

VERITAS Cluster Server

**Application Note: High Availability for
VMware ESX™ Virtual Machines**

Linux

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

VERITAS Legal Notice

Copyright © 2004 VERITAS Software Corporation. All rights reserved. VERITAS, the VERITAS Logo, and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS and the VERITAS logo, Reg. U.S. Pat. & Tm. Off. Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies.

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650-527-8000 Fax 650-527-2908
www.veritas.com

Third-Party Copyrights

Apache Software

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work.

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal,



or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.



Data Encryption Standard (DES)

Support for data encryption in VCS is based on the MIT Data Encryption Standard (DES) under the following copyright:

Copyright © 1990 Dennis Ferguson. All rights reserved.

Commercial use is permitted only if products that are derived from or include this software are made available for purchase and/or use in Canada. Otherwise, redistribution and use in source and binary forms are permitted.

Copyright 1985, 1986, 1987, 1988, 1990 by the Massachusetts Institute of Technology. All rights reserved.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided as is without express or implied warranty.

SNMP Software

SNMP support in VCS is based on CMU SNMP v2 under the following copyright:

Copyright 1989, 1991, 1992 by Carnegie Mellon University

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.



Contents

Chapter 1. Preface	i
Introduction	i
Getting Help	i
Telephone and Fax Support	ii
Conventions	ii
Chapter 2. Running VCS on a VMware ESX Server	1
Overview	1
Hardware Requirements for Running VCS on an ESX Server	2
Clustering a Virtual Machine Across Physical Nodes	3
Setting Up the ESX Server to Fail Over Virtual Machines	4
Agent to Monitor the VMware Virtual Machines	4
Installing VCS	5
Setting Up the Virtual Machine for Failover	5
Creating the Virtual Machine and Installing the Guest OS	5
Changing the Suspend File Location to a Location on a Shared Disk	5
Configuring the VM on Other Cluster Nodes	6
Creating the Service Group to Control the VM	7
Creating a Service Group	8
Adding the Virtual Machine Resource to the Group	8
Committing the Changes to the Configuration	9
Enabling Resources in the Group	9
Controlling the Virtual Machine Group	10



Appendix A. Using the TrySuspend Feature in the VMware Agent	11
Appendix B. Managing Applications in the VM Using the Remotegroup Agent [Unsupported]	13
Clustering a Virtual Machine	13
Using the RemoteGroup Agent	15
Index	19



Preface

Introduction

This paper explores using VERITAS Cluster Server (VCS) as a clustering solution for providing high availability for applications running within virtual machines. VCS accomplishes this by failing over virtual machines across physical machine boundaries. Using VCS, a virtual machine can move from one physical cluster node to another—protecting against hardware and software failures.

Getting Help

For technical assistance, visit the VERITAS Technical Services Web site at <http://support.veritas.com>. From there you can:

- ◆ Contact the VERITAS Technical Services staff and post questions to them.
- ◆ Download the latest patches and utilities.
- ◆ View the VCS Frequently Asked Questions (FAQ) page.
- ◆ Search the knowledge base for answers to technical support questions.
- ◆ Receive automatic notice of product updates.
- ◆ Learn about VCS training.
- ◆ Read white papers related to VCS.
- ◆ Access the latest product documentation and technical notes.

Contacting VERITAS Licensing

For license information call 1-800-634-4747 option 3, fax 1-650-527-0952, or e-mail amercustomer@veritas.com.



Telephone and Fax Support

Telephone and fax support for VCS is available only with a valid support contract. To contact Technical Services, dial the appropriate phone number listed on the *Technical Support Guide* included in the product box. Have your product license information ready to ensure you are routed to the proper support personnel.

The address for the VERITAS telephone support directory is:
<http://support.veritas.com/phone>.

Conventions

Typeface/Symbol	Usage
bold	names of screens, windows, tabs, dialog boxes, options, buttons
<i>italic</i>	new terms, book titles, emphasis, variables in tables or body text
Courier	computer output, command references within text
Courier (bold)	command-line user input, keywords in grammar syntax
<i>Courier (bold, italic)</i>	variables in a command
#	superuser prompt (for all shells)



Running VCS on a VMware ESX Server

1

Overview

VERITAS Cluster Server (VCS) is a high-availability software solution, designed to provide maximum uptime for enterprise applications. VCS operates by monitoring all resources required for an application to be available and to fail over the required resources to standby nodes in the event of a hardware or software failure on the primary node.

