VERITAS™

VERITAS Cluster Server 4.0

Release Notes

AIX

August 2004

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 Software

Copyright © 1998-2004 VERITAS Software Corporation. All rights reserved. VERITAS, VERITAS Software, the VERITAS logo, VERITAS Cluster Server, and all other VERITAS product names and slogans are trademarks or registered trademarks of VERITAS Software Corporation. VERITAS, the VERITAS Logo, and Cluster Server 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 650–527–2901
www.veritas.com

Third-Party Copyrights

Apache Software

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

The Apache Software License, Version 1.1

Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgement:

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Alternately, this acknowledgement may appear in the software itself, if and wherever such third-party acknowledgements normally appear.

4. The names "The Jakarta Project", "Tomcat", and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.

THIS SOFTWARE IS PROVIDED ''AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see http://www.apache.org/.

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.

VERITAS Cluster Server 4.0 Release Notes

This document provides important information regarding VERITAS Cluster Server (VCS) version 4.0 for AIX 5.1 (32-bit and 64-bit), and AIX 5.2 (32-bit and 64-bit). Review this document before installing VCS.

New Features and Updates

The features and updates described below are introduced in VCS version 4.0.

Global Cluster Option

The Global Cluster Option to VCS enables a collection of VCS clusters to work together to provide wide-area disaster recovery. Previously, the wide-area functionality was available in a separate product, "Global Cluster Manager." The functionality has now been incorporated into VCS 4.0.

VCS Simulator

VCS Simulator is a tool for simulating any cluster configuration and determining how service groups will behave during cluster or system faults. With the simulator, you can designate and fine-tune configuration parameters, view state transitions, and evaluate complex, multinode configurations. The tool is especially valuable because it enables you to design and evaluate a specific configuration without test clusters or changes to existing production configurations.

I/O Fencing

VCS 4.0 provides a new capability, called I/O fencing, to arbitrate cluster membership and ensure data integrity in the event of communication failure among cluster members. The I/O fencing kernel module uses SCSI-III Persistent Reservations and designated coordinator disks, as described in the *VERITAS Cluster Server 4.0 User's Guide.*

Fire Drill

Fire drill is a procedure for testing the fault readiness of a configuration. A fire drill on a VCS-controlled application uses a separate fire drill service group that contains a copy of the live application's resources. See the *VCS 4.0 User's Guide* for more information.

Steward

The Steward mechanism minimizes chances of a wide-area split-brain in two-node clusters. The steward process can run on any system outside of the clusters in a Global Cluster configuration. See the *VCS 4.0 User's Guide* for more information.

Web Console Features

- Support for Global Clustering
- Home Portal
- User Management

Java Console Features

- Support for Global Clustering
- VCS Simulator
- Display of agent logs

The cpuusage Event Trigger

The new cpuusage event trigger is invoked on systems where CPU usage exceeds the configured threshold value. See the *VCS 4.0 User's Guide* for more information.

The multinicb Event Trigger

The new multinicb event trigger is invoked when a network device under MultiNICB control changes its state. The trigger is also always called in the first monitor cycle. See the *VCS 4.0 User's Guide* for more information.

Action Entry Point

The action entry point enables agents to perform actions that can be completed within a few seconds and that are outside the scope of traditional actions such as online or offline.

Info Entry Point

The info entry point enables agents to gather specific information for an online resource.

New Bundled Agents

The following bundled agents were added in the VCS 4.0 Release. For details, refer to the *VERITAS Cluster Server 4.0 Bundled Agents Reference Guide*.

- IPMultiNICB Agent
- MultiNICB Agent

New Attributes

- Resource Type Attributes
  - ActionTimeout
  - FireDrill
  - InfoInterval
  - InfoTimeout
  - LogDbg
  - MonitorStatsParam
  - SupportedActions
- Resource Attributes
  - ComputeStats
  - MonitorTimeStats
  - ResourceInfo
- Service Group Attributes
  - Authority
  - ClusterFailoverPolicy
  - ClusterList
- System Attributes
  - CPUUsage
  - CPUUsageMonitoring
  - NoAutoDisable

- Cluster Attributes
  - AutoStartTimeout
  - ClusState
  - ClusterAddress
  - ConnectorState
  - Stewards
  - UseFence
  - VCSi3Info

New Attribute Category

Heartbeat attributes are introduced to VCS 4.0 with the new global cluster features.

