

Veritas™ Cluster Server One User's Guide

AIX, HP-UX, Linux, Solaris

5.0



Veritas™ Cluster Server One User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 5.0

Document version: 5.0.0

Legal Notice

Copyright © 2009 Symantec Corporation. All rights reserved.

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.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice file accompanying this Symantec product for more information on the Third Party Programs.

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.

THE 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 as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

http://www.symantec.com/business/support/assistance_care.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:

- Error messages and log files
- Troubleshooting that was performed before contacting Symantec
- Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to clustering_docs@symantec.com.

Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting.

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Section I Concepts

Chapter 1 Introducing Veritas Cluster Server One

About Veritas Cluster Server One	32
About the Simulator	32
What you can do with VCS One	33
Sample solutions using VCS One	33
Where to get more information about VCS One	34

Chapter 2 Components of Veritas Cluster Server One

Components of application management	36
About managed applications	36
About resources and resource dependencies	37
About service groups and service group dependencies	38
About composite service groups	40
About systems	41
About the Organization Tree	41
About users, user groups, and their roles	43
About extended attributes	44
Physical components of a VCS One environment	46
About the physical systems in the VCS One cluster	46
About customer systems	46
About storage in the VCS One cluster	47
About networking in the VCS One cluster	47
Policy Master components	47

Chapter 3 How VCS One works

How the Policy Master manages the applications	52
About the client daemon vcsoneclientd	52
About agents	52
How the Policy Master and the VCS One clients start up	54
First initialization of the VCS One cluster	54
Policy Master start up modes	54
How the Policy Master loads the VCS One cluster configuration	56

- How the Policy Master and client systems resolve
 - failures in communication 58
 - VCS One cluster membership 58
- How you can define service group load and system capacity 59
- How to control the scheduling class and scheduling
 - priority of agent operations 61
- How you can configure automated tasks and group operations 62
 - Schedule 62
 - Events 62
- How VCS One provides security in communications 63

Chapter 4 How VCS One global clusters work

- About VCS One global clusters 66
- About global cluster building blocks 67
- Typical VCS One global cluster setup 68
- How global clusters work 69
 - How VCS One global clusters communicate with each other 69
 - How VCS One enables wide-area failover of a multi-tier application . 71
 - How VCS One determines the state of a multi-tier application 72
 - How VCS One resolves authority for application that spans clusters 72
 - How VCS One responds to various disasters 73

Chapter 5 How the Policy Master cluster protects data

- About protecting data in the VCS One cluster 80
- About communications in the Policy Master cluster 80
 - About communications between systems in the Policy Master cluster 80
 - About inter-system Policy Master cluster communications 81
- About membership in the Policy master cluster 84
 - Initial joining of systems to the Policy Master cluster membership .. 85
 - Ongoing Policy Master cluster membership 86
- About membership arbitration in the Policy Master cluster 87
 - Components of membership arbitration 87
 - How the fencing module starts up 88
 - How membership arbitration works 89
- About data protection in the Policy Master cluster using SCSI-3 storage . 91
- How I/O fencing works 92
 - About the I/O fencing algorithm 92
 - Two system Policy Master cluster where one system fails 93
 - Four system Policy Master cluster where cluster interconnect fails .. 94
- Best practices for Policy Master cluster communications 96

Section II Getting started

Chapter 6 Starting and stopping Veritas Cluster Server One

- About VCS One user interfaces 102
- Setting the PATH variable to use the CLI 102
- Before starting the VCS One console 102
 - Changing Web browser settings 103
 - Starting and logging on to the VCS One console 104
 - Logging on to VCS One using the command line 105
- Logging off from the VCS One console 106

Chapter 7 Using the VCS One console

- About the VCS One console 108
- About VCS One console ports 108
- Managing SSL certificates 108
 - Configuring and Managing SSL certificates (optional) 109
- VCS One console layout 109
 - About the tab bar 110
 - About disabled menu items 111
 - About panes 111
 - About console refresh 112
 - About tables 112
 - About selecting menu commands 116
 - About filtering objects using the organization tree 116
 - About the History menu bar 117
 - About wizards 117
 - About VCS One Help 117
 - Logging off from the VCS One console 118
- Summary information on the Home tab 118
- Manage tab options 120
 - Workload tab menus 121
 - Service Groups tab operations 130
 - Composite Service Groups tab operations 139
 - Systems tab operations 142
 - Resources tab operations 145
 - Disaster Recovery tab operations 148
 - Jobs tab operations 151
 - Business Rules tab and Notification Rules tab operations 153
- Logs tab options 156
 - About log message filters 156
 - About log message deletion 161
- Administration tab options 162

Users tab operations	162
Roles tab operations	164
Organization Units tab operations	165
Extended Attributes tab operations	166
Sets tab operations	168
Settings tab operations	169
Summary information on the Search tab	172

Chapter 8 Using the Simulator

About the Simulator	174
The difference between a real and a simulated VCS One cluster	175
Choosing a configuration for the Simulator	175
Components of the Simulator	176
About the Simulator's start-up modes	177
About multiple Simulator instances	178
About Simulator scripts and commands	179
Viewing Simulator command usage	179
Starting the default Simulator instance	180
Adding a Simulator instance	181
Starting a Simulator instance	182
Starting a Simulator instance	182
Starting a Simulator instance with the same state information that is in the database	182
Starting a Simulator instance in read-only mode	183
Starting a Simulator instance with non-default ports	183
Loading or changing a configuration in the Simulator	186
Loading a sample configuration and starting a Simulator instance	186
Loading a custom configuration and starting a Simulator instance	186
Loading the real Policy Master configuration into a Simulator instance	187
Changing the configuration that is loaded in a Simulator instance	187
About logging on to the Simulator	189
Accessing the GUI for a Simulator instance	189
Accessing the GUI for the default Simulator	189
Accessing the GUI for a Simulator instance	190
Accessing the command line for a Simulator instance	190
Accessing the command line for the default Simulator instance	190
Accessing the command line for a Simulator instance	191
Creating and saving a custom configuration in the Simulator	192
Displaying the status of a Simulator instance	192
Listing Simulator instances	193
Listing port information for a Simulator instance	194
Setting up a disaster recovery configuration in the Simulator	194

- Simulating disaster recovery operations using the Simulator199
- Stopping a Simulator instance199
 - Stopping the default Simulator instance199
 - Stopping a Simulator instance200
- Removing a Simulator instance200

Section III Design

Chapter 9 Design overview

- Introduction204
- Planning204
 - Define your goals204
 - Determine the current environment205
 - Determine the difference between goals and current environment ..206
 - Planning your user privilege model209
 - Planning the names of your VCS One cluster objects and attributes 209
- Preparing211
- Implementing212
- Configuring and verifying213
 - Configuring the Policy Master cluster213
 - Configuring the VCS One cluster214