VMware™ ESX Server™ (VMware) is virtual machine (VM) software for consolidating and partitioning servers in high-performance environments. It is a cost effective, highly scalable virtual machine platform with advanced resource management capabilities.

VMware ESX Server lets system administrators minimize the total cost of ownership of server infrastructure by maximizing server manageability, flexibility and efficiency across the enterprise.

Using VMware, system administrators can:

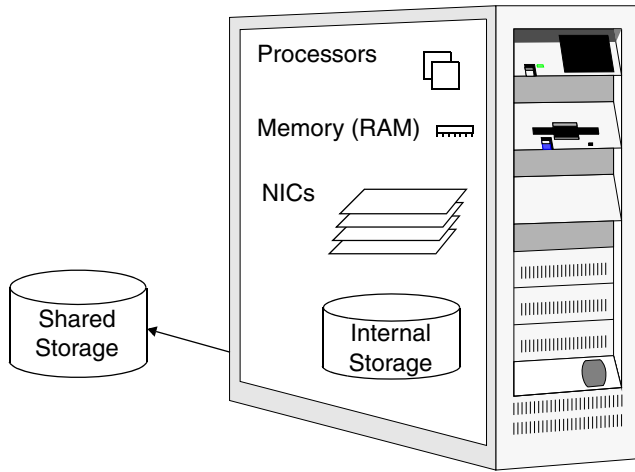
- ◆ Implement server consolidation by consolidating applications and infrastructure services onto fewer highly scalable, highly reliable enterprise-class servers.
- ◆ Deliver high availability and provide for disaster recovery. With a stable, uniform platform, system administrators can deliver more services and deploy new solutions faster and more efficiently.

Solutions featuring VMware and VCS together greatly increase availability of enterprise applications and deliver the savings and consolidation that VMware offers.



Hardware Requirements for Running VCS on an ESX Server

The following table lists the hardware requirements for each node that participates in the cluster. A minimum of two nodes are required and a maximum of 32 nodes can be used to form the cluster. The memory allocated to the Service Console should meet minimum VCS requirements since VCS runs on the Service Console.

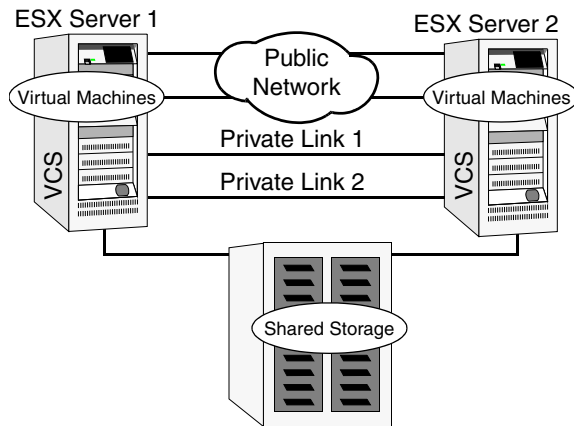


Item	Description
Internal Storage	While failing over virtual machines, internal storage is used only to store configuration files.
Processors	System processors must meet minimum VCS and VMware requirements. See the <i>VCS Installation Guide</i> and the VMware specs page.
NIC Cards	Three dedicated to the Console, one for the VM. Each physical node needs three NIC cards, where one is public and two private. Multiple VMs can share the fourth NIC for access to the public network.
RAM	While VCS requires 256 MB to run, ESX Server Service Console requires 272 MB to run 16 virtual machines. Use a minimum of 272 MB of RAM to ensure smooth performance.
Shared Storage	This requirement is for virtual machines when they fail over across physical machine boundaries. All virtual disks used by the virtual machine(s) have to reside on the shared disk(s).

Clustering a Virtual Machine Across Physical Nodes

A cluster is highly effective when an application fails over to a redundant system following hardware or software failures. To protect against hardware failures, a cluster must span multiple nodes. Setting up VCS in this environment is the preferred and recommended way to set up a cluster.

