

Veritas™ Cluster Server Bundled Agents Reference Guide

Windows 2000, Windows Server 2003

5.0

Veritas Cluster Server Bundled Agents Reference Guide

Copyright © 2007 Symantec Corporation. All rights reserved.

Veritas Cluster Server 5.0

Symantec, the Symantec logo, Veritas, and Veritas Storage Foundation are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THIS DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID, SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be “commercial computer software” and “commercial computer software documentation” as defined in FAR Sections 12.212 and DFARS Section 227.7202.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder. All third-party copyrights associated with this product are listed in the accompanying release notes.

Windows is a registered trademark of Microsoft Corporation.

Licensing and registration

Veritas Cluster Server is a licensed product. See the *Storage Foundation and High Availability Solutions for Windows, Installation and Upgrade Guide* for license installation instructions.

Technical support

For technical assistance, visit <http://entsupport.symantec.com> and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service.

Contents

Chapter 1	About VCS bundled agents	
	Resources and their attributes	12
	Modifying agents and their resources	12
	Attributes	12
	Attribute data types	13
	Attribute dimensions	13
	Categories of bundled agents	14
	Storage agents	14
	Network agents	14
	FileShare agents	14
	Printshare agents	15
	Services and applications agents	15
	VCS infrastructure and support agents	16
	Which agents should I use?	17
Chapter 2	Storage agents	
	Volume Manager Diskgroup (VMDg) agent	20
	Agent functions (Entry Points)	20
	State definitions	20
	Resource type definition	21
	Attribute definitions	21
	Sample configuration	24
	MountV agent	25
	Dependency	25
	Agent functions (Entry Points)	25
	State definitions	25
	Resource type definition	26
	Attribute definitions	27
	Sample configuration	29
Chapter 3	Network agents	
	NIC agent	32
	Agent functions (Entry Points)	32
	State definitions	32
	Resource type definition	33

Attribute definitions	33
Sample configuration	34
IP agent	35
Dependency	35
Agent functions (Entry Points)	35
State definitions	35
Resource type definitions	35
Attribute definitions	36
Sample configuration	36
IPMultiNicPlus agent	37
Agent functions (Entry Points)	37
State definitions	38
Resource type definition	38
Attribute definitions	39
Sample configuration	41
Lanman agent	42
Dependency	42
Agent functions (Entry Points)	43
State definitions	43
Resource type definition	44
Attribute definitions	45
Sample configurations	55

Chapter 4 FileShare agents

FileShare agent	58
Dependencies	58
Agent functions (Entry Points)	59
State definitions	59
Resource type definition	60
Attribute definitions	61
Sample configuration	65
CompositeFileShare agent	66
Dependencies	66
Agent functions (Entry Points)	67
State definitions	67
Resource type definition	67
Attribute definitions	68
Sample configuration	73

Chapter 5 PrintShare agents

PrintSpool agent	76
Dependencies	76
Agent functions (Entry Points)	76
State definitions	77
Resource type definition	77
Attribute definitions	77
Sample configuration	78
PrintShare agent	80
Dependency	80
Agent functions (Entry Points)	80
State definitions	80
Resource type definition	80
Attribute definitions	81
Sample configuration	81

Chapter 6 Services and applications agents

Microsoft Virtual Machine (MSVirtualMachine) agent	84
Dependencies	84
Agent functions (Entry Points)	84
State definitions	85
Resource type definition	85
Attribute definitions	86
Sample configuration	87
Internet Information Services agent	88
Agent functions (Entry Points)	88
State definitions	88
Resource type definition	88
Attribute definitions	89
Sample configurations	91
GenericService agent	96
Agent functions (Entry Points)	96
State definitions	96
Resource type definition	97
Attribute definitions	97
Sample configuration	99
ServiceMonitor agent	100
Agent functions (Entry Points)	100
State definitions	100
Resource type definition	101
Attribute definitions	102
Sample configurations	104

Process agent	105
Agent functions (Entry Points)	105
State definitions	105
Resource type definition	106
Attribute definitions	106
Sample configuration	110
MSMQ agent	111
Dependencies	111
Agent functions (Entry Points)	111
State definitions	111
Resource type definition	112
Attribute definitions	112
Sample configuration	113

Chapter 7

VCS infrastructure and support agents

NotifierMngr agent	116
Agent functions (Entry Points)	116
State definitions	116
Resource type definition	117
Attribute definitions	117
Sample configuration	120
Registry Replication (RegRep) agent	121
Dependency	121
Agent functions (Entry Points)	121
State definitions	122
Resource type definition	122
Attribute definitions	123
Sample configuration	127
VRTSWebApp agent	129
Dependency	129
Agent functions (Entry Points)	129
State definitions	129
Resource type definition	129
Attribute definitions	130
Sample configuration	131
Proxy agent	132
Agent functions (Entry Points)	132
State definitions	132
Resource type definition	132
Attribute definitions	133
Sample configurations	134
Phantom agent	135
Agent functions (Entry Points)	135

- State definitions 135
- Attribute definitions 135
- Sample configuration 135
- FileNone agent 136
 - Agent functions (Entry Points) 136
 - State definitions 136
 - Resource type definition 136
 - Attribute definitions 136
 - Sample configuration 136
- ElifNone agent 137
 - Agent functions (Entry Points) 137
 - State definitions 137
 - Resource type definition 137
 - Attribute definitions 137
 - Sample configuration 137
- FileOnOff agent 138
 - Agent functions (Entry Points) 138
 - State definitions 138
 - Resource type definition 138
 - Attribute definitions 138
 - Sample configuration 138
- FileOnOnly agent 139
 - Agent functions (Entry Points) 139
 - State definitions 139
 - Resource type definition 139
 - Attribute definitions 139
 - Sample configuration 139
- RemoteGroup agent 140
 - Dependency 140
 - Agent functions (Entry Points) 140
 - State definitions 141
 - Resource type definition 141
 - Attribute definitions 142
 - Sample scenario 146

Chapter 8 Troubleshooting bundled agents

- VCS logging 151
- Troubleshooting storage agents 153
 - Volume Manager (VMDg) agent error messages 153
 - MountV agent error messages 156
- Troubleshooting network agents 160
 - NIC agent error messages 160
 - IP agent error messages 162

IPMultiNicPlus agent error messages	164
Lanman agent error messages	168
Troubleshooting FileShare agents	172
FileShare agent error messages	172
CompositeFileShare agent error messages	174
Troubleshooting PrintShare agents	176
PrintSpool agent error messages	176
PrintShare agent error messages	178
Troubleshooting services and application agents	180
MSVirtualMachine agent error messages	180
IIS agent error messages	182
GenericService agent error messages	186
ServiceMonitor agent error messages	190
Process agent error messages	193
Troubleshooting infrastructure and support agents	197
Notifier Manager agent error messages	197
Registry Replication agent error messages	199
VRTSWebApp agent error messages	201
Proxy agent error messages	202
Phantom agent error message	202
FileNone agent error message	203
ElifNone agent error message	203
FileOnOff agent error messages	203
FileOnOnly agent error messages	204

About VCS bundled agents

Bundled agents are VCS processes that manage resources of predefined resource types. The agents manage resources according to commands received from the VCS engine, HAD. Bundled agents are a part of VCS, and are installed when VCS is installed. A system has one agent per resource type that monitors all resources of that type; for example, a single IP agent manages all IP resources.

When the agent is started, it obtains the necessary configuration information from VCS. It then periodically monitors the resources, and updates VCS with the resource status.

Agents typically:

- Bring resources online
- Take resources offline
- Monitor resources and report state changes to VCS

This document describes the VCS bundled agents along with their resource type definitions, attribute definitions, and sample configurations. The chapter on *Configuring Resources and Applications in VCS* in the *Veritas Cluster Server Administrator's Guide* describes how to configure these agents.

Resources and their attributes

Resources are the key parts of a system and are known by their type, such as a disk, a volume, or an IP address. Resource types are defined in the `types.cf` file by a collection of attributes. The VCS configuration file, `main.cf`, contains the values for the resource attributes and has an `include` directive to the `types.cf` file.

There are three categories of resources: On-Off, On-Only, and Persistent. The category of a resource governs the functions that the corresponding agent performs. For example, if the resources of an agent are of type On-Off, the agent could online and offline the resources. If the resources of an agent are of type On-Only, the agent could online the resources but cannot offline them. For persistent resources, the agent can neither online nor offline a resource.

An attribute's given value configures the resource to function in a specific way. By modifying the value of a resource attribute, you can change the way the VCS agent manages the resource. For example, the IP agent monitors an IP address resource. The specific address to be monitored is identified by the attribute `Address` whose value is the specific IP address.

Modifying agents and their resources

Use Cluster Manager (Java Console), Cluster Management Console (Single Cluster Mode) also known as Web Console, or the VCS command line to dynamically modify the configuration of the resources managed by an agent. See the *Veritas Cluster Server Administrator's Guide* for instructions on how to complete these tasks.

Attributes

Configure VCS components with attributes. Attributes contain data about the cluster, systems, service groups, resources, resource types, agent, and heartbeats—if you want to use global clusters. Each attribute has a definition and a value. Some attributes also have default values.

Attribute data types

Table 1-1 Attribute Data Types

Data Type	Description
string	<p>Enclose strings, which are a sequence of characters, in double quotes ("). You do not have to enclose strings in quotes when they begin with a letter, and contains only letters, numbers, dashes (-), and underscores (_). For example:</p> <ul style="list-style-type: none"> ■ A string defining a network interface such <code>ashme0</code> does not require quotes as it contains only letters and numbers. Enclosing the string in double quotes is also acceptable—<code>"ashme0"</code>. ■ A string defining an IP address requires quotes: <code>"100.101.102.1"</code> because the address contains periods. <p>A string can contain double quotes, but the quotes must be immediately preceded by a backslash. In a string, represent a backslash with two forward slashes (<code>\\</code>).</p>
integer	<p>Signed integer constants are a sequence of digits from 0 to 9. You can precede them with a dash. They are base 10. Integers cannot exceed the value of a 32-bit signed integer: 21471183247.</p>
boolean	<p>A boolean is an integer with the possible values of 0 (false) and 1 (true).</p>

Attribute dimensions

Table 1-2 Attribute Dimensions

Dimension	Description
scalar	<p>A scalar has only one value. This is the default dimension.</p>
vector	<p>A vector is an ordered list of values. Each value is indexed using a positive integer beginning with zero. A set of brackets ([]) denotes that the dimension is a vector. Find the specified brackets after the attribute name on the attribute definition in the <code>types.cf</code> file.</p>
keylist	<p>A keylist is an unordered list of unique strings in that list.</p>
association	<p>An association is an unordered list of name-value pairs. An equal sign separates each pair. A set of braces ({}) denotes that an attribute is an association. Braces are specified after the attribute name on the attribute definition in the <code>types.cf</code> file, for example: <code>str SnmpConsoles{}</code>.</p>

Categories of bundled agents

Bundled agents are categorized according to the type of resources they make available.

Storage agents

Storage agents make your shared disks, diskgroups, volumes, and mounts highly available.

- Volume Manager Diskgroup (VMDg) agent—Monitors shared disks configured using Storage Foundation for Windows (SFW)
- MountV agent—Monitors mount points configured on SFW-managed shared disks

Network agents

Network agents make your IP addresses and computer names highly available.

- NIC Agent—Monitors a NIC (Network Interface Card)
- IP Agent—Monitors an IP address
- IPMultiNicPlus Agent—Monitors multiple adapters and an IP address
- Lanman Agent—Monitors a virtual computer name

FileShare agents

Fileshare agents make shared directories and subdirectories highly available.

- FileShare Agent—Monitors a shared directory
- CompositeFileShare Agent—Monitors multiple shared directories

Printshare agents

The Printshare agents work together to make a shared network printer highly available.

- PrintSpool Agent—Monitors a print spooler
- PrintShare Agent—Monitors a shared network printer

Services and applications agents

Services and application agents make web sites, applications, generic services, and processes highly available.

- Microsoft Virtual Machine (MSVirtualMachine) Agent—Monitors virtual machines configured using Microsoft Virtual Server
- Internet Information Services (IIS) Agent—Monitors IIS sites and services
- GenericService Agent—Monitors generic services
- ServiceMonitor Agent—Monitors a service or starts a user-defined script
- Process Agent—Monitors a process
- MSMQ Agent—Creates a MSMQ service for a MSMQ resource, brings the MSMQ resource online, takes it offline, and monitors its status

VCS infrastructure and support agents

The VCS infrastructure and support agents provide high availability for VCS-related operations.

- NotifierMngr Agent—Monitors a notifier process
- Registry Replication (RegRep) Agent—Synchronizes the registries of cluster nodes by monitoring changes to the registry of the active node
- VRTSWebApp Agent—Monitors the Web applications running on a Web server
- Proxy Agent—Monitors the state of a resource on a local or remote system
- Phantom Agent—Determines the state of service groups having resources of type None only
- RemoteGroup Agent—Monitors and manages service groups in a remote cluster

You can use the following agents to test VCS functionality:

- ElifNone Agent—Monitors a file
- FileNone Agent—Monitors a file
- FileOnOff Agent—Creates a file, monitors it, and deletes it
- FileOnOnly Agent—Creates and monitors a file

Which agents should I use?

This information in the table enables you to decide which agent to use depending on the resource you want to make highly available.

Table 1-3 Resources and corresponding VCS agents

Resource to Make Highly Available	Agents to Use
Shared Storage Disks and volumes managed using SFW	VMDg, MountV
IP address Adapter and the associated IP address	NIC, IP Or IPMultiNICPlus
Computer name (virtual name)	Lanman
File shares	
Directory	Fileshare Or CompositeFileShare
Shared printer	Printspool, Printshare
Sites configured using Internet Information Services (IIS)	IIS
Processes (*.pl, *.sh, *.exe, and *.bat)	Process
Windows service residing in the Service Control Manager (SCM)	GenericService Or ServiceMonitor
Windows Registry	Registry Replication (RegRep)
Veritas Web Applications	VRTSWebApp
Virtual machines configured using Microsoft Virtual Server	MSVirtualMachine
Service group in another cluster	RemoteGroup

Storage agents

Storage agents make your shared storage highly available.

Use the Volume Manager Diskgroup (VMDg) and MountV agents to provide high availability for shared disks and volumes managed using Storage Foundation for Windows.

Volume Manager Diskgroup (VMDg) agent

The Volume Manager Diskgroup agent imports, monitors, and deports a cluster disk group configured using Storage Foundation for Windows. The agent makes the disk group highly available. The Volume Manager Diskgroup agent supports dynamic multi-pathing (DMP) and works in a SAN environment. The agent is represented by the VMDg resource type.

Note: Use this agent to manage disk groups configured using Storage Foundation for Windows. Do not use this agent if you use other software to manage shared storage.

Agent functions (Entry Points)

- **online**—Imports the configured disk group.
- **offline**—Deports the configured disk group.
- **monitor**—Verifies that the configured disk group is imported.

State definitions

- **ONLINE**—Indicates the configured disk group is imported.
- **OFFLINE**—Indicates the configured disk group is not imported.
- **UNKNOWN**—Indicates the agent could not detect the disk group.

Resource type definition

```

type VMDg (
    static i18nstr ArgList[] = {DiskGroupName, ForceImport,
    ForceDeport, ListMountedVolumes, ListApplications, VxVMFailAction,
    VxVMRestartAttempts, DetailMonitorFreq, DGGuid }
    str DiskGroupName
    boolean ForceImport = 0
    boolean ForceDeport = 0
    boolean ListMountedVolumes = 0
    boolean ListApplications = 0
    str VxObFailAction = RESTART_VXOB
    int VxObRestartAttempts = 10
    str VxVMFailAction = RESTART_VXVM
    int VxVMRestartAttempts = 10
    int DetailMonitorFreq = 10
    str DGGuid
)

```

Attribute definitions

Table 2-1 VMDg agent required attributes

Required Attribute	Type and Dimension	Description
DiskGroupName	string-scalar	The name of the cluster diskgroup configured using Storage Foundation. The diskgroup name may be retrieved from the SFW console by running the command <code>vxvg list</code> , or by using the <code>VMGetDrive</code> utility. See the description of the <code>VMGetDrive</code> utility in the <i>Veritas Cluster Server Administrator's Guide</i> for instructions.

Table 2-2 VMDg agent optional attributes

Optional Attributes	Type and Dimension	Description
DetailMonitorFreq	integer-scalar	The number of monitor cycles after which the agent monitors the resource in detail. Setting this value to 0 disables detail monitoring. Default is 10.

Table 2-2 VMDg agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
DGGuid	string-scalar	<p>The GUID of the cluster diskgroup configured using Storage Foundation. The diskgroup name may be retrieved by using the VMGetDrive utility. See the description of the VMGetDrive utility in the <i>Veritas Cluster Server Administrator's Guide</i> for instructions.</p>
ForceImport	boolean-scalar	<p>A flag that defines whether the agent forcibly imports the diskgroup when exactly half the disks are available. The value 1 indicates the agent imports the configured diskgroup when half the disks are available. The value 0 indicates it does not. Default is 0. This means that the diskgroup will be imported only when SFW acquires control over majority of the disks.</p> <p>Note: Set this attribute to 1 only after verifying the integrity of your data. If due caution is not exercised before setting this attribute to 1, you risk a split-brain condition, leading to potential data loss.</p>
ForceDeport	boolean-scalar	<p>A flag that defines whether the agent forcibly deports the diskgroup even if the disks within the diskgroup are being used. The value 1 indicates the agent forcibly deports diskgroups. The value 0 indicates it does not. Default is 0.</p> <p>Note: Set this attribute to 1 only after verifying the integrity of your data. If due caution is not exercised before setting this attribute to 1, you risk a potential data loss.</p>
ListApplications	boolean-scalar	<p>A flag that defines whether the agent lists the applications accessing the diskgroup while deporting. The value 1 indicates the agent lists the applications. The value 0 indicates it does not. Default is 0.</p> <p>Note: The list of applications can be seen in the agent's log.</p>

Table 2-2 VMDg agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
ListMountedVolumes	boolean-scalar	A flag that defines whether the agent lists all mounted volumes in the diskgroup. The value 1 indicates the agent lists the mounted volumes. The value 0 indicates it does not. Default is 0. Note: The list of mounted volumes can be seen in the agent's log.
VxObFailAction	string-scalar	This attribute has been deprecated. Use VxVMFailAction instead.
VxObRestartAttempts	integer-scalar	This attribute has been deprecated. Use VxVMRestartAttempts instead.
VxVMFailAction	string-scalar	Defines the agent behavior when the Veritas Storage Agent service (VxVM) fails. The value RESTART_VXVM indicates the agent attempts to restart the VxVM service every monitor cycle. The value SHUTDOWN indicates the agent attempts to restart the VxVM service the number of times defined in the attribute VxVMRestartAttempts. If it fails in restarting VxVM, the agent shuts down the system. When this occurs, all service groups online on the system fail over to another system in the cluster. For example, if VxVMRestartAttempts is set to 5, the agent attempts to start the service five times before shutting down the system. Default is RESTART_VXVM.
VxVMRestartAttempts	integer-scalar	The number of times the agent attempts to restart the failed VxVM service before shutting down the system. This attribute is considered only when VxVMFailAction is set to SHUTDOWN. Default is 10.

Sample configuration

```
VMDg DG_VCSDG (  
  DiskGroupName = VCSDG  
  ListMountedVolumes = 1  
  DGGuid = fb69e244-930f-479e-b9f5-c54449fe2fc0  
)
```

MountV agent

The MountV agent mounts, monitors, and unmounts volumes on cluster diskgroups imported using the Veritas Storage Foundation for Windows. The agent supports volumes formatted using the NTFS, FAT, and FAT32 file systems.

When a cluster disk group fails over to another system, the MountV agent ensures the new system accesses the volume in the same way it was accessed before failover. The MountV agent ensures a consistent device path by mounting the diskgroup with the same mount point (drive letter) on the new system. The agent also mounts a disk group as an NTFS folder. The agent ensures proper dismounting from a failed system when a resource or group is taken offline. When a disk partition is mounted, VCS creates an administrative share to enable remote administration of the disk.

The agent performs a file system check when it brings the resource online. If a drive letter is already assigned to the volume, the agent skips the file system check, and declares the resource online. Note that the volume to be monitored using the MountV agent must not be mounted multiple times.

Note: Use this agent to manage diskgroups configured using Veritas Storage Foundation for Windows. Do not use this agent if you use other software to manage shared storage.

Dependency

The MountV agent depends on the VMDg agent.

Agent functions (Entry Points)

- **online**—Mounts the volume as a drive letter or as an NTFS folder.
- **offline**—Unmounts the configured volume.
- **monitor**—Verifies the volume is mounted as per the configuration.

State definitions

- **ONLINE**—Indicates the configured volume is mounted and accessible.
- **OFFLINE**—Indicates the mounted drive is inaccessible.
- **UNKNOWN**—Indicates the agent could not determine the state of the configured volume.

Resource type definition

```
type MountV (  
    static keylist SupportedActions = {CheckFSAccess}  
    static i18nstr ArgList[] = {MountPath, VolumeName,  
  
    "VMDGResName:DiskGroupName",  
  
    ForceUnmount, ListApplications,  
  
    AutoFSClean, "VMDGResName:DGGuid",  
  
    "MountResName:MountPath", PurgeStaleMountPoints}  
    i18nstr MountPath  
    str VolumeName  
    str VMDGResName  
    str ForceUnmount = READ-ONLY  
    boolean ListApplications = 0  
    boolean AutoFSClean = 0  
    boolean PurgeStaleMountPoints = 0  
    str MountResName  
)
```

Attribute definitions

Table 2-3 MountV agent required attributes

Required Attributes	Type and Dimension	Description
MountPath	string-scalar	<p>The drive letter or path to an empty NTFS folder that will be assigned to the volume being mounted.</p> <p>When configuring a directory to host the mount, verify the following conditions:</p> <ul style="list-style-type: none">■ The configured path exists.■ The directory is empty.■ The volume on which the directory resides is NTFS-formatted.■ The directory is not a system directory. <p>The attribute can be specified as <code>X</code>, <code>X:</code>, <code>X:\</code>, <code>X:\Directory</code>, or <code>X:\Directory\</code>.</p> <p>These options are valid only if editing the attribute from Cluster Manager (Java Console). If editing the configuration file <code>main.cf</code> directly, you must specify two slashes (<code>\\</code>) instead of one; for example, <code>X:\\Directory\\</code>.</p> <p>Note: This attribute can take localized values.</p>
VolumeName	string-scalar	<p>The name of the volume to be mounted. For example, the name could be <code>Raid1</code>, <code>Stripe2</code>, <code>Volume01</code>, etc. Use the <code>VMGetDrive</code> utility to retrieve the volume name. See the description of the <code>VMGetDrive</code> utility in the <i>Veritas Cluster Server Administrator's Guide</i> for instructions.</p>
VMDGResName	string-scalar	<p>The name of the Volume Manager Diskgroup (VMDg) resource on which the MountV resource depends.</p>

Table 2-4 MountV agent optional attributes

Optional Attributes	Type and Dimension	Description
AutoFSClean	boolean-scalar	If the agent detects corruption, this attribute defines whether the agent automatically cleans the file system by running <code>Chkdsk /X</code> on the volume being brought online. The value 1 indicates the agent cleans the file system. The value 0 indicates it does not. Note that cleaning a file system may result in loss of data. Default is 0.
ForceUnmount	string-scalar	Defines whether the agent unmounts the volume forcibly when it is being used by other applications. The attribute takes the following values: <ul style="list-style-type: none"> ■ NONE: The agent does not unmount volume if an application is accessing it. ■ READ-ONLY: The agent unmounts the volume if applications are accessing it in a read-only mode. ■ ALL: The agent unmounts the volume irrespective of the type of access an application has. Default is READ-ONLY.
ListApplications	boolean-scalar	Defines whether the agent lists the applications accessing the volume while unmounting. Default is 0.
MountResName	string-scalar	This attribute is not required by the agent.
PurgeStaleMountPoints	boolean-scalar	This attribute is applicable to a global cluster configuration. In case of a global fail over, this attribute defines whether the agent purges volume mount point (NTFS folder mounts) properties before bringing the folder mount points online on the remote cluster. The default value is 0, which means that the agent does not purge the volume mount point properties.

Sample configuration

In the following configuration, the resource MountV_X is configured to mount the diskgroup VCSDG as a drive (X:). The resource MountV_X_Usrs_Data is configured to mount the diskgroup as a folder.

```
MountV MountV_X (  
  MountPath = X  
  VolumeName = Volume1  
  VMDGResName = DG_VCSDG  
)  
  
MountV MountV_X_Usrs_Data (  
  MountResName = MountV_X  
  MountPath = "X:\\users\\data"  
  VolumeName = Raid1  
  VMDGResName = DG_VCSDG  
)  
VMDg DG_VCSDG  
  DiskGroupName = VCSDG  
  ForceDeport = 1  
  ListMountedVolumes = 1  
  ListApplications = 1  
)  
MountV_X_Usrs_Data requires MountV_X  
MountV_X requires DG_VCSDG
```


Network agents

Network agents make IP addresses and computer names highly available.

- The NIC and IP agents work together to make a virtual IP address highly available.
- The IPMultiNICPlus agent makes a virtual IP address, configured on servers having multiple adapters, highly available.
- The Lanman agent makes a virtual computer name highly available. The Lanman agent requires the IP agent for operation.

NIC agent

The NIC (Network Interface Card) agent monitors the configured NIC. Some NICs maintain their connection status in a system-defined variable. The NIC agent uses this variable to determine the status of the NIC resource. If the NIC does not maintain its connection status, the agent uses a ‘ping’ or a User Datagram Protocol (UDP) echo broadcast to determine the status of the resource.

The agent does not support fault-tolerant NICs. For information on VCS-created fault-tolerant NICs, see “[IPMultiNicPlus agent](#)” on page 37.

Agent functions (Entry Points)

- **online**—Not applicable.
- **offline**—Not applicable.
- **monitor**—If the NIC maintains its connection status, the agent reads the system-defined variable to determine the status of the resource. If the NIC does not maintain its connection status, the agent verifies that the NIC has been assigned an IP address, and sends a ping to all the hosts listed in the attribute PingHostList. The agent counts the number of packets received by the NIC before and after the ping. If the count increases, the resource is marked **ONLINE**. If the count remains unchanged, the agent broadcasts a UDP echo request to the address derived from the administrative IP address and the associated subnet mask. The agent counts the number of packets received by the NIC before and after the broadcast. If the count increases, the resource is marked **ONLINE**. If the count remains the same or decreases, the resource is marked **FAULTED**. The NIC agent also calculates the percentage of erroneous packets transmitted during each monitor interval. If this percentage exceeds the value in the MaxTxErrorPercentage attribute for the number of consecutive monitor intervals specified by the value in the MaxTxErrInterval attribute, the NIC resource is marked **FAULTED**.

State definitions

- **ONLINE**—Indicates the NIC resource is online.
- **FAULTED**—Indicates a problem with the NIC or that a network link failed.
- **UNKNOWN**—Indicates the agent encountered errors while monitoring the NIC resource.

Resource type definition

```

type NIC (
    static i18nstr ArgList[] = {MACAddress, PingTimeoutMseconds,
    MaxTxErrorPercentage, MaxTxErrInterval,
    UseConnectionStatus, PingHostList }
    str MACAddress
    int PingTimeoutMseconds = 1000
    int MaxTxErrorPercentage = 50
    int MaxTxErrInterval = 10
    boolean UseConnectionStatus = True
    str PingHostList[]
)

```

Attribute definitions

Table 3-1 NIC agent required attributes

Required Attribute	Type and Dimension	Description
MACAddress	string-scalar	The physical address of the NIC to be monitored. Note that this attribute is always local, that is, it is different for each system. Note: You can use the <code>ipconfig -all</code> command to retrieve the physical address of a NIC.