- Heartbeat Attributes
  - AgentState
  - Arguments
  - AYAInterval
  - AYARetryLimit
  - AYATimeout
  - CleanTimeOut
  - ClusterList
  - InitTimeout
  - LogDbg
  - State
  - StartTimeout
  - StopTimeout

Installation Notes

The following section provides information on installing VERITAS Cluster Server and the system requirements for the installation.

Installing or Upgrading to VCS 4.0

Refer to the *VERITAS Cluster Server 4.0 Installation Guide* for instructions on how to install VCS 4.0 and how to upgrade to VCS 4.0 from earlier versions of VCS. The *VCS 4.0 Installation Guide* is in the `/docs` directory of the VERITAS product CD.

Obtaining License Keys for VCS

VCS is a licensed software product. For information on obtaining license keys for VCS, refer to the *VCS 4.0 Installation Guide.*

Supported Hardware

The compatibility list contains information about supported hardware and is updated regularly. Visit http://support.veritas.com for the latest information on supported hardware, or contact your VERITAS sales representative.

Note Before installing or upgrading VERITAS Cluster Server, review the current compatibility list to confirm the compatibility of your hardware and software.

Supported Software

- AIX 5.1 If you are using VxVM or VxFS, use Maintenance Level 6 with APAR IY56488; the XLC.aix50.rte must be at level 6.0.0.7 or higher.
- AIX 5.2 (Maintenance Level 3) with APAR IY56497. The XLC.aix50.rte must be at level 6.0.0.7 or higher. If you plan to use the VCS I/O fencing option, you must use AIX 5.2.
- VERITAS Volume Manager (VxVM) 3.2, 4.0
- VERITAS File System (VxFS) 3.4 Patch 2, 4.0
- Logical Volume Manager (LVM)
- Journaled File System (JFS) and Enhanced Journaled File System (JFS2)

For the latest information on updates, patches, and software issues for this release, review TechNote 269928:

http://support.veritas.com/docs/269928

System Requirements

Cluster Manager Requires AIX Developer Kit for Java

The VCS Web Console and VCS Java Console use the IBM AIX Developer Kit, Java 2 Technology Edition, Version 1.3.0 with either AIX 5.1 or AIX 5.2.

Requirements for Accessing the VCS Web Console

An Internet browser is required to access the VCS Web Console. The following supported Internet browsers have been tested:

- Internet Explorer 5.0, 5.5, and 6.0
- Netscape versions 6.2 and 7.0

Note The VCS Web Console requires the Java Plug-in enabled on the client browser. For information on downloading or enabling the Java Plug-in, see the *VERITAS Cluster Server 4.0 User's Guide* section titled "Java Plug-in Requirements for the Console."

Requirements for Accessing VCS Java Console

The VCS Java Console requires a minimum of 256MB RAM and 1280x1024 display resolution. The color depth of the monitor must be at least 8-bit (256 colors), although 24-bit is recommended. The Java Console does not run with a Colors setting of 16.

The minimum requirements for Windows clients are Pentium II, 300MHz, 256MB RAM, and 800x600 display resolution. (VERITAS recommends a minimum of Pentium III, 400MHz, and 512MB RAM.) The color depth of the monitor must be at least 8-bit (256 colors), and the graphics card must be able to render 2D images.