Chapter 10 Designing roles and privileges for users

- About designing roles and privileges for users218
 - About user groups218
 - About privileges218
 - What information identifies a user or user group219
 - About roles219
- About users and the Organization tree221
- How you manage users using the Organization Tree221
 - About the architecture of the Organization Tree223
- About user permissions in the organization tree225

Chapter 11 Designing actions taken after a fault

- About designing the actions taken after a fault228
 - Resource level control228
 - Service group level control230
 - System level control231
- Configuration examples of fault handling behavior232

Chapter 12 Designing attribute values using variables

About designing attribute values using variables	234
Examples of using a resource variable	234
Example 1	234
Example 2	235
Example 3	236
What can be defined using a resource variable	237
Where a variable can be used	238
Resource variable syntax	238
Where a variable cannot be used	239
Design implications of resource variables	240

Chapter 13 Designing service groups

About designing service groups	242
Managed applications planning	242
Defining a service group	243
Defining service group dependencies	243
Shared storage	244
Additional planning for applications in failover environments	244
About bringing running applications under VCS One control	245
Designing the type of service group	245
Designing the name of a service group	246
Designing the Priority of a service group	246
Designing application movement within a local site	246
Designing multi-tier applications	247
About designing service group dependencies	247
Design rules of service group dependencies	247
Types of service group dependencies	249
Service group dependency configurations	251
Design rules of composite service groups	258
Designing service groups that use off-host resources	260
About off-host resources in service groups	260
How off-host resources work	261
Counting off-host resources managed by an agent	262
Optimizing the off-host resource setup	263
Using multiple control groups to improve scalability	263
Off-host resources: user privileges	264
Designing service groups that run in Solaris zones	264
Overview of how VCS One works with zones	264
Designing attributes values for zone support	265
Designing resource dependencies	266
Designing service groups that run in AIX WPARs	269

- Overview of how VCS One works with WPARs269
- About the WPAR agent269
- Designing attributes values for WPAR support270
- Designing resource dependencies for WPAR-enabled service groups 271

Chapter 14 Designing application placement policy

- About designing application placement policy274
- About managing applications274
- Application start and stop configuration274
- Manual application switch configuration275
- About automated failover configurations275
- About Priority277
- About disruption factor and kickout277
- Application relationships through service group compatibility278
- About service group Load and system Capacity for physical systems280
- Breaking the tie: the FragmentationPolicy attribute281
- Mapping an application placement decision282
 - About the Group Transition Queue283
 - Choosing the best target system for groups without dependencies ..284
 - Choosing the best target system for groups with dependencies285
 - Events that re-examine intent-online GTQ entries286

Section IV Tasks: Managing components

Chapter 15 Managing systems

- Adding a system to the VCS One cluster292
 - Checking installation prerequisites292
 - Installing the VCS One client293
 - Adding a configured system to the VCS One cluster293
- Locating a system295
- Viewing system attributes296
- Editing system attributes297
- Adding a system to the VCS One cluster using the Simulator297
- Deleting a system from the VCS One cluster298
- Freezing a system300
- Unfreezing a system302
- Starting and stopping the VCS One client daemon on a system303
- Faulting a system305
- Faulting a system using the Simulator305
- Repairing a system using the Simulator306
- Moving a system to another organization tree node306
- Viewing a selected list of systems308

Displaying system information	308
Putting a system in the OFFLINE state	309
Simulating a system in DDNA state	309
Simulating a system heartbeat failure	310
Simulating a system heartbeat recovery	311

Chapter 16 Managing service groups

About service groups	315
Adding a service group	315
Locating a service group	321
Using the Group Dependency View	323
Locating the Group Dependency View	323
Performing operations from the Group Dependency View	323
Viewing service group attributes	324
Editing service group attributes	324
Editing attributes using the All Attributes link	325
Refreshing a service group's SystemList	325
Deleting a service group	326
Modifying a service group	327
Moving a service group to another organization tree node	327
Bringing a service group online	329
Taking a service group offline	333
Switching a service group	336
Flushing a pending action on a service group	337
Flushing the plan of action on all service groups in the GTQ	338
Stopping the current action for a service group in the GTQ	339
Freezing a service group	339
Unfreezing a service group	340
Enabling a service group	342
Disabling a service group	342
Faulting a service group in the Simulator	343
Clearing a service group fault	344
Linking service groups	345
Unlinking service groups	346
Enabling service group resources	347
Disabling service group resources	348
Probing service group resources	349
Bringing service group resources online	349
Taking service group resources offline	350
Cloning service groups	350
Changing a service group's priority value	351
Changing a service group's load value	352
Configuring a service group's SystemList with a list of systems	353

Configuring a service group's SystemList with an expression	354
Configuring a service group's compatibility list	355
Configuring a service group's fault policy	356
Creating an off-host resource in a service group	357
Creating an off-host resource with NetApp Filer	358
Viewing off-host resource sample configuration	361

Chapter 17 Managing composite service groups

About managing composite service groups	364
Creating a composite service group	364
Listing composite service groups and unassociated service groups	367
Viewing details about a composite service group	368
Modifying the group list of the CSG	369
Editing a composite service group's attributes	371
Deleting a composite service group	371
Moving a local composite service group in the organization tree	372
Bringing a composite service group online	373
Taking a composite service group offline	374
Flushing a pending action on a composite service group	375

Chapter 18 Managing resources

Using the Resource Dependency View	379
Locating the Resource Dependency View	379
Performing operations from Resource Dependency View	379
Arranging the Resource Dependency View using the Navigator	379
Adding a resource to a service group	380
Deleting a resource from a service group	381
Editing resource attributes	381
Modifying zone resource attributes	382
Enabling resources in a service group	383
Disabling resources in a service group	384
Bringing a resource online	384
Taking a resource offline	385
Taking parent and child resources offline concurrently	386
Probing a resource	386
Faulting a resource using the Simulator	387
Repairing a resource using the Simulator	388
Clearing a resource fault	388
Clearing resources in the ADMIN_WAIT state	389
Linking resources	390
Unlinking resources	392
Viewing resources in the configuration by resource type	392

Defining an attribute value with a resource variable	393
Displaying values to be affected by a change in a resource variables definition	394
Updating the value of a resource variable	395

Chapter 19 Managing application placement

About managing application placement	398
Defining the SystemList attribute for a service group	398
Defining service group priority	400
Defining service group compatibility or incompatibility	400
Defining a resource's fault policy	402
Defining a service group's fault policy	402
Defining a system's fault policy	403
Defining the VCS One cluster's load and capacity keys	404
Defining service group load	405
Defining system capacity	405
Defining the VCS One cluster's FragmentationPolicy attribute	406
Viewing the application placement	406