Table 3-2 NIC agent optional attributes

Optional Attributes	Type and Dimension	Description
MaxTxErrInterval	integer-scalar	The number of consecutive monitor intervals for which the percentage of erroneous packets should not exceed the value specified in MaxTxErrorPercentage. When this occurs, the NIC is declared <code>FAULTED</code> . Default is 10.
MaxTxErrorPercentage	integer-scalar	The threshold error percentage for the total packets sent between two consecutive monitor intervals. Default is 50.

Table 3-2 NIC agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
PingHostList	string-vector	A list of hosts that are always reachable from the NIC. If the UseConnectionStatus attribute is set to 0, make sure the attribute PingHostList is not empty.
PingTimeoutMseconds	integer-scalar	The timeout interval, in milliseconds, for a ping. Default is 1000 milliseconds.
UseConnectionStatus	boolean-scalar	A flag that defines whether the NIC maintains its connection status. The value True indicates the NIC maintains its status. The value False indicates it does not. If this attribute is set to False, you must specify a value for the attribute PingHostList. Default is True. VCS provides a utility, "NICTest," which determines whether a NIC maintains its connection status. You can use the NICTest utility to determine whether or not this attribute is required. See the description of the NICTest utility in the <i>Veritas Cluster Server Administrator's Guide</i> for instructions.

Sample configuration

In the following example, the NIC agent is configured to monitor the adapter with MAC address 00-B0-D0-31-7D-FA. The UseConnectionStatus attribute is set to False. The agent sends a ping to the hosts listed in the PingHostList attribute to determine the status of the NIC resource. If the percentage of erroneous packets transmitted exceeds 30 percent for three consecutive monitoring intervals, the NIC resource is marked **FAULTED**.

```
NIC NIC_RL20001 (
  MACAddress = "00-B0-D0-31-7D-FA"
  PingTimeOutMseconds = 500
  MaxTxErrorPercentage = 30
  MaxTxErrInterval = 3
  UseConnectionStatus = False
  PingHostList = { "172.16.1.19", "172.16.1.21" }
)
```

IP agent

The IP agent assigns a virtual IP address to the NIC, monitors the IP address, and removes it. The agent also monitors the associated subnet mask on a network interface card (NIC).

Dependency

The IP agent depends on the NIC agent.

Agent functions (Entry Points)

- **online**—Assigns a unique virtual IP address to an empty slot on the NIC after verifying that the IP address is not being used by another system.
- **offline**—Removes the virtual IP address assigned to the NIC.
- **monitor**—Verifies that the specified virtual IP address is assigned to the NIC.

State definitions

- **ONLINE**—Indicates the specified virtual IP address is assigned to the NIC.
- **OFFLINE**—Indicates the specified virtual IP address is not assigned to the NIC.
- **UNKNOWN**—Indicates the agent encountered errors while monitoring the IP resource.

Resource type definitions

```
type IP (  
    static i18nstr ArgList[] = {Address, SubNetMask, MACAddress}  
    str Address  
    str SubNetMask  
    str MACAddress  
)
```

Attribute definitions

Table 3-3 IP agent required attributes

Required Attributes	Type and Dimension	Description
Address	string-scalar	A unique virtual IP address to be assigned to the NIC.
SubNetMask	string-scalar	The subnet mask associated with the IP address.
MACAddress	string-scalar	The physical address of the NIC to which the virtual IP address is assigned. Note that this attribute is always local, that is, it is different for each system. Note: Use the <code>ipconfig -all</code> command to retrieve the physical address of a NIC.

Sample configuration

```
IP IP_192_168_100_20 (  
    Address = "192.168.100.20"  
    SubNetMask = "255.255.255.0"  
    MACAddress @SYSTEM1 = "00-60-08-08-BA-C4"  
    MACAddress @SYSTEM2 = "00-90-27-28-5A-7E"  
)
```

IPMultiNicPlus agent

The IPMultiNicPlus agent monitors multiple NICs on clustered systems. Specifically, it assigns an IP address to the active NIC on a system, monitors the IP address, and unassigns it. If the agent detects an active NIC is not working, it fails over the IP address to the next NIC configured in the system's adapter list. If all NICs on a system fail, the agent fails over the IP address to another system in the cluster. The IPMultiNicPlus agent provides VCS created fault-tolerant NICs.

Some NICs maintain their connection status in a system-defined variable. If all NICs in a system's adapter list maintain their status, the agent uses this variable to determine the status of individual NICs. If any NIC on a system does not maintain its connection status, the agent uses a ping or a User Datagram Protocol (UDP) broadcast to determine the status of the resource.

Agent functions (Entry Points)

- **online**—Assigns a unique virtual IP address to an empty slot on the active NIC after verifying that the IP address is not in use by another system, and that an empty slot is available.
- **offline**—Removes the assigned virtual IP address on the active NIC.
- **monitor**—Verifies the configured virtual IP address is assigned to the active NIC.

If the active NIC of the IPMultiNicPlus resource maintains its connection status, the agent reads the status variable of the active NIC to determine the status of the resource. If the resource does not maintain its connection status, the agent verifies that the active NIC has an IP address assigned, and sends a ping to all the hosts listed in the attribute PingHostList.

The agent counts the number of packets received by the NIC before and after the ping. If the count increases, the NIC is marked **WORKING**. If the count remains unchanged, the agent broadcasts a UDP echo request to the address derived from the administrative IP address and the associated subnet mask.

The agent also counts the number of packets received by the NIC before and after the broadcast. If the count increases, the NIC is marked **WORKING**. If the count remains the same or decreases, the NIC is marked **NOT WORKING**. Additionally, the agent calculates the percentage of erroneous packets transmitted during each monitor interval. If this percentage exceeds the **MaxTxErrorPercentage** for the number of consecutive monitor intervals specified by **MaxTxErrInterval**, the NIC is marked **NOT WORKING**.

If the agent detects the active NIC is not working, it selects the next-working NIC from the system's adapter list and makes it active by

assigning it the configured IP address. When the agent detects the last NIC listed in the adapter list is not working, the resource is declared `OFFLINE`. When this occurs, the service group switches to the next available system listed in the service group's `SystemList` attribute.

State definitions

- `ONLINE`—Indicates the specified virtual IP address is assigned to the active NIC.
- `OFFLINE`—Indicates the specified virtual IP address is not assigned to the active NIC, or that none of the NICs in the system's adapter list is functioning properly.
- `UNKNOWN`—Indicates the agent encountered errors while monitoring the IP resource.

Resource type definition

```
type IPMultiNicPlus (  
    static i18nstr ArgList[] = {AdapterList, PingTimeoutMseconds,  
  
    MaxTxErrorPercentage, MaxTxErrInterval,  
  
    UseConnectionStatus, AdminIPAddr,  
  
    AdminSubnetMask, Address, SubNetMask,  
  
    PingHostList }  
    str AdapterList[]  
    int PingTimeoutMseconds = 1000  
    int MaxTxErrorPercentage = 50  
    int MaxTxErrInterval = 10  
    boolean UseConnectionStatus = True  
    str AdminIPAddr  
    str AdminSubnetMask  
    str Address  
    str SubNetMask  
    str PingHostList[]  
)
```

Attribute definitions

Table 3-4 IPMultiNicPlus agent required attributes

Required Attributes	Type and Dimension	Description
AdapterList	string-vector	A list of MAC addresses (physical addresses) of NICs that form the IPMultiNicPlus resource. You can retrieve the physical addresses of NICs by using the command <code>ipconfig -all</code> .
Address	string-scalar	A unique virtual IP address to be assigned to the active NIC.
AdminIPAddr	string-scalar	Unique administrative IP address assigned to the active NIC in the AdapterList attribute. Every clustered system that has an IPMultiNicPlus resource must have a unique administrative IP address. This attribute is always local. Note: If this attribute is configured incorrectly, the system will not be accessible in the network until you bring the IPMultiNicPlus resource online on the system.
AdminSubnetMask	string-scalar	The subnet mask associated with the administrative IP address. This attribute is always local.
SubNetMask	string-scalar	The subnet mask associated with the virtual IP address to be assigned.

Table 3-5 IPMultiNicPlus agent optional attributes

Optional Attributes	Type and Dimension	Description
MaxTxErrInterval	integer-scalar	The number of consecutive monitor intervals for which the percentage of erroneous packets should not exceed MaxTxErrorPercentage. When this occurs, the NIC is declared NOT WORKING. Default is 10.
MaxTxErrorPercentage	integer-scalar	The threshold error percentage for the total packets sent between consecutive monitor intervals. Default is 50.

Table 3-5 IPMultiNicPlus agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
PingHostList	string-vector	A list of hosts that are always reachable from individual NICs. This attribute must be defined for the IPMultiNicPlus resource if the UseConnectionStatus attribute for that resource is set to 0.
PingTimeoutMseconds	integer-scalar	The timeout interval, in milliseconds, for a ping. Default is 1000 milliseconds.
UseConnectionStatus	boolean-scalar	A flag that defines whether all NICs on a system maintain their connection status. The value True indicates all NICs in the system's AdapterList maintain their status. The value False indicates at least one NIC in the system's AdapterList does not. If this attribute is set to False, you must define the PingHostList for every NIC in the IPMultiNicPlus resource. Default is True. Use the command <code>ipconfig -all</code> to retrieve information about the NIC.

Sample configuration

In the following example, the IPMultiNicPlus agent is configured to monitor NICs on two systems: SYSTEM1 and SYSTEM2. These systems form the service group IPMultiNicPlus_grp1.

- System SYSTEM1 has two NICs with MAC addresses 00-B0-D0-31-7D-FA and 00-B0-f0-62-9E-GB.
- System SYSTEM2 has two NICs with MAC addresses 00-B1-D1-32-7E-FB and 00-C0-E1-33-7D-DB.
- All NICs on SYSTEM1 maintain their connection status, so the UseConnectionStatus attribute for the system is set to True. At least one NIC on SYSTEM2 does not maintain its connection status. The UseConnectionStatus attribute for SYSTEM2 is set to False.
- Host 172.16.1.1 is always reachable from SYSTEM2 and is listed in the PingHostList.
- The attributes PingTimeOutMseconds, MaxTxErrorPercentage, and MaxTxErrInterval are configured with default values.

```
IPMultiNicPlus IPMultiNicPlus_grp1 (  
    AdapterList@SYSTEM1 = { "00-B0-D0-31-7D-FA",  
"00-B0-f0-62-9E-GB"}  
    AdapterList@SYSTEM2 = { "00-B1-D1-32-7E-FB",  
"00-C0-E1-33-7D-DB"}  
    AdminIPAddr@SYSTEM1 = "172.29.9.180"  
    AdminIPAddr@SYSTEM2 = "172.29.9.181"  
    PingHostList = { "172.16.1.1" }  
    AdminSubnetMask@SYSTEM1 = "255.255.254.0"  
    AdminSubnetMask@SYSTEM2 = "255.255.254.0"  
    UseConnectionStatus@SYSTEM1 = True  
    UseConnectionStatus@SYSTEM2 = False  
    Address = "172.29.9.71"  
    SubnetMask = "255.255.255.0"  
)
```

Lanman agent

The Lanman agent enables clients to access data and applications on a cluster node by associating the virtual IP address with the virtual computer name in the WINS database. The agent provides the option of associating multiple IP addresses from different subnets with the virtual computer name. The agent also provides the option of creating the virtual computer object in any organizational unit in the Active Directory and enhances the DNS updating capabilities of VCS.

The Lanman agent registers the following services with the WINS server:

- Server (20h)
- Workstation (00h)
- Messenger (03h)

The agent supports Kerberos authentication by providing the option of adding the virtual computer name to the Active Directory and adding the virtual IP address to the DNS. The agent uses the VCS Helper Service user context for AD and DNS updates.

The Lanman agent updates and monitors the canonical name (CNAME) mapping in the domain name server when failing over applications across subnets (performing a wide-area failover.) The Lanman agent also supports creating DNS records in different DNS zones.

DNS scavenging affects virtual servers configured in VCS because the Lanman agent uses DDNS to map virtual names with IP addresses. If you use scavenging, then you must set the `DNSRefreshInterval` attribute. This will enable the Lanman agent to refresh the resource records on the DNS servers. See the `DNSRefreshInterval` attribute description for more information.

Dependency

The Lanman agent depends on the IP agent.

Changing dependency

If you change your Lanman resource dependency to a new IP resource and bring the Lanman resource online, a ping to the virtual name might respond from the IP address of the previous IP resource until the next WINS broadcast. The WINS broadcast updates the WINS database with the changed association.

For example, if you took the Lanman resource offline, changed the Lanman resource dependency from `IP_A` to `IP_B`, and brought the Lanman resource online, a ping to the virtual name might still respond from `IP_A`. Note that the `IP_A` resource is kept online during this process. The ping will respond from `IP_B` after the next WINS broadcast updates the WINS database.

Agent functions (Entry Points)

- **online**—Binds the IP addresses with the specified virtual computer name. The agent also queries the name server of the domain for Host (A), PTR, and CNAME records and adds or updates the records on the name server.
- **offline**—Removes the IP address binding from the virtual computer name.
- **monitor**—Verifies the IP addresses are bound to the virtual computer name. If `DNSUpdateRequired` and `DNSRefreshInterval` is enabled and the resource is `ONLINE`, then the Lanman agent refreshes the DNS records every 24 hours. The agent queries the name servers for DNS records. It reports back `ONLINE` if the response from all the name servers contains the Host (A), PTR, and CNAME records. If no servers return the appropriate records, the monitor reports the resource as `OFFLINE`.

State definitions

- **ONLINE**—Indicates the IP addresses are bound to the virtual computer name and the DNS records are as expected.
- **OFFLINE**—Indicates the IP addresses are not bound to the virtual computer name. Failed to create the DNS records, or the expected DNS records were not found.
- **UNKNOWN**—Indicates the agent could not determine the status of the resource.

Resource type definition

```
type Lanman (  
    static keylist LogDbg = {DBG_21}  
    static i18nstr ArgList[] = {VirtualName, MultiNet,  
  
    "IPResName:Address",  
  
    "IPResName:SubNetMask", MultiNetInfo,  
  
    DNSUpdateRequired, ADUpdateRequired,  
  
    DNSCriticalForOnline, ADCriticalForOnline, ADContainer,  
  
    DNSOptions, AdditionalDNSServers, DNSRefreshInterval  
  
    DNSZones, AliasName, TSIGKeyFile, TTL}  
    str VirtualName  
    str IPResName  
    boolean MultiNet = 0  
    str MultiNetInfo[]  
    boolean DNSUpdateRequired = 0  
    boolean ADUpdateRequired = 0  
    boolean DNSCriticalForOnline = 0  
    boolean ADCriticalForOnline = 0  
    str ADContainer  
    str DNSOptions[]  
    str AdditionalDNSServers{}  
    int DNSRefreshInterval = 0  
    str DNSZones{}  
    str AliasName = ""  
    str TSIGKeyFile = ""  
    int TTL = 0  
)
```

Attribute definitions

Table 3-6 Lanman agent required attributes

Required Attributes	Type and Dimension	Description
IPResName	string-scalar	The name of the IP resource on which the Lanman resource depends. Do not define a value for this attribute if the MultiNet attribute is set to 1.
VirtualName	string-scalar	The virtual computer name to be assigned to the server. The virtual name must be fewer than 16 characters. Note that if you specify a virtual computer name in lowercase letters, the agent converts it to uppercase. For example, the name VCSServer is converted to VCSSERVER.

Table 3-7 Lanman agent optional attributes

Optional Attributes	Type and Dimension	Description
ADContainer	string-scalar	<p>Specifies the distinguished name of the Active Directory container or the organizational unit (OU) for the newly created computer object. If no value is specified for this attribute, the Lanman resource creates the computer object in the default container "Computers." Note that the user account for VCS Helper service must have adequate privileges on the specified container to create and update computer accounts. Refer to Microsoft documentation for information on assigning user privileges for a container.</p> <p>By default, the attribute contains no value.</p> <p>Note: Value specified for this attribute will be effective only if ADUpdateRequired is set to 1.</p>

Table 3-7 Lanman agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
ADCriticalForOnline	boolean-scalar	A flag that defines whether the Lanman resource faults if the agent fails to update the Active Directory. The value 1 indicates that the resource faults in case of a failure to update the Active Directory. The value 0 indicates that it does not. Default is 0.

Table 3-7 Lanman agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
AdditionalDNSServers	string-association	<p>An array that specifies the IP addresses of the additional DNS servers that will be updated by the Lanman resource. For all the Windows DNS servers, the forward and reverse lookup zones must be configured. For all the BIND servers, only the forward lookup zones are required. Note that on BIND servers only CNAME records are created.</p> <p>All additional DNS servers are considered as Windows DNS servers by default. If any additional DNS server is a Berkeley Internet Name Domain (BIND) server, you will have to specify it in the attribute value.</p> <p>Example:</p> <pre>{“10.10.10.9” = ““, “10.10.10.10” = “BIND”}</pre> <p>Where 10.10.10.9 is the IP address of a Windows DNS server, and 10.10.10.10 is the IP address of a BIND DNS server.</p> <p>By default, the attribute contains no value. Values specified for this attribute will be effective only if DNSUpdateRequired is set to 1.</p> <p>Note: In cases where the default DNS is a BIND DNS server, set the value of the DNSOptions attribute to IgnoreDefault, and specify the BIND DNS server details in this attribute.</p> <p>Note: If the BIND DNS servers are configured for secure updates, then you must configure the TSIG keys either in the DNSZones attribute or the TSIGKeyFile attribute. See “TSIGKeyFile” on page 52 for more information on TSIG keys.</p>

Table 3-7 Lanman agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
ADUpdateRequired	boolean-scalar	A flag that defines whether the Lanman resource updates the Active Directory with the virtual name. The value 1 indicates that the agent updates the Active Directory. The value 0 indicates it does not. Default is 0.
DNSCriticalForOnline	boolean-scalar	A flag that defines whether the Lanman resource faults if the agent fails to update the DNS. The value 1 indicates that the resource faults in case of a failure to update the DNS. The value 0 indicates that it does not. Default is 0.

Table 3-7 Lanman agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
DNSOptions	string-vector	<p>An array that specifies the way in which the Lanman resource updates the DNS servers. This attribute can take one or all of the following values:</p> <ul style="list-style-type: none">■ UpdateAll: Updates all the default DNS servers specified in the TCP/IP properties for the cluster node, and the additional DNS servers specified in the AdditionalDNSServers attribute.■ IgnoreDefault: Ignores the default DNS servers and updates only the additional DNS servers.■ PurgeDuplicate: Removes duplicate DNS entries from the DNS servers. Symantec recommends you set this value for service groups configured for wide area failover. <p>Any combination of these values can be specified for the attribute. See “Updating DNS servers” on page 54 for more information.</p> <p>This attribute takes effect only when the Lanman resource comes online.</p> <p>By default, the attribute contains no value. Values specified for this attribute will be effective only if DNSUpdateRequired is set to 1 and additional DNS servers are specified in the AdditionalDNSServers attribute.</p> <p>Note: In cases where the default DNS is a BIND DNS server, set this attribute value to IgnoreDefault, and specify the BIND DNS server details in the AdditionalDNSServers attribute.</p>

Table 3-7 Lanman agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
DNSUpdateRequired	boolean-scalar	<p>A flag that defines whether the Lanman resource updates the DNS with the virtual IP address. The value 1 indicates that the resource updates the DNS. The value 0 indicates it does not. Default is 0.</p> <p>Note: The Lanman resource does not update the DNS for the manual DNS entries. See “Updating manual DNS entries” on page 53 for instructions.</p>
DNSRefreshInterval	integer-scalar	<p>This attribute represents the time interval, in seconds, after which the Lanman agent attempts to refresh the resource records (RRs) on the DNS servers. You must set a value for this attribute if you want the Lanman agent to refresh the records on the DNS servers.</p> <p>The default value is zero, which indicates that the Lanman agent does not attempt to refresh the records on the DNS servers.</p> <p>The Lanman agent logs warning messages if it is not able to refresh the DNS records. After 3 failed attempts, the Lanman agent logs error messages for subsequent failures.</p> <p>If the Lanman agent is unable to refresh the DNS records, and the records are removed as a result of a scavenging operation or by the DNS administrator, the Lanman resource will fault.</p>

Table 3-7 Lanman agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
DNSZones	string-association	<p>An array that specifies a list of DNS zones (in case of multi-domain environments with parent-child configurations) for which the Lanman resource should create and update Address (A) records and canonical name (CNAME) records in the DNS server of the parent domain.</p> <p>Example: {"child1.company.com", "child2.company.com"}</p> <p>Where child1.company.com and child2.company.com are DNS zones representing different child domains.</p> <p>By default, the attribute contains no value. This means that the Lanman agent will create and update resource records only in the DNS name servers for the zones in which the nodes exist.</p> <p>Note: If multiple zones are being updated on BIND DNS servers that are configured for secure updates, then each zone may require a different TSIG key. In such a case, you must specify the absolute path of the TSIG key file in the attribute value.</p> <p>Example:</p> <pre>{"child1.company.com" = "C:\TSIGKey1.key", "child2.company.com" = "C:\TSIGKey2.key"}</pre> <p>Where TSIGKey1.key is the TSIG key for the DNS zone child1.company.com, and TSIGKey2.key is the TSIG key for the DNS zone child2.company.com.</p> <p>See "TSIGKeyFile" on page 52 for more information on TSIG keys.</p>

Table 3-7 Lanman agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
AliasName	string-scalar	<p>A string representing the alias to the canonical name. The Lanman agent creates a CNAME record using the value specified in this attribute.</p> <p>Example: “www”</p> <p>Where www is the alias to the canonical name mtv.veritas.com.</p> <p>By default, the attribute contains no value.</p>
TSIGKeyFile	string-scalar	<p>Required when you configure BIND DNS for secure updates. Specify the absolute path to the file that contains the private Transaction Signature (TSIG) key. This key is used by the nsupdate utility to perform secure BIND DNS updates.</p> <p>See the BIND man pages for more information about secure DNS updates.</p> <p>You must copy the files containing the keys (typically the .key and the .private file) on each of the nodes that is listed in the service group’s SystemList.</p> <p>By default, the attribute contains no value.</p> <p>Example: C:\TSIG\Kveritas.com.+157+00000.key</p> <p>Note: The Lanman agent supports BIND version 8 and above.</p>
TTL	integer-scalar	<p>This value defines the Time To Live (TTL) value (in seconds) that gets stored in the DNS records created by the agent.</p> <p>By default, the value is zero.</p> <p>Example: TTL = 7200</p>

Table 3-7 Lanman agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
MultiNet	boolean-scalar	A flag that defines whether the Lanman resource binds multiple IP addresses with the virtual name. The value 1 indicates the resource binds multiple IP addresses specified in MultiNetInfo with the virtual computer name. The value 0 indicates the resource binds a single IP address specified in IPResName. Default is 0.
MultiNetInfo	string-vector	An array that specifies details of the IP addresses to be bound to the virtual computer name. If MultiNet is set to 1, configure this attribute in the following format: MultiNetInfo = { " IP= <i>ip_address1</i> Mask= <i>subnetmask1</i> WINS= <i>wins_ip_address1</i> " , " IP= <i>ip_address2</i> Mask= <i>subnetmask2</i> WINS= <i>wins_ip_address2</i> " }

Updating manual DNS entries

Perform the following steps to update the DNS for manual DNS entries.

To update the DNS for manual DNS entries

- 1 For the manually added DNS entry, add the user in whose context the VCS Helper service is running.
- 2 Assign "Full Control" privilege to the newly added user.

Refer to Microsoft documentation for information about adding users and assigning privileges.

Updating DNS servers

[Table 3-8](#) presents possible combinations of values for the DNSOptions attribute and the updates effected by the Lanman resource corresponding to each value set.

Table 3-8 DNSOptions attribute and Lanman agent behavior

UpdateAll	Ignore Default	Purge Duplicate	Effect
-	-	-	Updates any one default DNS server.
-	-	✓	Updates any one default DNS server and removes duplicate entries, if any.
-	✓	-	Updates any one additional DNS server.
-	✓	✓	Updates any one additional DNS server and removes duplicate entries, if any.
✓	-	-	Updates all the default and additional DNS servers.
✓	-	✓	Updates all the default and additional DNS servers and removes duplicate entries, if any.
✓	✓	-	Updates all the additional DNS servers.
✓	✓	✓	Updates all additional DNS servers and removes duplicate entries, if any.

Sample configurations

In the following example, the Lanman agent is configured to bind a single IP address with the virtual computer name VNAMEX1. The Lanman agent will also add the computer object to the specified Active Directory container and update the additional DNS servers.

```
IP VIP1 (
  Address = "172.29.9.159"
  SubNetMask = "255.255.254.0"
  MACAddress @SYSTEM1 = "00-B0-D0-AB-4E-22"
  MACAddress @SYSTEM2 = "00-B0-D0-D1-69-7D"
)

Lanman VNAMEX1 (
  VirtualName = VNAMEX1
  IPResName = VIP1
  ADContainer = "OU=myUnit,DC=myCompany,DC=com"
  DnsOptions = { UpdateAll, PurgeDuplicate }
  AdditionalDNSServers = {"10.212.100.20", "10.212.100.21"}
)

VNAMEX1 requires VIP1
```

In the next example, the Lanman agent is configured to bind multiple IP addresses with the virtual computer name VNAMEX1.

```
IP IP_RES1 (
  Address = "11.212.96.182"
  SubNetMask = "255.255.254.0"
  MACAddress @SYSTEM3 = "00-D0-B7-4A-03-D8"
  MACAddress @SYSTEM4 = "00-D0-B7-4A-04-19"
)

IP IP_RES2 (
  Address = "11.212.99.214"
  SubNetMask = "255.255.254.0"
  MACAddress @SYSTEM3 = "00-D0-B7-4A-03-71"
  MACAddress @SYSTEM4 = "00-D0-B7-4A-03-7D"
)

Lanman LANMAN_VNAMEX1 (
  VirtualName = VNAMEX1
  MultiNet = 1
  MultiNetInfo = {
    "IP=11.212.96.182 MASK=255.255.254.0
WINS=10.212.100.120",
    "IP=11.212.99.214 MASK=255.255.254.0
WINS=10.212.100.120" }
)

NIC NIC-EXCH_GRP1 (
  MACAddress @SYSTEM3 = "00-D0-B7-4A-03-D8"
```

```
MACAddress @SYSTEM4 = "00-D0-B7-4A-04-19"  
)  
  
NIC NIC-EXCH_GRP2 (  
  MACAddress @SYSTEM3 = "00-D0-B7-4A-03-71"  
  MACAddress @SYSTEM4 = "00-D0-B7-4A-03-7D"  
)  
  
IP_RES1 requires NIC-EXCH_GRP1  
IP_RES2 requires NIC-EXCH_GRP2  
LANMAN_VNAMEX1 requires IP_RES2  
LANMAN_VNAMEX1 requires IP_RES1
```

FileShare agents

Fileshare agents make file shares highly available.

- The FileShare agent ensures high availability for a shared directory
- The CompositeFileShare agent ensures high availability for multiple sub-directories.