Package Contents

The following packages are included on the VERITAS Cluster Server CD:

VCS Packages

The following packages for VCS are in the `pkgs` directory:

- `VRTScpi`, VERITAS Cross-platform Installer
- `VRTScscm`, VCS Cluster Manager (Java Console)
- `VRTScscw`, VCS Configuration Wizards
- `VRTScssim`, VCS Simulator
- `VRTScutil`, VERITAS Cluster Utility
- `VRTSgab`, Group Membership and Atomic Broadcast
- `VRTSjre`, VERITAS redistribution of JRE
- `VRTSllt`, Low Latency Transport
- `VRTSperl`, VERITAS redistribution of Perl 5.8.0
- `VRTSvcs`, VERITAS Cluster Server
- `VRTSvcsag`, VCS Bundled Agents
- `VRTSvcs.msg.en_US`, VCS Message Catalogs
- `VRTSvcs.man`, VCS Manual Pages
- `VRTSvcsw`, Cluster Manager (Web Console)
- `VRTSvlic`, VERITAS License Utilities
- `VRTSveki`, VERITAS Kernel Interface
- `VRTSvxfen`, I/O Fencing
- `VRTSweb`, VERITAS Web GUI Engine
- `VRTSvcs.doc`, VCS Documentation
- `WindowsClusterManager`, VCS Cluster Manager (Java Console), a Java-based graphical user interface for Windows clients

Bundled Agents

The following agents are included with VCS. For information on any of the agents listed below, refer to the *VERITAS Cluster Server 4.0 Bundled Agents Reference Guide*.

Application	DiskGroup	DNS
ElifNone	FileNone	FileOnOff
FileOnOnly	IP	IPMultiNIC
IPMultiNICB	LVMVG	Mount
MultiNICA	MultiNICB	NFS
NIC	NotifierMngr	Phantom
Process	Proxy	ServiceGroupHB
Share	Volume	VRTSWebApp

Enterprise Agents

Enterprise agents are sold separately. Contact your VERITAS sales representative for details about these agents, additional agents under development, and agents available through VERITAS Consulting Services.

Note Before configuring an enterprise agent with VCS 4.0, verify that you have the latest version of the agent.

Supported Enterprise Agents

VCS 4.0 supports the VCS enterprise agents listed below. Refer to this table for supported application and operating system versions. VCS agents support a specified application version on AIX if the application vendor supports that version on AIX.

Supported VCS Agent	Agent version	VCS version			Application		OS	
		2.0	3.5	4.0			5.1	5.2
Oracle	4.0	p	p	s	Oracle	8.0.x, 8*i*, 9*i* R1, 9*i* R2 10g	s	s
DB2	4.0	p	p	s	DB2 Enterprise Server Edition	7.2, 8.1	s	s
NetBackup	3.5	s	s	s	NetBackup* (including 64-bit)	4.5	s	s
SRDF	4.0	n	n	s	EMC Symmetrix Remote Data Facility		s	s
PPRC	4.0	n	n	s	IBM Peer-to-Peer Remote Copy		s	s

s – supported configuration p – supported by previous version of agent

* NetBackup 5.0 ships with an agent that supports VCS 4.0

Software Limitations in VCS 4.0

The following limitations apply to VCS version 4.0.

Cluster Manager (Java Console)

Java Console for VCS 4.0 is Required

Cluster Manager (Java Console) from VCS versions earlier than 2.0 cannot be used to manage VCS 4.0 clusters. VERITAS recommends always using the latest version of Cluster Manager. See the *VERITAS Cluster Server 4.0 Installation Guide* for instructions on upgrading to the VCS 4.0 version of Cluster Manager.

Running Java Console on a Non-Cluster System is Recommended

VERITAS recommends not running Cluster Manager (Java Console) for an extended period on a system in the cluster.

Cluster Manager (Web Console)

Cluster Name Should Not Include Single or Double Quotes

If a cluster name includes single or double quotes, some cluster views and operations in the Web Console will not function correctly.
Workaround: Verify that the ClusterName attribute for the cluster includes only valid characters.

Changes to UserStrGlobal for ClusterService May Disrupt Cross-Product Navigation

The Web Console uses the UserStrGlobal attribute of the ClusterService service group. Changes to this attribute may disrupt cross-product navigation through the Web Console.
Workaround: Do not edit the default value of UserStrGlobal for the ClusterService service group.

Web Console Requires Java Plug-In Version 1.4.1_x Enabled

The VCS Web Console requires the Java Plug-in enabled on the client browser. See the *VERITAS Cluster Server 4.0 User's Guide* for instructions regarding the Java Plug-in.