Chapter 20 Managing automated tasks

About managing automated tasks	410
Automated business rules	410
Automated notification rules	410
Creating a rule	411
Creating a business rule	411
Creating a notification rule	414
Adding or modifying conditions and filters for the rule	417
Listing rules	419
Displaying the details of a rule	419
Viewing rules and jobs that are associated with an object	420
Cloning a rule	420
Creating a job	421
Associating a job with a rule	423
Cloning a job	423
Modifying a job	423
Running a job	424
Deleting a job	424
Changing the owner of a rule	425
Enabling a rule	425
Disabling a rule	426
Modifying a rule	427
Deleting a rule	428

- About configuring tasks428
- Exporting a rule or a job to an XML file428
- Importing a rule or a job from an XML file429

Section V Tasks: Managing virtualization technologies

Chapter 21 Managing objects in Solaris zones

- About managing objects in Solaris zones434
- Zone configuration prerequisites435
- Deciding on the zone root location436
- Creating a Solaris zone436
- About installing applications in a zone438
- Configuring the application service group for the zone439
- Configuring the local zone to run ha-commands439
- Configuring Zone-Policy Master communication440
 - Configuring Zone-Policy Master communication within a local site440
 - Configuring Zone-Policy Master communication with a disaster recovery configuration441
- Viewing zone operations442
- Modifying zone resource attributes442
- Example of configuring an application to run inside a zone443

Chapter 22 Managing objects in AIX Workload Partitions (WPARs)

- About managing service groups in AIX Workload Partitions454
- Prerequisites for configuring VCS One in WPARs454
- Setting the WPAR root path455
 - Creating a WPAR root on local disk456
 - Creating WPAR root on shared storage using NFS457
- Installing the application458
- Creating the WPAR-enabled service group459
- Configuring WPAR-Policy Master communication459
- Adding the WPAR hostname as a principal461
- Maintenance tasks464

Section VI Tasks: Setting up and managing global clusters

Chapter 23 Setting up VCS One global clusters

- About setting up VCS One global clusters470
- Setting up a global cluster configuration471
 - Configuring application and replication471
 - Configuring clusters472

Configuring service groups	473
Configuring global CSGs	473
Testing VCS One disaster recovery support	474

Chapter 24 Managing remote clusters

About managing remote clusters	478
Adding remote clusters	478
Determining the connection role of clusters	480
Viewing remote clusters	481
Viewing remote cluster details	482
Editing remote cluster attributes	483
Deleting remote clusters	484
Enabling connections between clusters	485
Disabling connections between clusters	485
Viewing the status of individual network links	486
Viewing the consolidated status of network links	487
Viewing the state of the clusters	488
Modifying remote cluster configuration	488
Changing the local cluster's DR port value	491
Changing the local cluster's DR address value	492
Faulting a remote cluster using the Simulator	492
Clearing a simulated cluster fault using the Simulator	493
Simulating a link fault	493
Clearing a simulated link fault	494

Chapter 25 Managing global composite service groups

About managing global composite service groups	498
Configuring a global CSG	498
Requesting authority for a global CSG	499
Bringing a global CSG online	500
Switching a global CSG	502
Taking over a global CSG	503

Section VII Tasks: Administering your Enterprise environment

Chapter 26 Administering the organization tree

About administrating the organization tree	508
About building an organization tree	508
How to build an organization tree	508
Administering the organization tree	510

	Viewing the organization tree hierarchy	510
	Moving systems, service groups, or users between organization tree nodes	511
	List the OUName for an OUValue	511
	List the set of OUValues for an OUName	511
	List the defined set of objects associated with an organizational unit	512
	Deleting an OUName node from the organization tree	512
	Deleting OUValue nodes from the organization tree	513
Chapter 27	Administering attributes and settings	
	About administering attributes and settings	516
	Editing VCS One cluster attributes	516
	About extended attributes	517
	Defining an extended attribute	518
	Assigning an extended attribute a value	519
	Combining extended attributes in an expression	520
	Deleting an extended attribute	521
	Modifying the value of an inherited extended attribute	521
	Modifying the value of a locally defined extended attribute	523
	Modifying notification settings	523
	Enabling notification settings	525
	Disabling notification settings	526
	Enabling syslog notifications	526
	Disabling syslog notifications	527
	Enabling script execution	527
	Disabling script execution	527
	Testing notification settings	528
Chapter 28	Administering users and roles	
	About administering users and roles	530
	Checking your VCS One cluster privileges	530
	Adding or deleting a user or usergroup	530
	Adding a user or usergroup	531
	Cloning a user or user group	532
	Deleting a user or usergroup	532
	Assigning or unassigning a role and objects to a user or usergroup	533
	Adding custom roles	534
	Cloning a role	536
	Editing a role	536
	Deleting a role	537
	Modifying user or usergroup settings	538
	Editing user or user group attributes	538

Moving a user to another Organization Tree node:	539
Enabling a user or usergroup	539
Disabling a user or usergroup	540
Viewing a user's or user group's settings, roles and associated objects ...	541
Displaying roles	542
Displaying role types	542
Displaying the permitted operations for a role type:	542
Authenticating VCS One users	543
Issuing commands from the command line	544
Issuing commands through a script from client systems	546

Chapter 29 Administering sets of objects

About administrating sets of objects	550
Building a set	550
Viewing objects in a set	552
Viewing the details of a set definition	552
Deleting a set	552
Modifying a set	553
Configuring a custom view of the organization tree and extended attributes	553
Deleting a custom view	555
Modifying a custom view	555

Section VIII Tasks: Administering the Veritas Cluster Server One product

Chapter 30 Administering the Policy Master service group

About administering the Policy Master service group	560
About the Policy Master service group	560
Monitoring the state of the Policy Master service group	561
Tuning attributes of the Policy Master service group	562
Tuning the DetailMonitoring attribute of the Policy Master resource	562
Bringing the PMSG online	563
Taking the PMSG offline	563

Chapter 31 Administering the VCS One cluster configuration database

About the VCS One configuration	566
About the configuration files	567
Location of the configuration files	567
About the types file	568
Starting the Policy Master in COLD mode	570

Managing the configuration database	571
Starting the database	571
Cleaning the database	571
Verifying the configuration	572
Seeding the database using XML files	572
Seeding the database using existing database files	572
Stopping the database	573
Restarting the database	573
Viewing the database status	573
Changing the database password	574
Initializing the database	574
Backing up and restoring VCS One data	575
Backing up the VCS One configuration database	575
Restoring the VCS One configuration database	577
Backing up Symantec Product Authentication Service configuration information	578
Restoring Symantec Product Authentication Service configuration information	578

Chapter 32 Troubleshooting VCS One issues

About VCS One log messages	582
Adding custom log messages to the log file	582
Policy Master logs	583
VCS One client logs	583
Simulator logs	584
Symantec Web server logs	584
Turning on Symantec Product Authentication Service logs	584
Viewing logs from commands generated by the VCS One console	585
About logs generated from events	585
About logs generated from rules	586
Deleting event and rule log entries	586
Deleting job log entries	586
About the first failure data capture (FFDC) log	587
Interpreting VCS One log messages	587
Troubleshooting VCS One issues	589
Using the Simulator to reproduce issues	589
How to use the Simulator to duplicate your live installation	589
About disabled menu items	590
CLI commands appear to hang	590
The Search tab does not display	591
Tuning the Policy Master to use a higher number of file descriptors	591
ha- commands run slowly when NIS or LDAP is unavailable	592
State of service group is UNKNOWN	592