FileShare agent

The FileShare agent enables systems to share a directory and its subdirectories, making the shared directory highly available. The directory to be shared is stored on a shared disk. Using the FileShare agent, you can also:

- create hidden shares for a specific share or subdirectories
- dynamically share subdirectories created after the resource was brought online
- configure and control existing shares

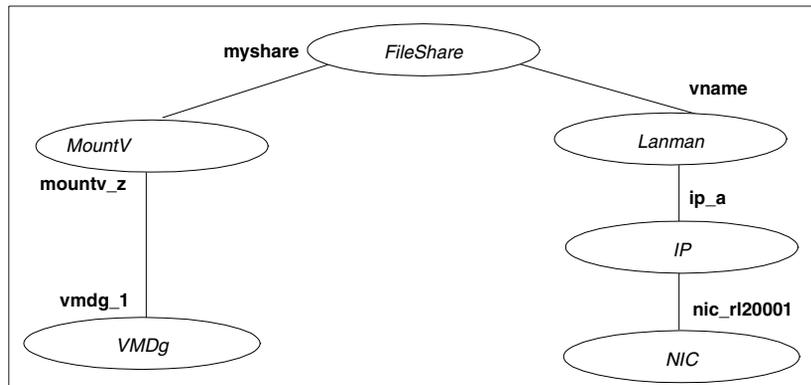
The FileShare agent enables sharing directories shared outside VCS. However, you cannot add special shares (shares created by the operating system for administrative and system use) to the VCS configuration. For example, you cannot add the shares ADMIN\$, print\$, IPC\$, and *DriveLetter\$* to the VCS configuration.

You can configure a file share service group using the FileShare configuration wizard. See the *Veritas Cluster Server Administrator's Guide* for instructions. To share multiple directories, use the CompositeFileshare agent, described in “[CompositeFileShare agent](#)” on page 66.

Dependencies

The FileShare agent depends on the MountV agent. A FileShare service group also requires a Lanman resource that is dependent on the FileShare resource, as illustrated in the following dependency graph.

Figure 4-1 File Share service group dependency graph



Agent functions (Entry Points)

- **online**—Shares the specified directories with designated permissions.
- **offline**—Removes the shares for the specified directories.
- **monitor**—Verifies at least one specified directory is shared with the designated permissions.

State definitions

- **ONLINE**—Indicates at least one specified directory is shared.
- **OFFLINE**—Indicates no specified directory is shared.
- **UNKNOWN**—Indicates the agent could not determine the status of the resource.

Note: Sharing a directory with a large number of subdirectories and enabling the `ShareSubdirectories` flag could cause increased failover time and high CPU and memory utilization.

Resource type definition

```
type FileShare (  
    static i18nstr ArgList[] = {PathName, ShareName,  
  
    "LanmanResName:VirtualName", MaxUsers,  
  
    "MountResName:MountPath", HiddenShare,  
  
    ShareSubdirectories, HideChildShares,  
  
    AutoShare, AutoControl, ClientCacheType,  
  
    IgnorePermissions, UserPermissions }  
    i18nstr PathName  
    i18nstr ShareName  
    str LanmanResName  
    str MaxUsers = 10  
    str MountResName  
    i18nstr UserPermissions{} = { Everyone=NO_ACCESS }  
    boolean HiddenShare = 0  
    boolean ShareSubdirectories = 0  
    boolean HideChildShares = 0  
    boolean AutoShare = 1  
    boolean AutoControl = 1  
    str ClientCacheType = MANUAL  
    boolean IgnorePermissions = 0  
)
```

Attribute definitions

Table 4-1 FileShare agent required attributes

Required Attributes	Type and Dimension	Description
LanmanResName	string-scalar	The name of the Lanman resource on which the FileShare depends. This attribute is ignored by the agent.
MountResName	string-scalar	The name of the MountV resource on which the FileShare resource depends.
PathName	string-scalar	The path of the directory to be shared. If a drive is to be shared, the PathName is specified as \. If a directory on the mounted drive is shared, the PathName is specified as <i>\dir_name</i> . Note: This attribute can take localized values.
ShareName	string-scalar	The name by which the share is known to clients. This attribute can take localized values.

Table 4-2 FileShare agent optional attributes

Optional Attributes	Type and Dimension	Description
AutoControl	boolean-scalar	A flag that defines the agent behavior when a share created outside VCS is added to the agent configuration. The value 1 indicates the agent controls the share and makes it highly available after the resource is manually brought online. The value 0 indicates the agent does not control the share. To make an existing share highly available, the share name and the share permissions in the configuration file must be the same as those for the file share. Default is 1.

Table 4-2 FileShare agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
AutoShare	boolean-scalar	<p>A flag that defines agent behavior when a directory is added to a VCS file share with shared subdirectories. The value 1 indicates the agent automatically shares the newly added subdirectory in its next monitor cycle. The value 0 indicates the agent does not. This attribute is considered only if the attribute ShareSubdirectories is set to 1. Default is 1.</p>
ClientCacheType	string-scalar	<p>A string that specifies whether the documents or programs on the shared folder are cached locally, when accessed by other users. It also specifies how the files are cached. The cached files would then be available offline.</p> <p>Note: The agent does not cache the files or folders itself. It sets the value so that the server and client interfaces do the needful.</p> <p>This attribute can have the following values:</p> <ul style="list-style-type: none"> ■ MANUAL: Indicates that the agent requires you to specify individual documents or programs to be cached. ■ NONE: Indicates the agent does not cache the documents and programs from the share. ■ DOCS: Indicates that the user accessed documents are available offline. ■ PROGRAMS: Indicates that the user accessed documents and programs are available offline. <p>Default is MANUAL.</p>
HiddenShare	boolean-scalar	<p>A flag that defines whether the agent hides the file share. The value 1 indicates the agent hides the file share. The value 0 indicates it does not. Default is 0.</p> <p>Note: To create a hidden share, set the HiddenShare attribute to 1. Do not append the share name with a \$ (dollar) sign.</p>

Table 4-2 FileShare agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
HideChildShares	boolean-scalar	A flag that defines whether the agent hides the subdirectory shares. This attribute is considered only if the attribute ShareSubdirectories is set to 1. The value 1 indicates the agent hides the subdirectory shares. The value 0 indicates it does not. Default is 0.
IgnorePermissions	boolean-scalar	A flag that defines whether the agent takes into consideration the share permissions for a particular share. The value 1 indicates the agent does not consider share permissions. The value 0 indicates it does. Default is 0.
MaxUsers	string-scalar	The maximum number of users allowed access to the resource. Default is null, which indicates access to an unlimited number of users. Note: If the attribute is defined to have a value larger than 32767, the value rolls over. For example, if MaxUsers is set to 32768, the agent accepts the value as 1.
ShareSubdirectories	boolean-scalar	A flag that defines whether the agent shares the subdirectories of the file shares defined in the attribute PathName and ShareName. Subdirectories are shared with their own names, that is, the share name of a subdirectory is the same as the subdirectory name. If a share with the same name exists, the subdirectory will not be shared. However, this does not effect the state of the resource. The value 1 indicates the agent shares the subdirectories. The value 0 indicates it does not. Default is 0.

Table 4-2 FileShare agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
UserPermissions	string-association	<p>The permissions by which the directories are shared by users. The permissions associated with the FileShare agent are:</p> <ul style="list-style-type: none"> ■ FULL_CONTROL: Permission to read, write, create, execute, and delete the resource, and to modify its attributes and permissions. ■ READ_ACCESS: Permission to read, and execute the resource. ■ CHANGE_ACCESS: Permission to read, write, execute, and delete the resource. ■ NO_ACCESS: No access to the resource. <p>The UserPermissions are specified in the format 'Domain_Name\Username'=Permission. For example, to give full control to user John who belongs to the domain vcs_domain, the syntax is 'VCS_DOMAIN\John'=FULL_CONTROL. Note that the domain name and the user name must be enclosed in quotation marks. Default is {'Everyone' = no_access}. A maximum of 50 users can be configured for each file share. To configure more than 50 users for a file share, configure user groups.</p> <p>Note: This attribute can take localized values.</p>

Sample configuration

```
FileShare FileShare_SG-FileShare (
  PathName = "\\ToShare"
  ShareName = ToShare
  LanmanResName = FileShare_SG-Lanman
  MountResName = FileShare_SG-MountV
  UserPermissions = { "VCSNET\Administrator" = READ_ACCESS }
)

IP FileShare_SG-IP (
  Address = "10.212.100.184"
  SubNetMask = "255.255.254.0"
  MACAddress @SYSTEM1 = "00-02-B3-AD-CE-E4"
  MACAddress @SYSTEM2 = "00-02-B3-AD-CB-D0"
)

Lanman FileShare_SG-Lanman (
  VirtualName = VNAME
  IPResName = FileShare_SG-IP
)

MountV FileShare_SG-MountV (
  MountPath = "J:"
  VolumeName = PS-SPOOL
  VMDGResName = FileShare_SG-VMDg
)

NIC FileShare_SG-NIC (
  MACAddress @SYSTEM1 = "00-02-B3-AD-CE-E4"
  MACAddress @SYSTEM2 = "00-02-B3-AD-CB-D0"
)

VMDg FileShare_SG-VMDg (
  DiskGroupName = PRINTSHARE_DG
  DGGuid = e40b8ab5-88ac-42e3-ae61-cbea3a164af2
)

FileShare_SG-Lanman requires FileShare_SG-IP
FileShare_SG-MountV requires FileShare_SG-VMDg
FileShare_SG-FileShare requires FileShare_SG-Lanman
FileShare_SG-FileShare requires FileShare_SG-MountV
FileShare_SG-IP requires FileShare_SG-NIC
```

CompositeFileShare agent

The CompositeFileShare agent enables systems to share multiple subdirectories for each of the shared directories. The directories to be shared are stored on shared disks. Using the CompositeFileShare agent, you can also:

- create hidden shares for shared directories or subdirectories.
- dynamically share the subdirectories created after the resource was brought online.
- configure and control existing shares.

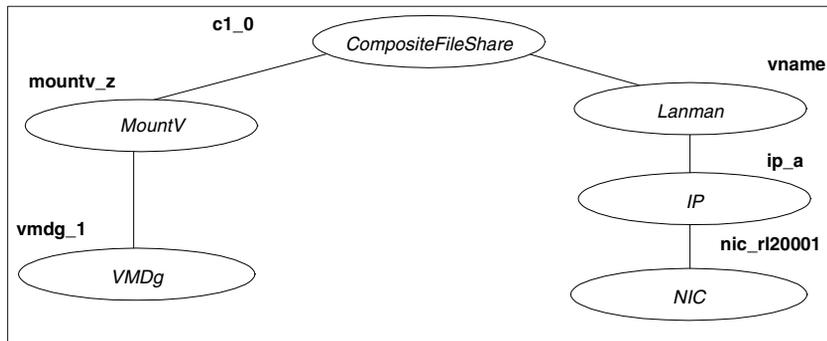
The CompositeFileShare agent enables sharing directories shared outside VCS. However, you cannot add special shares (those created by the operating system for administrative and system use) to the VCS configuration. For example, you cannot add the shares ADMIN\$, print\$, IPC\$, and *DriveLetter\$*.

The agent simplifies the process of configuring multiple file shares. It defines file shares in an array, thereby eliminating the need to specify dependencies for each FileShare resource. Each CompositeFileShare resource can be configured for a maximum of 50 file shares.

Dependencies

The CompositeFileShare agent depends on the MountV agent. A CompositeFileShare service group also requires a Lanman resource that is dependent on the CompositeFileShare resource, as illustrated in the following dependency graph.

Figure 4-2 CompositeFileShare service group dependency graph



Agent functions (Entry Points)

- **online**—Shares the specified directories with designated permissions.
- **offline**—Removes the shares for the specified directories.
- **monitor**—Verifies at least one specified directory is shared with the designated permissions.

State definitions

- **ONLINE**—Indicates at least one specified directory is shared.
- **OFFLINE**—Indicates no specified directory is shared.
- **UNKNOWN**—Indicates the agent could not determine the status of the resource.

Resource type definition

```
type CompositeFileShare (  
    static i18nstr ArgList[] = {"LanmanResName:VirtualName",  
    MaxUsers,  
  
    "MountResName:MountPath", HiddenShare,  
  
    ShareSubdirectories, HideChildShares,  
  
    AutoShare, AutoControl, ClientCacheType,  
  
    IgnorePermissions, PathAndShareName,  
  
    UserPermissions }  
    str LanmanResName  
    str MaxUsers = 10  
    str MountResName  
    i18nstr UserPermissions{} = { Everyone=NO_ACCESS }  
    boolean HiddenShare = 0  
    boolean ShareSubdirectories = 0  
    boolean HideChildShares = 0  
    boolean AutoShare = 1  
    boolean AutoControl = 1  
    i18nstr PathAndShareName{}  
    str ClientCacheType = MANUAL  
    boolean IgnorePermissions = 0  
)
```

Attribute definitions

Table 4-3 CompositeFileShare agent required attributes

Required Attributes	Type and Dimension	Description
LanmanResName	string-scalar	The name of the Lanman resource on which the FileShare depends. This attribute is ignored by the agent.
MountResName	string-scalar	The name of the MountV agent on which the CompositeFileShare resource depends.
PathandShareName	string-association	A list specifying the respective paths and share names of the directories to be shared. If the path of a shared directory is <code>\Documents</code> , and the share name is <code>UserDocs</code> , the attribute is defined in the configuration file as <code>PathandShareName is {"\Documents" = "UserDocs"}</code> . Note: This attribute can take localized values.

Table 4-4 CompositeFileShare agent optional attributes

Optional Attributes	Type and Dimension	Description
AutoControl	boolean-scalar	A flag that defines the agent behavior when a share created outside VCS is added to the agent configuration. The value 1 indicates the agent controls the share and makes it highly available after the resource is manually brought online. The value 0 indicates the agent does not control the share. To make an existing share highly available, the share name and the share permissions in the configuration file must be the same as those for the file share. Default is 1.

Table 4-4 CompositeFileShare agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
AutoShare	boolean-scalar	<p>A flag that defines agent behavior when a directory is added to a VCS file share with shared subdirectories. The value 1 indicates the agent automatically shares the newly added subdirectory in its next monitor cycle. The value 0 indicates the agent does not. This attribute is considered only if the attribute ShareSubdirectories is set to 1. Default is 1.</p>
ClientCacheType	string-scalar	<p>A string that specifies whether the documents or programs on the shared folder are cached locally, when accessed by other users. It also specifies how the files are cached. The cached files would then be available offline.</p> <p>Note: The agent does not cache the files or folders itself. It sets the value so that the server and client interfaces do the needful.</p> <p>This attribute can have the following values:</p> <ul style="list-style-type: none">■ MANUAL: Indicates that the agent requires you to specify individual documents or programs to be cached.■ NONE: Indicates that the agent does not cache the documents and programs from the share.■ DOCS: Indicates that the user accessed documents are available offline.■ PROGRAMS: Indicates that the user accessed documents and programs are available offline. <p>Default is MANUAL.</p>

Table 4-4 CompositeFileShare agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
HiddenShare	boolean-scalar	<p>A flag that defines whether the agent hides the file share. The value 1 indicates the agent hides the file share. The value 0 indicates it does not. Default is 0.</p> <p>Note: To create a hidden share, set the HiddenShare attribute to 1. Do not append the share name with a \$ (dollar) sign.</p>
HideChildShares	boolean-scalar	<p>A flag that defines whether the agent hides the subdirectory shares. This attribute is considered only if the attribute ShareSubdirectories is set to 1. The value 1 indicates the agent hides the subdirectory shares. The value 0 indicates it does not. Default is 0.</p>
IgnorePermissions	boolean-scalar	<p>A flag that defines whether the agent takes into consideration the share permissions for a particular share. The value 1 indicates the agent does not consider share permissions. The value 0 indicates it does. Default is 0.</p>
MaxUsers	string-scalar	<p>The maximum number of users allowed access to the resource. Default is null, which indicates access to an unlimited number of users.</p> <p>Note: If the attribute is defined to have a value larger than 32767, the value rolls over. For example, if MaxUsers is set to 32768, the agent accepts the value as 1.</p>

Table 4-4 CompositeFileShare agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
ShareSubdirectories	boolean-scalar	<p>A flag that defines whether the agent shares the subdirectories of the file shares defined in the attribute PathAndShareName. Subdirectories are shared with their own names, that is, the share name of a subdirectory is the same as the subdirectory name. If a share with the same name exists, the subdirectory will not be shared. However, this does not effect the state of the resource.</p> <p>The value 1 indicates the agent shares the subdirectories. The value 0 indicates it does not. Default is 0.</p>

Table 4-4 CompositeFileShare agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
UserPermissions	string-association	<p>The permissions by which the directories are shared by users. Note that user permissions do not apply to individual file shares. User permissions apply to all file shares that form the CompositeFileShare resource. The permissions associated with the CompositeFileShare agent are:</p> <ul style="list-style-type: none"> ■ FULL_CONTROL: Permission to read, write, create, execute, and delete the resource, and to modify its attributes and permissions. ■ READ_ACCESS: Permission to read, and execute the resource. ■ CHANGE_ACCESS: Permission to read, write, execute, and delete the resource. ■ NO_ACCESS: No access to the resource. <p>The UserPermissions are specified in the format 'Domain_Name\Username'=Permission. For example, to give full control to user John who belongs to the domain vcs_domain, the syntax is 'VCS_DOMAIN\John'=FULL_CONTROL. Note that the domain name and the user name must be enclosed in quotation marks. Default is {'Everyone' = no_access}. A maximum of 50 user can be configured for each file share. To configure more than 50 users for a file share, configure user groups.</p> <p>Note: This attribute can take localized values.</p>

Sample configuration

```
CompositeCFS CFS-RES (
  LanmanResName = CFS_SG-Lanman
  MountResName = CFS_SG-MountV
  PathAndShareName = { "\\share2" = share2, "\\share3" =
share3 }
)

IP CFS_SG-IP (
  Address = "10.212.100.184"
  SubNetMask = "255.255.254.0"
  MACAddress @SYSTEM1 = "00-02-B3-AD-CE-E4"
  MACAddress @SYSTEM2 = "00-02-B3-AD-CB-D0"
)

Lanman CFS_SG-Lanman (
  VirtualName = VNAME
  IPResName = CFS_SG-IP
)

MountV CFS_SG-MountV (
  MountPath = "J:"
  VolumeName = PS-SPOOL
  VMDGResName = CFS_SG-VMDg
)

NIC CFS_SG-NIC (
  MACAddress @SYSTEM1 = "00-02-B3-AD-CE-E4"
  MACAddress @SYSTEM2 = "00-02-B3-AD-CB-D0"
)

VMDg CFS_SG-VMDg (
  DiskGroupName = PRINTSHARE_DG
  DGGuid = e40b8ab5-88ac-42e3-ae61-cbea3a164af2
)

CFS_SG-Lanman requires CFS_SG-IP
CFS_SG-MountV requires CFS_SG-VMDg
CFS-RES requires CFS_SG-Lanman
CFS-RES requires CFS_SG-MountV
CFS_SG-IP requires CFS_SG-NIC
```


PrintShare agents

The PrintShare agents work together to make a shared network printer highly available. The PrintSpool agent provides high availability for a print spooler and the PrintShare agent makes a network printer highly available.

PrintSpool agent

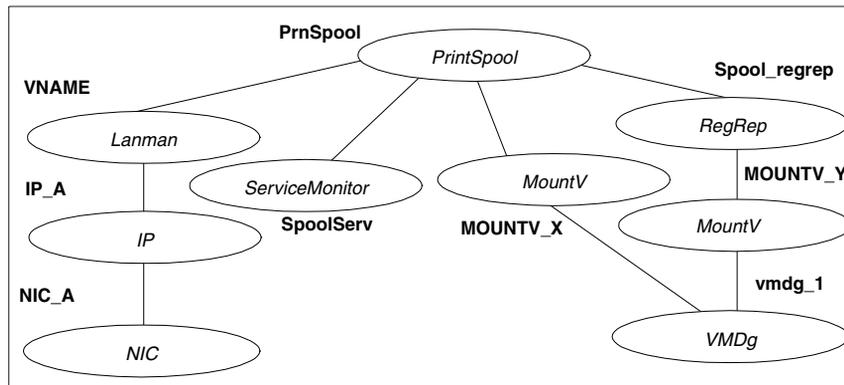
The PrintSpool agent makes a print spooler highly available and binds it to the virtual computer. It ensures that spooling does not occur locally. The agent is used in conjunction with the PrintShare agent to make a print server highly available. You can configure only one PrintSpool resource for one virtual computer.

Dependencies

The PrintSpool agent depends on the MountV, Lanman, and Registry Replication agents for operation. It also requires the Print Spooler service configured as a ServiceMonitor resource.

The following figure illustrates the PrintSpool agent's dependency graph:

Figure 5-1 PrintSpool service group dependency graph



Agent functions (Entry Points)

- **online**—Creates a virtual spooler and binds it with the virtual computer.
- **offline**—Stops the virtual spooler.
- **monitor**—Verifies the spooler is bound to the virtual computer.

State definitions

- ONLINE—Indicates the virtual spooler is active on the virtual computer.
- OFFLINE—Indicates the virtual spooler is not active on the virtual computer.
- UNKNOWN—Indicates the agent could not determine the status of the virtual spooler.

Resource type definition

```
type PrintSpool (
    static i18nstr ArgList[] = {"LanmanResName:VirtualName",
    "IPResName:Address",
    "MountResName:MountPath", SpoolDir }
    str LanmanResName
    str IPResName
    str MountResName
    i18nstr SpoolDir
)
```

Attribute definitions

Table 5-1 PrintSpool agent required attributes

Required Attributes	Type and Dimension	Description
IPResName	string-scalar	The name of the IP resource on which the Lanman resource specified by the attribute LanmanResName depends.
LanmanResName	string-scalar	The name of the Lanman resource on which the PrintSpool resource depends. The print spooler is bound to the virtual computer associated with this Lanman resource.
MountResName	string-scalar	The name of the MountV resource on which the PrintSpool resource depends. This resource must point to the drive on the shared disk where the spool directory will reside.
SpoolDir	string-scalar	A directory on the shared disk to be used for spooling. The value for SpoolDir attribute must be relative to the drive letter for MountResName. Note: This attribute can take localized values.

Sample configuration

The following sample configuration creates a PrintSpool resource with the required Lanman, MountV, Service Monitor, and Registry Replication resources.

```
IP IP-10-212-100-184 (
  Address = "10.212.100.184"
  SubNetMask = "255.255.254.0"
  MACAddress @SYSTEM1 = "00-02-B3-AD-CB-D0"
  MACAddress @SYSTEM2 = "00-02-B3-AD-CE-E4"
)

Lanman Lanman-PRINTSHAREMAN (
  VirtualName = PRINTSHAREMAN
  IPResName = IP-10-212-100-184
  ADCriticalForOnline = 1
)

MountV MountV-JDrive (
  MountPath = "J:"
  VolumeName = PS-SPOOL
  VMDGResName = VMDg-PRINTSHARE_DG
)

MountV MountV-IDrive (
  MountPath = "I:"
  VolumeName = PS-REGREP
  VMDGResName = VMDg-PRINTSHARE_DG
)

NIC NIC-PRINSHARE-SG (
  MACAddress @SYSTEM1 = "00-02-B3-AD-CB-D0"
  MACAddress @SYSTEM2 = "00-02-B3-AD-CE-E4"
)

PrintSpool PSSpool (
  LanmanResName = Lanman-PRINTSHAREMAN
  IPResName = IP-10-212-100-184
  MountResName = MountV-JDrive
  SpoolDir = "\\SPOOLER"
)
```

```
RegRep RegRep (
    MountResName = MountV-IDrive
    ReplicationDirectory = "\\PS-REGREP"
    Keys = {"HKLM\\Software\\Veritas\\VCS\\BundledAgents\\
PrintSpool
                                                \\PSSpool" }
)

ServiceMonitor ServiceMonitor-PrintSpooler (
    ServiceOrScriptName = "Print Spooler"
)

VMDg VMDg-PRINTSHARE_DG (
    DiskGroupName = PRINTSHARE_DG
)

IP-10-212-100-184 requires NIC-PRINSHARE-SG
Lanman-PRINTSHAREMAN requires IP-10-212-100-184
MountV-JDrive requires VMDg-PRINTSHARE_DG
MountV-IDrive requires VMDg-PRINTSHARE_DG
PSSpool requires Lanman-PRINTSHAREMAN
PSSpool requires MountV-JDrive
PSSpool requires ServiceMonitor-PrintSpooler
PSSpool requires RegRep
RegRep requires MountV-IDrive
```

PrintShare agent

The PrintShare agent enables systems to share a network printer from a cluster so that the clients can access it. The agent adds, monitors, and removes a share to the network printer from the virtual computer. Configure a PrintShare service group using the PrintShare configuration wizard, described in the *Veritas Cluster Server Administrator's Guide*.

Dependency

The PrintShare agent depends on the PrintSpool agent.

Agent functions (Entry Points)

- `online`—Adds a share to the network printer on the virtual computer.
- `offline`—Deletes the share to the network printer from the virtual computer.
- `monitor`—Verifies that the share to the network printer exists.

State definitions

- `ONLINE`—Indicates the network printer is shared from the virtual computer.
- `OFFLINE`—Indicates the network printer is not shared from the virtual computer.
- `UNKNOWN`—Indicates the agent could not determine the status of the resource.

Resource type definition

```
type PrintShare (
    static i18nstr ArgList[] = {PrinterName, ShareName,
    "LanmanResName:VirtualName" }
    i18nstr PrinterName
    i18nstr ShareName
    str LanmanResName
)
```

Attribute definitions

Table 5-2 PrintShare agent required attributes

Required Attributes	Type and Dimension	Description
LanmanResName	string-scalar	The name of the Lanman resource configured for the virtual computer.
PrinterName	string-scalar	The name of the network printer to be shared. This attribute can take localized values.
ShareName	string-scalar	The name by which the network printer will be shared. This attribute can take localized values.

Sample configuration

The following sample configuration creates a PrintShare resource with the required PrintSpool and ServiceMonitor resources.

```

IP IP-10-212-100-184 (
    Address = "10.212.100.184"
    SubNetMask = "255.255.254.0"
    MACAddress @SYSTEM1 = "00-02-B3-AD-CB-D0"
    MACAddress @SYSTEM2 = "00-02-B3-AD-CE-E4"
)

Lanman Lanman-PRINTSHAREMAN (
    VirtualName = PRINTSHAREMAN
    IPResName = IP-10-212-100-184
    ADCriticalForOnline = 1
)

MountV MountV-JDrive (
    MountPath = "J:"
    VolumeName = PS-SPOOL
    VMDGResName = VMDg-PRINTSHARE_DG
)

MountV MountV-IDrive (
    MountPath = "I:"
    VolumeName = PS-REGREP
    VMDGResName = VMDg-PRINTSHARE_DG
)

NIC NIC-PRINSHARE-SG (
    MACAddress @SYSTEM1 = "00-02-B3-AD-CB-D0"
    MACAddress @SYSTEM2 = "00-02-B3-AD-CE-E4"
)
    
```

```

PrintShare PSShare (
    PrinterName = "HP LaserJet 4050 Series PCL"
    ShareName = "HP LaserJet 4050 Series PCL"
    LanmanResName = Lanman-PRINTSHAREMAN
)

PrintSpool PSSpool (
    LanmanResName = Lanman-PRINTSHAREMAN
    IPResName = IP-10-212-100-184
    MountResName = MountV-JDrive
    SpoolDir = "\\SPOOLER"
)

RegRep RegRep (
    MountResName = MountV-IDrive
    ReplicationDirectory = "\\PS-REGREP"
    Keys = {"HKLM\\Software\\ Veritas\\VCS\\BundledAgents
\\PrintSpool
                                \\PSSpool" }
)

ServiceMonitor ServiceMonitor-PrintSpooler (
    ServiceOrScriptName = "Print Spooler"
)

VMDg VMDg-PRINTSHARE_DG (
    DiskGroupName = PRINTSHARE_DG
)

IP-10-212-100-184 requires NIC-PRINSHARE-SG
Lanman-PRINTSHAREMAN requires IP-10-212-100-184
MountV-JDrive requires VMDg-PRINTSHARE_DG
MountV-IDrive requires VMDg-PRINTSHARE_DG
PSShare requires PSSpool
PSSpool requires Lanman-PRINTSHAREMAN
PSSpool requires MountV-JDrive
PSSpool requires ServiceMonitor-PrintSpooler
PSSpool requires RegRep
RegRep requires MountV-IDrive
VNAME requires IP_A

```

Services and applications agents

Services and applications agents make generic services and other applications highly available.