Web Console for VCS 4.0 AIX Does Not Support Secured VCS 4.0 Clusters

The Web Console for VCS 4.0 on AIX is not designed to connect with post-4.0 VCS clusters that have the VERITAS Security Subsystem (VxSS) enabled.

IBM Home Page Reader Does Not Enable Service Group Priority and Startup Options

The Priority and Startup options are not enabled when a service group is configured using IBM Home Page Reader.
Workaround: If necessary, edit the Priority and AutoStartList attributes after adding the service group.

I/O Fencing

Stopping Systems in Clusters with I/O Fencing Configured

The I/O fencing feature protects against data corruption resulting from a failed cluster interconnect, or "split brain." See the *VERITAS Cluster Server 4.0 User's Guide* section titled "VCS Communications, Membership and I/O fencing" for a description of the problems a failed interconnect can create and the protection I/O fencing provides.

I/O fencing uses SCSI-III Persistent Reserve keys to implement data protection. Keys are placed on I/O fencing coordinator disks and on data disks. The VCS administrator must be aware of several operational changes needed when working with clusters protected by I/O fencing. Specific shutdown procedures ensure keys are removed from coordinator disks and data disks to prevent possible difficulties with subsequent cluster startup.

Using the `reboot` command rather than the `shutdown` command bypasses shutdown scripts and can leave keys on the coordinator disks and data disks. Depending on the order of reboot and subsequent startup events, the cluster may warn of a possible split brain condition and fail to start up.
Workaround: Use the `shutdown -r` command on one node at a time and wait for each node to complete shutdown.

The vxfentsthdw -g or -c Options May Fail

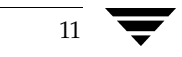
You must not use the `-g` or the `-c` option of the `vxfentsthdw` command when testing disk groups to determine whether disks support SCSI-3 Persistent Reservation (PR). This is because of a known problem pertaining to the way disks within disk groups are identified on AIX systems.

The `-g` option specifies a disk group for the test. The disk group could be made up of data disks or coordinator disks. The `-c` option specifies that the disks are to be used as coordinator disks and not for data.

To test disks for SCSI-3 PR support and for I/O fencing, either use other options or use the `vxfentsthdw` command without options.

The vxfentsthdw -s Option is Not Supported

The `vxfentsthdw` command option `-s` is not supported for this release of SFRAC on AIX. The `-s` option specifies that the two test systems use SSH for communications.



Undocumented Commands, Command Options, and Libraries

VCS contains undocumented commands and command options intended for VERITAS development use only. Undocumented commands are not supported by VERITAS.

NameRule Attribute is Deprecated in VCS 4.0

The resource type attribute, NameRule, has been removed from VCS 4.0. Previously, NameRule was used to generate a resource name when none was specified.

Change in Behavior: Specifying a resource name is mandatory. VCS reports an error if a resource name is not specified in the configuration. Now, if NameRule is defined in a `types.cf` file, it is recognized as a valid keyword but is not interpreted.

System Names in VCS

The name of a system specified in the VCS configuration file, `main.cf`, must not use the fully qualified form; that is, the name must not include periods. The name in `main.cf` must be consistent with the name used in `/etc/llthosts`. If the name listed in `/etc/llthosts` is fully qualified, VCS uses only the first segment of the name. If you create the file `/etc/VRTSvcs/conf/sysname` such that it contains the system name to be used by `main.cf`, VCS uses it to verify the system name.

Global Cluster Address Requires Resolved Virtual IP

The Virtual IP address must have a DNS entry if virtual IP is used for heartbeat agents.

File Systems Must be Listed in /etc/filesystems on AIX 5.x

In a cluster running AIX 5.1 or AIX 5.2, the `/etc/filesystems` file on *each* node must contain entries for all JFS and VxFS file systems in the cluster. The VCS Mount agent uses the `fsck` utility when file system corruption occurs. On AIX 5.1 or 5.2 systems, the `fsck` utility requires entries in the `/etc/filesystems` file. If the required entries are not present, an error resembling the following is displayed:

```
Cannot find the Vfs value for file system <BlockDevice>
```

Refer to the *VERITAS Cluster Server Bundled Agents Reference Guide* for information on specifying the Mount resource and creating entries in the `/etc/filesystems` file. Note that the `crfs` command creates an entry in `/etc/filesystems` only on the system where the file system was created. The `mkfs` command does not create entries for `/etc/filesystems`.