State of service group is incorrect	592
Faulted resource state not reflected in service group state	593
Duplicate TCP line messages	593
VCS One client does not connect to Policy Master	594
Policy Master service group stuck in PARTIAL state	594
Increasing LogFileSize generates error	594
Negative values not displayed in the Workload section	595
User gets unexpectedly logged out from the VCS One console	595
Small fonts displayed in Flash components	596
Organization Tree and Extended Attributes views not click-able	596
Organization Tree right-click menu not functional on Linux Firefox	597
Summary and Workload sections not automatically refreshed	597
Web browser crashes while performing AWM tasks	597
Views containing Flash content take a long time to load	598
I/O fencing on client system appears to fail	598
Console displays an unexpected error message	598
Loading XML configuration into the database fails	599
Service group will not go offline	599
Resource stuck in the unable to offline state	600
A rule does not execute	600
VCS One ha- commands do not work in a WPAR	601
Resource does not come online in the WPAR	601
Error messages occur when using the command script generated from the haconf command	601
Troubleshooting Simulator issues	603
Console connection issue when using multiple Simulator instances through Firefox	603
Non-administrator users cannot start the Simulator on Windows Vista	603
Simulator does not start	603
Simulator fails to start in remote sessions	604
Network connection error during Simulator startup	605
Enterprise users cannot execute non-Simulator commands	605
Simuser log on failure with real-time VCS One cluster configuration	606
Troubleshooting VCS One global cluster issues	608
Unable to establish connection between VCS One clusters	608
VCS One cannot online DRSG service group	609
Unable to view or modify remote cluster attributes	610
Unable to view CSG attributes for a remote cluster	610
Inter-cluster operations fail for the CSG	611
No concurrency violation triggered when CSG is online at both sites	611
Service groups that belong to a CSG fail to come online	612

- Resources or groups that belong to a CSG fail to come online612
- CSG concurrency violation when the state of the CSG is up-to-date .613
- CSG concurrency violation when the state of the CSG is stale613
- ATTN flag is set for the CSG614
- VCS One does not clear the PENDING flag in the CSGState
 - attribute614
- Value of the LinkStatus attribute toggles
 - between UP and DISABLED615
- Troubleshooting authentication issues616
 - Changing FQDN causes authentication failure616
 - Authentication broker and Policy Master trust not established616
 - Symantec Web Server log on failure617
 - VCS One client certificate verification failure618
 - VCS One console fails to start620
 - VCS One CLI commands fail to execute620
 - Business policy automation not working621
- About the hagetcf utility622
- About Symantec Technical Support623

Section IX Reference

Chapter 33 Reference of privileges

- Pre-defined roles in VCS One628
- About role categories629
- About privileges categories630
 - Catalog of farm privileges630
 - Catalog of object privileges631
 - Catalog of system privileges632
 - Catalog of group privileges633
 - Catalog of composite service group privileges635
 - Catalog of resource privileges636
 - Catalog of user privileges637
 - Catalog of organization tree privileges637
 - Catalog of notifier privileges638
 - Catalog of VObject privileges638
 - Catalog of Pframe privileges639
 - Catalog of Vframe privileges640
 - Catalog of automation privileges641

Chapter 34 Automated tasks reference

- About events644
 - Policy Master events reference645

About rules	660
Rule conditions reference	661
About jobs	662
Components of a job	662
Privileges of a job	662
About tasks	663
Privileges of a task	666

Chapter 35 Configuration file reference

About the VCS One configuration in XML	668
Building blocks of an XML configuration file	668
The main.xml file format	669
Sample main.xml configuration file	671
The bpa.xml file format	673
Business rule definition	673
Job Definition	673
Notification rule definition	673
Automation Settings	674
Sample bpa.xml configuration file	674
The prefs.xml file	676

Chapter 36 Attributes reference

About attributes	678
About the data-type of attributes	678
About the dimension of attributes	678
Viewing and editing attributes	679
VCS One cluster level attributes	680
Composite service group attributes	692
Remote cluster attributes	697
System attributes	702
Service group attributes	712
Resource type attributes	720
Overriding static resource type attributes	720
Resource attributes	737
Role attributes	744
User attributes	747
Group Transition Queue attributes	754
Action entry attributes	755
Set name attributes	758
OUname attributes	758
OUvalue attributes	759

Chapter 37	State reference	
	Cluster states in VCS One global clusters	762
	Examples of VCS One cluster state transitions	763
	Network link states in VCS One global clusters	763
	Examples of network link state transitions	765
Glossary		767
Index		773

Concepts

This section includes the following chapters:

- [“Introducing Veritas Cluster Server One”](#) on page 31.
- [“Components of Veritas Cluster Server One”](#) on page 35.
- [“How VCS One works”](#) on page 51.
- [“How VCS One global clusters work”](#) on page 65
- [“How the Policy Master cluster protects data”](#) on page 79.

Introducing Veritas Cluster Server One

This chapter includes the following topics:

- [About Veritas Cluster Server One](#)
- [About the Simulator](#)
- [What you can do with VCS One](#)
- [Sample solutions using VCS One](#)
- [Where to get more information about VCS One](#)

About Veritas Cluster Server One

Veritas™ Cluster Server One (VCS One) solves many of the problems that are found in the complex modern datacenter. It continues to support the familiar concepts that are used in Veritas Cluster Server, such as service groups, resources, and agents. However, VCS One introduces a new product architecture. This new architecture allows many powerful capabilities to be added to the high-availability and application management features of VCS. VCS One builds upon the expertise of the use of VCS in mission-critical environments with an architecture that is ready for the newest challenges that face your datacenter.

VCS One has the following functional modes:

- VCS One HA
All functionality in VCS One is available in the VCS One HA mode.
- VCS One Start
All functionality in VCS One except the following features:
 - Auto-failover
 - Priority-based application availability

The attributes `GrpFaultPolicy` and `NodeFaultPolicy` determine the functional mode.

See [“GrpFaultPolicy”](#) on page 714.

See [“NodeFaultPolicy”](#) on page 716.

About the Simulator

You can use the simulator to simulate a VCS One cluster. You can view, modify, and test the VCS One cluster configuration and behavior.

The simulator includes the following features:

- Runs an instance of the Policy Master that simulates the Policy Master running in a real VCS One cluster. Simulator behavior is identical to the behavior in a real VCS One cluster.
- Imports the configuration from an actual VCS One cluster into the Simulator. You can troubleshoot configuration issues and perform root cause analysis in a safe simulation that does not affect the production environment.
- Induces simulated faults and view how they affect the VCS One cluster and execute failover policy. You can create and fine-tune the VCS One cluster

configuration separately from a production environment. The simulated configuration can then be imported into your production environment.