- The MSVirtualMachine agent brings virtual machines configured using Microsoft Virtual Server online, monitors their status, and takes them offline.
- The Internet Information Services (IIS) agent brings IIS sites and services online, monitors their status, and takes them offline.
- The GenericService agent brings services online, monitors their status, and takes them offline.
- The ServiceMonitor agent only monitors a service or starts a user-defined script and interprets the exit code of the script.
- The Process agent brings processes online, monitors their status, and takes them offline.
- The MSMQ agent works with the Microsoft Message Queuing (MSMQ) service. The MSMQ agent creates an MSMQ service for an MSMQ resource, brings the MSMQ service online, takes it offline, and monitors its status.

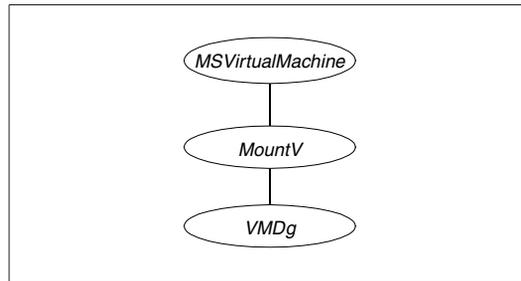
Microsoft Virtual Machine (MSVirtualMachine) agent

The Microsoft Virtual Machine agent provides high availability to virtual machines configured using Microsoft Virtual Server. Specifically, the agent brings virtual machines online, monitors their status, and takes them offline. The agent is represented by the MSVirtualMachine resource type in the VCS configuration.

Dependencies

The MSVirtualMachine agent depends on the MountV and Volume Manager Diskgroup (VMDg) agents for operation.

Figure 6-1 MSVirtualMachine service group dependency graph



Agent functions (Entry Points)

- **online**—Starts the virtual machine.
- **offline**—Stops the virtual machine.
- **monitor**—Verifies the virtual machine is running.

The agent provides two levels of monitoring: basic and detailed. Basic monitoring verifies the configured virtual machine is running. Detailed monitoring verifies the state of the virtual machine by monitoring heartbeats between the virtual machine and Microsoft Virtual Server. Note that you must install and configure Virtual Machine Additions to enable detailed monitoring. See the Microsoft documentation for more information about heartbeats between the virtual machine and

State definitions

- ONLINE—Indicates the virtual machine is running.
- OFFLINE—Indicates the virtual machine is not running.
- UNKNOWN—Indicates the agent could not determine the status of the resource.

Resource type definition

```
type MSVirtualMachine (  
    static int MonitorInterval = 30  
    static int NumThreads = 1  
    static i18nstr ArgList[] = { VMName, MonitorHB,  
FailedHBThreshold }  
    i18nstr VMName  
    int MonitorHB  
    int FailedHBThreshold  
)
```

Attribute definitions

Table 6-1 MSVirtualMachine agent required attributes

Required Attribute	Type and Dimension	Description
VMName	string-scalar	The name of the virtual machine. This attribute can take localized values.

Table 6-2 MSVirtualMachine agent optional attributes

Optional Attributes	Type and Dimension	Description
MonitorHB	boolean-scalar	A flag that defines whether the agent monitors the virtual machine heartbeats. The value 1 indicates that the agent will monitor heartbeats. This option requires Virtual Machine Additions to be installed and configured.
FailedHBThreshold	integer-scalar	The number of consecutive monitor cycles the agent waits to detect heartbeats from the virtual machine before declaring the resource as faulted. For example, setting this value to 5 indicates that if the agent fails to detect heartbeats from the virtual machine for five consecutive monitor cycles, the agent declares the resource as faulted. Setting this value 0 indicates that the agent will log messages, but will not fault the resource when it fails to detect heartbeats from the virtual machine.

Sample configuration

```
group MVS (  
    SystemList = { THORPC111 = 0, THORPC121 = 1 }  
    AutoStartList = { THORPC111, THORPC121 }  
)  
  
MountV MountV (  
    MountPath = "L:\\\  
    VolumeName = DG1_Vol1  
    VMDGResName = VMDG  
)  
  
VMDg VMDG (  
    DiskGroupName = DG1  
)  
  
MSVirtualMachine VMS (  
    VMName = shared_w2k  
    MonitorHeartbeat = 1  
)  
  
MountV requires VMDG  
VMS requires MountV
```

Internet Information Services agent

The Internet Information Services (IIS) agent provides high availability to sites configured using IIS 5.0 and 6.0. Specifically, the agent brings IIS sites online, monitors their status, and takes them offline.

The agent provides two ways of monitoring application pools associated with IIS Web sites:

- One IIS resource configures a Web site and sets monitoring options for application pools associated with the site
- One IIS resource configures a Web site; other resources configure individual application pools.

Agent functions (Entry Points)

- `online`—Starts the configured site or application pool.
- `offline`—Stops the configured site or application pool.
- `monitor`—Verifies the configured site or application pool is running.

State definitions

- `ONLINE`—Indicates the configured site or application pool is available.
- `OFFLINE`—Indicates the configured site or application pool is not available.
- `UNKNOWN`—Indicates the agent could not determine the status of the resource.

Resource type definition

```
type IIS (  
    static i18nstr ArgList[] = {SiteType, SiteName,  
  
    "IPResName:Address", PortNumber,  
  
    AppPoolMon, DetailMonitor,  
  
    DetailMonitorInterval }  
    str SiteType  
    i18nstr SiteName  
    int PortNumber = 80  
    str AppPoolMon = NONE  
    boolean DetailMonitor = 0  
    int DetailMonitorInterval = 5  
    str IPResName  
)
```

Attribute definitions

To configure the agent to monitor an application pool, configure the SiteType and SiteName attributes only. The agent ignores other attributes when it is configured to monitor an application pool.

Table 6-3 IIS agent required attributes

Required Attributes	Type and Dimension	Description
SiteType	string-scalar	<p>Defines whether the resource is configured to monitor an IIS site or an application pool.</p> <p>If the resource is configured to monitor an application pool, set the attribute to APPPOOL.</p> <p>If the resource is configured to monitor an IIS site, set this attribute to the name of the IIS service associated with the site. The attribute can take any of the following values:</p> <ul style="list-style-type: none"> ■ W3SVC ■ MSFTPSVC ■ SMTPSVC ■ NNTPSVC
SiteName	string-scalar	<p>The name of the IIS site, the virtual server, or the application pool to be monitored by the agent.</p> <p>The value of this attribute depends on that of the SiteType attribute. The SiteName attribute can take the following values:</p> <ul style="list-style-type: none"> ■ The name of a site, if SiteType is W3SVC or MSFTPSVC ■ The name of a virtual server, if SiteType is SMTPSVC or NNTPSVC ■ The name of an application pool, if SiteType is APPPOOL <p>Note: This attribute can take localized values.</p>
IPResName	string-scalar	The name of the IP resource configured for the IP to which the site is bound.
PortNumber	string-scalar	The port to which the site is bound.

Table 6-4 IIS agent optional attributes

Optional Attributes	Type and Dimension	Description
AppPoolMon	integer-scalar	<p>Defines the monitoring modes for the application pool associated with the Web site being monitored.</p> <p>Configure this attribute only if SiteType is W3SVC and IIS is configured to run in the Worker Process Isolation mode.</p> <p>The attribute can take one of the following values:</p> <ul style="list-style-type: none"> ■ NONE: Indicates that the agent will not monitor the application pool associated with the Web site. ■ DEFAULT: Indicates that the agent will monitor the <i>root</i> application pool associated with the Web site. If this attribute is set, the agent starts, stops, and monitors the root application pool associated with the Web site. If the root application pool is stopped externally, the agent fails over the service group. ■ ALL: Indicates the agent will start all application pools associated with the Web site, but will monitor and stop the <i>root</i> application pool only.
DetailMonitor	boolean-scalar	<p>A flag that defines whether the agent monitors the site in detail. The value 1 indicates the agent will monitor each site in detail by attempting an actual socket connection to the port.</p>
DetailMonitorInterval	integer-scalar	<p>The number of monitor cycles after which the agent attempts detail monitoring. For example, the value 5 indicates that the agent will monitor the resource in detail after every 5 monitor cycles.</p>

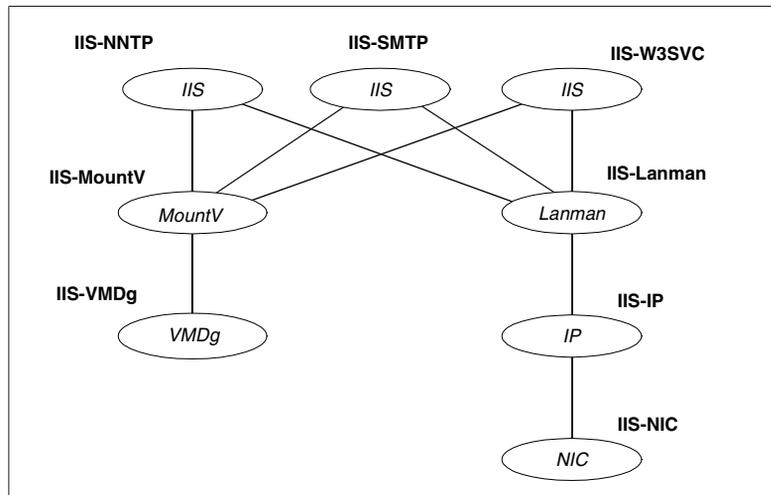
Sample configurations

This section describes two sample configurations. The first configuration depicts how you can configure one IIS resource monitors a Web site and its associated application pools. The second configuration depicts how you can configure separate IIS resources to monitor Web sites and application pools.

Sample configuration I

In the following configuration the IIS sites are located in a shared disk group, which is configured using the VMDg resource type.

Figure 6-2 IIS service group dependency graph



A MountV resource configures a drive letter for the shared disk group. The IIS sites share a virtual name and IP address, configured using the Lanman and IP resource types respectively. The IIS resources depend on the Lanman and MountV resources and can be started after these resources are brought online.

Sample main.cf file

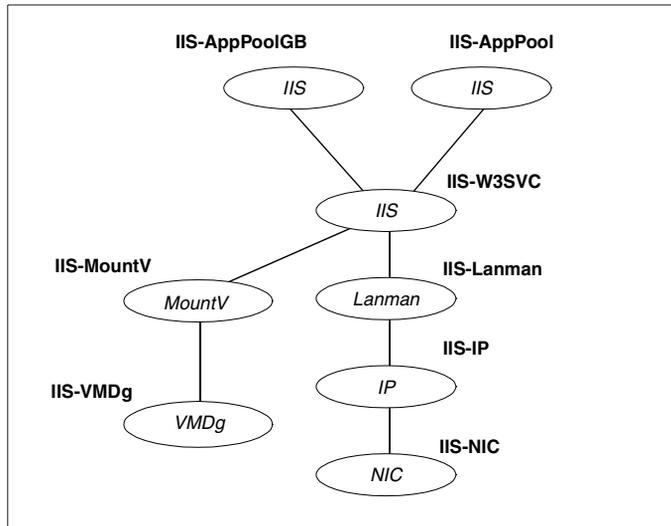
```
IIS IIS-W3SVC (  
    SiteType = W3SVC  
    SiteName = "My Site"  
    AppPoolMon = DEFAULT  
    DetailMonitor = 1  
    IPResName = IIS-IP  
)  
  
IIS IIS-SMTP (  
    SiteType = SMTPSVC  
    SiteName = "Default SMTP Virtual Server"  
    PortNumber = 25  
    DetailMonitor = 1  
    IPResName = IIS-IP  
)  
  
IIS IIS-NNTP (  
    SiteType = NNTPSVC  
    SiteName = "Default NNTP Virtual Server"  
    PortNumber = 119  
    DetailMonitor = 1  
    IPResName = IIS-IP  
)  
  
IP IIS-IP (  
    Address = "10.182.145.223"  
    SubNetMask = "255.255.252.0"  
    MACAddress @SYSTEM1 = "00-50-04-1E-62-E0"  
    MACAddress @SYSTEM2 = "00-50-04-25-0E-C0"  
)  
  
Lanman IIS-Lanman (  
    VirtualName = VNAME  
    IPResName = IIS-IP  
)  
  
MountV IIS-MountV (  
    MountPath = "X:"  
    VolumeName = web  
    VMDGResName = IIS-VMDg  
    ForceUnmount = ALL  
)  
  
NIC IIS-NIC (  
    MACAddress @SYSTEM1 = "00-50-04-1E-62-E0"  
    MACAddress @SYSTEM2 = "00-50-04-25-0E-C0"  
)  
  
VMDg IIS-VMDg (  
    DiskGroupName = DG_1  
)  
  
IIS-W3SVC requires IIS-Lanman
```

IIS-W3SVC requires IIS-MountV
 IIS-SMTP requires IIS-Lanman
 IIS-SMTP requires IIS-MountV
 IIS-NNTP requires IIS-Lanman
 IIS-NNTP requires IIS-MountV
 IIS-IP requires IIS-NIC
 IIS-Lanman requires IIS-IP
 IIS-MountV requires IIS-VMDg

Sample configuration II

In the following configuration the IIS Web site is located in a shared disk group, which is configured using the VMDg resource type.

Figure 6-3 IIS service group dependency graph



A MountV resource configures a drive letter for the shared disk group. The virtual name and IP address for the IIS resource are configured using the Lanman and IP resource types respectively. The application pools associated with the Web site are configured as separate resources of type IIS.

Sample main.cf file

```
IIS IIS-W3SVC (  
    SiteType = W3SVC  
    SiteName = "My Site"  
    AppPoolMon = DEFAULT  
    DetailMonitor = 1  
    IPResName = IIS-IP  
)  
  
IIS IIS-APPPPOOL (  
    SiteType = APPPOOL  
    SiteName = DefaultAppPool  
)  
  
IIS IIS-APPPPOOL_GB (  
    SiteType = APPPOOL  
    SiteName = GuestBook  
)  
  
IP IIS-IP (  
    Address = "10.182.145.223"  
    SubNetMask = "255.255.252.0"  
    MACAddress @SYSTEM1 = "00-50-04-1E-62-E0"  
    MACAddress @SYSTEM2 = "00-50-04-25-0E-C0"  
)  
  
Lanman IIS-Lanman (  
    VirtualName = VNAME  
    IPResName = IIS-IP  
)  
  
MountV IIS-MountV (  
    MountPath = "X:"  
    VolumeName = web  
    VMDGResName = IIS-VMDg  
    ForceUnmount = ALL  
)  
  
NIC IIS-NIC (  
    MACAddress @SYSTEM1 = "00-50-04-1E-62-E0"  
    MACAddress @SYSTEM2 = "00-50-04-25-0E-C0"  
)  
  
VMDg IIS-VMDg (  
    DiskGroupName = DG_1  
)  
  
IIS-W3SVC requires IIS-Lanman  
IIS-W3SVC requires IIS-MountV  
IIS-IP requires IIS-NIC  
IIS-Lanman requires IIS-IP  
IIS-MountV requires IIS-VMDg
```

IIS-APPPPOOL requires IIS-W3SVC
IIS-APPPPOOL_GB requires IIS-W3SVC

GenericService agent

The GenericService agent brings services online, takes them offline, and monitors their status. Note that a service is an application type supported by Windows that conforms to the interface rules of the Service Control Manager (SCM).

Services are defined as resources of type GenericService. You can configure the GenericService agent to monitor multiple services by defining a resource for each service to be monitored. You can monitor a service in a user-context by specifying the user name, password, and domain. You can start and monitor services in the virtual computer context by enabling the UseVirtualName attribute. Configure a service group for GenericService agent using the Application Configuration wizard, described in the *Veritas Cluster Server Administrator's Guide*.

Note: The service to be configured using the GenericService agent must have the status as Stopped and the startup type as Manual.

Agent functions (Entry Points)

- **online**—Starts the configured service.
- **offline**—Stops the configured service.
- **monitor**—Retrieves the current state of the configured service. It also verifies the user context, if applicable.

State definitions

- **ONLINE**—Indicates the service being monitored is online.
- **OFFLINE**—Indicates the service being monitored is offline.
- **UNKNOWN**—Indicates the service operation is in a pending state, or that the agent could not determine the state of the resource.

Resource type definition

```

type GenericService (
    static i18nstr ArgList[] = {ServiceName, DelayAfterOnline,
    DelayAfterOffline, UserAccount, Password,
    Domain, service_arg, UserVirtualName, "LanmanResName:VirtualName" }
    i18nstr ServiceName
    int DelayAfterOnline = 10
    int DelayAfterOffline = 10
    i18nstr UserAccount
    str Password
    i18nstr Domain
    str service_arg[]
    boolean UseVirtualName
    str LanmanResName
)
    
```

Attribute definitions

Table 6-5 GenericService agent required attributes

Required Attribute	Type and Dimension	Description
ServiceName	string-scalar	Name of the service to be monitored. The service name can be the Service Display Name or the Service Key Name. Note: This attribute can take localized values.

Table 6-6 GenericService agent optional attributes

Optional Attributes	Type and Dimension	Description
DelayAfterOffline	integer-scalar	Number of seconds the offline routine waits for the service to go offline. Default is 10 seconds.
DelayAfterOnline	integer-scalar	Number of seconds the online routine waits for the service to go online. Default is 10 seconds.
Domain	string-scalar	The domain name to which the user specified in the UserAccount attribute belongs. Note: This attribute can take localized values.

Table 6-6 GenericService agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
Password	string-scalar	The password of the user, in whose context, the service would be started. If the UserAccount attribute is empty or contains a built-in service account, this attribute is ignored.
service_arg	string-vector	An array of arguments passed to the service.
UserAccount	string-scalar	<p>A valid user account in whose context the service will be monitored. Username can be of the form username@domain.com or domain.com\username.</p> <p>If you do not specify a value for this attribute, then the user account of the service in the SCM is ignored. To monitor service under built-in accounts, you must provide explicit values. For example:</p> <ul style="list-style-type: none"> ■ On Windows 2000: UserAccount='LocalSystem' ■ On Windows 2003: UserAccount='LocalSystem', 'Local Service', or 'Network Service'. Domain='NT Authority'. <p>The 'NT Authority' domain is not applicable for the 'LocalSystem' account.</p> <p>Note: This attribute can take localized values.</p>
UseVirtualName	boolean-scalar	<p>Set this value to enable the service specified by the ServiceName attribute to inherit the Virtual Server context of Lanman resource specified in LanmanResName attribute. If this attribute is set, the LanmanResName becomes a mandatory attribute.</p> <p>Note: It is recommended that you do not set this attribute for system services. If you configure system services using the GenericService agent, then this attribute is not supported.</p>

Table 6-6 GenericService agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
LanmanResName	string-scalar	The name of the Lanman resource on which the GenericService resource depends. Note: It is recommended that you do not set this attribute for system services. If you configure system services using the GenericService agent, then this attribute is not supported.

Sample configuration

```
GenericService Telephony_Service (  
  ServiceName = "Telephony Service"  
  DelayAfterOnline = 10  
  DelayAfterOffline = 10  
  UserAccount = Administrator  
  Password = bphNepE  
  Domain = VCS-DOMAIN  
  service_arg = { 3 }  
)
```

ServiceMonitor agent

The ServiceMonitor agent monitors a service or starts a user-defined script and interprets the exit code of the script. A service is an application type supported by Windows that conforms to the interface rules of the SCM. The agent can be configured to monitor a service using the Service Control Manager (SCM) or through a user-defined script.

When configured to monitor using the SCM, the agent queries the SCM database for the status of the service. When configured to monitor using a script or an executable, the agent executes the script on each system in the cluster, once every monitor cycle. The agent returns `ONLINE`, `OFFLINE`, or `UNKNOWN` depending on the exit code of the script. The exit code must conform to VCS standards. Refer to chapter on agent entry points in the *Veritas Cluster Server Agent Developer's Guide* for details.

You can monitor a service or run a script in a user-context by specifying the user name, password, and domain. Configure a service group for ServiceMonitor agent using the Application Configuration wizard, described in the *Veritas Cluster Server Administrator's Guide*.

Note: The ServiceMonitor resource cannot be made dependent on other resources.

Agent functions (Entry Points)

- `online`—Not applicable.
- `offline`—Not applicable.
- `monitor`—If the agent is configured to monitor a service, the agent queries the SCM for the status of the service. If the agent is configured to start a script, the agent spawns the specified script and interprets the exit code of the script.

State definitions

- `ONLINE`—Indicates the specified service is running, or that the configured script returned an online exit code.
- `FAULTED`—Indicates the specified service is not running, or that the configured script returned an offline exit code.
- `UNKNOWN`—Indicates the agent could not determine the state of the resource.

Resource type definition

```
type ServiceMonitor (
    static i18nstr ArgList[] = {MonitorService, ServiceOrScriptName,
    MonitorProgTimeout, UserAccount,
    Password, Domain }
    boolean MonitorService = 1
    i18nstr ServiceOrScriptName
    int MonitorProgTimeout = 30
    i18nstr UserAccount
    str Password
    i18nstr Domain
)
```

Attribute definitions

Table 6-7 ServiceMonitor agent required attributes

Required Attribute	Type and Dimension	Description
ServiceOrScriptName	string-scalar	<p>The name of the service to be monitored or script to be spawned for monitoring the service. You must specify the complete path of the script, including any command-line arguments. This attribute can take localized values.</p> <p>Note: The exit code of the script must conform to VCS conventions: 110 for <code>ONLINE</code> and 100 for <code>OFFLINE</code>. For exit values outside the range 100-110, the status is considered <code>UNKNOWN</code>. Refer to the <i>Veritas Cluster Server Agent Developer's Guide</i> for more information.</p>

Table 6-8 ServiceMonitor agent optional attributes

Optional Attributes	Type and Dimension	Description
Domain	string-scalar	<p>The domain to which the user belongs, as specified by the attribute <code>UserAccount</code>. If the domain name is not specified, the agent assumes the user to belong to the local machine.</p> <p>Note: This attribute can take localized values.</p>
MonitorProgTimeout	integer-scalar	<p>The maximum wait time, in seconds, for the agent to receive a return value from the monitor script. This attribute is ignored if the <code>MonitorService</code> flag is set to 1. Default is 30 seconds.</p>
MonitorService	boolean-scalar	<p>A flag that defines whether the agent monitors a service or starts a script. If the flag is set to 1, the agent monitors a service specified by the attribute <code>ServiceOrScriptName</code>. If the flag is set to 0 the agent starts a script specified by the attribute <code>ServiceOrScriptName</code>. Default is 1.</p>

Table 6-8 ServiceMonitor agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
Password	string-scalar	<p>The password for the user account, encrypted using the VCS Encrypt utility. This attribute is valid only if the MonitorService is set to 0 and UserAccount is not empty.</p> <p>For more information about the VCS Encrypt utility, see the <i>Veritas Cluster Server Administrator's Guide</i>.</p>
UserAccount	string-scalar	<p>A valid user account in whose context the service will be monitored. Username can be of the form <i>username@domain.com</i> or <i>domain.com\username</i>.</p> <p>If you do not specify a value for this attribute, then the user account of the service in the SCM is ignored. To monitor service under built-in accounts, you must provide explicit values. For example:</p> <ul style="list-style-type: none"> ■ On Windows 2000: UserAccount="LocalSystem" ■ On Windows 2003: User Account="LocalSystem", "Local Service", or "Network Service". Domain="NT Authority". The 'NT Authority' domain is not applicable for the 'LocalSystem' account. <p>Note: This attribute can take localized values.</p>

Sample configurations

In the following example, the ServiceMonitor agent is configured to spawn a script and interpret the script's exit code.

```
ServiceMonitor ScriptBasedMonitor (  
  MonitorService = 0  
  ServiceOrScriptName = "C:\\Programs\\monitor-script.bat"  
  MonitorProgTimeout = 15  
)
```

In the next example, the agent is configured to monitor a service.

```
ServiceMonitor Telephony_Service (  
  MonitorService = 1  
  ServiceOrScriptName = "Telephony Service"  
  UserAccount = Administrator  
  Password = bphNepE  
  Domain = VCS-DOMAIN7  
)
```

Note: While monitoring a service, the Password attribute is ignored.

Process agent

The Process agent brings processes online, takes them offline, and monitors their status. You can specify different executables for each process routine. By default, processes are monitored in the context of the LocalSystem account. You can run a process with user privileges by specifying the user name, password, and domain. Configure a service group for Process agent using the Application Configuration wizard, described in the *Veritas Cluster Server Administrator's Guide*.

Agent functions (Entry Points)

- **online**—Starts the process configured as the start program.
- **offline**—Terminates the process, or starts the process configured as the stop program.
- **monitor**—Verifies the status of the process, or starts the process configured as the monitor program.

State definitions

- **ONLINE**—Indicates the process being monitored is running properly.
- **OFFLINE**—Indicates the process being monitored is not running properly.
- **UNKNOWN**—Indicates the agent could not determine the status of the resource.

Resource type definition

```

type Process (
    static i18nstr ArgList[] = {StartProgram, StopProgram,
    MonitorProgram, UserName, Password,
    Domain, MonitorProgramTimeout,
    InteractWithDesktop, CleanProgram, StartupDirectory,
    StopProgramTimeout, CleanProgramTimeout }
    i18nstr StartProgram
    i18nstr StartupDirectory
    i18nstr StopProgram
    i18nstr CleanProgram
    i18nstr MonitorProgram
    i18nstr UserName
    str Password
    i18nstr Domain
    int MonitorProgramTimeout = 30
    boolean InteractWithDesktop = 0
    int StopProgramTimeout = 30
    int CleanProgramTimeout = 30
)
    
```

Attribute definitions

Table 6-9 Process agent required attributes

Required Attribute	Type and Dimension	Description
StartProgram	string-scalar	<p>The process to be monitored by the agent. You must specify the complete path of the executable, its file extension, and command-line arguments, if any. If you define the start program as a batch file or a script to launch another program, you must specify the monitor program in the configuration file.</p> <p>If you define the start program as a script (a perl script, or a vbs script), the start program should be the program that interprets the script (perl.exe, or cscript.exe) and the script itself should be passed as an argument.</p> <p>Note: This attribute can take localized values.</p>

Table 6-10 Process agent optional attributes

Optional Attributes	Type and Dimension	Description
CleanProgram	string-scalar	<p>The full path of the clean process that is launched when the resource needs a forceful offline. If no value is specified for this attribute, for a clean operation the agent kills the process indicated by the StartProgram attribute.</p> <p>Note: This attribute can take localized values.</p>
CleanProgramTimeout	integer-scalar	<p>The maximum time, in seconds, that the agent must wait before killing the process specified in the CleanProgram attribute.</p> <p>The default value is 30 seconds.</p>
Domain	string-scalar	<p>The domain in which the user specified by the attribute UserName exists. This attribute is ignored if the user name is not specified.</p> <p>Note: This attribute can take localized values.</p>
InteractWithDesktop	boolean-scalar	<p>A flag that defines whether the configured process interacts with the desktop. Enabling desktop interaction enables user intervention for the process. The value 1 indicates the process will interact with the desktop. The value 0 indicates it will not. Default is 0.</p>

Table 6-10 Process agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
MonitorProgram	string-scalar	<p>A program that monitors the process specified as the start program. You must specify the complete path of the executable, its file extension, and command-line arguments, if any. If you do not specify a value for this attribute, VCS monitors the start program. However, if the start program is a batch file or a script to launch another program, you must specify a monitor program.</p> <p>This attribute can take localized values.</p> <p>Note: The monitor program is spawned every monitor cycle and must return before the program specified in MonitorProgram times out. The return values for the monitor program must conform to VCS conventions: 110 for ONLINE and 100 for OFFLINE. For exit values outside the range 100-110, the status is considered UNKNOWN. Refer to the <i>VCS Agent Developer's Guide</i> for more information.</p>
MonitorProgramTimeout	integer-scalar	<p>The maximum wait time, in seconds, for the agent to receive a return value from the monitor routine. This attribute is ignored if the monitor program is not specified. Default is 30 seconds.</p>
Password	string-scalar	<p>The encrypted password of the user specified by the UserName. Note that the password must be encrypted using the VCSEncrypt utility. See the <i>VCS Administrator's Guide</i> for more information about the utility.</p> <p>This attribute is ignored if the user name is not specified.</p>
StartupDirectory	string-scalar	<p>The startup directory for the process indicated by the StartProgram attribute.</p> <p>Note: This attribute can take localized values.</p>

Table 6-10 Process agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
StopProgram	string-scalar	<p>A program that stops the process specified as the start program. You must specify the complete path of the program, its file extension, and command-line arguments, if any. If you do not specify a value for this attribute, VCS stops the start program.</p> <p>This attribute can take localized values.</p> <p>Note: If successful, the StopProgram returns a positive value. The agent framework calls the Monitor routine after those many seconds, as returned by StopProgram. Also, while writing a stop program, make sure to stop all the processes launched by the start program.</p>
StopProgramTimeout	integer-scalar	<p>The maximum time, in seconds, that the agent must wait before killing the process specified in the StopProgram attribute.</p> <p>The default value is 30 seconds.</p>
UserName	string-scalar	<p>The user name in whose context the configured process executes. Username can be of the form <code>username@domain.com</code> or <code>domain.com\username</code>.</p> <p>If a user name is not specified, the configured process runs in the context of the user account used by HAD.</p> <p>Note: This attribute can take localized values.</p>

Note: When defining the StartProgram, StopProgram, or MonitorProgram attributes, enclose the path of the executable file in double quotes. Do not enclose arguments in double quotes.