A virtual machine that possesses the capability to move from one node to another greatly increases the availability of the applications that it hosts. In the event of a hardware failure on the node that the virtual machine is running, the VM could be brought up on a corresponding standby host and resume servicing its clients.



The preceding diagram illustrates how two ESX Servers can be set up to cluster and failover virtual machines. The ESX Servers contain VCS and are clustered together to form an n-node cluster. The virtual machines are set up such that their disk images reside on the shared storage that both ESX Servers can see.

The virtual machine to be made highly available should be configured on both nodes using the VMware Management Interface. The VM should be configured identically across both the machines such that the virtual disks used by the VMs are available on the shared disks visible on both nodes.



Setting Up the ESX Server to Fail Over Virtual Machines

To set up ESX Server to fail over virtual machines across physical machine boundaries, VCS needs to be installed on an ESX Server. VCS enables the ESX Server cluster to move virtual machines across physical nodes and greatly increases the availability of applications running within the VM.

The following steps need to be performed in order to set up VCS on ESX Servers.

- ◆ Install an ESX Server on two or more nodes that will form the cluster. The example will use two nodes (Node1 and Node2), but the example can be extended to the maximum number of nodes supported by VCS.
- ◆ Make sure hardware requirements of the ESX Servers are met, see “[Hardware Requirements for Running VCS on an ESX Server](#)” on page 2.
 - ◆ Increase the amount of RAM allocated to the VMware Service Console. By default, the Service Console needs 272 MB to run sixteen VMs, whereas VCS requires 256 MB of memory to run. Therefore, the minimum of 272 MB should be allocated to ensure smooth performance.
- ◆ Set up network connections so that there are two NICs connected to the public network and two to the private networks between the nodes. Out of the two public NICs, one is needed by the Service Console and one will be dedicated for the virtual machines.
- ◆ Follow the VCS installation guidelines to set up the NICs (public and private) and the shared storage. Shared storage that is visible from all nodes in the cluster is a mandatory requirement to be able to fail over virtual machines. Refer to the *ESX Server SAN Compatibility Guide* for VMware approved SAN environments.
- ◆ Install VCS with the nodes as members of the cluster. To perform this task, follow the *VERITAS Cluster Server™ Installation Guide* for Linux.

Once VCS is installed on the ESX Servers, you should have a (n-node) cluster with members as the ESX Servers. The cluster is ready to fail over virtual machines once VCS is installed.

Agent to Monitor the VMware Virtual Machines

VCS adds components that are needed to fail over virtual machine on an ESX Server. A new VCS agent fails over the virtual machines. The agent is called *VMware*, and is used to online/offline and monitor a virtual machine for failure.



Installing VCS

To be able to fail over virtual machines, VCS will have to be installed on ESX Server Service Console. To perform this step, consult the VCS installation documentation and install VCS on the systems to be used for failover.

Once VCS is set up on ESX Server Service Console, the next step is to set up a virtual machine and configure it so that it can failover across the physical machine boundaries.

Setting Up the Virtual Machine for Failover

Setting up a virtual machine for failover involves configuring the ESX Servers which are part of the cluster to register a virtual machine that can be started on each of the systems. All disk images will have to reside on shared storage to facilitate failover.

Creating the Virtual Machine and Installing the Guest OS

First, create the virtual machine on one of the VMware nodes by following the instructions given in the VMware documentation. Note that all disk images created during the process of creating a virtual machine should reside on shared storage that is accessible from both nodes, so as to facilitate failover.

Once the virtual machine has been created on the first node, make the following changes to the configuration to enable VCS to take advantage of advanced features of VMware.

Changing the Suspend File Location to a Location on a Shared Disk

1. Log in to the VMware Management Interface, click the name of the virtual machine to open the virtual machine configuration page.
2. Under the Configuration section, click the **Options...** hyperlink.
3. On the Options page, click the **Edit...** hyperlink.
4. On the edit page, change the **Suspend file location** entry to a partition that exists on a shared disk and is visible from all the nodes of the cluster.

