

Two Active or Two Passive Nodes

Should both nodes (Primary and Secondary) become active or passive at the same time, you should address the issue immediately.

Two Active Nodes

Two active nodes live on the same network is critical and referred to as Split-brain syndrome. This condition must be resolved immediately.

Problem

Split-brain syndrome is identified by the following symptoms:

- Both nodes in a 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 pair running vCenter Server Heartbeat on the Public IP address in a LAN
- In a WAN environment the Primary and Secondary connect to the network using different IP addresses.
- Clients (for example, vSphere Client and vSphere Web Client) cannot connect to the node running vCenter Server Heartbeat

Cause

The most common causes of two active nodes (Split-brain syndrome) are as follows:

- Loss of the VMware Channel connection (most common in a WAN environment)
- The active node is too busy to respond to heartbeats
- Incorrect configuration 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.

Solution

Identifying the node with the most up-to-date data

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

- Check the date and time of files on both nodes. Make the most up-to-date node the active node.
- From a client PC on a LAN, run nbtstat -A 192.168.1.1 where the IP address is the Public IP address of the node. This can help identify the MAC address of the node currently visible to client machines.

Note If both active nodes were servicing clients, perhaps at different WAN locations, you can make only one node active. Both nodes contain recent data that cannot be merged using vCenter Server Heartbeat. To restart replication, make one node active and one node passive. When replication restarts, the active node overwrites all data on the passive node. You can manually extract the up-to-date data from the passive node 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.

Resolving two active nodes (Split-brain syndrome)

The following procedure corrects two active nodes and results in an active and passive pair.

1 Identify the node with the most up-to-date data or the node to make active.

2 Shut down vCenter Server Heartbeat on both nodes (if running).

3 On the node to make passive, right-click the Task bar icon, and select the *Server Configuration* wizard.

4 Select the *Machine* tab and set the role to passive. Do not change the identity of the node (Primary or Secondary).

5 Click **Finish**.

6 Restart this node.

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) as appropriate.

8 On the active node, right-click the Task bar icon and select the *Server Configuration* wizard.

9 Select the *Machine* tab and verify that the role is set to active. Do not change the identity of the node (Primary or Secondary).

10 Click **Finish**.

11 Restart this node. As the node restarts, it connects to the passive node and starts replication. The active node overwrites data on the passive node.

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 Start vCenter Server Heartbeat Console.

14 Check that the nodes have connected and replication has started.

Two Passive Nodes

The Primary and Secondary nodes are both passive at the same time. This situation prevents clients from accessing protected applications and should be resolved immediately.

Problem

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

Cause

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

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

- The active node fails before the handshake that establishes the VMware Channel connection. The passive node cannot detect that the active node is not responding when the failure occurs and cannot determine the condition of the active node. The active node suffers a transient failure and the passive node cannot respond assuming the active role, leaving both nodes in a passive state
- Both Primary and Secondary nodes 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 nodes are restarted, 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 node 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.

Solution

To correct two passive nodes:

1 Determine the active node.

2 Shut down vCenter Server Heartbeat on both nodes. Leave any protected applications running on the node to make active.

3 On the node to make active, start the *Server Configuration* wizard, and select the active role. Do not change the identity (Primary or Secondary).

4 On the node to make passive, start the *Server Configuration* wizard, and confirm the passive node. Do not change the identity (Primary or Secondary).

5 Restart the passive node. All protected application services stop.

6 Start vCenter Server Heartbeat on both nodes.

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 node are present on the passive node
- All protected file and folder structures from the active node are present on the passive node

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-sync or Synchronized and busy processing. The following typical scenarios are described with possible causes and workarounds.

Services Running on the Passive Node

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

Problem

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

Cause

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

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

Note This occurs if the vSphere Client is left running on the passive node.

Services that keep files locked on the passive node are:

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

Note vCenter Server Heartbeat periodically checks for and stops any services running on the passive node.

Solution

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

1. Set Protected Application services to *Manual* on both nodes and verify that they are not running on the passive node.
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-malware protection is not part of the protected set as the file level anti-malware and the corresponding services are running on both machines.

Incorrect VMware Channel Configuration

An incorrectly configured channel connection can prevent proper communication and replication.

Problem

The following problems are experienced:

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

Cause

The list below provides the most common misconfigurations:

- Identical IP addresses at each end of the VMware Channel
- IP addresses in different subnets without static routing at each end of the VMware Channel
- VMware Channel NIC configured for DHCP when a DHCP server is not available

During installation, vCenter Server Heartbeat configures the VMware Channel NICs with user-provided information. Incorrect information or incorrectly modifying the VMware Channel NIC configuration after installation causes the VMware Channel to fail communicating.