Sample configuration

Sample 1

In the following configuration, the online entry point spawns the executable `test.exe` with `online` as a command-line argument. The `offline` entry point spawns the executable `test.exe` with `offline` as the command-line argument. The `monitor` entry point monitors the attribute value for `StartProgram`, `test.exe`, and checks the state.

```
Process Process_Test (
    StartProgram = "\"X:\\bin\\test.exe\" /online"
    StopProgram = "\"X:\\bin\\test.exe\" /offline"
    UserName = "Administrator"
    Password = bphNepE
    Domain = "VCS_DOMAIN"
)
```

Sample 2

In the following configuration, the batch file `start.bat` starts an instance, `MyProcess`, of the executable `process.exe`. The batch file `stop.bat` stops the process instance of `process.exe`. The batch file `monitor.bat` monitors the attribute value for `StartProgram`, and checks the state of the `process.exe`. Note that the executable `process.exe` resides in the directory `C:\\batchfiles`, which is specified as the `StartupDirectory`.

```
PROCESS-Process_SG (
    StartProgram = "C:\\batchfiles\\start.bat MyProcess"
    StartupDirectory = "C:\\batchfiles"
    StopProgram = "C:\\batchfiles\\stop.bat MyProcess"
    MonitorProgram = "C:\\batchfiles\\monitor.bat MyProcess"
    UserName = Administrator
    Password = jxpVmxM
    Domain = "mydomain.mycompany.com"
)
```

MSMQ agent

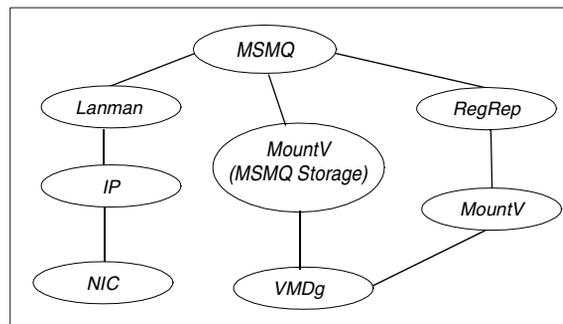
The MSMQ agent is a bundled agent that works with the Microsoft Message Queuing (MSMQ) service. The MSMQ agent creates an MSMQ service for an MSMQ resource, brings the service online, takes it offline, and monitors its status. The agent provides high availability for the MSMQ service and the queues hosted by the service, in a clustered environment.

You can configure an MSMQ resource using the command line. See the *Veritas Cluster Server Administrator's Guide* for instructions.

Dependencies

The MSMQ agent depends on the MountV, Lanman, and the Registry Replication agents for operation. The MSMQ resource starts after each of these resources is brought online. The following figure illustrates the agent's dependency graph.

Figure 6-4 MSMQ agent dependency graph



Agent functions (Entry Points)

- online—Starts the MSMQ service.
- offline—Stops the MSMQ service.
- monitor—Verifies that the MSMQ service is running.

State definitions

- ONLINE—Indicates that the MSMQ service is running properly.
- OFFLINE—Indicates that the MSMQ service has stopped.
- UNKNOWN—Indicates that the agent could not determine the status of the MSMQ service.

Resource type definition

```

type MSMQ (
    static i18nstr ArgList[] ={"IPResName:Address",
                              "LanmanResName:VirtualName",
                              "MountResName:MountPath",
                              StoragePath, DetailMonitor }

    str IPResName
    str LanmanResName
    str MountResName
    i18nstr StoragePath
    boolean DetailMonitor = 0
)

```

Attribute definitions

Table 6-11 MSMQ agent required attributes

Required Attribute	Type and Dimension	Description
IPResName	string-scalar	The name of the IP resource. Configure the IP resource to provide a virtual IP binding for the MSMQ service. Note: Every time you make changes to this attribute, you must disable the MSMQ resource and enable it again.
LanmanResName	string-scalar	The name of the Lanman resource. MSMQ uses the virtual name configured in the specified Lanman resource to set the virtual environment for the MSMQ service.
MountResName	string-scalar	The name of the MountV resource. Configure the MountV resource to monitor the volume on which the MSMQ service stores it queue related data.
StoragePath	string-scalar	The root storage path of the MSMQ service. Note: This attribute can take localized values.
DetailMonitor	boolean-scalar	Used to enable detail monitoring for the MSMQ service.

Sample configuration

The following configuration creates the MSMQ resource with the required Lanman, MountV, and the RegRep resources.

```
MSMQ test (  
  IPResName=msmqip  
  LanmanResName=msmqLanman  
  MountResName=msmqMountV  
  StoragePath=\\msmqStorage  
)
```


VCS infrastructure and support agents

The VCS infrastructure and support agents provide high availability for VCS-related operations. You can use some of these agents to test VCS functionality.

- NotifierMngr agent—Monitors a notifier process.
- RegRep Agent—Replicates the system registry.
- VRTSWebApp Agent—Monitors the Veritas Web consoles.
- Proxy Agent—Monitors the state of a resource on a local or remote system.
- Phantom Agent—Enables VCS to determine the status of parallel service groups that do not include OnOff resources.
- ElifNone Agent—Monitors a file.
- FileNone Agent—Monitors a file.
- FileOnOff Agent—Monitors a file.
- FileOnOnly Agent—Monitors a file.
- RemoteGroup Agent—Monitors and manages service groups in a remote cluster.

NotifierMngr agent

The NotifierMngr agent starts, stops, and monitors a notifier process, making it highly available. The notifier process manages the reception of messages from VCS and Global Cluster Manager (GCM) and the delivery of the messages to SNMP consoles and SMTP servers. VCS can send notification to SNMP console and SMTP servers. See the *Veritas Cluster Server Administrator's Guide* for a description of types of events that generate notification. The agent is represented by the NotifierMngr resource type. Note that only one instance of the notifier process can run in a cluster. Therefore, a notifier process cannot run in a parallel service group.

Note: The attributes of the NotifierMngr agent cannot be changed dynamically using the `hares -modify` command. Changes made using this command are effective after notifier is restarted.

Agent functions (Entry Points)

- `online`—Starts the notifier process with its required arguments.
- `offline`—Stops the notifier process.
- `monitor`—Monitors the notifier process.

State definitions

- `ONLINE`—Indicates the notifier process is running.
- `OFFLINE`—Indicates the notifier process is not running.
- `UNKNOWN`—Indicates the agent encountered errors while monitoring the NotifierMgr resource.

Resource type definition

```

type NotifierMngr (
    static i18nstr ArgList[] = {MessageQueue, NotifierListeningPort,
    SnmpdTrapPort, SnmpCommunity,
    SnmpConsoles, SmtServer,
    SmtServerVrfyOff, SmtServerTimeout,
    SmtReturnPath, SmtFromPath,
    SmtRecipients }
    int MessageQueue = 30
    int NotifierListeningPort = 14144
    int SnmpdTrapPort = 162
    str SnmpCommunity = public
    str SnmpConsoles{}
    str SmtServer
    int SmtServerTimeout
    str SmtReturnPath
    str SmtFromPath
    str SmtRecipients{}
    boolean SmtServerVrfyOff
)

```

Attribute definitions

Table 7-1 NotifierMngr agent required attributes

Required Attributes	Type and Dimension	Description
SnmpConsoles	string-association	The system name of the SNMP manager and the severity level of the messages to be delivered to the SNMP manager. The severity levels of messages are Information, Warning (default), Error, and SevereError. Specifying a severity level for messages generates delivery of all messages of equal or higher severity. For example, "172.29.10.89"=Error, "172.29.10.56"=Information
SmtServer	string-scalar	The system name of the SMTP server.

Table 7-2 NotifierMngr agent optional attributes

Optional Attributes	Type and Dimension	Description
MessageQueue	integer-scalar	Size of the VCS engine's message queue size. Default is 30 messages.
NotifierListeningPort	integer-scalar	Any valid, unused TCP/IP port number. Default is 14144.
SnmptdTrapPort	integer-scalar	The port on which SNMP trap PDUs are sent. The value specified for this attribute is used for all consoles if more than one SNMP console is specified. Default is 162.
SnmCommunity	string-scalar	The community ID for the SNMP manager. Default is "public."
SmtpFromPath	string	This attribute must be set to a valid email address, if a custom email address is desired for the FROM: field in the email sent by notifier.
SmtpRecipients	string-association	<p>The email address to which information is sent and the severity level of the messages to be received. The severity levels of messages are Information, Warning (default), Error, and SevereError. Specifying a severity level for messages indicates that all messages of equal or higher severity are received.</p> <p>For example,</p> <p>"james@veritas.com"=SevereError "admin@veritas.com"=Warning</p> <p>Note: SmtpReceipients is a required attribute if SmtpServer is specified.</p>
SmtpReturnPath	string	<p>This attribute must be set to a valid email address, if a custom email address is desired for the Return-Path: field in the email sent by notifier.</p> <p>Note: If the mail server specified in the SmtpServer does not support VRFY, then you need to set the SmtpServerVrfyOff to 1 in order for the SmtpReturnPath to come into effect.</p>

Table 7-2 NotifierMngr agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
SmtpServerTimeout	integer	This attribute represents the time, in seconds, for which the notifier waits for a response from the mail server for the SMTP commands sent to the mail server. Increase the specified value if the mail server takes long to send response for the SMTP commands sent by the notifier. Default is 10.
SmtpServerVrfyOff	boolean	Setting this value to 1 results in notifier not sending a SMTP VRFY request to the mail server specified in SmptServer attribute, while sending emails. Set this to 1 if your mail server does not support SMTP VRFY command. Default is 0.

Sample configuration

The NotifierMngr resource sets up notification for all events to the SnmpConsole, `your_console`. In the following example, only messages of SevereError level are sent to the SmtServer, "`smtp.your_company.com`," and the recipient, "`vcadmin@your_company.com`."

Note: Because only one instance of the notifier process can run in a cluster, the process cannot run in a parallel group.

```
IP csg_ip (
  Address = "10.212.100.14"
  SubNetMask = "255.255.254.0"
  MACAddress @SYSTEM1 = "00:B0:D0:D1:69:7D"
  MACAddress @SYSTEM2 = "00:B0:D0:AB:4E:22"
)

NIC csg_nic (
  MACAddress @SYSTEM1 = "00:B0:D0:D1:69:7D"
  MACAddress @SYSTEM2 = "00:B0:D0:AB:4E:22"
)

NotifierMngr ntfr(
  SnmpConsoles = { your_console = Information }
  SmtServer = "smtp.your_company.com"
  SmtRecipients = { "vcadmin@your_company.com" = Information
}
)

csg_ip requires csg_nic
ntfr requires csg_nic
```

Registry Replication (RegRep) agent

To ensure efficient failover of an application, the registry of the node on which the application was taken offline and the registry of the node on which the application is brought online must be synchronized.

The Registry Replication agent synchronizes the registry of both the nodes by monitoring the designated registry keys. When an application changes the registry keys on the active cluster node, the agent logs these changes to the shared disk. When failover occurs, the agent updates the registry of the system on which the application is brought online using the logs on the shared disk. The RegRep agent provides you the option to:

- exclude certain subkeys from being replicated.
- mark keys for replication or exclusion, even though they do not exist when the agent is configured.
- mark keys for replication or exclusion dynamically, even when the resource is online.

When the Registry Replication agent is started, it forks an independent process to monitor registry changes. Even if the VCS engine, HAD, dies, the process continues logging registry changes to the shared disk.

If you wish to replicate the registry of an application running on a node outside VCS, run the utility VCSRegUtil on that particular node. See the *Veritas Cluster Server Administrator's Guide* for more information on VCSRegUtil utility.

Note: The Registry Replication agent runs in the context of the local system user while the HKEY_CURRENT_USER (HKCU) hive has values in the context of the current user. Because the local system user account does not map to a current user account, the Registry Replication agent does not replicate the keys under the HKCU hive.

Dependency

The RegRep agent depends on the MountV agent.

Agent functions (Entry Points)

- online—Starts logging changes to specified registry keys to the shared disk.
- offline—Stops logging changes to specified registry keys to the shared disk.
- monitor—Verifies that the process that logs changes to registry keys is running.

State definitions

- **ONLINE**—Indicates the agent is logging changes to specified registry keys to the shared disk.
- **OFFLINE**—Indicates the agent is not logging changes to specified registry keys to the shared disk.
- **UNKNOWN**—Indicates the agent could not determine the status of the resource.

Note: The Registry Replication agent is for failover service groups only. Do *not* use the agent for parallel applications or service groups.

Resource type definition

```
type RegRep (
    static i18nstr ArgList[] = {"MountResName:MountPath",

    ReplicationDirectory, Keys, ExcludeKeys,

    ListOpenKeys, ForceRestore,

    RestoreLocally, DebugMonitor }
    str MountResName
    i18nstr ReplicationDirectory = "\\REGREP\\DEFAULT"
    i18nstr Keys{}
    i18nstr ExcludeKeys[]
    boolean ListOpenKeys = 1
    boolean ForceRestore = 1
    boolean RestoreLocally = 0
    int DebugMonitor = 1
)
```

Attribute definitions

Table 7-3 RegRep agent required attributes

Required Attributes	Type and Dimension	Description
Keys	string-association	<p>The list of registry keys to be monitored. From the 'name-value' pair of a registry key, you must provide the name of the registry keys to be synchronized and not the value for that key.</p> <p>When defining the keys, you must use the abbreviations listed in “Configuring registry keys” on page 126.</p> <p>The agent also enables you to replicate a registry key without replicating the subkeys. See “Ignoring subkeys” on page 127 for instructions.</p> <p>This attribute can take localized values.</p> <hr/> <p>Warning: Do not configure more than 63 keys for a single RegRep resource otherwise the resource will go in an UNKNOWN state.</p> <hr/>
MountResName	string-scalar	<p>The name of the MountV resource on which the Registry Replication agent depends. The MountV resource specifies the mount drive on the shared disk where the log file is created.</p>
ReplicationDirectory	string-scalar	<p>The directory on the shared disk in which the registry changes are logged. The agent creates a directory with the specified name if one does not exist. Default is "\\REGREP\DEFAULT".</p> <p>Note: This attribute can take localized values.</p>

Table 7-4 RegRep agent optional attributes

Optional Attributes	Type and Dimension	Description
DebugMonitor	integer-scalar	<p>A flag that defines whether debug logging is to be enabled for the executable (RegRepMonitor.exe) that monitors the registry keys. The value 0 indicates that the logging is enabled. The value 1 indicates that it is not. Default is 1.</p>
ExcludeKeys	string-vector	<p>A list of the subkeys to be excluded from replication. For more information on how the agent excludes keys, see “Excluding keys” on page 126. When defining the keys, you must use the abbreviations listed in “Configuring registry keys” on page 126.</p> <p>Note: This attribute can take localized values.</p>
ForceRestore	boolean-scalar	<p>A flag that defines the agent behavior when the registry update fails on a node where the resource is being brought online. A registry update may fail if any of the keys being updated are open.</p> <p>If the flag is set to 1 and the registry update fails, the agent tries to forcibly restore the keys by:</p> <ul style="list-style-type: none"> ■ backing up the configured registry keys of the node being brought online. ■ deleting the configured registry keys from the node being brought online. ■ updating the configured registry keys with the changed values. <p>If the update fails again, the agent reapplies the original values of the registry keys from the backup.</p> <p>If the flag is set to 0, the agent does not try to forcibly update the registry when an update fails. Default is 0.</p>

Table 7-4 RegRep agent optional attributes (continued)

Optional Attributes	Type and Dimension	Description
ListOpenKeys	boolean-scalar	A flag that defines whether the agent lists a set of registry keys, including keys having open handles, when a registry update fails. The list is logged to the agent log. The value 1 indicates the agent lists the registry key set. The value 0 indicates the agent does not. Default is 1.
RestoreLocally	boolean-scalar	A flag that defines whether the agent restores the keys on the node if it was taken offline from the same node. For example, if the agent was taken offline from SystemA and brought online again on SystemA, the flag determines whether the registry keys would be restored on SystemA. The value 1 indicates the agent restores the keys on the system. The value 0 indicates it does not. Default is 0.

Excluding keys

This section describes the algorithm the Registry Replication agent uses while excluding keys. For example, assume a registry key `KEY_X` has a subkey of `KEY_Y`, which has a subkey `KEY_Z`. This key would appear as `KEY_X\KEY_Y\KEY_Z` in the Registry Editor. [Table 7-5](#) describes various scenarios of keys marked for replication and for exclusion. The Result column describes the agent behavior in these scenarios.

Table 7-5 RegRep agent exclude keys and behavior

Keys for Replication	Exclude Keys	Result
KEY_X	KEY_Y\KEY_Z	KEY_Y is excluded. So is KEY_Z.
KEY_X	KEY_Y	KEY_Y is excluded. So is KEY_Z.
KEY_X	KEY_X	KEY_X is <i>not</i> excluded and an error message is logged.
KEY_X\KEY_Y	KEY_X	KEY_X is <i>not</i> excluded and an error message is logged.

Configuring registry keys

To configure a registry key to be replicated or excluded, use the abbreviation corresponding to the registry hive, as listed in [Table 7-6](#).

Table 7-6 RegRep agent registry hive

Registry Hive	Abbreviation
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_CURRENT_CONFIG	HKCC
HKEY_CLASSES_ROOT	HKCR

Ignoring subkeys

Use the IgnoreSubKeys option for the Keys attribute to prevent the RegistryReplication agent from replicating the subkeys. [Table 7-7](#) describes possible combination of values for the Keys attribute. The Result column describes the agent behavior in these scenarios:

Table 7-7 RegRep agent IgnoreSubKeys and behavior

Value Specified for “Keys” Attribute	Result
"HKLM\SOFTWARE\VERITAS\VCS"	Replicates the subkeys
"HKLM\SOFTWARE\VERITAS\VCS"=IgnoreSubKeys	Does not replicate the subkeys
"HKLM\SOFTWARE\VERITAS\VCS"=IgnoreSubKeys:Yes	Does not replicate the subkeys
"HKLM\SOFTWARE\VERITAS\VCS"=IgnoreSubKeys:No	Replicates the subkeys
"HKLM\SOFTWARE\VERITAS\VCS"=<any other value>	Replicates the subkeys

Additional considerations for using IgnoreSubKeys

Symantec recommends not to set the "IgnoreSubKeys" value when the RegRep resource is online. Even if the value is set with the resource online, the changes will be applicable after the next online routine.

Sample configuration

In the following sample configuration, the Registry Replication agent is configured to replicate the print spooler registry key.

```
IP IP-10-212-100-184 (
  Address = "10.212.100.184"
  SubNetMask = "255.255.254.0"
  MACAddress @SYSTEM1 = "00-02-B3-AD-CB-D0"
  MACAddress @SYSTEM2 = "00-02-B3-AD-CE-E4"
)

Lanman Lanman-PRINTSHAREMAN (
  VirtualName = PRINTSHAREMAN
  IPResName = IP-10-212-100-184
  ADCriticalForOnline = 1
)

MountV MountV-JDrive (
  MountPath = "J:"
  VolumeName = PS-SPOOL
  VMDGResName = VMDg-PRINTSHARE_DG
)
```

```
MountV MountV-IDrive (
  MountPath = "I:"
  VolumeName = PS-REGREP
  VMDGResName = VMDg-PRINTSHARE_DG
)
NIC NIC-PRINSHARE-SG (
  MACAddress @SYSTEM1 = "00-02-B3-AD-CB-D0"
  MACAddress @SYSTEM2 = "00-02-B3-AD-CE-E4"
)

PrintShare PSShare (
  PrinterName = "HP LaserJet 4050 Series PCL"
  ShareName = "HP LaserJet 4050 Series PCL"
  LanmanResName = Lanman-PRINTSHAREMAN
)

PrintSpool PSSpool (
  LanmanResName = Lanman-PRINTSHAREMAN
  IPResName = IP-10-212-100-184
  MountResName = MountV-JDrive
  SpoolDir = "\\SPOOLER"
)

RegRep RegRep (
  MountResName = MountV-IDrive
  ReplicationDirectory = "\\PS-REGREP"
  Keys = {"HKLM\\Software\\ Veritas\\VCS\\BundledAgents
\\PrintSpool
          \\PSSpool" }
)

ServiceMonitor ServiceMonitor-PrintSpooler (
  ServiceOrScriptName = "Print Spooler"
)

VMDg VMDg-PRINTSHARE_DG (
  DiskGroupName = PRINTSHARE_DG
)

IP-10-212-100-184 requires NIC-PRINSHARE-SG
Lanman-PRINTSHAREMAN requires IP-10-212-100-184
MountV-JDrive requires VMDg-PRINTSHARE_DG
MountV-IDrive requires VMDg-PRINTSHARE_DG
PSShare requires PSSpool
PSSpool requires Lanman-PRINTSHAREMAN
PSSpool requires MountV-JDrive
PSSpool requires ServiceMonitor-PrintSpooler
PSSpool requires RegRep
RegRep requires MountV-IDrive
VNAME requires IP_A
```

VRTSWebApp agent

The VRTSWebApp agent brings Veritas Web applications online, takes them offline, and monitors their status. The application is a Java Web application conforming to the Servlet Specification 2.2 and runs inside of the Java Web server, which installed as a part of the VRTSweb package. This agent is used to monitor the Web Consoles of various Symantec products, such as VCS and VVR.

Dependency

The VRTSWebApp agent depends on the IP agent.

Agent functions (Entry Points)

- **Online**—Starts the Web application with the specified parameters. If the Web server is not already running, it will first start the server.
- **Offline**—Removes the Web application from the Web server. If no other Web application is running, it shuts down the Web server.
- **Monitor**—Checks if the specified Web application is currently running inside the Web server. If the application is running, monitor reports **ONLINE**. If the application is not running, monitor reports **OFFLINE**.
- **Clean**—Removes the Web application from the Web server. If no other Web application is running, it shuts down the Web server.

State definitions

- **ONLINE**—Indicates the web application is running inside the Web server.
- **OFFLINE**—Indicates the web application is not running inside the Web server.
- **UNKNOWN**—Indicates the agent could not determine the status of the resource.

Resource type definition

```
type VRTSWebApp (  
    static i18nstr ArgList[] = { AppName, InstallDir, TimeForOnline  
}  
    i18nstr AppName  
    i18nstr InstallDir  
    int TimeForOnline  
)
```

Attribute definitions

Table 7-8 VRTSWebApp agent required attributes

Required Attributes	Type and Dimension	Description
AppName	string-scalar	<p>Name of the application as it appears in the Web server.</p> <p>For example, for VCS, use <code>vcs</code>. Access the applications at: http://localhost:8181/vcs.</p> <p>Note: This attribute can take localized values.</p>
InstallDir	string-scalar	<p>Path to the Web application installation. The Web application must be installed as a <code>.war</code> file with the same name as the <code>AppName</code> parameter; the VCS application must be installed as <code>vcs.war</code>. This attribute should point to the directory that contains this <code>.war</code> file.</p> <p>For example, if <code>AppName</code> is <code>vcs</code> and <code>InstallDir</code> is <code>C:\Program Files\Veritas\</code>, the agent constructs the path for the Web application as <code>C:\Program Files\Veritas\vcs.war</code>.</p> <p>Note: This attribute can take localized values.</p>
TimeForOnline	integer-scalar	<p>The time the Web application takes to start after it is loaded into the Web server. This parameter is returned as the exit value of the online script, which inform VCS of the time it needs to wait before calling monitor routine on the Web application resource. Typically, this attribute is at least five seconds.</p>

Sample configuration

```
IP csg_ip (  
    Address = "10.212.100.14"  
    SubNetMask = "255.255.254.0"  
    MACAddress @SYSTEM1 = "00:B0:D0:D1:69:7D"  
    MACAddress @SYSTEM2 = "00:B0:D0:AB:4E:22"  
)  
  
NIC csg_nic (  
    MACAddress @SYSTEM1 = "00:B0:D0:D1:69:7D"  
    MACAddress @SYSTEM2 = "00:B0:D0:AB:4E:22"  
)  
  
VRTSWebApp VCSweb (  
    AppName = vcs  
    InstallDir @SYSTEM1 = "C:\Program  
Files\Veritas\VRTSweb\Veritas"  
    InstallDir @SYSTEM2 = "C:\Program  
Files\Veritas\VRTSweb\Veritas"  
    TimeForOnline = 5  
)  
  
csg_ip requires csg_nic  
VCSweb requires csg_ip
```

Proxy agent

The Proxy agent monitors and mirrors the state of a resource on a local or remote system. The agent can be used to reduce monitoring overheads in configurations where multiple resources point at the same physical device. For example, if multiple service groups use the same NIC, configure one service group to monitor the NIC and have Proxy resources in the other service groups to mirror the state of the NIC resource. The agent can also determine the status of an OnOff resource in a different service group.

Symantec recommends the use of Proxy agent to monitor persistent resources such as NIC, Service Monitor, ElifNone, and FileNone.

Agent functions (Entry Points)

- online—Not applicable.
- offline—Not applicable.
- monitor—Determines the status of the target resource.

State definitions

- ONLINE—Indicates the target resource is online.
- OFFLINE—Indicates the target resource is offline.

Resource type definition

```
type Proxy (  
    static il8nstr ArgList[] = {TargetResName, TargetSysName,  
  
    "TargetResName:Probed",  
  
    "TargetResName:State"}  
    static str Operations = None  
    str TargetResName  
    str TargetSysName  
)
```

Attribute definitions

Table 7-9 Proxy agent required attributes

Required Attribute	Type and Dimension	Description
TargetResName	string-scalar	The name of the target resource whose status is monitored and mirrored by the Proxy resource.

Table 7-10 Proxy agent optional attributes

Optional Attribute	Type and Dimension	Description
TargetSysName	string-scalar	The name of the system associated with the target resource. If this attribute is not specified, the Proxy resource assumes the system is local.