This configuration enables VCS to start and restart a virtual machine by suspending it to disk and resuming it on a different physical machine. This feature is available as part of the VMware agent for VCS.

Note Before continuing, make sure that you have powered off the VM that you just created.

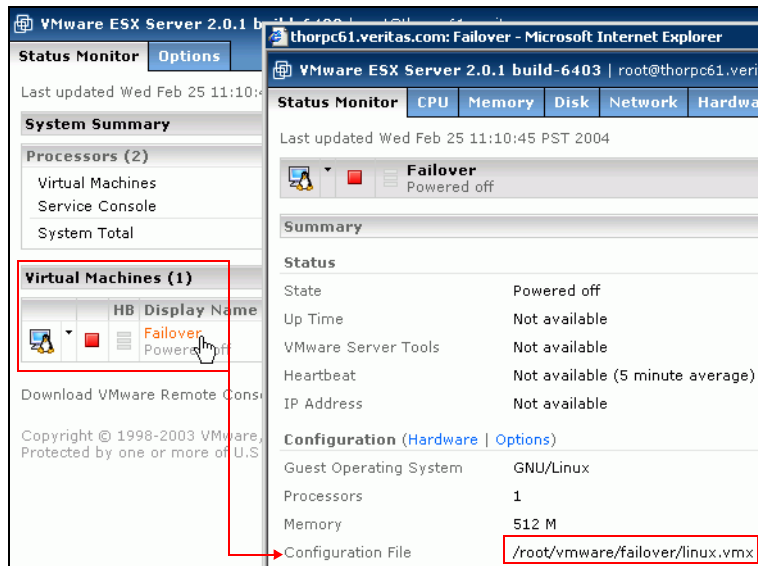


Configuring the VM on Other Cluster Nodes

Once the virtual machine has been created on one node, configure the other nodes in the cluster to run the same virtual machine, so that they can be effective failover targets.

1. Copy the configuration files of the virtual machine from the first node.

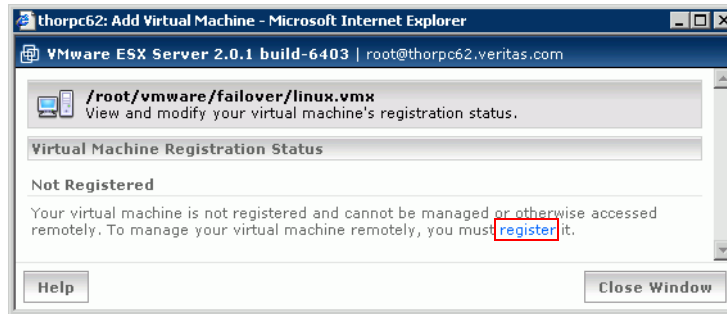
To find the full path of the configuration file, open the VMware Management Interface, and on the Status Monitor page, click the name of the virtual machine on the first node (see the following screen shot). Look for the Configuration section that specifies the configuration file.



2. Copy all the contents of the directory in which the configuration file exists to the second node. For the above example, on the second node, create a directory called **failover** under `/root/vmware` and copy all the files from the first node into this directory.
3. Once the files are copied, you are ready to register this virtual machine on the second node. To do this, on the Status Monitor tab of the second node, click **Manage files...**
4. This will bring up an explorer type interface with the files in the root filesystem of the second node. Navigate to the directory `/root/vmware/failover` in this tree, so that the files under this directory are visible on the right-hand pane.
5. On the right-hand pane, click the `.vmx` file that contains the VM configuration (in this case, `linux.vmx`).



6. A new window opens with the configuration details. Register the VM by clicking the **register** link.



7. Close the popup screen and click **Refresh** in the Status Monitor window. The imported virtual machine should show up in the list of virtual machines.
8. Power on the virtual machine on the second node.
9. Repeat this procedure with all the nodes that form the cluster and that are needed to run the virtual machine.