Engine Log Messages Report All Web Console Users as “root”

With VCS 4.0, the engine log messages for the Web Console do not distinguish among users. Messages report all users as “root.”

Using Agents in NIS

Programs using networked services (for example, NIS, NFS, RPC, or a TCP socket connection to a remote host) can hang if the host is disconnected from the network. If such a program is used as an agent entry point, a network disconnect can cause the entry point to hang and possibly timeout. For example, if the host is configured to use NIS maps as a client, basic commands such as `ps -ef` can hang if there is network disconnect. VERITAS recommends creating users locally and that /etc/nsswitch.conf reflect local users.

Networking Agents Do Not Support IPv6 Protocol

The VCS 4.0 bundled agents IP, NIC, IPMultiNIC, MultiNICA, IPMultiNICB, and MultiNICB do not support the IPv6 enhanced IP protocol.

Volume Agent Clean May Forcibly Stop Volume Resources

When the attribute FaultOnMonitorTimeouts calls the Volume agent `clean` entry point after a monitor timeout, the `vxvol -f stop` command is also issued. This command forcibly stops all volumes, even if they are still mounted.

VCS Does Not Provide a Bundled Agent for Volume Sets

VCS 4.0 does not provide a bundled agent to detect Volume Manager volume sets, Problems with volumes and volume sets can only be detected at the DiskGroup and Mount resource levels.
Workaround: Set StartVolumes and StopVolumes attributes of the DiskGroup resource that contains volume set to 1. If a file system is created on the volume set, use a Mount resource to mount the volume set.

Compiling Custom Agents

Custom agents developed in C++ must be compiled using the IBM C for AIX Compiler Version 4.3.0.1. Use the `-brtl` flag for runtime linking with the framework library.

VCS Oracle Agent Uses pfile for Initialization

The VCS Enterprise Agent for Oracle obtains its initialization parameters from the pfile. If an Oracle instance is created from the spfile, VCS cannot monitor the instance. To obtain initialization parameters from the spfile, specify the path to the spfile in your pfile entry.

Fire Drill Does Not Support Volume Sets

The fire drill feature for testing fault readiness of a VCS configuration supports only regular Volume Manager volumes. Volume sets are not supported in this release.

VCS Simulator Does Not Support I/O Fencing

When running the Simulator, be sure the UseFence attribute is set to the default, "None."

Systems in a Cluster Must Have Same System Locale Setting

VCS 4.0 does not support clustering of systems with different system locales. All systems in a cluster must be set to the same locale.

NFS Locking

NFS lock failover is not yet supported.

EMC Disk Arrays Do Not Support GAB Disk Objects

EMC disk arrays do not support the creation of GAB disk objects, and therefore do not support the creation of disk heartbeat regions or service group heartbeat regions.

Group Dependency Limitations

No Failover for Some Instances of Parent Group

In service groups in which the group dependency is configured as parallel parent/failover child, online global, remote soft or firm, the parent group may not online on all nodes after a child group faults.

Online Local Firm Dependency Violation

If the parent group and the child group are online on node 1, and if the child group faults, VCS begins to take the parent group offline. However, this occurs at the same time the child group is failing over to node 2. If the parent group fails to go completely offline and the child group goes online on node 2, thus resulting in a dependency violation.

Online Remote Firm Dependency Violation

If the parent group is online on node 1 and the child group is online on node 2 and faults, the child group selects node 1 as its failover target. This scenario results in a dependency violation because the parent group fails to go offline on node 1.

Concurrency Violation with Online Firm Dependencies

The concurrency violation trigger cannot offline a service group if the group has a parent online on the system with local firm dependency. The concurrency violation continues until the parent is manually taken offline.
Workaround: In this situation, VCS sends notification that the violation trigger failed to offline a service group that is in concurrency violation. The administrator can manually offline the parent group and then the child group.