- Tests the configurations from different operating systems. For example, you can run VCS One Simulator on a Windows system and test configurations for Linux and Solaris VCS One clusters.
- Educate VCS One users in a protected environment. The simulator has the same look-and-feel as the actual VCS One software. You can reproduce your own environment for realistic lab scenarios.
- Runs on a stand-alone system.
Does not require any additional storage or networking hardware.
- Runs in either non-secure mode or secure mode.
In secure mode, all communications take place over secure channels.
- Runs from the VCS One Console or from the command line.

See [“About the Simulator”](#) on page 174.

What you can do with VCS One

Use the following VCS One capabilities to improve operations center staff efficiency and to better manage a large number of applications:

- Control applications and application components from a single interface, scalable to hundreds of systems and thousands of applications. Start, stop, and monitor applications and their related application components.
- View all applications in a data center.
- Create, control, and visualize dependencies between components of an application, as well as between applications.
- Control access to specific applications. Security and user level settings give operations staff control of specific applications without the need to provide a local logon account to the system.
- Manage application hosts with a lightweight storage, processor, and memory footprint on the client system.
- Control application hosts with secure encrypted communications.

Sample solutions using VCS One

VCS One resolves the following datacenter issues:

Where to get more information about VCS One

- Allows all applications to be monitored and controlled uniformly, with levels of availability configured as necessary for each application. In the past, these features usually were available only for highly-critical applications.
- Reduces or eliminates the need for front line operations staff to possess application-specific knowledge to start, restart, or stop complex applications.
- Removes the need to write, deploy, and maintain custom scripts to start, stop, and monitor applications in many cases.

Where to get more information about VCS One

More information about VCS One is available on the Symantec Web site:

<http://www.symantec.com>

Components of Veritas Cluster Server One

This chapter includes the following topics:

- [Components of application management](#)
- [Physical components of a VCS One environment](#)
- [Policy Master components](#)

Components of application management

The components of application management wrap a structure around your application and provide powerful tools to monitor and control your application both manually and automatically.

About managed applications

A managed application is an application service under the control of VCS One. An application service is the entire collection of hardware and software components that are required to provide an application to the end user. For example, an end user accesses an Oracle database by connecting to a particular host system.

The application is the database but the application service consists of all of the following components:

- Oracle database software, including the listener
- File systems containing data files
- Disk groups that have volumes on which the file systems reside
- One or more IP addresses
- Network Interface Card (NIC)

An application service can comprise more than one application. The database may connect to a financial application, and the financial application may have a web-based front end. In this case the application service consists of three applications: the database, the financial application, and the web-based interface.

Each managed application typically requires the following types of components:

- Application
- Storage
- Networking

[Table 2-1](#) shows the components of a managed Oracle database.

Table 2-1 Components of a managed Oracle database

Type of component	Component
Application	<ul style="list-style-type: none"> ■ Database instance ■ Database listener
Storage Components	<ul style="list-style-type: none"> ■ File system ■ Disk group

Table 2-1 Components of a managed Oracle database

Type of component	Component
Networking Components	<ul style="list-style-type: none"> ■ IP address ■ Network interface card

If a managed application is moved to another system, all of the components of the managed application move together.

About resources and resource dependencies

The hardware components and software components that make up the managed application are called resources. Resources are objects in the VCS One configuration.

As an example, an Oracle database managed application consists of the following resources:

- Database instance
- Database listener
- File System
- Disk groups
- IP address
- Network interface card

To control a managed application, you control all the resources that make up that application service. You can perform the following operations to control a resource:

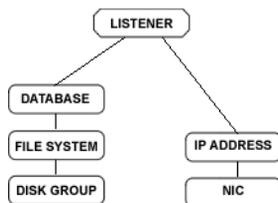
- Bring it online, or start the resource
- Take it offline, or stop the resource
- Monitor it for status and failure detection

To manage the application you must also know how the individual resources that make up the application interrelate. Resource dependencies indicate the resources that depend on each other because of application or operating system requirements.

Resource dependencies are hierarchical. This hierarchy is called a resource dependency tree. The resources higher up in the tree (parent) depend on the resources lower down in the tree (child).

[Figure 2-1](#) shows the hierarchy for an Oracle database managed application.

Figure 2-1 Sample resource dependency tree



Resource dependencies determine the order in which resources are brought online or taken offline. Child resources must be online before parent resources can be brought online. Likewise, parent resources are brought offline before child resources are taken offline.

For example, you must configure and import a disk group before you mount the file system. Conversely, file systems must be unmounted before disk groups are deported.

To start a managed application, each child resource is brought online. Then the parent that depends on the resource is brought online. This pattern continues up the tree, until finally the application is started. Conversely, to take a managed application offline, the resources at the top of the hierarchy are taken offline first.

If the resources do not have parent-child interdependencies, they can be brought online or taken offline concurrently. In the Oracle database example, the database listener is stopped first. Next, the Oracle database application and the IP address can be stopped concurrently because they do not have a resource dependency between them.

About service groups and service group dependencies

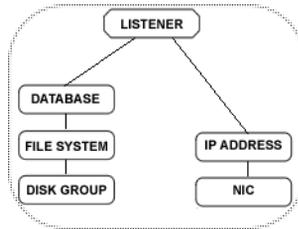
A service group is a virtual container that contains all the hardware resources and software resources that are required to run the managed application. Service groups are objects in the VCS One configuration.

Service groups allow VCS One to control all the resources of the managed application as a single unit. When a failover occurs in VCS One, the entire service group fails over as a unit. Resources do not fail over individually.

A service group can have several states, which indicate the state of the managed application.

See “[State](#)” on page 718.

[Figure 2-2](#) shows a sample service group.

Figure 2-2 Sample service group

A system may host multiple service groups, where each service group provides a discrete managed application to networked customer client systems.

If multiple service groups are running on a single system, they are monitored and managed independently. Independent management enables a service group to be manually idled or switched to another system without having an impact on the other service groups.

A service group may also be configured to failover automatically under certain predefined conditions, such as a system failure.

Actions performed on a service group

You can perform the following actions on a service group:

- Start
- Monitor
- Stop
- Switch
- Failover
- Freeze
- Unfreeze

You can perform administrative operations on individual resources and on service groups. When you perform administrative operations at the service group level, a series of commands is initiated for all of the resources within the service group.

For example, when you direct a service group to go online, an online command is initiated for each resource within that service group.

See [“Managing service groups”](#) on page 313.