Creating the Service Group to Control the VM

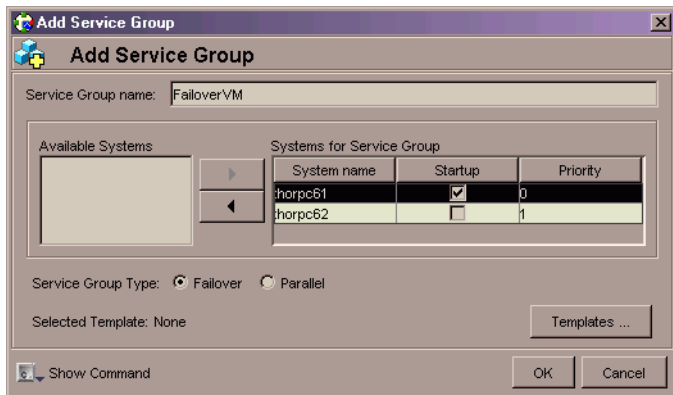
The next step is to create a VCS service group to monitor the virtual machine.

Create a group that consists of a single resource of the *VMware* type. The Virtual Machine resource will monitor the virtual machine.



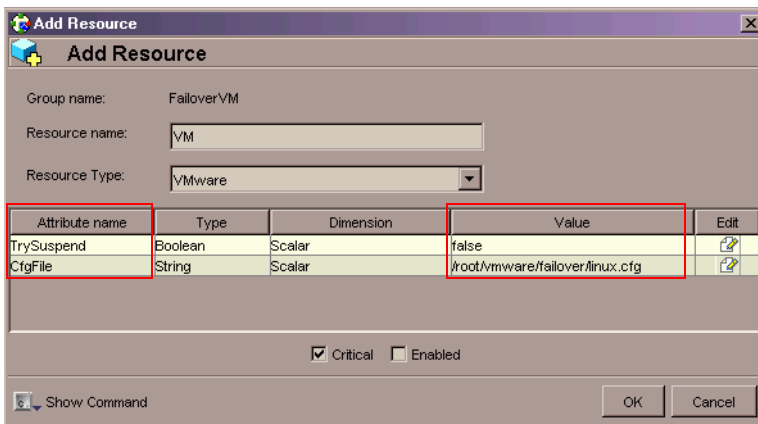
Creating a Service Group

Use the Cluster Manager (Java Console) or command line to create a group to which the resources will be added.



Adding the Virtual Machine Resource to the Group

Add a resource to monitor the virtual machine.



Set the attributes of this resource to the correct values.

TrySuspend: Leave the value as false.

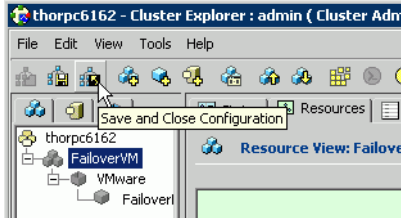
CfgFile: Edit this attribute and enter the full path of the configuration file for this VM.

Committing the Changes to the Configuration

Run `haconf -dump -makeo` to save the changes to the configuration.

Or

From the Cluster Manager (Java Console), click the **Save and Close Configuration** button.

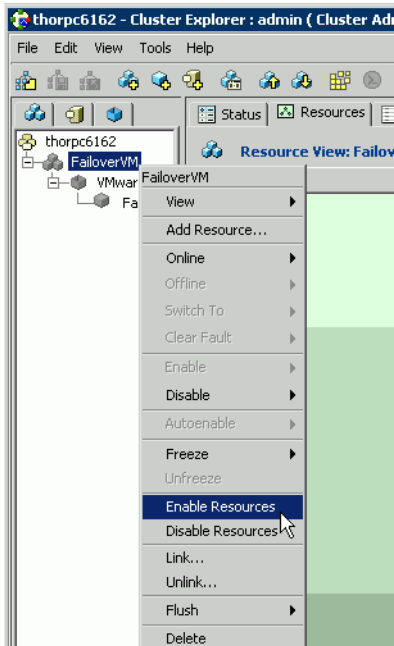


Enabling Resources in the Group

Run `hagrps -enableresources <GrpName>` to enable the resources in the group.