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

Solution

The installation process manually assigns the correct IP addresses to each NIC on the Secondary node. If no VMware Channel connection occurs between the nodes, verify the configuration of the IP addresses on the Secondary's channel NICs. Check the settings for the Public NIC. The configuration error can remain unrecognized until a failover occurs.

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

ipconfig /all > ipconfig.txt

The output of this command saves the name, TCP/IP configuration, and MAC address of each NIC on the Secondary to a file called ipconfig.txt, which is present on that node after the PnP 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 this was updated by the PnP process.

Incorrect or Mismatched Disk Configuration

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

Problem

If any entry 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 nodes, and only supports protection of NTFS partitions.

Cause

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

- The Primary has drive G:, a valid NTFS partition, but no corresponding drive exists on the Secondary.
- The Primary has drive G:, a valid NTFS partition. The equivalent drive on the Secondary is a CD or DVD drive, or a FAT or FAT32 partition that cannot be protected.

In either scenario, 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**.

Solution

- Follow the steps documented in knowledge base article 1008458 – *Troubleshooting a set of File Filters that is reset to C:\Protected***.

Passive Node Has Less Available Space than Active Node

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

Problem

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) was exceeded.

Cause

The passive node has less available disk space than the active node, preventing updates from being replicated to the passive node. The quantity of updates from the active node exceeds the passive node's available disk space.

Solution

- Free up some additional disk space on the passive node. Do not delete data from the protected set to prevent data loss in the event of a failover. You could update the disk subsystem on the passive node. After allocating space, start replication.

Registry Status is Out-of-Sync

The Registry can be reported as Out-of-sync when one or more Registry keys fail to synchronize.

Registry Security Issues

Inability to access the registry prevents replication of the registry.

Problem

vCenter Server Heartbeat is unable to read, synchronize, or replicate the registry.

Cause

If a protected registry key has permissions that deny Write access to the System account, this can prevent vCenter Server Heartbeat from synchronizing or replicating it.

Solution

- 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 nodes, the following scenarios can occur.

Performance Issues

Poor performance can be experienced as a result of a channel loss.

Problem

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.

Cause

This unusual condition points to an application or Windows experiencing a fault on the passive node. A sudden restart of the passive node can occur due to the following causes:

- The node is configured for automatic software update management and some updates force the node to restart
- A software or operating system issue that occasionally fails and requires a system restart
- The VMware vCenter Server Heartbeat service experiences problems, does not respond, or terminates unexpectedly

Solution

To resolve the issue, perform the following checks.

1. Determine the likely source by examining the Windows event logs.
2. If the node does not display evidence of a system restart or unresponsive application, one or both of the VMware Channel NICs could be forcing a channel disconnection. See "Hardware or Driver Issues on VMware Channel NICs," on page 86 for more information on this topic.

Passive Node Does Not Meet Minimum Hardware Requirements

Inadequate hardware can cause channel drops and result in poor performance.

Problem

The data rate between nodes is very fast during a Full System Check and the VMware Channel drops.

Cause

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

Solution

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

Hardware or Driver Issues on VMware Channel NICs

NIC malfunctions and old or incorrect drivers can cause channel drops resulting in poor performance.

Problem

The VMware Channel intermittently drops or disconnects and reconnects.

Cause

The following are common causes of NIC problems:

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

- Improper configuration of NICs used for the VMware Channel connection
- ISP problems in a WAN environment

Solution

When a NIC problem is encountered, perform the following checks:

1. Verify that VMware Channel NIC drivers are the correct and latest versions. Known issues are identified with HP/Compaq ProLiant NC67xx/NC77xx Gigabit Ethernet NICs. Check other NIC types. See knowledge base article 1008383 – *VMware vCenter Server Heartbeat and Gigabit Ethernet NIC drivers (NC77XX)*
2. Verify hubs and Ethernet switches are operating properly. Identify and replace any defective components.
3. Test for defective Ethernet patch or crossover cables and replace if defective.
4. Correctly configure the NICs used for the VMware Channel connection.
5. Check the physical link for ISP problems.

Firewall Connection

In a LAN or WAN deployment, the VMware Channel can be connected through one or more internet firewalls. Because firewalls block unauthorized network traffic, configure firewalls on the route of the VMware Channel to allow channel traffic.

Problem

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

Cause

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 node and its counterpart on the Secondary node.

Solution

- 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 node and its counterpart on the Secondary node.

Channel Fails to Connect After Configuring Firewall Ports

Problem

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

Cause

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

Solution

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

Incorrect VMware Channel Configuration

An incorrectly configured channel connection can prevent proper communication and replication.