Sample configurations

```
group NicGrp (
    SystemList = { SYSTEM1, SYSTEM2 }
    Parallel = 1
)

Phantom my_phantom (
)

NIC NicGrp_public (
    MACAddress @SYSTEM1 = "00-50-04-24-F9-60"
    MACAddress @SYSTEM2 = "00-50-04-24-E3-30"
    UseConnectionStatus= True
)

group Grp1 (
    SystemList = { SYSTEM1,SYSTEM2 }
    AutoStartList = { SYSTEM1 }
)
NotifierMngr ntfmr(
    SnmpConsoles = { your_console = Information }
    SntpServer    = "smtp.your_company.com"
    SntpRecipients = { "vcsadmin@your_company.com" = Information
}
)

Proxy nicproxy (
    TargetResName="NicGrp_public"
)

ntfmr requires nicproxy
```

Phantom agent

The Phantom agent enables VCS to determine the status of parallel service groups that do not include OnOff resources (resources that VCS starts and stops as required.) The Phantom agent provides a “dummy” resource that can be brought online and taken offline. Without such a dummy resource, VCS cannot assess the status of service groups containing only None (Persistent) and OnOnly resources because the state of these resources is not considered in the process of determining whether a group is online.

Agent functions (Entry Points)

- online—Not applicable.
- offline—Not applicable.
- monitor—Determines status based on the status of its service group.

State definitions

- ONLINE—Indicates the service group is online.
- OFFLINE—Indicates the service group is offline.

Attribute definitions

Not applicable.

Sample configuration

```
FileNone FILE_1 (  
    PathName = "C:\\Temp\\file1"  
)  
  
FileOnOnly FILE_2 (  
    PathName = "C:\\Temp\\file2"  
)  
  
ElifNone FILE_3 (  
    PathName = "C:\\Temp\\file3"  
)  
  
Phantom PHANTOM_1 (  
)
```

FileNone agent

The FileNone agent monitors a file. The monitor routine returns ONLINE if the specified file exists.

Agent functions (Entry Points)

- online—Not applicable.
- offline—Not applicable.
- monitor—Verifies that the specified file exists.

State definitions

- ONLINE—Indicates the specified file exists.
- FAULTED—Indicates the specified file does not exist.

Resource type definition

```
type FileNone (
    static i18nstr ArgList[] = { PathName }
    i18nstr PathName
)
```

Attribute definitions

Table 7-11 FileNone agent required attributes

Required Attributes	Type and Dimension	Description
PathName	string-scalar	The complete path of the file to be monitored. This attribute can take localized values.

Sample configuration

```
FileNone tmp_file01_txt (
    PathName = "C:\\tmp\\file01.txt"
)
```

ElifNone agent

The ElifNone agent monitors a file. The monitor routine returns ONLINE if the specified file does not exist.

Agent functions (Entry Points)

- online—Not applicable.
- offline—Not applicable.
- monitor—Verifies that the specified file exists.

State definitions

- ONLINE—Indicates the specified file does not exist.
- FAULTED—Indicates the specified file exists.

Resource type definition

```
ElifNone (
    static i18nstr ArgList[] = { PathName }
    i18nstr PathName
)
```

Attribute definitions

Table 7-12 ElifNone agent required attributes

Required Attributes	Type and Dimension	Description
PathName	string-scalar	The complete path of the file to be monitored. This attribute can take localized values.

Sample configuration

```
ElifNone tmp_file01_txt (
    PathName = "C:\\tmp\\file01.txt"
)
```

FileOnOff agent

The FileOnOff agent creates, removes, and monitors files.

Agent functions (Entry Points)

- **online**—Creates an empty file with the specified name if the file does not already exist.
- **offline**—Removes the specified file.
- **monitor**—Verifies that the specified file exists.

State definitions

- **ONLINE**—Indicates the specified file exists.
- **OFFLINE**—Indicates the specified file does not exist.

Resource type definition

```
type FileOnOff (
    static i18nstr ArgList[] = { PathName }
    i18nstr PathName
)
```

Attribute definitions

Table 7-13 FileOnOff agent required attributes

Required Attributes	Type and Dimension	Description
PathName	string-scalar	The complete path of the file to be monitored. This attribute can take localized values.

Sample configuration

```
FileOnOff tmp_file01_txt (
    PathName = "C:\\tmp\\file01.txt"
)
```

FileOnOnly agent

The FileOnOnly agent creates and monitors a file.

Agent functions (Entry Points)

- online—Creates the specified file.
- offline—Not applicable.
- monitor—Verifies that the specified file exists.

State definitions

- ONLINE—Indicates the specified file exists.
- FAULTED—Indicates the specified file does not exist.

Resource type definition

```

type FileOnOnly (
    static i18nstr ArgList[] = { PathName }
    i18nstr PathName
)

```

Attribute definitions

Table 7-14 FileOnOnly agent required attributes

Required Attributes	Type and Dimension	Description
PathName	string-scalar	The complete path of the file to be monitored. This attribute can take localized values.

Sample configuration

```

FileOnOnly tmp_file01_txt (
    PathName = "C:\\tmp\\file01.txt"
)

```

RemoteGroup agent

Use the RemoteGroup agent to monitor or manage service groups that exist in a remote cluster. The RemoteGroup agent establishes dependencies between applications that are configured on different VCS clusters. For example, you configure an Apache resource in a local cluster, and a MySQL service group in a remote cluster. In this example, the Apache resource depends on the MySQL service group. You can use the RemoteGroup agent to establish this dependency between the two service groups.

Some points about configuring the RemoteGroup resource are:

- For each remote service group that you want to monitor or manage, you must configure a corresponding RemoteGroup resource in the local cluster.
- Multiple RemoteGroup resources in a local cluster can manage corresponding multiple remote service groups in different remote clusters.
- You can include the RemoteGroup resource in any kind of resource or service group dependency tree.
- A combination of the state of the local service group and the state of the remote service group determines the state of the RemoteGroup resource.
- Global groups are not supported as remote service groups.

Dependency

As a best practice, establish a RemoteGroup resource dependency on a NIC resource. Symantec recommends that the RemoteGroup resource not be by itself in a service group.

Agent functions (Entry Points)

- **Online**—Depending on the ControlMode setting, this function brings the remote service group online. See “ControlMode” on page 144 for more information.
- **Offline**—Depending on the ControlMode setting, this function takes the remote service group offline. See “ControlMode” on page 144 for more information.
- **Monitor**—Monitors the state of the remote service group. The true state of the remote service group is monitored only on the online node in the local cluster. See “VCSysName” on page 143 for more information.
- **Clean**—Depending on the ControlMode setting, Clean takes the remote service group offline whenever the RemoteGroup resource faults. See “ControlMode” on page 144 for more information.

State definitions

- **ONLINE**—Indicates that the remote service group is either in an **ONLINE** or **PARTIAL** state.
- **OFFLINE**—Indicates that the remote service group is in an **OFFLINE** or **FAULTED** state. The true state of the remote service group is monitored only on the online node in the local cluster.
- **FAULTED**—Indicates that the remote service group has unexpectedly gone offline.
- **UNKNOWN**—Indicates that a problem exists either with the configuration or the ability of the RemoteGroup resource to determine the state of the remote service group.

Resource type definition

```
type RemoteGroup (  
    static int OnlineRetryLimit = 2  
    static int ToleranceLimit = 1  
    static i18nstr ArgList[] = { IPAddress, Port, Username,  
Password,  
    GroupName, VCSSysName, ControlMode, OfflineWaitTime,  
DomainType, BrokerIp }  
    str IPAddress  
    int Port = 14141  
    str Username  
    str Password  
    str GroupName  
    str VCSSysName  
    str ControlMode  
    int OfflineWaitTime  
    str DomainType  
    str BrokerIp  
)
```

Attribute definitions

Table 7-15 RemoteGroup agent required attributes

Required Attribute	Type and Dimension	Description
IPAddress	string-scalar	<p>The IP address or DNS name of a node in the remote cluster, with which the agent communicates to get the status of the remote service group. The IP address can be either physical or virtual.</p> <p>If the IP address is a virtual IP address, make sure that this virtual IP address is not configured as an IP resource in the remote service group that is to be monitored.</p> <p>Example: "www.example.com" or "11.183.12.214"</p>
Port	integer-scalar	<p>The port on the remote node with which the agent communicates. This is an optional attribute, unless the remote cluster listens on another port. The default value is 14141.</p>
Username	string-scalar	<p>This is the login user name for the remote cluster.</p> <p>When you set the ControlMode attribute to OnOff or OnlineOnly, the Username must have administrative privileges for the remote service group that you specify in the GroupName attribute.</p> <p>When you use the RemoteGroup Wizard to enter your username data, you need to enter your username and the domain name in separate fields. For a cluster that has the Symantec Product Authentication Service, you do not need to enter the domain name.</p> <p>Example: "jsmith@example.com"</p>

Table 7-15 RemoteGroup agent required attributes (continued)

Required Attribute	Type and Dimension	Description
Password	string-scalar	<p>This is the password that corresponds to the user that you specify in the Username attribute. You must encrypt the password using the VCS Encrypt utility. For more information about the VCS Encrypt utility, see the <i>VCS Administrator's Guide</i>.</p> <p>Do not use the vscencrypt utility when entering passwords from a configuration wizard or from the Cluster Management Console or the Cluster Manager (Java Console).</p>
GroupName	string-scalar	<p>The name of the service group on the remote cluster that you want the RemoteGroup agent to monitor or manage.</p> <p>Example: "DBGrp"</p>
VCSSysName	string-scalar	<p>You must set this attribute to either the VCS system name or the ANY value.</p> <ul style="list-style-type: none"> ■ ANY The RemoteGroup resource goes online if the remote service group is online on any node in the remote cluster. ■ VCSSysName Use the name of a VCS system in a remote cluster where you want the remote service group to be online when the RemoteGroup resource goes online. Use this to establish a one-to-one mapping between the nodes of the local and remote clusters. <p>Example: "vcssystem1" or "ANY"</p>

Table 7-15 RemoteGroup agent required attributes (continued)

Required Attribute	Type and Dimension	Description
ControlMode	string-scalar	<p>Select only one of these values to determine the mode of operation of the RemoteGroup resource: MonitorOnly, OnlineOnly, or OnOff.</p> <ul style="list-style-type: none"> ■ OnOff The RemoteGroup resource brings the remote service group online or takes it offline. When you set the VCSSysName attribute to ANY, the SysList attribute of the remote service group determines the node where the remote service group comes online. ■ MonitorOnly The RemoteGroup resource only monitors the state of the remote service group. The RemoteGroup resource cannot bring the remote service group online or take it offline. Make sure that you bring the remote service group online before you bring the RemoteGroup resource online. ■ OnlineOnly The RemoteGroup resource only brings the remote service group online. The RemoteGroup resource cannot take the remote service group offline. When you set the VCSSysName attribute to ANY, the SysList attribute of the remote service group determines the node where the remote service group comes online.

Table 7-16 RemoteGroup agent optional attributes

Optional Attribute	Type and Dimension	Description
OfflineWaitTime	integer-scalar	<p>The maximum expected time in seconds that the remote service group may take to go offline. VCS calls the Clean function for the RemoteGroup resource if the remote service group takes a longer time to offline than the time that you have specified for this attribute. The default value is 0.</p>

Table 7-16 RemoteGroup agent optional attributes (continued)

Optional Attribute	Type and Dimension	Description
DomainType	string-scalar	Enter the domain type information for the specified user. This is for a secure remote cluster only. For users who have the domain type unixpwd, you do not have to set this attribute. Example: "nis", "nisplus"
BrokerIp	string-scalar	For a secure remote cluster only, if the user needs the RemoteGroup agent to communicate to a specific authentication broker, then set this attribute. Enter the information for the specific authentication broker in the format "IP". Example: "128.11.295.51"
OnlineRetryLimit OnlineWaitLimit ToleranceLimit MonitorInterval AutoFailover	integer-scalar	In case of remote service groups that take a longer time to come online, Symantec recommends that you modify the default OnlineWaitLimit and OnlineRetryLimit attributes. If you expect the RemoteGroup agent to tolerate sudden offlines of the remote service group, then modify the ToleranceLimit attribute. See the <i>Veritas Cluster Server Administrator's Guide</i> for more information about these attributes.

About the ControlMode attribute

In the ControlMode attribute, you can use these values, depending on your needs: OnOff, MonitorOnly, and OnlineOnly.

OnOff

Select the OnOff value of this attribute when you want the RemoteGroup resource to manage the remote service group completely.

The username provided in the Username attribute should have administrator privileges for the service group on the remote cluster.

In case of one-to-one mapping, set the value of the AutoFailover attribute of the remote service group to 0. This avoids unnecessary onlining or offlining of the remote service group.

MonitorOnly

Select the MonitorOnly value of this attribute when you want to monitor the state of the remote service group. When you choose the MonitorOnly attribute, the RemoteGroup agent does not have control over the remote service group and cannot bring it online nor take it offline.

The remote service group should be in an ONLINE state before you bring the RemoteGroup resource online.

Symantec recommends that you set the AutoFailover attribute of the remote service group to 1.

OnlineOnly

Select the OnlineOnly value of this attribute when the remote service group takes a long time to come online or to go offline. When you use OnlineOnly for the ControlMode attribute, a switch or fail over of the local service group with VCSSysName set to ANY does not cause the remote service group to be taken offline and brought online.

The username provided in the Username attribute needs to have administrator privileges for the remote service group.

The Offline of the RemoteGroup resource does not offline the remote service group.

If you are choosing one-to-one mapping between the local nodes and remote nodes, then the value of the AutoFailover attribute of the remote service group must be 0.

Note: When you set the value of ControlMode to OnlineOnly or to MonitorOnly, the recommended value of the VCSSysName attribute of the RemoteGroup resource is ANY. If you want one-to-one mapping between the local nodes and the remote nodes, then a switch or fail over of local service group is impossible. It is important to note that in both these configurations the RemoteGroup agent does not take the remote service group offline.

Sample scenario

In this example, a local VCS cluster (front-end cluster) provides high availability for Web-services and a remote VCS cluster (back-end cluster) provides high availability for the database required by the Web-services. The cluster setup is as follows:

- The local cluster is a two-node cluster, where local1 and local2 are the names of the two local nodes.

- The remote cluster is a two-node cluster, where remote1 and remote2 are the names of the two remote nodes.
- LocGrp is the local service group that contains the WebRes resource (for example: Apache, etc.) configured for the Web-server that runs in the local cluster.
- RemGrp is the remote service group that contains the DBRes resource (for example: MySQL or Oracle, etc.) configured for the database in the remote cluster.

The database resource (DBRes) needs to come online before the Web server resource (WebRes) comes online. You can use the RemoteGroup agent to establish this inter-cluster application dependency.

To configure the remotegroup agent for this setup

- 1 Create a RemoteGroup resource (RGRes) in the local service group (LocGrp) for monitoring or managing the DBRes resource in the remote cluster.
- 2 Link the resources such that the WebRes resource depends on the RGRes resource.
- 3 Set the attributes for the RemoteGroup resource (RGRes) as follows:
 - **IpAddress**—Set to the IP address or DNS name of a node in the remote cluster. For this example, the value is remote1. You can also set this value as remote2 (second node in the remote cluster).

The RemoteGroup agent keeps a list of remote nodes (remote1, remote2) on the local node. The IP address that you specify should be reachable the first time the RemoteGroup agent tries to communicate to the remote cluster. In case the specified IP address is not reachable after the first communication, the RemoteGroup agent talks to the second remote node to retrieve the state of RemGrp.
 - **GroupName**—Set the value to RemGrp (the remote service group).
 - **VCSSysName**—Set appropriate values so as to establish a one-to-one mapping between the systems in the local and remote clusters. RGRes will completely manage the remote service group (RemGrp) that contains the DBRes resource. Make this a local attribute for the RGRes.
 - **ControlMode**—Set the value to OnOff.
 - **Username**—Set the value to user_admin. The user needs to have administrative privileges for RemGrp.
 - **Password**—Password for user_admin. You must encrypt the password using the VCS Encrypt command. See the *VCS Administrator's Guide* for more information on the VCS Encrypt utility.
 - **VCSSysName@local1**—Set this value to remote1.

- **VCSSysName@local2**—Set this value to remote2.
You have to set the value of BrokerIp for a remote cluster that has the Symantec Product Authentication Service enabled.
- 4 Set the value of the AutoFailover attribute of the RemGrp to 0. This avoids unnecessary online or offline of the remote service group in case of a fail over. If the value of the VCSSysName attribute is ANY, then the value of the AutoFailover attribute of RemGrp should be 1.

Service group behavior

Consider the following actions to better understand the service group behavior in this configuration.

- **Bringing the LocGrp local service group online**
The Online functions of all the resources in LocGrp (local service group) are called starting from the lower-most resource on local1. In this configuration, WebRes depends on RGRes. The RGRes Online function is called before the WebRes Online function. In the Online function, the RemoteGroup agent communicates to the remote cluster and authenticates the specified user. The RemoteGroup agent brings RemGrp online on remote1. RemGrp is in an ONLINE state on remote1 and RGRes is in an ONLINE state on local1. The Online function of WebRes is then called. WebRes is now in an ONLINE state.
Thus, you have established an application-level dependency across two different VCS clusters. The WebRes does not go online before the RGRes goes online. RGRes does not go online before the RemGrp goes online.
- **An unexpected offline of the RemGrp remote service group**
LocGrp is online on the local1. WebRes and RGRes are both online on local1. RemGrp is online on remote1. If RemGrp faults on remote1, RGRes detects that RemGrp has gone OFFLINE or has FAULTED on remote1 and goes into a FAULTED state. All the resources in LocGrp are taken offline on local1. LocGrp now fails over to local2. All the resources including WebRes and RGRes go into an ONLINE state on local2. As part of the fail over of LocGrp on local2, RemGrp goes online on remote2. LocGrp shows ONLINE on node local2 and OFFLINE OR FAULTED on local1.
- **Taking the LocGrp service group offline on local1**
LocGrp is online on local1 and RemGrp is online on remote1. If you take LocGrp offline, all the resources dependent on RGRes are taken offline. First, the WebRes resource goes offline and then the offline for RGRes is called. As the ControlMode is OnOff, the RemoteGroup agent communicates to the remote cluster and issues an offline command for RemGrp. Once RemGrp has gone offline, RGRes goes into OFFLINE state. Thus, the Web-server is taken offline before the database goes offline.

Troubleshooting bundled agents

This chapter describes how to troubleshoot common problems in bundled agents. The chapter lists bundled agent error messages (shown in bold text), and describes the problems associated with each agent. Recommended action is included, where applicable.

This chapter lists most of the error messages associated with the VCS bundled agents. For error messages other than the ones described here, contact Symantec Technical Support.

VCS logging

VCS generates two error message logs: the engine log and the agent log. Log file names are appended by letters. Letter A indicates the first log file, B the second, C the third, and so on.

The agent log is located at %VCS_HOME%\log\agent_A.txt. The format of agent log messages is:

Timestamp (Year/MM/DD) | Mnemonic | Severity | UMI | Agent Type |
Resource Name | Entry Point | Message Text

- *Timestamp*: the date and time the message was generated.
- *Mnemonic*: the string ID that represents the product (for example, VCS).
- *Severity*: levels include CRITICAL, ERROR, WARNING, NOTICE, and INFO (most to least severe, respectively).
- *UMI*: a unique message ID.
- *Message Text*: the actual message generated by VCS.

A typical agent log resembles:

```
2004/03/02 16:34:07 VCS WARNING V-16-10051-5008
NotifierMngr:ntfr:monitor:Expected correct SNMP and | or SMTP
options
```

Troubleshooting storage agents

Storage agents comprise the Volume Manager Diskgroup agent and MountV agent.

Volume Manager (VMDg) agent error messages

The Agent is shutting down the system because it is configured so or it failed to start VxVM Service.

The VMDg agent is shutting down your system because you have provided SHUTDOWN as a value for VxVMFailAction attribute. This action is taken when the VMDg agent attempts to restart the Veritas Storage Agent service for the number of times specified in VxVMRestartAttempts attribute.

Cluster Server license is not enabled in Volume Manager.

Storage Foundation for Windows was not installed with the HA license.
Recommended Action: Contact Symantec Technical Support.

Diskgroup not configured

No value specified for the DiskGroupName attribute.
Recommended Action: Verify the DiskGroupName attribute defined in the configuration file is assigned a value.

Could not initialize Volume Manager connection. Error = *Error_code*

The Veritas Enterprise Administrator Service is either not in a running state or is not responding to service request.
Recommended Action: Verify that the service is in a running state.

Could not get SCM handle [*Error Type:Error Code*]

The agent could not open a handle to the Service Control Manager.
Recommended Action: See the error type and error code for more information. Contact Symantec Technical Support if the problem persists.

Online diskgroup. Less than half of total disks available in the diskgroup.

Less than half the disks are available in the diskgroup.

Recommended Action: For the ForceImport to work, make sure at least 50% of the disks are available.

Online diskgroup : *Error_description*

The agent failed to bring the diskgroup online.

Recommended Action: See the corresponding error description for more information.

Offline diskgroup : *Error_description*

The agent failed to bring the diskgroup offline.

Recommended Action: See the corresponding error description for more information.

Init diskgroup : *Error_description*

The agent failed to initialize the diskgroup.

Recommended Action: See the corresponding error description for more information.

Failed to start VxOb Service (Error = *Error Type:Error Code*)

The agent failed to start the VxOb service.

Recommended Action: Try to start the VxOb service manually. See the corresponding error type and error code for more information.

Failed to query VxOb (Error = *Error Type:Error Code*)

The agent failed to query VxOb.

Recommended Action: Try to query VxOb manually. See the corresponding error type and error code for more information.

Failed to open VxOb (Error = *Error Type:Error Code*)

The agent failed to open VxOb.

Recommended Action: Try to open VxOb manually. See the corresponding error type and error code for more information.

Query imported cluster diskgroups : *Error_description*

Recommended Action: See the corresponding error description for more information.

Query SCSI Reservation : *Error_description*

Recommended Action: See the corresponding error description for more information.

One or more disks in this diskgroup are unsteady

One or more disks or volumes in the diskgroup are not in a healthy state.

Recommended Action: View the disks using the Veritas Enterprise Administrator console and verify the state of the disks.

Disk availability check : *Error_description*

Recommended Action: See the corresponding error description for more information.

Init diskgroup failed : The diskgroup and GUID do not match

Recommended Action: Use the `vmgetdrive -details` command to find the correct GUID.

MountV agent error messages

Could not initialize Volume Manager connection. Error = *Error_code*

The Veritas Enterprise Administrator Service is either not in a running state or is not responding to service request.

Recommended Action: Verify that the service is in a running state.

Cluster Server license is not enabled in Volume Manager.

Storage Foundation for Windows was not installed with the HA license.

Recommended Action: Contact Symantec Technical Support.

***Attribute_name* not configured**

No value provided for the specified attribute.

Recommended Action: Verify the specified attribute defined in the configuration file is assigned a value.

Failed to get volume properties [*Error_type:Error_code*]

The agent failed to get the properties of the configured volume.

Recommended Action: See the corresponding error type and error code for more information.

Volume *folder_mount_path* is also mounted as Driveletter *drive_letter*

The specified volume is already mounted. The agent does not allow a volume to be mounted on multiple drives.

Recommended Action: Verify that the volume is not mounted at another drive letter. Also check that the volume is not mounted as an NTFS mount point.

Volume *drive_letter* is also mounted as NTFS Folder mount(s) at *folder_mount_path*

The agent does not allow a volume to be mounted on multiple drives.

Recommended Action: Verify that the volume is not mounted at a drive letter. Also check that the volume is not mounted as an NTFS mount point.

Volume *drive_letter* is Mounted as *mount_path* but configured as *volume_name*

The mount path for the volume specified in the configuration file is different from the actual mount path.

Recommended Action: Verify the mount path specified in the configuration file is correct.

Volume *volume_name* is already mounted as NTFS Folder *folder_mount_path*

The agent does not allow a volume to be mounted on multiple drives.

Recommended Action: Verify that the volume is not mounted at a drive letter. Also check that the volume is not mounted as an NTFS mount point.

Volume *volume_name* has been mounted multiple times (*no_of_times*)

The agent does not allow a volume to be mounted on multiple drives.

Recommended Action: Verify that the volume is not mounted at a drive letter. Also check that the volume is not mounted as an NTFS mount point.

Volume *volume_name* has also been mounted as (*drive_letter*)

The agent does not allow a volume to be mounted on multiple drives.

Recommended Action: Verify that the volume is not mounted at a drive letter. Also check that the volume is not mounted as an NTFS mount point.

Diskgroup not present

The specified diskgroup is not present on the system.

Recommended Action: Verify that the diskgroup exists on the system.

Volume not present

The specified volume is not present on the system.

Recommended Action: Verify that the volume exists on the system.

Connection to VM not initialized

The Veritas Enterprise Administrator Service is either not in a running state or is not responding to service request.

Recommended Action: Verify that the service is in a running state.

Mount_path is not suitable for folder mount [Error_type:Error_code]

The specified MountPath is not suitable for a folder mount.

Recommended Action: See the description for the MountPath attribute for the VMDg agent. See the corresponding error type and error code for more information.

Mount_path is not on an NTFS formatted volume

The specified MountPath is not an NTFS formatted volume.

Failed to unlock volume [Error_type:Error_code]

The agent could not unlock the volume while dismounting, indicating a potential hardware error or that other applications are accessing the volume.

Recommended Action: Ensure that no other applications, including Windows Explorer, are accessing the volume. Verify the installed disk and the configured partition. Contact Symantec Technical Support if the problem persists.

Failed to lock volume [Error_type:Error_code]

The agent could not lock the volume while dismounting, indicating a potential hardware error or that other applications are accessing the volume.

Recommended Action: Verify that no other applications, including Windows Explorer, are accessing the volume. Verify the installed disk and the configured partition. Set the ListApplications attribute to 1 to obtain a list of applications that are accessing the volume.

Filesystem at drive_letter/mount_path is not clean [Error_type:Error_code]

The file system at the specified drive letter or mount path is not clean

Recommended Action: Set the AutoFSClean to 1 if you want the agent to clean the filesystem. Otherwise, clean the filesystem manually.

Failed to add administrative share

The agent could not assign the default administrative share. An administrative share is already added for this volume.

Failed to delete administrative share [*Error_type:Error_code*]

The agent could not remove the administrative share assigned during the online operation.

Recommended Action: See the corresponding error type and error code for more information.

Troubleshooting network agents

Network agents comprise the NIC agent, IP agent, IPMultiNicPlus agent, and Lanman agent.

NIC agent error messages

Initialization failed

The agent failed to retrieve network information. This is a VCS internal error.

Recommended Action: Contact Symantec Technical Support.

Invalid MAC Address format

Incorrect format for MAC Address specified in the MACAddress attribute.

Recommended Action: Verify the MAC Address is in the format AA-BB-CC-DD.

Invalid MAC Address (*MAC_Address*) specified.

Invalid value specified for adapters physical address.

Recommended Action: Verify the MACAddress attribute defined in the configuration file is assigned a value.

Adapter (*Adapter_Name*) Connection status cannot be found

The agent failed to retrieve the connection status of the NIC.

Recommended Action: Contact Symantec Technical Support.

PingHostList not specified

No value is specified for PingHostList attribute even though the UseConnectionStatus is set to False.

Recommended Action: Specify a value for PingHostList.

UDP echo attempt failed

This is a network error.

Recommended Action: Contact Symantec Technical Support.

UDP check failed

This is a network error.

Recommended Action: Contact Symantec Technical Support.

Failed to clear all IPs from adapter *Adapter_Name*

The agent failed to deallocate all IPs assigned to a network card. The agent does so to avoid IP conflict.