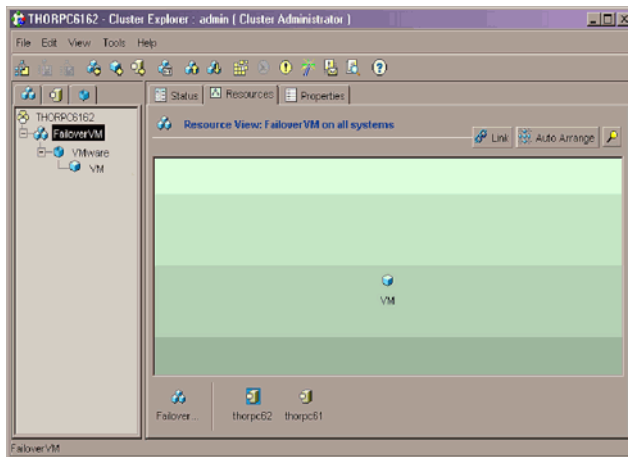
Or

Right-click the cluster name, and select **Enable Resources**, to enable the resources in the group.



Controlling the Virtual Machine Group

Once the group is set up, it can be managed and monitored using the VCS GUI. The group set up on the Service Console can be used to online/offline/switch and monitor the status of the virtual machine. If the virtual machine faults, VCS running on the Service Console fails over the virtual machine to a failover target, thus ensuring high availability.



Using the TrySuspend Feature in the VMware Agent



TrySuspend is an attribute of the VMware agent, which enables the agent to perform a fast failover of the virtual machine to a failover target.

The VMware agent tests for the *TrySuspend* attribute to be set before it attempts to switch a virtual machine. If it is set to true, the offline entry point of the agent suspends the virtual machine instead of shutting it down. If the VM is suspended, the online entry point resumes the VM instead of doing a cold boot. Suspending and Resuming a virtual machine result in faster failover times than what it takes for a VM to shut down and restart on another physical node.

Under normal conditions, *TrySuspend* should be set to false (0), because the feature is effective only when the virtual machine switch is planned. Unplanned failures cause loss of state, therefore causing the VM to be restarted on the failover node. *TrySuspend* can be set to true (1), just before a planned migration of the VM and reset to false (0) after the migration is complete.

To use *TrySuspend*, test the virtual machine and make sure that the virtual machine is able to suspend and resume without any errors on each physical node. This is important since it is better to test if the feature works before running into problems during an actual migration.

Note For this feature to work properly, the suspend file location set in the configuration file should be identical across all the nodes of the cluster.





Managing Applications in the VM Using the Remotegroup Agent [Unsupported]

B

VCS provides an additional agent to monitor an application running within a virtual machine called the *RemoteGroup* agent. As the name suggests, this agent monitors a VCS group running within the virtual machine, and reflects the groups's status as the status of a resource running on the VMware Service Console. This allows VCS on the ESX Server Service Console to monitor applications running within the virtual machine, and therefore improve the availability.

Clustering a Virtual Machine

Traditionally, VCS clusters physical machines and enables applications running on physical machines to fail over to a redundant server. The VMware ESX Server adds a new dimension to the task of high availability of applications by partitioning a single server into multiple virtual machines. The applications to be monitored run within these virtual machines, therefore, making it mandatory for the virtual machines as well as the applications within them to be monitored by VCS, in order to achieve a highly available system.

▼ **To achieve high availability of an application running within a virtual machine, VCS monitors**

1. The virtual machine itself.
2. The application running within the VM.

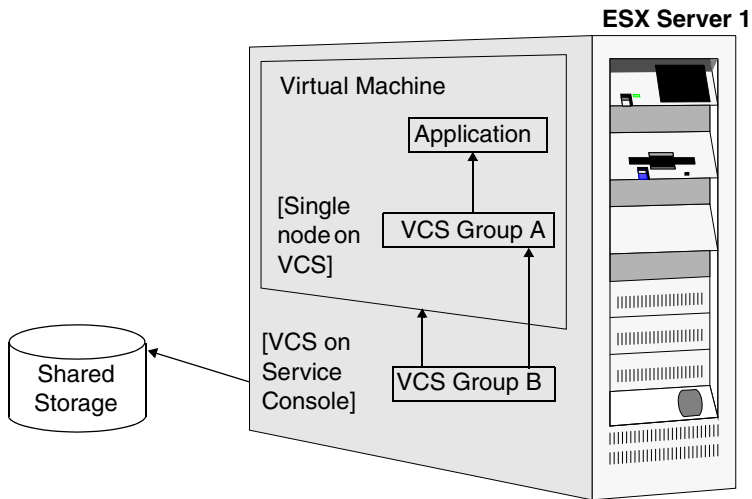
To monitor the virtual machines running under VMware on an ESX Server, VCS must run on the Service Console. Virtual machines can be considered as applications, a VCS agent can be used to monitor the virtual machine and report the status periodically.