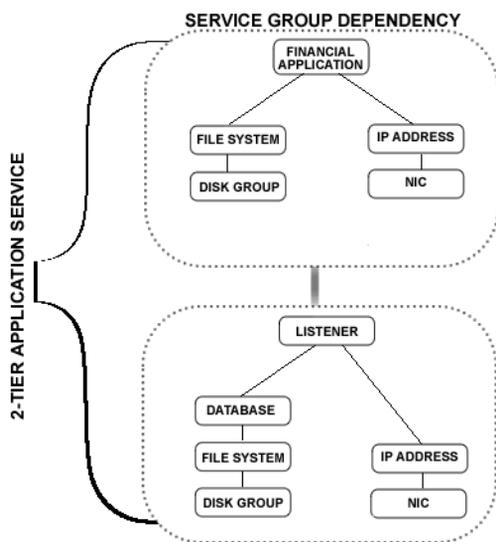
About service group dependencies

Service groups can be dependent on each other. For example a Web application can be a front end to a finance application that is in turn dependent on a database application.

The dependent service group is called the parent service group, and the service group on which it is depends is called the child service group.

Figure 2-3 is an example of a two tier service group dependency.

Figure 2-3 Two tier service group dependency



Because the managed application comprises all the components that are required to provide the application service, service group dependencies create more complex managed applications.

See [“About designing service group dependencies”](#) on page 247.

Service group dependencies affect how the service groups can come online, go offline, or move to another system.

See [“About designing application placement policy”](#) on page 274.

About composite service groups

A composite service group (CSG) is a collection of objects. Use composite service groups to manage a group of objects as a single logical object.

In this release, service groups are the only CSG-supported object. A service group may only be part of one composite service group at a time.

A composite service group can be local or global. A global composite service group is the unit of failover between different VCS One clusters.

The following examples are ways you may use composite service groups:

- To manage a multi-tier application as a single logical unit in a VCS One cluster.
- To switch a multi-tier application between two separate VCS One clusters, for example as part of a maintenance plan.
- To perform a takeover of a multi-tier application between two separate VCS One clusters, for example during disaster recovery conditions.

See [“Managing composite service groups”](#) on page 363.

In a multi-cluster environment and with global composite service groups, only one site has the authority to bring the composite service group online.

See [“Authority”](#) on page 692.

About systems

A VCS One cluster system is an entity that hosts one or more service groups (managed applications) and is associated with the following elements:

- Operating system
- VCS One client daemon (vcsoneclientd)
- Unique Symantec Product Authentication Service (AT) principal for secure communications

Systems can be of any supported platform. A VCS One cluster supports different platforms in the same VCS One cluster.

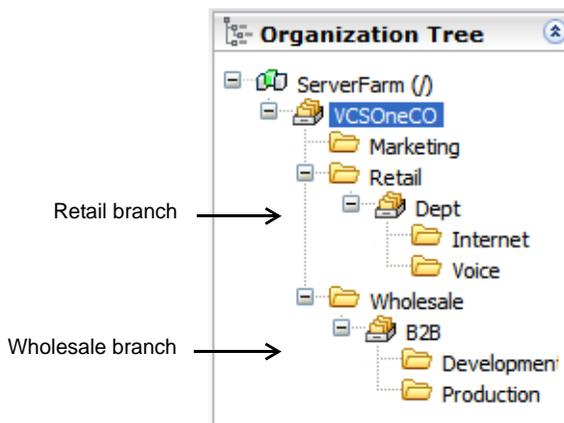
About the Organization Tree

The VCS One managed environment is collectively referred to as the VCS One cluster. An Organization Tree is a logical hierarchical structure of the VCS One cluster. The Organization Tree provides an infrastructure that is used to delineate the user views and privileges of your managed applications and the systems that run them.

The Organization Tree can be changed and the objects can move around in the tree. As the tree changes, the user privileges are dynamically updated.

[Figure 2-4](#) shows a sample Organization Tree.

Figure 2-4 Sample Organization Tree



The Organization Tree is made up of branches and nodes. In [Figure 2-4](#), Retail and Wholesale constitute separate branches of the tree. Each individual component part is termed a node of the tree.

When you add a system, service group, user, or user group to the VCS One cluster, you anchor, or attach, that object to a particular node of the Organization Tree.

Users must be granted explicit privileges to perform operations on objects. The following exceptions exist to this rule:

- The local root user on a client-side system can perform all client-side operations on the node, such as starting an agent on the system or taking a service group on that system offline.
- The local root user on the active Policy Master can perform all operations on all objects.
The local root user on an inactive Policy Master does not have privileges to perform operations.
See [“Policy Master components”](#) on page 47.

The objects for which a user is granted permission must reside at or under the node where the user is anchored. A user cannot be granted permission for any object outside of their anchored node or subtree.

The Organization Tree in [Figure 2-4](#) can be used to illustrate how privileges are related to the location of an object in the tree. An operator anchored at the Wholesale node can have the privilege to online or offline service groups on any system in the Wholesale branch. If additional systems are added to the Wholesale branch, the privileges of that user are automatically updated to include the new systems.

The same operator will not see the Retail branch of the tree.

See [“About users and the Organization tree”](#) on page 221.

See [“About the architecture of the Organization Tree”](#) on page 223.

About users, user groups, and their roles

Users are objects in the VCS One configuration. A user is created and assigned a role. A role is a named collection of privileges. Privileges define what actions the user can perform, such as adding a system to the VCS One cluster or modifying a service group. Every action a user can perform is individually defined as a privilege.

Roles and privileges are a flexible way to manage your users for the following reasons:

- You can associate a pre-defined role to a new user to decrease start-up time.
- You can create custom roles, with any appropriate privileges.
- You can create as many custom roles as you need in your environment.

When a user performs an operation, VCS One authorizes the action and the objects the user can act on using the user’s configured privileges. If the user does not have appropriate privileges, the operation will not execute.

VCS One has both predefined roles and the ability to create custom roles. A chart that compares the privileges of each of the predefined roles is available.

See [“Reference of privileges”](#) on page 627.

About user privileges

Because every action in VCS One requires a privilege, the privileges are organized into privilege categories for ease of administration. The privilege categories sort the individual actions the role can perform by the type of object to which the action is related.

For example, the System Privilege category contains the privileges to freeze a system or to add the system to a service group’s SystemList attribute. Similarly, the Notifier Privilege category contains the privilege to change the notification settings.

The total privileges of a user are a union of the following sets of privileges:

- Privileges explicitly granted to the user
- Privileges granted to any user group of which the user is a member

About user groups

A VCS One user group object can represent existing groups of users already configured in the datacenter. Some examples of existing groups of external users are the user groups defined with NIS or with LDAP.

VCS One uses Symantec Product Authentication Service (AT) to identify the membership of the external user to a VCS One user group. Roles and privileges are assigned to a user group in the same manner as they are assigned to an individual user.

A user is associated with a user group dynamically. The user is implicitly associated with all the groups specified in the user credentials. The credentials of the user include the credentials of the user groups to which the user belongs.

About extended attributes

An extended attribute (EA) is customer-defined metadata assigned to a system or a service group that defines a characteristic for that object.