Known Issues in VCS 4.0

The following issues have been reported for VCS version 4.0.

Cluster Manager Installation on Windows XP

When installing Cluster Manager on a Windows XP system, you may encounter the error: "The installer has insufficient privileges to access this directory: C:\Config.Msi."

Workaround: Select Retry rather than Cancel in the error dialog. The installer continues to install Cluster Manager correctly.

Cluster Manager (Web Console)

Web Console Erroneously Displays VCS Version as 4.1

The VCS Web Console erroneously displays the product version as 4.1. The correct version of this VCS release is 4.0.

Security Alert May Appear Upon Connection to the Web Console

When connecting to the Web Console, you may receive a security alert. Click Yes on the Security Alert dialog box to accept the self-signed certificate issued by VERITAS. If you receive additional warnings about the certificate, you can safely ignore the warnings.

Web Console May Lose Connection When ClusterService Group Fails Over

When the ClusterService service group fails over to another node, the Web Console may lose its connection and display a "Page Not Found" error.
Workaround: If connection is lost, log in to the node again.

The myVCS Page May Not Display Correctly After Initial Configuration

The myVCS page may not display correctly the first time you navigate to it in the Web Console.
Workaround: If the myVCS page or any Cluster Manager page does not display correctly, refresh the page.

Netscape Browser May Not Display Attribute ScreenTips Completely

The Netscape browser may not display the entire ScreenTip for an attribute in the VCS Web Console.
Workaround: If the ScreenTip for an attribute is not completely visible, open the attribute dialog box to view the full description.

Internet Explorer Browser May Not Permit Successful Log In to Cluster

The Internet Explorer browser may not permit users to log in to the VCS Web Console if a system name contains underscores. Attempts to log in are redirected back to the login page.
Workaround: Try one of the following methods to log in to the cluster:

- In Internet Explorer, use the IP address, instead of the system name, in the URL.
- Use Netscape instead of Internet Explorer.
- Edit the /etc/hosts file on the AIX system to have an alternate host name without underscores. Edit the hosts file on the Windows system running Internet Explorer to contain the alternate host name. Use this alternate host name in the URL.

Global Service Groups

Switch Across Clusters May Cause Concurrency Violation

If you try to switch a global group across clusters while the group is in the process of switching across systems within the local cluster, then the group may go online on both the local and remote clusters. This issue affects only global groups. Local groups do not experience this behavior
Workaround: Ensure that the group is not switching locally before attempting to switch the group remotely.

Group Does Not Go Online on AutoStart Node

Upon cluster startup, if the last system on which the global group is probed is not part of the group's AutoStartList, then the group will not AutoStart in the cluster. This issue affects only global groups. Local groups do not experience this behavior.
Workaround: Ensure that the last system to join the cluster is a system in the group's AutoStartList.

Web Console May Not Bring Application Online After Switch to Remote Cluster

When a global cluster fault occurs, the Web Console receives an alert. If you choose to switch all global service groups from the primary cluster to the secondary cluster, the Web Console may not bring the application online on the secondary cluster.
Workaround: On the secondary cluster, issue the command

```
# haclus -declare outage -clus cluster_name -failover
```


Declare Cluster Dialog May Not Display Highest Priority Cluster as Failover Target

When a global cluster fault occurs, the Declare Cluster dialog enables you to fail groups over to the local cluster. However, the local cluster may not be the cluster assigned highest priority in the cluster list.
Workaround: To bring a global group online on a remote cluster, do one of the following:

- From the Java Console, right-click the global group in the Cluster Explorer tree or Service Group View, and use the Remote Online operation to bring the group online on a remote cluster.
- From the Web Console, use the Operations links available on the Service Groups page to bring the global group online on a remote cluster.

Erroneous Message in Engine Log File

When VCS tries to mount a `vxfs` file system for the first time, you may receive a misleading message resembling the following:

```
/dev/vx/dsk/sharedg/vol03 is not a vxfs file system
```

Before VCS can mount a `vxfs` file system for the first time, the `fsck` utility needs to run. The message shown above is displayed, `fsck` is run, and the file system is mounted.