Recommended Action: Contact Symantec Technical Support

Adapter (*Adapter_Name*) not found

The agent could not detect the specified adapter.

Recommended Action: Verify the MACAddress attribute defined in the configuration file is assigned a value.

Adapter (*Adapter_Name*) is not connected

The adapter specified in the MACAddress attribute is not available on the network.

Recommended Action: Check the network connections. If the problem persists, verify the MACAddress attribute defined in the configuration file is assigned a value.

Failed to get IFEntry for adapter *Adapter_Name*

The agent failed to retrieve an entry for the specified adapter from the IF table. This is a VCS internal error.

Recommended Action: Contact Symantec Technical Support.

TCP/IP is not enabled for adapter (*Adapter_Name*)

TCP/IP is not enabled for the specified adapter.

Recommended Action: Enable TCP/IP for the adapter.

Error percentage exceeded for (*Adapter_name*)

The adapter has exceeded the error percentage for sending packets, specified in the MaxTxErrorPercentage attribute.

Recommended Action: Contact Symantec Technical Support.

Error percentage exceeded limit

The adapter has exceeded the error percentage, specified by MaxTxErrorPercentage, by the number of times specified in MaxTxErrInterval attribute.

Recommended Action: Contact Symantec Technical Support.

IP agent error messages

Initialization failed

The agent failed to retrieve network information. This is a VCS internal error.

Recommended Action: Contact Symantec Technical Support.

Invalid attributes

Invalid values specified for the agent attributes.

Recommended Action: Verify the attributes defined in the configuration file are assigned a correct value.

Invalid MacAddress format

Incorrect format for MAC Address specified in the MacAddress attribute.

Recommended Action: Verify the MAC Address is in the format AA-BB-CC-DD.

Invalid IP format

Incorrect format for IP address specified in the Address attribute.

Recommended Action: Verify the IP address is in the correct format.

Ping failed for IP (*IP_Address*)

The agent failed to ping the specified IP address.

Recommended Action: Verify the specified IP address exists in the network. Check the network connections if the problem persists.

Host *IP_Address* already exists

The specified IP address already exists in the network

Recommended Action: Verify the value specified for Address attribute is unique.

IP (*IP_Address*) is Admin IP

The specified virtual IP is the base ID for a NIC in the network.

Recommended Action: Specify a unique IP address.

Incorrect IP (*IP_Address*)

Invalid value specified for the Address attribute.

Recommended Action: Verify the Address attribute defined in the configuration file is assigned a correct value.

Incorrect subnet mask (*SubNet_Mask*)

Invalid value specified for the SubNetMask attribute.

Recommended Action: Verify the SubNetMask attribute defined in the configuration file is assigned a correct value.

Adapter (*IP_Address*) not found

The agent could not detect the specified adapter in the network.

Recommended Action: Verify the Address attribute defined in the configuration file is assigned a correct value.

DHCP is enabled on Adapter (*IP_Address*)

DHCP is enabled on the specified adapter.

Recommended Action: Disable DHCP and specify an IP address for the adapter.

Invalid Adapter (*IP_Address*)

Invalid value specified for the Address attribute.

Recommended Action: Verify the Address attribute defined in the configuration file is assigned a correct value.

Invalid MacAddress (*MAC_Address*) specified

Invalid value specified for the MACAddress attribute.

Recommended Action: Verify the MACAddress attribute defined in the configuration file is assigned a correct value.

TCP/IP is not enabled for adapter (*Adapter_Name*)

TCP/IP is not enabled for the specified adapter.

Recommended Action: Enable TCP/IP for the adapter.

IPMultiNicPlus agent error messages

AdapterList is Invalid. Please check the configuration

Invalid MAC addresses specified in the AdapterList attribute.

Recommended Action: Verify the AdapterList attribute defined in the configuration file is assigned a correct value.

Admin IP address not specified. Check the configuration.

No value specified for AdminIPAddr attribute.

Recommended Action: Verify the AdminIPAddr attribute defined in the configuration file is assigned a value.

IP address *IP_Address* is not in standard 'a.b.c.d' form

The specified IP address is not in the standard format.

Recommended Action: Verify the IP address is in the format a.b.c.d.

Invalid Admin IP address. Check the configuration. Admin IP: *IP_Address*

Invalid value specified for AdminIPAddr attribute

Recommended Action: Verify the AdminIPAddr attribute defined in the configuration file is assigned a correct value.

Admin SubnetMask not specified. Check the configuration

No value specified for AdminSubnetMask attribute.

Recommended Action: Verify the AdminSubnetMask attribute defined in the configuration file is assigned a value.

SubNetMask *SubNetMask* is not in standard 'a.b.c.d' form

The specified subnet mask is not in the standard format.

Recommended Action: Verify the subnet mask is in the format a.b.c.d.

Invalid Admin SubNetMask. Check the configuration. Admin SubNetMask: Subnet_Mask

Invalid value specified for AdminSubnetMask attribute.

Recommended Action: Verify the AdminSubnetMask attribute defined in the configuration file is assigned a correct value.

WaitForSingleObject() Failed

The Windows API, `WaitForSingleObject()`, failed.

Recommended Action: Restart the agent. Contact Symantec Technical Support if the problem persists.

WaitForMultipleObjects() Failed

The Windows API, `WaitForMultipleObjects()`, failed.

Recommended Action: Restart the agent. Contact Symantec Technical Support if the problem persists.

AdminIP configured is used by an adapter which is not present in the configuration

The AdminIP specified in the AdminIPAddr attribute is not assigned to an adapter in the AdapterList attribute.

Recommended Action: Specify a different Admin IP or make sure that the adapter having the AdminIP is listed in the AdapterList attribute.

Invalid MAC address MAC_Address specified in adapter List

Invalid MAC address specified in the AdapterList attribute.

Recommended Action: Verify a valid MAC address is listed in the AdapterList attribute defined in the configuration file.

No adapters specified in the AdapterList.

The AdapterList attribute does not contain a MAC address.

Recommended Action: Verify a MAC address is listed in the AdapterList attribute defined in the configuration file.

PingHostList is Empty

No value specified for the PingHostList attribute.

Recommended Action: Verify the PingHostList attribute defined in the configuration file is assigned a value.

IP Address not specified. Check the configuration.

No value specified for the Address attribute.

Recommended Action: Verify the Address attribute defined in the configuration file is assigned a value.

Invalid IP Address: *IP_Address*. Check the configuration.

Invalid value specified for Address attribute.

Recommended Action: Verify the Address attribute defined in the configuration file is assigned a correct value.

SubNetMask not specified. Check the configuration.

No value specified for the SubNetMask attribute.

Recommended Action: Verify the SubNetMask attribute defined in the configuration file is assigned a value.

Invalid SubNetMask: *Subnet_Mask*. Check the configuration.

No value specified for the SubNetMask attribute.

Recommended Action: Verify the SubNetMask attribute defined in the configuration file is assigned a value.

Invalid MAC address specified in the AdapterList. MAC Address: *MAC_Address*

Invalid value specified for MACAddress attribute.

Recommended Action: Verify the MACAddress attribute defined in the configuration file is assigned a correct value.

TCP/IP is not enabled for MAC address *MAC_Address* specified in adapter List

TCP/IP is not enabled for the specified adapter.

Recommended Action: Enable TCP/IP for the adapter.

Invalid IP format (*IP_Address*)

The specified IP address is not in the standard format.

Recommended Action: Verify the IP address is in the standard format.

DHCP is enabled on Adapter (*MAC_Address*)

DHCP is enabled on the specified adapter.

Recommended Action: Disable DHCP and specify an IP address for the adapter.

Invalid Adapter (*MAC_Address*)

Invalid MAC address specified for the adapter.

Recommended Action: Specify a valid MAC address for the adapter.

Lanman agent error messages

Virtual server name specified in the configuration is invalid (*Virtual Server Name*)

The virtual server name exceeds the limit of 16 characters, or it contains invalid characters.

Recommended Action: Verify that the NetBios name is less than sixteen characters, and that it does not contain any of the following characters: `^:.?*?"<>|=.`

Virtual name already exists in the network

The specified virtual name already exists in the network.

Recommended Action: Verify the VirtualName attribute defined in the configuration file is assigned a unique value.

Failed to update DNS entry (error_type: *Error Type*, error_code: *Error Code*)

The agent failed to update the DNS entry.

Recommended Action: Verify the DNS server is alive, and the reverse lookup zone is configured.

Failed to update Computer account in Active directory (error_type: *Error Type*, error_code: *Error Code*)

The agent failed to add the computer account to the Active Directory.

Recommended Action: Verify whether the user, in whose context the Veritas Helper Service runs, has the required permissions.

Failed to register Virtual server name to Netbios (error_type: *Error type*, error_code: *Error Code*)

The agent failed to register the virtual server name with the NetBios.

Recommended Action: Verify whether the virtual name is already configured. Run `nbtstat - n` to check NetBios bindings. Contact Symantec Technical Support if the problem persists.

Failed to start the 'Veritas Cluster Server Helper' service. (error_type: *Error Type*, error_code:*Error Code*)

The agent failed to start the specified service.

Recommended Action: Verify whether the service is installed on the node. Also verify whether the user, in whose context the service will run, has the required permissions.

IP address specified for MultiNetInfo is invalid (entry=*IP Address*)

Invalid IP address specified in the MultiNetInfo attribute.

Recommended Action: Verify the MultiNetInfo attribute defined in the configuration file is assigned correct values.

SubnetMask specified for MultiNetInfo is invalid (entry=*subnet_mask*)

Invalid subnet mask specified in the MultiNetInfo attribute.

Recommended Action: Verify the MultiNetInfo attribute defined in the configuration file is assigned correct values.

WINS address specified for MultinetInfo is invalid (entry=*wins_address*)

Invalid WINS address specified in the MultiNetInfo attribute.

Recommended Action: Verify the MultiNetInfo attribute defined in the configuration file is assigned correct values.

VirtualName attribute is not specified in the configuration

No value specified for VirtualName attribute.

Recommended Action: Verify the VirtualName attribute defined in the configuration file is assigned a value.

IP address specified in the configuration is invalid

Invalid value specified for the IP address.

Recommended Action: Verify the value specified for the IP address is valid.

SubnetMask specified in the configuration is invalid

Invalid value specified for the subnet mask.

Recommended Action: Verify the value specified for the subnet mask is valid.

MultiNetInfo attribute specified in the configuration is in invalid format

The value specified for MultiNetInfo attribute is not in the standard format.

Recommended Action: Verify the format for the MultiNetInfo attribute.

There are no valid IP addresses specified in the configuration

All the IP addresses specified in the configuration are invalid.

Recommended Action: Verify the IP addresses specified in the configuration file.

IP address specified in the configuration is not online. (ip= IP Address)

The specified IP address is not online in the cluster.

Recommended Action: Verify the specified IP address exists in the network.

Mismatch in the subnet mask specified in configuration and the actual subnet mask configured for the adapter

The subnet mask specified in the configuration file does not match with the subnet mask for the configured adapter.

Recommended Action: Verify the subnet mask specified in the MultiNetInfo attribute is correct.

WINS address specified in the configuration is not found in the adapter's WINS address list

The specified WINS address does not exist in the WINS address list of the adapter.

Recommended Action: Verify the WINS address specified in the MultiNetInfo attribute is correct.

**Attempt to start 'Veritas Cluster Server Helper' service has failed.
(error_type: *Error Type*, error_code: *Error Code*)**

The agent failed to start the specified service.

Recommended Action: Verify whether the service is installed on the node. Also verify whether the user, in whose context the service will run, has the required permissions.

**Attempt to stop 'Veritas Cluster Server Helper' service has failed.
(error_type: *Error Type*, error_code: *Error Code*)**

The agent failed to stop the specified service.

Recommended Action: Verify whether the service is installed on the node. Also verify whether the user, in whose context the service will run, has the required permissions.

**Attempt to online the Lanman resource has failed. (error_type: *Error Type*,
error_code: *Error Code*)**

The agent failed to online the Lanman resource. This is a VCS internal error.

Recommended Action: See the Windows error code for more information. Contact Symantec Technical Support if the problem persists.

Troubleshooting FileShare agents

FileShare agents comprise the FileShare agent and the CompositeFileShare agent.

FileShare agent error messages

Attribute value(s) invalid for *attr_name*

The specified attribute name has invalid value.

Recommended Action: Verify the configuration file and make sure the correct attribute value is specified.

Failed to open folder *folder_name* [*ErrorType:Error Code*]

The agent failed to open the folder specified in the ShareName attribute.

Recommended Action: Verify whether the specified folder exists. Check the permissions for the folder.

Folder *folder_name* (\\system_name\\share_name) already shared

The specified folder name is already shared.

Recommended Action: Verify the configuration file for the specified ShareName.

Failed to share folder *folder_name* as (\\system_name\\share_name) [*ErrorType:Error Code*]

The agent failed to share the specified folder.

Recommended Action: Verify the configuration file for the specified ShareName.

MaxUsers for share *share_name* is less than configured

The number of users authorized to access a share is less than the number of users specified in the MaxUsers attribute.

Recommended Action: Make sure the number of users authorized to access a share and the number of users specified in the MaxUsers attribute is same.

**Failed to unshare folder *folder_name* as (\\|system_name|share_name)
 [ErrorType:Error Code]**

The agent failed to unshare the specified folder.

Recommended Action: Verify the configuration file for the specified share name.

Path mismatch for share *share_name*

The specified path name is already shared.

Recommended Action: Verify that the share name does not already exist on the network. If the share does not exist, contact Symantec Technical Support.

System error occurred for folder *folder_name* Error [Error_code]

Recommended Action: See the Windows error code for more information. Contact Symantec Technical Support if the problem persists.

FileShare Error : The Server service is not available

The agent requires the Server service to be started before it can bring the resource online.

Recommended Action: Verify that the Server service is running properly.

Permissions error occurred for folder *folder_name* Error [error_id]

Recommended Action: See the corresponding error_id for more information. Error ID 6 denotes a mismatch in the configured permission and the actual permission for the folder share. Error ID 7 denotes an error while matching the configured permission and actual permission for the share.

Share name *share_name* contains invalid characters

The specified share name contains invalid characters.

Recommended Action: Make sure the specified share name does not contain special characters (\, /, :, *, ?, <, >, |).

CompositeFileShare agent error messages

Attribute value(s) invalid for *attr_name*

The specified attribute name has an invalid value.

Recommended Action: Verify the configuration file and make sure the correct attribute value is specified.

Failed to open folder *folder_name* [ErrorType:Error Code]

The agent failed to open the folder specified in the ShareName attribute.

Recommended Action: Verify whether the specified folder exists. Check the permissions for the folder.

Folder *folder_name* (\\|system_name|share_name) already shared

The specified folder name is already shared.

Recommended Action: Verify the configuration file for the specified ShareName.

Failed to share folder *folder_name* as (\\|system_name|share_name) [ErrorType:Error Code]

The agent failed to share the specified folder.

Recommended Action: Verify the configuration file for the specified ShareName.

MaxUsers for share *share_name* is less than configured

The number of users authorized to access a share is less than the number of users specified in the MaxUsers attribute.

Recommended Action: Make sure the number of users authorized to access a share and the number of users specified in the MaxUsers attribute is same.

Failed to unshare folder *folder_name* as (\\|system_name|share_name) [ErrorType:Error Code]

The agent failed to unshare the specified folder.

Recommended Action: Verify the configuration file for the specified share name.

Path mismatch for share *share_name*

The specified path name is already shared.

Recommended Action: Verify that the share name does not already exist on the network. If the share does not exist, contact Symantec Technical Support.

Composite FileShare Error : The Server service is not available

The agent requires the Server service to be started before it can bring the resource online.

Recommended Action: Verify that the Server service is running properly.

Permissions error occurred for folder *folder_name* Error [*error_id*]

Recommended Action: See the corresponding *error_id* for more information. Error ID 6 denotes a mismatch in the configured permission and the actual permission for the folder share. Error ID 7 denotes an error while matching the configured permission and actual permission for the share.

Share name *share_name* contains invalid characters

The specified share name contains invalid characters.

Recommended Action: Make sure the specified share name does not contain special characters (\, /, :, *, ?, <, >, |).

Troubleshooting PrintShare agents

PrintShare agents comprise the PrintSpool agent and the PrintShare agent.

PrintSpool agent error messages

LanmanResName attribute has not been configured.

No value specified for the LanmanResName attribute.

Recommended Action: Verify the LanmanResName attribute defined in the configuration file is assigned a value.

IPResName attribute has not been configured.

No value specified for the IPResName attribute.

Recommended Action: Verify the IPResName attribute defined in the configuration file is assigned a value.

MountResName attribute has not been configured.

No value specified for the MountResName attribute.

Recommended Action: Verify the MountResName attribute defined in the configuration file is assigned a value.

SpoolDirectory attribute has not been configured.

No value specified for the SpoolDir attribute.

Recommended Action: Verify the SpoolDir attribute defined in the configuration file is assigned a value.

The spooler path '*spooler_path*' is not valid.

Invalid spooler path specified in the SpoolDir attribute.

Recommended Action: Specify the correct spooler path in the SpoolDir attribute.

Spooler is not running

The agent was not able to detect a running PrintSpooler service.

Recommended Action: Verify that the Spooler service is running properly.

Duplicate Lanman name (*Lanman_name*) provided. Another PrintSpool resource exists with this Lanman name.

The specified Lanman name already exists in the cluster.

Recommended Action: Specify a unique Lanman name in the LanmanResName attribute.

Duplicate IP address (*ip_address*) provided. Another PrintSpool resource exists with this IP.

The specified IP address already exists in the cluster.

Recommended Action: Specify a unique IP address in the IPResName attribute.

Attribute mismatch for Lanman resource. Attribute change is not supported.

The value specified for the Lanman resource was changed manually after the resource was brought online.

Recommended Action: Offline the service group with the PrintSpool resource, disable the PrintSpool resource, and specify the value for LanmanResName attribute. Enable the PrintSpool resource and online the service group.

Attribute mismatch for IP resource. Attribute change is not supported.

The value specified for the IP resource was changed manually after the resource was brought online.

Recommended Action: Offline the service group with the PrintSpool resource, disable the PrintSpool resource, and specify the value for IPResName attribute. Enable the PrintSpool resource and online the service group.

Failed to online the virtual spooler. Error= *Error Code*.

The agent failed to online the virtual spooler.

Recommended Action: See the Windows error code for more information. Contact Symantec Technical Support if the problem persists.

PrintShare agent error messages

Attribute value(s) invalid for *attr_name*

The specified attribute name has an invalid value.

Recommended Action: Verify the configuration file and make sure the correct attribute value is specified.

Unknown error for printer (\\system_name\printer_name) [ErrorType:Error Code]

Recommended Action: See the Windows error code for more information on the error. Contact Symantec Technical Support if the problem persists.

Printer *printer_name* (\\system_name\printer_name) already shared

The specified folder name is already shared.

Recommended Action: Verify the configuration file for the specified ShareName.

Failed to share printer *printer_name* as (\\system_name\printer_name) [ErrorType:Error Code]

The agent failed to share the specified folder.

Recommended Action: Verify the configuration file for the specified ShareName.

Failed to unshare printer *printer_name* as (\\system_name\printer_name) [ErrorType:Error Code]

The agent failed to unshare the specified folder.

Recommended Action: Verify the configuration file for the specified share name.

Printer mismatch for share *share_name*

The specified printer name is already shared.

Recommended Action: Verify that the share name does not already exist on the network. If the share does not exist, contact Symantec Technical Support.

PrintShare Error: The Server service is not available.

The agent requires the Server service to be started before it can bring the resource online.

Recommended Action: Verify that the Server service is running properly.

Share name *share_name* contains invalid characters

The specified share name contains invalid characters.

Recommended Action: Make sure the specified share name does not contain special characters (\, /, :, *, ?, <, >, |).

Troubleshooting services and application agents

Services and application agents comprise MSVirtualMachine, GenericService, ServiceMonitor, and Process agent.

MSVirtualMachine agent error messages

Virtual Server COM interface could not be initialized. Reported Error: [%01X]"

This could occur because of a corrupt DLL or if the application (Microsoft Virtual Server) was uninstalled.

Recommended Action: See the accompanying error message for more information.

GetVM Query failed for VM %s. Reported Error: [%01X]", new_args[0]

An internal function failed.

Recommended Action: See the accompanying error message for more information.

Failed to retrieve state for VM %s. Reported Error [%01X].", new_args[0]

Recommended Action: See the accompanying error message for more information.

MonitorHB failed. Could not create instance for the Guest OS for VM %s. Reported Error [%01X]

This could occur if Virtual Machine Additions is not installed, but the MonitorHB attribute is set to True.

Recommended Action: Verify Virtual Machine Additions is installed and running on the virtual machine. If you do not plan to monitor heartbeats, set the MonitorHB attribute to false.

MonitorHB failed. Could not communicate with Virtual machine Additions for VM %s. Reported Error [%01X]

Virtual Machine Additions is not installed or is not running properly.

Recommended Action: Verify Virtual Machine Additions is installed on the virtual machine.

VM %s has stopped heartbeating.

This error indicates a hung machine or a blue screen. The agent returns offline in this situation.

Power on for VM %s failed. Reported Error: [%01X]", new_args[0]

The agent could not start the virtual machine.

Recommended Action: See the accompanying error message for more information.

Could not get a handle for the Guest OS running in VM %s.", new_args[0]

This could occur if VM Additions is not installed.

Recommended Action: Verify Virtual Machine Additions is installed on the virtual machine. See the accompanying error message for more information.

OS Shutdown failed for VM %s. Reported Error: [%01X].", new_args[0]

The agent could not shut down the operating system on the virtual machine.

Recommended Action: See the accompanying error message for more information.

IIS agent error messages

Failed to create the IIS services map.

Recommended Action: Verify the SiteType attribute is defined correctly in the configuration. See the associated Windows error type and error code for more information.

Failed to parse the argument list.

The agent could not pass all arguments associated with the agent's resource type definition.

Recommended Action: Verify the configuration definition of the agent.

Failed to allocate memory for IIS Service resource object.

Recommended Action: Verify the system has adequate memory to run IIS and VCS.

Failed to find the service object. Please check the SiteType attribute.

Recommended Action: Verify the configuration definition of the SiteType attribute.

Arguments are not specified correctly, Please check ArgList, ResName

Some attributes associated with the agent are not defined correctly.

Recommended Action: Verify the configuration definition of the specified attribute.

Configuration error. Attribute *attribute* is not configured.

Recommended Action: Verify the configuration definition of the specified attribute.

Failed to convert IP address to ASCII. Error Type. Error Code.

Recommended Action: Verify the configuration definition of the IP resources. See the associated Windows error type and error code for more information.

Failed to start/stop the application pool.

Recommended Action: Verify the name of the application pool is correctly defined in the agent's configuration.

Failed to get the application pool state. *Error Type. Error Code.*

The agent could not determine the state of the configured application pool.

Recommended Action: Verify the name of the application pool is correctly defined in the agent's configuration. See the associated Windows error type and error code for more information.

Failed to get the IIS virtual directory object *object_name*. *Error Type. Error Code.*

The agent could not access the specified virtual directory object.

Recommended Action: Verify the virtual directory object for the site exists. See the associated Windows error type and error code for more information.

Failed to start the application pool *poolname*. *Error Type. Error Code.*

The agent could not start the specified application pool.

Recommended Action: Verify the configuration definition of the application pool.

Failed to get the application pool interface. *Error Type. Error Code.*

The agent could not access the COM interfaces for the application pool.

Recommended Action: See the associated Windows error type and error code for more information.

Failed to stop the application pool *poolname*. *Error Type. Error Code.*

The agent could not stop the specified application pool.

Recommended Action: Verify the configuration definition of the application pool.

Failed to start the IIS site/virtual server. *Error Type. Error Code.*

The agent could not start the specified IIS site or virtual server.

Recommended Action: Verify the specified site or server exists and verify its configuration definition.

Failed to stop the IIS site/virtual server. *Error Type. Error Code.*

The agent could not stop the specified IIS site or virtual server.

Recommended Action: Verify configuration definition of the specified site or server.

Failed to determine the state of the IIS site/virtual server. *Error Type. Error Code.*

The agent could not determine the state of the specified IIS site or virtual server.

Recommended Action: Verify configuration definition of the specified site or server.

Failed to get the application pool state and the bind path. *Error Type. Error Code.*

The agent could not determine the state of the specified application pool.

Recommended Action: Verify configuration definition of the specified application pool.

Failed to get the IIS version. *Error Type. Error Code.*

The agent could retrieve the version information for IIS.

Recommended Action: Verify that a supported IIS version is installed on all nodes in the cluster. See the associated Windows error type and error code for more information.

Failed to get the registry *keyname. Error Type. Error Code.*

The agent could not access the specified registry key.

Recommended Action: Verify the specified registry key exists.

Failed to start service *servicename. Error Type. Error Code.*

The agent could not start the specified service.

Recommended Action: Verify the service exists and is correctly defined in the configuration file. Verify that the service is supported by the host.

Failed to get the state of service *servicename. Error Type. Error Code.*

The agent could not determine the state of the specified service.

Recommended Action: Verify the service exists and is correctly defined in the configuration file. Verify that the service is supported by the host

Failed to stop service *servicename*. *Error Type*. *Error Code*.

The agent could not stop the specified service.

Recommended Action: Verify the service exists and is correctly defined in the configuration file. Verify that the service is supported by the host

Failed to initialize service object *servicename*. *Error Type*. *Error Code*.

The agent could not initialize the specified service.

Recommended Action: Verify the service exists and is correctly defined in the configuration file. Verify that the service is supported by the host

GenericService agent error messages

The ServiceName attribute has not been configured

No value specified for the ServiceName attribute.

Recommended Action: Verify the ServiceName attribute defined in the configuration file is assigned a value.

The password attribute has not been configured

No value specified for the Password attribute.

Recommended Action: Verify the Password attribute defined in the configuration file is assigned a value.

Failed to get the password attribute. Error = *Error Code*

The agent failed to decrypt the specified password.

Recommended Action: Use the vcsencrypt utility to get an encrypted password. Specify the encrypted password to the Password attribute in the configuration file.

Failed to convert the password attribute. Error = *Error Code*

The agent failed to convert the password attribute. This is a VCS internal error.

Recommended Action: Offline and online the service group. Contact Symantec Technical Support if the problem persists.

Failed to allocate memory

The agent failed to allocate the memory. This is a VCS internal error.

Recommended Action: Offline and online the service group. Contact Symantec Technical Support if the problem persists.

Failed to lookup the account name '*Account_Name*'. Error = *Error Code*

The agent failed to obtain the SID for the specified user.

Recommended Action: Verify that the domain controller is accessible, or the specified user exists. See the error code if the problem persists.

Failed to open the SCM handle. Error = *Error Code*

The agent failed to obtain the SCM handle. This occurs if the specified Service Control Manager (SCM) database does not exist, or the requested access is denied.

Recommended Action: Verify that SCM can be run on the host.

The service '*Service_Name*' is not in stopped state

The agent failed to online the service because the service was not in STOPPED state.

Recommended Action: Verify the state of the service and re-issue the online command.

Failed to decrypt the password

The agent failed to decrypt the specified password.

Recommended Action: Verify that it the password is encrypted using the VCS Encrypt utility (described in the *Veritas Cluster Server Administrator's Guide*).

Failed to change the user context of the service '*Service_Name*' to '*DomainNameUsername*'. Error = *Error Code*

The agent failed to change the user context in which the service will run.

Recommended Action: See the Windows error code for further information.

Failed to start the service '*Service_Name*'. Error = *Error Code*

The agent failed to start the specified service.

Recommended Action: Verify the binaries for the specified service exist, or the service is configured to run in the context of the specified user. Start the service manually if the problem persists.