Types of extended attributes

Extended attributes can be one of the following types:

System	Defines a characteristic for all system objects that are attached to that node and below in the Organization Tree.
Service group	Defines a characteristic for all service group objects that are attached to that node and below in the Organization Tree.
Common	Defines a characteristic for all system objects and service group objects that are attached to that node and below in the organization tree.

Values of extended attributes

You define extended attributes at a node in the Organization Tree. When a system or a service group object is anchored at or beneath that same Organization Tree node, the defined extended attributes can be given a corresponding value.

The Organization Tree in [Figure 2-4](#) can be used to illustrate how values of extended attributes work. You can define a system extended attribute named Location at the B2B node. This Location system attribute automatically exists at the Production and Development nodes because those nodes are beneath the B2B node.

Because this is a system extended attribute, all systems attached to the B2B, Production, and Development nodes inherit the Location attribute.

If you configure a default value for this Location attribute, such as Location = London, all systems attached at the B2B, Production, and Development nodes have the value Location = London. If there is not a default value configured, you must explicitly define the Location system attribute for each system at those nodes.

See [“About extended attributes”](#) on page 517.

Uses for extended attributes

You can use extended attributes for the following application management tasks:

- To perform operations on multiple objects
- To categorize objects in reports or scripts
- To help troubleshoot issues

When you use extended attributes as part of an expression, the objects that the expression affects are dynamically updated. For example:

You can configure a system extended attribute named OracleInstalled.

You can use an expression to build a collection of the systems in your environment that have the OracleInstalled attribute. You can save this collection of systems as a set.

You can then use the set to perform operations on all the systems in that set.

If you then add more systems to your environment and assign the OracleInstalled attribute to them, the set automatically includes these new systems.

Extended attributes can be used in an expression in the following ways:

- To create a set of objects in the Organization Tree
For example, to online a set of service groups that the expression defines rather than to create a list of the service groups.
- To filter the view of objects in the Organization Tree
For example, to display all systems in a particular location.
- As part of a command when using the command line instead of the console
- As a variable in a resource attribute value, with certain restrictions.
See [“Defining an attribute value with a resource variable”](#) on page 393.

Physical components of a VCS One environment

The following components are the physical aspects of a VCS One environment:

- Physical systems in the VCS One cluster
- Customer systems
- Data storage
- Networking

About the physical systems in the VCS One cluster

VCS One uses a client-server architecture to provide a scalable and highly-available application management solution.

The VCS One cluster consists of physical systems that are used for the following general purposes:

- VCS One cluster systems to run managed applications
These systems are the clients in the client-server architecture. These systems host the managed applications.
- Policy Master cluster systems that manage the VCS One cluster
These systems are the server in the client-server architecture. Best practice recommends that these systems are not used to host managed applications. See [“Policy Master components”](#) on page 47.

Systems that run different operating systems can co-exist inside the same VCS One cluster.

Each VCS One cluster system is connected to networking hardware. A VCS One cluster system usually is connected to storage hardware as well.

A VCS One cluster system contains the following elements:

- Operating system
- VCS One client daemon (vcsoneclientd)
- Unique Authentication Service (AT) principal for secure communications

The client daemon on a VCS One cluster system communicates only with the Policy Master daemon. It does not communicate with the client daemon on other VCS One cluster systems.

About customer systems

Customer systems access the managed applications on the VCS One cluster systems. This access is by an IP address on a public network.

In configurations where an application may move between systems, customers access a virtual IP address instead of a static IP address.

The virtual IP address allows customer systems to connect to the same IP address regardless of which VCS One cluster system is currently running the service group.

About storage in the VCS One cluster

Storage is a key resource of most applications services, and therefore most service groups. A service group can only be started on a system that has access to the data files associated with the application service.

If a service group can move between systems in the VCS One cluster, any system that hosts the service group must make available the associated data files that are needed by the managed application. Typically, this availability requires some form of shared storage. VCS One supports shared storage on NAS and SAN. To ensure data integrity, configure shared storage to allow VCS One to restrict access to only the active node that currently hosts the service group. On NAS based storage, VCS One provides the ability to control NFS exports from a NetApp based NAS filer. On SAN based storage, VCS One uses Veritas Storage Foundation to control SCSI-III reservations at the disk group level.

About networking in the VCS One cluster

Networking in the VCS One cluster is used for the following purposes:

- To communicate between the VCS One cluster systems and the Policy Master cluster.
- To communicate within the Policy Master cluster.

See [“How VCS One provides security in communications”](#) on page 63.

See [“How the Policy Master and client systems resolve failures in communication”](#) on page 58.

Redundant paths are recommended.

For more information on networking design, see *Veritas Cluster Server One Installation Guide*.

Policy Master components

The Policy Master is the core of VCS One. The Policy Master is a single, highly-available, specialized application that provides the central logic of VCS One. Also known as the Policy Master daemon, or `vcsoned`, it is responsible for all configuration and management of the VCS One environment.

The Policy Master has the following components:

Policy Master daemon (vcsoned)	<p>The Policy Master daemon is the main VCS One daemon. It provides the core logic of VCS One.</p> <p>The Policy Master daemon does the following tasks:</p> <ul style="list-style-type: none">■ Builds a running VCS One cluster configuration from the configuration database on startup■ Updates the configuration database with configuration and status changes■ Determines the system membership in the VCS One cluster■ Communicates with agents to monitor and manage resources on the VCS One cluster systems■ Implements all managed application placement policy■ Responds to operator input and provides service to the Web server and user interface components
Policy Master Web server	<p>The Policy Master Web server is a Java application. It accepts connections from Web clients, connects to the Policy Master daemon, and acts as a front end for all user interaction. It also authenticates users, interprets commands, and logs in on behalf of Web users.</p>
Policy Master configuration database	<p>The Policy Master controls the configuration database and stores all the information for the entire VCS One cluster.</p> <p>The following information is stored in the configuration database:</p> <ul style="list-style-type: none">■ Configuration and status of all the VCS One cluster objects, such as service groups, resources, sets, and users■ Policies, such as scheduled jobs■ GUI settings■ Custom views for both the Policy Master and the VCS One cluster systems <p>The database is highly available because it is configured as a resource of the Policy Master service group that runs in the Policy Master cluster.</p> <p>The database only accepts connections from the Policy Master. It does not permit outside connections for any purpose. You can use the hadb utility to perform operations on the configuration database.</p> <p>See “Managing the configuration database” on page 571.</p>

The Policy Master application is encapsulated into a service group, called the Policy Master service group (PMSG). This encapsulation allows the components of the Policy Master to become a managed application.