Problem

The following problems are experienced:

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

Cause

The list below provides the most common misconfigurations:

- Identical IP addresses at each end of the VMware Channel
- IP addresses in different subnets without static routing at each end of the VMware Channel
- VMware Channel NIC configured for DHCP when a DHCP server is not available

During installation, vCenter Server Heartbeat configures the VMware Channel NICs with user-provided information. Incorrect information or incorrectly modifying the VMware Channel NIC configuration after installation causes the VMware Channel to fail communicating.

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

Solution

The installation process manually assigns the correct IP addresses to each NIC on the Secondary node. If no VMware Channel connection occurs between the nodes, verify the configuration of the IP addresses on the Secondary's channel NICs. Check the settings for the Public NIC. The configuration error can remain unrecognized until a failover occurs.

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

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

The output of this command saves the name, TCP/IP configuration, and MAC address of each NIC on the Secondary to a file called ipconfig.txt, which is present on that node after the PnP 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 this was updated by the PnP process.

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

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

Problem

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

Cause

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

Solution

- Click the *Properties* tab for each Channel NIC on both nodes and verify that the check box for *vCenter Server Heartbeat Packet Filter* is cleared, so that the Packet Filter is disabled on that NIC.

Subnet or Routing Issues

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

LAN Deployment

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

Problem

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

Cause

The channel disconnects or fails to connect due to the Public NIC and/or one or more channels sharing the same subnet.

Solution

- If vCenter Server Heartbeat is deployed in a LAN environment, the Public IP address and the VMware Channel IP address on a node should be in separate subnets. When multiple redundant channels are present, each should have its own subnet. Check the network configuration for each NIC on both nodes in the pair and correct any issues.

WAN Deployment

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

Problem

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 might not be configured or might be configured incorrectly.

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

Solution

- Refer to knowledge base article 1023026 - *Creating a static route for the VMware Channel* for a detailed discussion about WAN channel routing issues, and for instructions on configuring a static route for the VMware Channel.

MaxDiskUsage Errors

vCenter Server Heartbeat uses queues to buffer the flow of replication data from the active node to the passive node. This configuration provides resilience in the event of user activity spikes, VMware Channel bandwidth restrictions, or VMware Channel drops across a WAN deployment. Some types of file write activity also require buffering as they can cause a sharp increase in the amount of channel traffic. The queues are referred to as the send queue (on the active node) or the receive queue (on the passive node).

Send Queue

vCenter Server Heartbeat considers the active node's send queue as unsafe because data in this queue has not yet been replicated across the VMware Channel to the passive node and therefore could be lost in the event of a failover. As a result of a failover caused by a hardware, operating system, or network communications failure, some data loss is inevitable, with the exact amount depending on the relationship between available VMware Channel bandwidth and the required data transmission rate. If the required data transmission rate exceeds available VMware Channel bandwidth, the send queue fills. If the available VMware Channel bandwidth exceeds the required data transmission rate, the send queue empties. This situation is most commonly seen in a WAN environment, where VMware Channel bandwidth is restricted. In a LAN that normally has high bandwidth on a dedicated channel, the size of the send queue is zero or near zero most of the time. On a node not protected by vCenter Server Heartbeat, all data is technically unsafe and subject to loss if the node fails.

Receive Queue

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

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

Two methods to set the queue size:

■ Using vCenter Server Heartbeat Console:

1 Start vCenter Server Heartbeat

2 Open the vCenter Server Heartbeat Console, and select *Data: Traffic Queues*.

3 Click **Configure**.

4 Configure the *Allow a maximum value* and click **OK**.

5 Shut down and restart vCenter Server Heartbeat to effect the change. You are not required to stop protected applications.

■ Using the Server Configuration wizard:

1 Shut down vCenter Server Heartbeat.

2 Open the Server Configuration wizard and select the *Logs* tab.

3 Configure the *Maximum Disk Usage* value and click **Finish**.

4 Start vCenter Server Heartbeat.

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

MaxDiskUsage Error Messages

The following error messages display when available disk space on the nodes is exceeded.

[L9]Exceeded the Maximum Disk Usage (VCChannelExceededMaxDiskUsageException)

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

Problem

vCenter Server Heartbeat exceeds its preconfigured queue size.

Cause

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

Solution

◆ 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

This message indicates that you have exceeded the amount of allocated disk space reserved for the active node's send queue.

Problem

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

Cause

A temporary interruption in the VMware Channel, or insufficient VMware Channel bandwidth to support the volume of replication traffic starts filling the active node's send queue. The size of the queue eventually exceeds the configured disk quota.

Solution

- Assuming no other channel connection issues exist (see knowledge base article 1008551 – *Troubleshooting VMware vCenter Server Channel Drops)*, you can increase the amount of disk space allotted to the queues. The default setting is 1GB, which can be insufficient on nodes 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) so vCenter Server Heartbeat can use any free disk space to store the queues.