Similarly, the application running within the virtual machine also has to be monitored. Since VCS is running within the Service Console, there is no way within the virtual machine to monitor the application. Therefore, a lightweight, single-node version of VCS will run within the virtual machine. A VCS group will be created for the application running within the VM, which will monitor the application and report status periodically.



From the Service Console, VCS will monitor the virtual machine as well as the group monitoring the application within the virtual machine. With this setup, all failures can be monitored and recovered from. The following diagram summarizes the setup.

The VCS configuration using the RemoteGroup agent to monitor an application running in a VM



From the preceding diagram, VCS Group B is the group running on the Service Console, which monitors the virtual machine as well as the application VCS group (Group A) that is running within the virtual machine. Monitoring the VCS group A gives the Group B information about the status of the application running within the virtual machine. This also lets VCS leverage all of the existing application agents to report status without making any changes to them. The VCS group A acts like a proxy to the application specific agents to report status to the VCS on the Service Console.

Using this procedure, application availability can be monitored within a virtual machine, and on failures, virtual machines can be failed over to another physical node.

Many such groups can co-exist running under the VCS on the Service Console, to monitor various applications running on individual virtual machines. Inside the virtual machine however, it is best to limit the number of groups to a single group per application being monitored.

Using the RemoteGroup Agent

▼ To use the RemoteGroup agent to monitor applications within the cluster

1. Set up the virtual machine and a group running on the ESX Server Service Console that controls the virtual machine, see the “[Setting Up the Virtual Machine for Failover](#)” on page 5 for more information.

2. Install VCS within the virtual machine.

Follow instructions from the *VCS Installation Guide* and install VCS for the Guest OS within the virtual machine. Single-node VCS will monitor the application running within the VM.

3. Install the application and create VCS service group.

The next step is to install the application to be made highly available and set up the VCS group to monitor this application.

Using the *VERITAS Cluster Server™ User's Guide*, configure the application to be made highly available on the single node VCS within the VM. The VCS group should monitor the application and should be capable of bringing it online and taking it offline. Add all necessary resources which the application is dependant on in the group being configured.

At the end of this step, the application should be controlled by a VCS group running within the virtual machine.

Note The *Autostart* attribute for the group should be set to 1 (true). The *AutoStartList* attribute for the group should be set to the node name of the virtual machine. This ensures that when VCS starts up, the group is automatically brought online.

4. Set up a group operator user for executing group operations.

Since the group set up within the virtual machine will be monitored over the network, in order to perform operations on the group (online/offline), a username and password will have to be supplied to the RemoteGroup agent. Therefore it is a good idea to create a user with group operator privileges for the group created within the virtual machine. Refer to the *VERITAS Cluster Server™ User's Guide* for instructions.



5. Add the RemoteGroup resource to the group.

Add Resource

Group name: FailoverVM

Resource name: Grp

Resource Type: RemoteGroup

Attribute name	Type	Dimension	Value	Edit
FQSysName	String	Scalar	THORPC241.VERITAS.COM	[Edit]
VCSSysName	String	Scalar	THORPC241	[Edit]
GrpName	String	Scalar	FailoverGrp	[Edit]
User	String	Scalar	admin	[Edit]
Password	String	Scalar	password	[Edit]
VMResName	String	Scalar	VM	[Edit]

Critical Enabled

Show Command OK Cancel

The description of the attributes to be configured are as follows:

FQSysName (fully qualified system name): Enter the fully qualified network name of the virtual machine along with domain information.

VCSSysName: Enter the VCS node name of the virtual machine.

GrpName: Enter the name of the group created in the virtual machine to monitor the application.

User : Enter the name of the group operator user created in [step 4](#).