The service '*Service_Name*' did not start within the specified time limit

The agent failed to online the service within the time specified in the DelayAfterOnline attribute.

Recommended Action: Verify the state of the service in the SCM. If the state of the service is START PENDING, increase the time specified in DelayAfterOnline attribute. If the problem persists, start the service manually.

Failed to wait for the service '*Service_Name*' to start. Error = *Error Code*

The agent did not wait for the service to start. This is a VCS internal error. Refer to the documentation specific to the service to determine the cause.

Failed to get the user context of the running service '*Service Name*'. Error = *Error Code*

The agent failed to obtain the information about the user in whose context, the specified service will run.

Recommended Action: Verify that the user exists, or the domain controller is accessible. See the error code if the problem persists.

Failed to get the SID for user '*DomainNameUsername*'

The agent failed to obtain the SID for the specified user.

Recommended Action: Verify that the domain controller is accessible, or the specified user exists. See the error code if the problem persists.

The service '*Service_Name*' is not running under the context of user *DomainNameUsername*

The user information specified in the UserAccount information is different from the user information, in whose context the service will run.

Recommended Action: Stop the service and modify the user information. Re-issue the online command.

The service '*Service_Name*' shares the same process with other services. Killing it might affect those services

If the service has an invalid state, the agent attempts to offline the service. The agent fails to offline the service, if the process is shared with other services. In such cases, the agent attempts to kill the shared process. You risk potential data loss.

Failed to enable the '*Privilege_Name*' privilege. Error = *Error Code*

The agent failed to enable the privilege required to kill a process. See the Windows error code for further information.

Failed to open the service '*Service_Name*'. Error = *Error Code*

The resource definition in the configuration file contains an invalid, or incorrect service name.

Recommended Action: Verify the ServiceName attribute defined in the configuration file is the same as the display name used by SCM. Verify that the specified service was opened successfully.

Failed to query the status of the service '*Service Name*'. Error = *Error Code*

The agent failed to determine the status of the service. This is a VCS internal error.

Recommended Action: Offline and online the service group. Contact Symantec Technical Support if the problem persists.

The service '*Service_Name*' is not in running state. Attempt to stop it might be unsuccessful.

The agent failed to offline the service because the service is not in STARTED state.

Recommended Action: Verify the state of the service and re-issue the online command.

The service '*Service_Name*' did not stop. Error = *Error Code*.

The agent failed to stop the specified service.

Recommended Action: Verify the binaries for the specified service exist, or the service is configured to run in the context of the specified user. Stop the service manually if the problem persists.

The service '*Service_Name*' did not stop within the specified timeout. Error = *Error Code*

The agent failed to offline the service within the time specified in the DelayAfterOffline attribute.

Recommended Action: Verify the state of the service in the SCM. If the state of the service is STOP PENDING, increase the time specified in DelayAfterOffline. If the problem persists, stop the service manually.

ServiceMonitor agent error messages

The ServiceOrScriptName attribute has not been configured

No value specified for the ServiceOrScriptName attribute.

Recommended Action: Verify the ServiceOrScriptName attribute defined in the configuration file is assigned a value.

Failed to lookup the account name '*Account_Name*'. Error = *Error Code*

The agent failed to obtain the SID for the specified user.

Recommended Action: Verify that the domain controller is accessible, or the specified user exists. See the error code if the problem persists.

The password attribute has not been configured

No value specified for the Password attribute.

Recommended Action: Verify the Password attribute defined in the configuration file is assigned a value and contains alphabets only.

Failed to get the password attribute. Error = *Error Code*

The agent failed to decrypt the specified password.

Recommended Action: Verify that the password is encrypted using the VCS Encrypt utility (described in the *Veritas Cluster Server Administrator's Guide*).

Failed to convert the password attribute. Error = *Error Code*

The agent failed to convert the password attribute. This is a VCS internal error.

Recommended Action: Offline and online the service group. Contact Symantec Technical Support if the problem persists.

Failed to open the SCM handle. Error = *Error Code*

The agent failed to obtain the SCM handle. This occurs if the SCM database does not exist, or if the SCM manager denies the requested access.

Recommended Action: Verify that SCM can be run on the host.

Failed to open the service '*Service_Name*'. Error = *Error Code*

The resource definition in the configuration file contains an invalid, or incorrect service name.

Recommended Action: Verify that the ServiceOrScriptName defined in the configuration file is the same as the display name used by SCM. Also verify that the specified service is supported by the SCM version on the host and that the specified service was opened successfully.

Failed to query the status of the service '*Service_Name*'. Error = *Error Code*

The agent failed to determine the status of the service. This is a VCS internal error.

Recommended Action: Verify that the attribute ServiceOrScriptName defined in the configuration file is the same as the display name used by SCM. Otherwise, offline and online the service group. Contact Symantec Technical Support if the problem persists.

The service '*Service_Name*' is not in running state

The agent failed to offline the service because the service is not in STARTED state.

Recommended Action: Verify the state of the service and re-issue the online command.

Failed to get the user context of the running service '*Service_Name*'. Error = *Error Code*

The agent failed to obtain the information about the user in whose context, the specified service will run.

Recommended Action: Verify that the user exists, or the domain controller is accessible. See the error code if the problem persists.

Failed to get the SID for user '*DomainNameUsername*'

The agent failed to obtain the SID for the specified user.

Recommended Action: Verify that the domain controller is accessible, or the specified user exists. See the error code if the problem persists.

The service '*Service_Name*' is not running under the context of user *DomainNameUsername*

The user information specified in the UserAccount information is different from the user information, in whose context the service will run.

Recommended Action: Stop the service and modify the user information. Re-issue the online command.

Failed to launch the monitor script '*Script_Name*'. Error = *Error Code*

The agent failed to launch the script to monitor the service.

Recommended Action: Verify that the script is accessible. See the Windows error code if the problem persists.

Monitor script has not responded within the specified timeout of *Timeout period* seconds. Error = *Error Code*

The agent failed to receive a response from the monitor script.

Recommended Action: Review the configuration definition of the attribute *MonitorProgTimeout*. Increase its value if required.

Failed to terminate the monitor program. Error = *Error Code*

The agent failed to terminate the script specified in the *MonitorService* attribute.

Recommended Action: Stop the agent. See the Windows error code, if the problem persists.

Failed to get exit code of the monitor program. Error = *Error Code*

The agent failed to get a response from the script that monitors a specified service.

Recommended Action: Verify that the exit codes returned by the script conform to VCS standards. See the Windows error code for further information. Contact Symantec Technical Support if the problem persists.

Failed to enable the *Privilege_Name*' privilege. Error = *Error Code*

The agent failed to enable the privilege required to kill a process. See the Windows error code for further information.

Invalid Service name [*service_name*].

The resource definition in the configuration file contains an invalid or incorrect service name.

Recommended Action: Verify that the attribute *ServiceOrScriptName* defined in the configuration file is the same as the display name used by SCM. Also verify that the specified service is supported by the SCM version on the host.

Process agent error messages

Failed to convert the argument list. Error = *Error Code*

The agent failed to convert the argument list. This is a VCS internal error.

Recommended Action: Offline and online the service group. Contact Symantec Technical Support if the problem persists.

Failed to lookup the account name for the user '*Account_Name*'. Error = *Error Code*

The agent failed to obtain the SID for the specified user.

Recommended Action: Verify that the domain controller is accessible, or the specified user exists. See the error code if the problem persists.

The password attribute has not been configured

No value specified for the Password attribute.

Recommended Action: Verify the Password attribute defined in the configuration file is assigned a value and contains alphabets only. If the problem persists, verify that the password is encrypted using the VCS Encrypt utility (described in the *Veritas Cluster Server Administrator's Guide*).

Failed to get the password attribute. Error = *Error Code*

The agent failed to decrypt the specified password.

Recommended Action: Use the vcsencrypt utility to get an encrypted password. Specify the encrypted password to the Password attribute in the configuration file.

Failed to convert the password attribute. Error = *Error Code*

The agent failed to convert the password attribute. This is a VCS internal error.

Recommended Action: Offline and online the service group. Contact Symantec Technical Support if the problem persists.

StartProgram has not been configured

No value specified for the StartProgram attribute.

Recommended Action: Verify the StartProgram attribute defined in the configuration file is assigned a value.

The process (*Process ID*) is not alive. Error = *Error Code*

The process specified in the StartProgram attribute is not alive.

Recommended Action: Verify the StartProgram attribute defined in the configuration file is assigned a value. See the Windows error code if the problem persists.

Failed to get cmd line of the process(*Process_ID*). Error= Error Code

The agent failed to determine the command line string for the process mentioned in the StartProgram attribute.

Recommended Action: Verify the StartProgram attribute defined in the configuration file is assigned a value. See the Windows error code if the problem persists.

The command line of the process(*Process_ID*) does not match with that configured in the attributes

The command line of the process, determined by the agent, did not match with the command line specified in the StartProgram attribute.

Recommended Action: Verify the StartProgram attribute defined in the configuration file is assigned a correct value.

Failed to get the user context of the process(*Process_ID*). Error= Error Code

The agent failed to obtain the information about the user in whose context, the specified process will run.

Recommended Action: Verify that the user exists, or the domain controller is accessible. See the error code if the problem persists.

The user context of the process (*Process_ID*) does not match with that configured in the attributes

The user context of the process, determined by the agent, did not match with the user context specified in the UserName attribute.

Recommended Action: Verify the UserName attribute defined in the configuration file is assigned a correct value.

Failed to determine whether the process is running or not. Error = Error Code

The agent failed to determine whether the process specified in the StartProgram attribute is running.

Recommended Action: Verify the StartProgram attribute defined in the configuration file is assigned a value. See the Windows error code if the problem persists.

Failed to enable '*Privilege_Name*' privilege. Error = Error Code

The agent failed to enable the privilege required to kill a process. See the Windows error code for further information.

Failed to launch the program '*Program_Name*'. Error = Error Code

The agent failed to launch the program specified in the StartProgram, CleanProgram, MonitorProgram, or StopProgram attributes.

Recommended Action: Verify the attributes defined in the configuration file are assigned a value. See the Windows error code if the problem persists.

Failed to get command line of the process (*Process_ID*). Error= Error Code

The agent failed to determine the command line of the process.

Recommended Action: Verify the attributes defined in the configuration file are assigned a value. See the Windows error code if the problem persists.

Failed to wait for the process (*Process_ID*) to stop. Error = Error Code. Killing it

The process specified in the StartProgram, CleanProgram, MonitorProgram, or StartProgram attribute did not respond in the specified timeout. The agent will try to kill the process.

Recommended Action: Increase the timeout specified in the MonitorProgramTimeout attribute. See the Windows error code if the problem persists.

Failed to get the ACL information. Error = Error Code

The agent failed to retrieve the Access Control List of the interactive desktop and window station.

Recommended Action: See the Windows error code for more information. Contact Symantec Technical Support if the problem persists.

Failed to get the ACE. Error = *Error Code*

The agent failed to retrieve the Access Control Entry for the ACL of the interactive desktop and window station.

Recommended Action: See the Windows error code for more information. Contact Symantec Technical Support if the problem persists.

Failed to add an ACE entry. Error = *Error Code*

The agent failed to add an ACE to the ACL of the interactive desktop and window station.

Recommended Action: See the Windows error code for more information. Contact Symantec Technical Support if the problem persists.

Troubleshooting infrastructure and support agents

Infrastructure and Support agents comprise NotifierMngr agent, Registry Replication agent, Proxy agent, Phantom agent, FileNone agent, ElifNone agent, FileOnOff agent, and FileOnOnly agent.

Notifier Manager agent error messages

Failed to Start Notifier Process *Process_ID*. (Windows Error Code = *Error Code*)

The agent failed to start the specified notifier process. This could occur due to an incorrect path name specified in the configuration, low memory on the system, or a Windows-specific error, defined by the corresponding error code.

Recommended Action: Verify the configuration definition of the agent. Verify that the system has adequate memory.

Failed to Open Notifier Process. PID = *Process_ID* (Windows Error Code = *Error Code*)

The notifier process was terminated.

Recommended Action: VCS marks the resource as faulted. Wait, then try to bring the resource online again.

Failed to Offline Notifier Process. PID = *Process_ID* (Windows Error Code = *Error Code*)

The agent could not terminate the notifier process. This indicates a Windows-specific error, defined by the corresponding error code.

Recommended Action: Try terminating the process manually using Task Manager.

Failed to Clean Notifier Process. PID = *Process_ID* (Windows Error Code = *Error Code*)

The agent could not terminate the notifier process. This indicates a Windows-specific error, defined by the corresponding error code.

Recommended Action: Try terminating the process manually using Task Manager.

Invalid SNMP severity specified

Invalid severity level specified for SNMP notifications,

Recommended Action: Verify the severity level specified in the SmpConsoles attribute has “Warning”, “Information”, “Error”, or “SevereError” as the severity level.

Invalid SMTP severity specified

Invalid severity level specified for SMTP notifications,

Recommended Action: Verify the severity level specified in the SmtipRecipients attribute has “Warning”, “Information”, “Error”, or “SevereError” as the severity level.

Expected correct SNMP and I or SMTP options

Invalid values specified for SNMP and SMTP attributes.

Recommended Action: Verify the attributes defined in the configuration file are assigned valid values.

Unable to online resource.Please specify correct SNMP and I or SMTP options

Invalid values specified for SNMP and SMTP attributes.

Recommended Action: Verify the attributes defined in the configuration file are assigned valid values.

Unable to find VCS_HOME. Error Code = Error Code

The value for VCS_HOME environment variable is incorrect.

Recommended Action: Verify the value for the VCS_HOME environment variable. Contact Symantec Technical Support if the problem persists.

Registry Replication agent error messages

Directory does not exist (or) could not create (directory=*Drive name:path*)

The registry replication directory specified in the configuration either does not exist or could not be created.

Recommended Action: Verify that the shared drive is accessible, and that no file in that drive has the same name as that of the ReplicationDirectory attribute. Also, verify whether the required permissions are available to create the directory.

The name of the local host is invalid (hostname= *host_name*)

This is a VCS internal error.

Recommended Action: Verify that the local host has a valid name. Contact Symantec Technical Support if the problem persists.

Failed to restore the registry (key= *Key_name*, filename= *File_name*). Possibly some applications might have keys open eg.,REGEDIT.EXE. Please close them.

The agent failed to restore the specified registry key.

Recommended Action: Close the application that accesses the specified registry keys. Contact Symantec Technical Support if the problem persists.

Duplicate key (or) Already part of notification (key=*Key_name*)

The specified registry key is already specified in the configuration.

Recommended Action: Verify that the values specified in Keys and ExcludeKeys attribute are unique.

Could not locate the file (file=*file_name*)

The agent was unable to locate the registry replication files.

Recommended Action: Verify that the files exist in the directory.

Failed to set %s

The agent failed to enable debug monitoring.

Recommended Action: Verify that monitor.exe is running. Contact Symantec Technical support if the problem persists.

Agent module and Registry-change-monitor module are not of the same version (received= %s, expected= %s)

The Registry Replication agent consists of two modules: Registry Replication and Registry Monitoring. If the versions of these modules are different, the agent will not come online.

Recommended Action: Verify the version of both agent modules. Contact Symantec Technical Support if problem persists.

Configuration Error : Key '*Key_name*' is configured in Replication Key List as well as in Exclude Key List

The specified key is configured both for Keys and ExcludeKeys attribute.

Recommended Action: Verify the configuration definition of the attributes Keys and ExcludeKeys. Make sure a specific key is not defined for both the attributes.

Configuration Error : Key '*Key_name*' configured in Replication Key List is a Sub Key of key '*Key_name*' configured in Exclude Key List

The specified key is configured for replication while its super key is configured for exclusion.

Recommended Action: Verify the configuration definition of the attributes Keys and ExcludeKeys.

VRTSWebApp agent error messages

Invalid parameters. Resource name not specified

No name specified for the resource.

Recommended Action: Verify the configuration and assign a name to the resource.

Invalid parameters. AppName not specified

No value specified for the AppName attribute.

Recommended Action: Verify the configuration file and specify a value for the AppName attribute.

Invalid parameters. InstallDir not specified

No value specified for the InstallDir attribute.

Recommended Action: Verify the configuration file and specify a value for the InstallDir attribute.

Invalid parameters. TimeForOnline not specified

No value specified for the TimeForOnline attribute.

Recommended Action: Verify the configuration file and specify a value for the TimeForOnline attribute.

Error executing command: *command*. Assuming the default path for VRTSweb

The agent failed to run the utility, vrtswbinfo.exe. The agent uses this utility to determine the path of the Veritas Web Server.

Recommended Action: Contact Symantec Technical Support.

Proxy agent error messages

Target Resource Name is not a valid name

The resource name specified in the TargetResName attribute is invalid.

Recommended Action: Verify the TargetResName attribute defined in the configuration file is assigned a correct value.

Target resource is not Probed

The agent cannot monitor the target resource because the target resource has not been probed.

Recommended Action: Verify that the target resource has been probed. To get the probed status of the target resource, execute `hares -display` from the command prompt.

Phantom agent error message

Contact Symantec Technical Support for any errors associated with the Phantom agent.

FileNone agent error message

File Name is not specified

The configuration file does not contain the path name, or the configured path name is incorrect.

Recommended Action: Verify that the attribute PathName is correctly defined in the configuration file.

ElifNone agent error message

FileName is not valid

The configuration file does not contain the path name, or the configured path name is incorrect.

Recommended Action: Verify that the attribute PathName is correctly defined in the configuration file.

FileOnOff agent error messages

Unable to create the file

The agent was unable to create the specified file.

Recommended Action: Verify that the filename specified in the PathName attribute does not contain any special characters, and the directory where the file will be created, exists on the node.

Unable to delete the file

The agent was unable to delete the specified file.

Recommended Action: Verify the filename specified in the PathName attribute exists, and the file is not locked by another user.

FileOnOnly agent error messages

ERROR! FileName is not valid

The configuration file does not contain the path name, or the configured path name is incorrect.

Recommended Action: Verify that the attribute PathName is correctly defined in the configuration file.

Unable to create the file

The agent was unable to create the specified file.

Recommended Action: Verify that the filename specified in the PathName attribute does not contain any special characters, and the directory where the file will be created, exists on the node.

Index

A

agent functions

- CompositeFileShare 67
- ElifNone 137
- FileNone 136
- FileOnOnff 138
- FileOnOnly 139
- FileShare 59
- GenericService 96
- IIS 88
- IP 35
- IPMultiNicPlus 37
- Lanman 43
- MSMQ 111
- MSVirtualMachine 84
- NIC 32
- NotifierMngr 116
- Phantom 135
- PrintShare 80
- PrintSpool 76
- Process 105
- Proxy 132
- RegRep agent 121
- RemoteGroup 140
- ServiceMonitor 100
- VMDg 20
- VRTSWebApp 129

agent log

- format 151
- location 151

agents

- CompositeFileShare 66
- ElifNone 137
- FileNone 136
- FileOnOff 138
- FileOnOnly 139
- FileShare 58
- GenericService 96
- IIS 88
- IP 35
- IPMultiNicPlus 37

- Lanman 42
- MountV 25
- MSMQ 111
- MSVirtualMachine 84
- NIC 32
- NotifierMngr 116
- Phantom 135
- PrintShare 80
- PrintSpool 76
- Process 105
- Proxy 132
- RegRep 121
- RemoteGroup 140
- ServiceMonitor 100
- VMDg 20
- VRTSWebApp 129

application agents

- IIS agent 88
- MSVirtualMachine 84

attribute definitions

- CompositeFileShare agent 68
- ElifNone agent 137
- FileNone agent 136
- FileOnOff agent 138
- FileOnOnly agent 139
- FileShare agent 61
- GenericService agent 97
- IIS agent 89
- IP agent 36
- IPMultiNicPlus agent 39
- Lanman agent 45
- MountV agent 27
- MSMQ agent 112
- MSVirtualMachine agent 86
- NIC agent 33
- NotifierMngr agent 117
- Phantom agent 135
- PrintShare agent 81
- PrintSpool agent 77
- Process agent 106
- Proxy agent 133
- RegRep agent 123

- RemoteGroup agent 142
- ServiceMonitor agent 102
- VMDg agent 21
- VRTSWebApp agent 130
- attributes
 - data types 13
 - dimensions 13

B

- bundled agents
 - categories 14
 - definition of 11

C

- CompositeFileShare agent
 - agent functions 67
 - attribute definitions 68
 - dependencies 66
 - description 66
 - error messages 174
 - sample configuration 73
 - state definitions 67
 - type definition 67

D

- DNS servers, updating 54

E

- ElifNone agent
 - agent functions 137
 - attribute definitions 137
 - description 137
 - error messages 203
 - sample configuration 137
 - state definitions 137
 - type definition 137
- error messages
 - agent log 151
 - See Also troubleshooting

F

- FileNone agent
 - agent functions 136
 - attribute definitions 136
 - description 136
 - error messages 203

- sample configuration 136
- state definitions 136
- type definition 136

FileOnOff agent

- agent functions 138
- attribute definitions 138
- description 138
- error messages 203
- sample configuration 138
- state definitions 138
- type definitions 138

FileOnOnly agent

- agent functions 139
- attribute definitions 139
- description 139
- error messages 204
- sample configurations 139
- state definitions 139
- type definition 139

FileShare agent

- agent functions 59
- attribute definitions 61
- dependencies 58
- description 58
- error messages 172
- sample configuration 65
- state definitions 59
- type definition 60

FileShare agents

- CompositeFileShare agent 66
- FileShare agent 58

G

- GenericService agent
 - agent functions 96
 - attribute definitions 97
 - description 96
 - error messages 186
 - sample configuration 99
 - state definitions 96
 - type definition 97

I

- IIS agent
 - agent functions 88
 - attribute definitions 89
 - description 88
 - error messages 182

- sample configurations 91
- state definitions 88
- type definition 88
- infrastructure and support agents
 - ElifNone agent 137
 - FileNone agent 136
 - FileOnOff 138
 - FileOnOnly 139
 - NotifierMngr agent 116
 - Phantom agent 135
 - Proxy agent 132
 - RegRep agent 121
 - RemoteGroup agent 140

IP agent

- agent functions 35
- attribute definitions 36
- dependency 35
- description 35
- error messages 162
- sample configuration 36
- state definitions 35
- type definition 35

IPMultiNicPlus agent

- agent functions 37
- attribute definitions 39
- description 37
- error messages 164
- sample configuration 41
- state definitions 38
- type definition 38

L

Lanman agent

- agent functions 43
- attribute definitions 45
- changing dependency 42
- dependency 42
- description 42
- error messages 168
- sample configuration 55
- state definitions 43
- type definition 44
- updating DNS servers 54

logging

- agent log 151

M

MountV agent

- agent functions 25
- attribute definitions 27
- dependency 25
- description 25
- error messages 156
- sample configuration 29
- state definitions 25
- type definition 26

MSMQ agent

- attribute definitions 112
- dependencies 111
- description 111
- sample configuration 113
- state definitions 111
- type definition 112

MSVirtualMachine agent

- agent functions 84
- attribute definitions 86
- dependencies 84
- error messages 180
- functions 84
- sample configuration 87
- state definitions 85
- type definition 85

N

network agents

- IP agent 35
- IPMultiNicPlus agent 37
- Lanman agent 42
- NIC agent 32

NIC agent

- agent functions 32
- attribute definitions 33
- description 32
- error messages 160
- sample configuration 34
- state definitions 32
- type definition 33

NotifierMngr agent

- agent functions 116
- attribute definitions 117
- description 116
- error messages 197
- state definitions 116
- type definition 117

P

Phantom agent

- agent functions 135
- description 135
- error messages 202
- sample configuration 135
- state definitions 135

PrintShare agent

- agent functions 80
- attribute definitions 81
- dependency 80
- description 80
- error messages 178
- sample configuration 81
- state definitions 80
- type definition 80

PrintShare agents

- PrintShare agent 80
- PrintSpool agent 76

PrintSpool agent

- agent functions 76
- attribute definitions 77
- dependencies 76
- description 76
- error messages 176
- sample configuration 78
- state definitions 77
- type definition 77

Process agent

- agent functions 105
- attribute definitions 106
- description 105
- error messages 193
- sample configuration 110
- state definitions 105
- type definition 106
- using batch files 110

Proxy agent

- agent functions 132
- attribute definitions 133
- description 132
- error messages 202
- state definitions 132
- type definition 132

R

registry keys

- abbreviations 126

configuring 126

excluding 126

RegRep agent

- agent functions 121
- attribute definitions 123
- configuring registry keys 126
- dependency 121
- description 121
- error messages 199
- excluding registry keys 126
- sample configuration 127
- state definitions 122
- type definition 122

RemoteGroup agent

- agent functions 140
- attribute definitions 142
- description 140
- state definitions 141
- type definition 141

resource type definition

- CompositeFileShare agent 67
- ElifNone agent 137
- FileNone 136
- FileOnOff agent 138
- FileOnOnly agent 139
- FileShare agent 60
- GenericService 97
- IIS agent 88
- IP agent 35
- IPMultiNicPlus agent 38
- Lanman agent 44
- MountV agent 26
- MSMQ agent 112
- MSVirtualMachine agent 85
- NIC agent 33
- NotifierMngr agent 117
- PrintShare agent 80
- PrintSpool agent 77
- Process agent 106
- Proxy agent 132
- RegRep agent 122
- RemoteGroup agent 141
- ServiceMonitor 101
- VMDg agent 21
- VRTSWebApp agent 129

S

ServiceMonitor agent

- agent functions 100

- attribute definitions 102
- description 100
- error messages 190
- sample configurations 104
- state definitions 100
- type definition 101
- services agents
 - GenericService agent 96
 - MSMQ agent 111
 - Process agent 105
 - ServiceMonitor agent 100
- state definitions
 - CompositeFileShare agent 67
 - ElifNone agent 137
 - FileNone agent 136
 - FileOnOff agent 138
 - FileOnOnly agent 139
 - FileShare agent 59
 - GenericService agent 96
 - IIS agent 88
 - IP agent 35
 - IPMultiNicPlus 38
 - Lanman agent 43
 - MountV agent 25
 - MSMQ agent 111
 - MSVirtualMachine agent 85
 - NIC agent 32
 - NotifierMngr agent 116
 - Phantom agent 135
 - PrintShare agent 80
 - PrintSpool agent 77
 - Process agent 105
 - Proxy agent 132
 - RegRep 122
 - RemoteGroup agent 141
 - ServiceMonitor agent 100
 - VMDg agent 20
 - VRTSWebApp agent 129
- storage agents
 - MountV agent 25
 - VMDg agent 20

T

- troubleshooting
 - CompositeFileShare agent 174
 - ElifNone agent 203
 - FileNone agent 203
 - FileOnOff agent 203
 - FileOnOnly agent 204

- FileShare agent 172
- GenericService agent 186
- IIS agent 182
- IP agent 162
- IPMultiNicPlus agent 164
- Lanman agent 168
- logging 151
- MountV agent 156
- MSVirtualMachine agent 180
- NIC agent 160
- NotifierMngr agent 197
- Phantom agent 202
- PrintShare agent 178
- PrintSpool agent 176
- Process agent 193
- Proxy agent 202
- RegRep agent 199
- ServiceMonitor agent 190
- VMDg agent 153
- VRTSWebApp agent 201

type definition. See resource type definition

V

- VCS
 - about bundled agents 11
 - logging 151
- Volume Manager Diskgroup agent (VMDg)
 - agent functions 20
 - attribute definitions 21
 - description 20
 - error messages 153
 - sample configuration 24
 - state definitions 20
 - type definition 21
- VRTSWebApp agent
 - agent functions 129
 - attribute definitions 130
 - dependency 129
 - description 129
 - error messages 201
 - sample configuration 131
 - state definitions 129
 - type definition 129