MultiNICB Agent May Not Fail Over

If one of the physical interfaces monitored by MultiNICB goes down, the MultiNICB agent does not successfully fail over the default IP address to another physical interface under its control.
Workaround: When using the MultiNICB agent, configure the default IP address on all physical interfaces under MultiNICB control.

LVMVG Agent with Big Volume Groups

For big volume groups, the LVMVG agent does not properly synchronize the ODM.
Workaround: Set the attribute SyncODM = 0 and manually synchronize the ODM when adding a volume group.

The uninstallvcs Script May Not Remove all VCS Filesets

Running the `uninstallvcs` script may not remove all VCS 4.0 filesets.
Workaround: Manually uninstall remaining filesets using the `installp -u` command.

Engine May Hang in LEAVING State

When the command `hares -online` is issued for a parent resource when a child resource faults, and the `hares -online` command is followed by the command `hastop -local` on the same node, then the engine transitions to the LEAVING state and hangs.
Workaround: Issue the command `hastop -local -force`.

Monitoring PidFiles May Give False Concurrency Violation

When using PID Files to monitor application resources, the Application agent may report a false concurrency violation after a system crash. The PID files created by an application contain the PIDs for processes that are monitored by the Application agent. These files remain even after a node running the application crashes.

When restarting the node, the operating system may assign the PIDs listed in the PID files to other processes running on the node. If the Application agent monitors the resource using the PidFiles attribute only, the agent may discover the processes running and report a false concurrency violation. This scenario could result in some processes that are not under VCS control being killed.

Error Handling by VCS Enterprise Agent for Oracle

The VCS Enterprise Agent for Oracle provides enhanced handling of Oracle errors encountered during detailed monitoring. The agent uses the reference file `oraerror.dat`, which consists of a list of Oracle errors and the actions to be taken. For a description of the actions, refer to the *VERITAS Cluster Server Enterprise Agent 4.0 for Oracle Installation and Configuration Guide*.

Currently, the reference file specifies that the NOFAILOVER action is taken when the following Oracle errors are encountered:

```
ORA-00061, ORA-02726, ORA-6108, ORA-06114
```

The NOFAILOVER action means that the agent sets the resource's state to OFFLINE and freezes the service group.

You may stop the agent, edit the `oraerror.dat` file, and change the NOFAILOVER action to another action that is appropriate for your environment. The changes go into effect when the agent is restarted.

Documentation

Documentation for VERITAS Cluster Server is available as Adobe Portable Document Format (PDF) files on the product CD. Documentation is also available in HTML format on the software disc included with your software purchase.

The following section lists the documents installed with this product.

VCS Documentation

The installation guide for VCS is in the directory `cluster_server/docs`. Release Notes for VCS are in the directory `cluster_server/release_notes`.

- `vcs_ig.pdf`, *Installation Guide*
- `vcs_notes.pdf`, *Release Notes* in PDF format

  VERITAS recommends copying the installation guide and release notes from the CD to the `/opt/VRTSvcs/docs` or `/opt/VRTSvcs/docs` directory so that they are available on your system for reference.

Additional documentation for VCS is in the `/opt/VRTSvcs/docs` directory:

- `vcs_adg.pdf`, *Agent Developer's Guide*
- `vcs_barg.pdf`, *Bundled Agents Reference Guide*
- `vcs_ug.pdf`, *User's Guide*

VERITAS Documentation Online

To download VERITAS Cluster Server documentation from current and previous releases,

visit the website for VERITAS Cluster Server for UNIX:

http://support.veritas.com/menu_ddProduct_CLUSTERSERVER.htm

Hard-Copy Documentation Set

Copies of VERITAS software guides are available for purchase through the VERITAS Web Store at http://webstore.veritas.com.

The following guides for VCS 4.0 on AIX are available:

- *Installation Guide*
- *User's Guide*

- *Bundled Agents Reference Guide*
- *Agent Developer's Guide*

Manual Pages

The manual pages for the VRTSllt, VRTSgab, and VRTSvcs are installed in /opt/VRTS/man. Set the MANPATH environment variable so the man command can point to the VCS manual pages.