Password: Enter the password for the group operator user created in [step 4](#).

VMResName: Enter the name of the Virtual Machine resource configured before the RemoteGroup resource.

Note Using a VCS GUI here is more efficient.

6. Link the VMware and RemoteGroup resources.

Establish a dependency between the VMware and RemoteGroup resources. The RemoteGroup resource should depend upon the Virtual Machine resource. To make this link, you can use a VCS GUI or run the following command on the ESX Server Service Console.

```
hares -link <parent res> <child res>
```

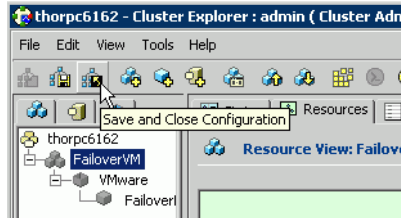
Here, the parent will be the RemoteGroup resource and child will be the Virtual Machine resource.

7. Commit the changes to the configuration.

Run `haconf -dump -maker0` to dump the changes to the configuration.

Or

From the Cluster Manager (Java Console), click the **Save and Close Configuration** button.

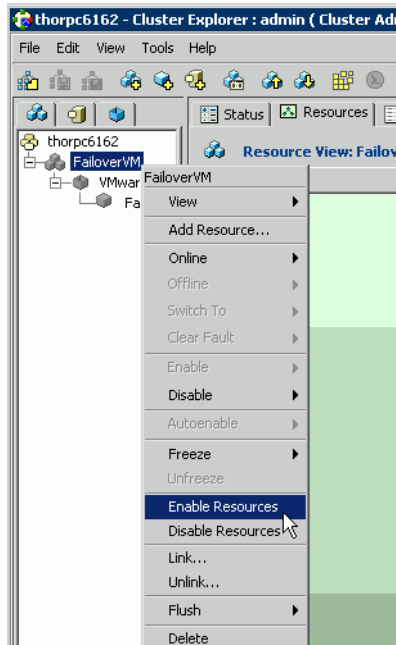


8. Enable all resources in the group.

Run `hagrp -enableresources <GrpName>` to enable all resources in the group.

Or

Right-click the cluster name, and select **Enable Resources**, to enable the resources in the group.





Index

- A**
 - adding
 - virtual machine resource 8
 - agents
 - RemoteGroup 13
 - VMware 4
 - attributes
 - CfgFile 8
 - TrySuspend 8
- C**
 - CfgFile attributes 8
 - changing
 - suspend file location 5
 - clustering virtual machines 3
 - committing changes
 - haconf 9, 17
 - configuring
 - cluster nodes with VM 6
 - creating
 - service group 7
 - creating, virtual machines 5
- E**
 - enabling resources 9
 - hagrp 17
 - establishing dependency
 - hares 16
 - ESX Server, setting up 4
- F**
 - failing over, virtual machines 4
 - FQSysName attribute 16
- G**
 - GrpName attribute 16
- H**
 - haconf 9, 17
 - hagrp 9, 17
 - hardware requirements
 - internal storage 2
 - NIC Cards 2
 - processors 2
 - RAM 2
 - Shared Storage 2
 - hares 16
- I**
 - installing, VCS 5
 - internal storage requirements 2
- M**
 - managing, virtual machine groups 10
- N**
 - NICs 4
 - n-node cluster 3
- P**
 - Password attribute 16
- R**
 - RAM requirements 2
 - RemoteGroup resources
 - FQSysName 16
 - GrpName 16
 - Password 16
 - User 16
 - VCSSysName 16
 - VMResName attribute 16
 - RemoteGroup, agent 13
 - resources 8
- S**
 - setting up virtual machines
 - failing over 5
 - setting up, ESX Server 4
 - suspend file
 - changing location 5



T

TrySuspend attribute 8

U

User attribute 16

V

VCS, installing 5

VCSSysName attribute 16

VERITAS Cluster Server
overview 1

virtual machine

VMware™ ESX Server™ 1

virtual machines

failing over 4

setting up 4

setting up for failover 5

VMFS partitions

clustering access 5

shared access 5

VMware agents 4

TrySuspend attribute 11

VMware™ ESX Server™

overview 1