[L9]Exceeded the Maximum Disk Usage on the PASSIVE Server

This message indicates that you have exceeded the amount of allocated disk space reserved for the passive node's receive queue.

Problem

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

Cause

Two of the most common causes are shown below:

- The bottleneck lies between the VMware Channel NIC and the disk subsystem on the passive node. Replication traffic passes across the VMware Channel faster than it can be written to disk on the passive node. The excess is buffered temporarily in the passive node's receive queue. The size of the queue can eventually exceed the allotted disk quota.
- If the passive node is much less powerful than the active node in terms of processor speed, RAM, or disk performance, it can lag behind the active node 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 can indicate a problem. Upgrade one or more physical or resource components of the node.

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

Solution

To resolve this issue:

- If you have multiple physical disks on each node, locate the vCenter Server Heartbeat send and receive 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 Configure the path for *Message Queue Logs Location* and click **Finish**.

4 Start vCenter Server Heartbeat on both nodes.

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

- 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 node's receive queue can increase sharply in response to certain types of file write activity on the active node, 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 can be far greater than the physical size of the files on the disk, and the receive queue can 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 node, including critical applications protected by Heartbeat. Allocate sufficient resources for all the applications and services running on such a node to provide maximum performance, stability, and resilience for changing client, server, and network activity.

[L20]Out of Disk Space (VCChannelOutOfDiskSpaceException)

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

Problem

Replication stops and the vCenter Server Heartbeat Event Log displays the error message originating from either node 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 5GB, but only 3GB of physical disk space remains, this error message is reported if one of the queues exceeds 3GB in size.

Solution

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

Application Slowdown

Operations performed by the application can take longer to complete, and in turn, can affect the time required to log in to a remote client, or to open or save a file. This is true for both nodes running vCenter Server Heartbeat and for nodes 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 support the load, the protected applications, and any other critical applications running on the same pair.

Poor Application Performance

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

Problem

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

Cause

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

Solution

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

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

Any software installed on a node 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. Increased demand caused by additional user activity can have an impact on the performance.

Problem

Increased user activity slows application response time.

Cause

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

Solution

- If the situation is sporadic, it can correct itself when the load decreases. If the increase is sustained and permanent, upgrade the hardware or allocate additional resources.

One Node Can Provide Adequate Resource Support, but the Other Cannot

If total resource requirements of applications exceed available physical resources, the operating system attempts to provide resources, but leaves some applications under-resourced. When this situation occurs, an application cannot obtain enough memory to operate normally, or a process must wait before accessing the hard disk.

Problem

Applications operate normally when the Primary node is active but operate slowly when the Secondary node is active (or the reverse).

Cause

A large discrepancy occurs in the processing power between the Primary and Secondary nodes. One node can handle the operational load while the other cannot. The load on a node is greater while in the active role when the protected application starts. Applications on the pair run successfully when the Primary is active, but experience performance issues when the Secondary is active (or the reverse). Problems can arise even when the more powerful node is active.

Solution

- Both nodes must have approximately equivalent processing power, RAM and disk performance. Upgrade the hardware or allocate additional resources on one node in the pair so that the two nodes have roughly the same performance.

Scheduled Resource Intensive Tasks

Scheduling multiple resource intensive tasks at the same time can adversely impact node performance and affect application performance.

Problem

Resource-intense scheduled tasks impact performance at certain times.

Cause

Two or more resource-intense processes run simultaneously or one process performs 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 anti-malware scans.

Solution

- Schedule operations so that they do not overlap and schedule them outside regular working hours, when fewer users are accessing the protected application and consequently less load on the node.

Glossary

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

Alert
A notification provided by vCenter Server Heartbeat sent to a user or entered into the system log indicating an exceeded threshold.

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

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

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

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

Basic Input/Output System (BIOS)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Machine Name
The Windows or NETBIOS name of a computer.

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

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

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

Pair
See vCenter Server Heartbeat Pair above.

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

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

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

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

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

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

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

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

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

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

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

Quality of Service (QoS)
An effort to provide different prioritization levels for different types of traffic over a network. For example, vCenter Server Heartbeat data replication may have a higher priority than ICMP traffic, as the consequences of interrupting data replication are more obvious than slowing down ICMP traffic.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Subnet
Division of a network into an interconnected but independent segment or domain, intended to improve performance and security.

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

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

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

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

Task
An action performed by vCenter Server Heartbeat when defined conditions are met.

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

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

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

Unprotected Application
An application not monitored nor its data replicated by vCenter Server Heartbeat.

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

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

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

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

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

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

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

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

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