For Bourne or Korn shell (sh or ksh), type:

```
# MANPATH=$MANPATH:/opt/VRTS/man
# export MANPATH
```

For C shell (csh or tcsh), type:

```
# setenv MANPATH ${MANPATH}:/opt/VRTS/man
```

For more information, refer to the man manual page.

For more information, refer to the man(1) manual page.

Note The nroff versions of the VERITAS online manual pages are not readable using the man command unless the bos.txt.tfs fileset is installed. However, when you install VCS, ASCII versions of the manual pages are installed in the /opt/VRTS/man/cat* directories that are readable without the bos.txt.tfs fileset.

Getting Help

VERITAS offers you a variety of support options.

Accessing the VERITAS Support Web Site

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

Subscribing to VERITAS Email Notification Service

Subscribe to the VERITAS Email notification service to be informed of software alerts, newly published documentation, beta programs, and other services.

Go to http://support.veritas.com. Select a product and click "E-mail Notifications" on the right side of the page. Your customer profile ensures you receive the latest VERITAS technical information pertaining to your specific interests.

Accessing VERITAS Telephone and Fax Support

Telephone support for VERITAS Cluster Server is only available with a valid support contract. To contact VERITAS for technical support, dial the appropriate phone number listed on the Support Guide included in the product box and have your product license information ready for quick navigation to the proper support group.

The address for the VERITAS telephone support directory is http://support.veritas.com. Select a product and click "Contact Support" on the right side of the page.

Contacting VERITAS Licensing

For license information, call 1-650-527-0300 or fax 1-650-527-0952.

Using VRTSexplorer

The `VRTSexplorer` program can help VERITAS Technical Support engineers diagnose technical problems associated with VERITAS products. You can install this program from the VERITAS CD or download it from the VERITAS FTP site. For more information, consult the README file in the `VRTSexplorer` directory on the VERITAS CD.

▼ To install VRTSexplorer from the VERITAS CD

1. Log in as root.
2. Place the VERITAS CD into a CD-ROM drive connected to your system and enter:

   ```
   # mount -rV cdrfs /dev/cd0 /mnt
   ```

3. Move to the `/support` directory and install the `VRTSspt` package:

   ```
   # cd /mnt/support
   # installp -ad . VRTSspt.bff VRTSspt
   ```

   The program is installed in the `/opt/VRTSspt` directory.

▼ To download VRTSexplorer from the VERITAS FTP site

1. Use a web browser or the `ftp` program to download the `VRTSexplorer` program from the following URL:

   ftp://ftp.veritas.com/pub/support/vxexplore.tar.Z

   Save the file to the `/opt/VRTSspt` directory. Create the directory `/opt/VRTSspt` if it does not exist.

2. Log in as root on the affected system, and use the following commands to extract the contents of the downloaded file to the directory **`/opt/VRTSspt`**:

   ```
   # cd /opt/VRTSspt
   # zcat vxexplore.tar.Z | tar xvf -
   ```


▼ To run the VRTSexplorer program

1. Run the `VRTSexplorer` program from the VRTSexplorer directory by entering the following command:

   ```
   # /opt/VRTSspt/VRTSexplorer/VRTSexplorer
   ```

   `VRTSexplorer` prompts you for a destination directory for the information that it collects.

2. Press Return to accept the default directory `/tmp`, or enter a path name of your own choice.

   `VRTSexplorer` writes information to a compressed tar file named `VRTSexplorer_`*`casenumber_hostname`*`.tar.Z` in the specified directory.

3. Use the file upload facility of your web browser, or the `ftp` program, to transfer the `VRTSexplorer` output file to the VERITAS Technical Support anonymous FTP site:

   `ftp://ftp.veritas.com/incoming`

4. When you call VERITAS Technical Support, provide the name of the file you transferred to the FTP site.

   Alternatively, if you have already been assigned a call ID number by VERITAS Technical Support, email `support@veritas.com` and include your case ID number in the subject line.