The following components are in the Policy Master service group:

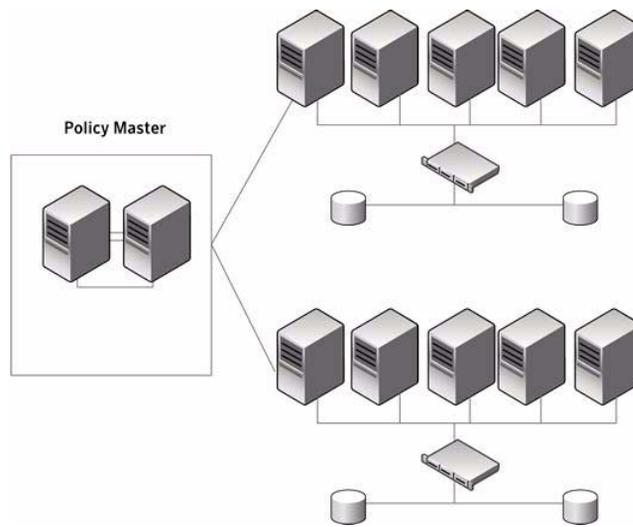
- Policy Master daemon (vcsoned)
- Policy Master Web server (VCSOneWeb)
- Policy Master configuration database (vcsonedb)
- Storage (disk group, volume, and mount, or NetApp NFS storage)
- Networking (pmip and pmnic)
- Authentication broker resource (atd)

To ensure that the Policy Master application is highly-available, the Policy Master service group runs in a small cluster of up to four systems. The Policy Master cluster systems are separate from the VCS One cluster systems and are only used for Policy Master functionality. Application service groups do not run in the Policy Master cluster.

The Policy Master cluster runs Veritas Cluster Server.

[Figure 2-5](#) shows the VCS One cluster systems alongside the Policy Master cluster.

Figure 2-5 Policy Master cluster with VCS One cluster



How VCS One works

This chapter includes the following topics:

- [How the Policy Master manages the applications](#)
- [How the Policy Master and the VCS One clients start up](#)
- [How the Policy Master loads the VCS One cluster configuration](#)
- [How the Policy Master and client systems resolve failures in communication](#)
- [How you can define service group load and system capacity](#)
- [How to control the scheduling class and scheduling priority of agent operations](#)
- [How you can configure automated tasks and group operations](#)
- [How VCS One provides security in communications](#)

How the Policy Master manages the applications

The Policy Master controls the managed applications by controlling the resources in the service group that encapsulate the managed application.

At a high level, the following process manages an application:

- The Policy Master determines the logic of what action to perform on a resource.
- The Policy Master daemon, `vcsoned`, communicates the action to the daemon running on the client system, which is `vcsonclientd`.
- The client daemon, `vcsonclientd`, communicates the action to the agent that controls the resource.
- The agent for that resource performs the action, such as online the resource.

About the client daemon `vcsonclientd`

The VCS One client daemon is the main VCS One component that runs on each of the VCS One cluster systems. It is responsible for the following tasks:

- Forming secure communications with the Policy Master
- Sending and receiving a heartbeat signal with the Policy Master
- Starting and stopping the agents on the local system

A `vcsonclientd` daemon shadow tries to restart `vcsonclientd` if it fails.

About agents

Every resource has a resource type, such as Oracle, Disk or IP. Each type of resource that runs in the VCS One cluster has a corresponding agent. The agent contains the logic of how to perform all supported actions on resources of that resource type.

For example, VCS One uses the Oracle agent to control all resources of type Oracle. The Oracle agent contains all the code that is needed to start, stop, and monitor instances of Oracle.

When you configure a new Oracle resource in the VCS One cluster, you only need to provide the information that is unique to that instance, such as the home directory and system identifier (SID). This information is passed to the agent that controls the resource.

Likewise when you configure a new IP resource, you provide the IP address and the subnet mask. The agent contains the code to use this information to start, stop, and monitor the health of that IP resource.

When a service group is configured to run on a specific set of system, the corresponding agents for the resources in that service group run on the same set of systems. This action lets the agent continuously monitor the resource whether or not it is online.

One instance of the agent controls all the resources of that resource type on the system. If no resources of a particular resource type are used, the agent is not started. For example, if there are no Oracle resources in your configuration, the Oracle agent is not started on any system.

The agents can take the following actions on a resource. The monitor, online and offline actions are also called agent entry points.

monitor	Determines if the resource is running properly.	All resources are monitored at regular intervals of time, whether they are online or offline.
online	Starts the resource.	Resources are brought online to start the managed application. The Policy Master controls the order the resources come online with respect to resource dependencies.
restart	Tries to online the resource again.	The Policy Master may try to restart a resource upon detection of failure depending on the value of the RestartLimit attribute.
offline	Stops the resource.	Resources are brought offline to stop the managed application. The Policy Master controls the order the resources go offline with respect to resource dependencies.
clean	Ensures that the resource is completely offline.	<p>The clean function is called for the following events:</p> <ul style="list-style-type: none"> ■ An online command to the resource fails. ■ An offline command to the resource fails. ■ The resource goes offline unexpectedly. Unexpectedly means that the following actions took place: The resource was in an online state Without the user issuing an offline command, the agent monitors the status of the resource to be in an offline state. ■ The monitor of the resource fails consecutively for the number of times that is configured in the resource attribute FaultOnMonitorTimeout. <p>The clean function is always called before a resource fault is reported to the Policy Master</p>

In the rare case where an agent does not already exist for a resource in your environment, you can develop a custom agent. An agent framework provides a level of abstraction to the agent that makes it easier for a developer or consultant to write a custom agent.

More information is available on writing custom agents.

See *Veritas Cluster Server One Agent Developer's Guide*.

How the Policy Master and the VCS One clients start up

This topic describes the various startup actions for the Policy Master and the client systems.

First initialization of the VCS One cluster

The sequence of events for VCS One cluster startup is as follows:

- On each client system, operating system scripts start the client daemon, `vcstoneclientd`, when the system initially starts.
- The `vcstoneclientd` daemon initiates a connection to the Policy Master by sending a connection request.
- The Policy Master responds to the connection request.
- The `vcstoneclientd` daemon indicates to the Policy Master that the system is in startup mode.
- The Policy Master sends a configuration snapshot to the system.

The configuration snapshot contains information specific to that VCS One cluster system, such as what agents to start up, the attributes of all the resources configured to run on that system, and a configuration version number.

The configuration version number keeps track of configuration changes for the system. Whenever there is a configuration change, both the Policy Master and the client system independently increment their configuration version number. This keeps the message exchange during a reconnect between the Policy Master and `vcstoneclientd` to a minimum.

This action completes the initialization of the client system.

The Policy Master start up mode determines the next action to take place.

Once the Policy Master and client systems are up and running, actions in response to any state changes in resources, service groups or systems are dictated by configured policy.

Policy Master start up modes

When the Policy Master starts up, either due to a system start up or a Policy Master failover, the following modes are available:

- Warm (Normal)
- Cold

The `hastart` command denotes the Policy Master start up mode.

See the *Veritas Cluster Server One Command Line Reference Guide*.

Warm (normal) start up mode

When the Policy Master service group starts after a failover or switch to an alternate system at the same site, warm mode is the default action.

In warm mode, the Policy Master enforces the configuration and state of the VCS One cluster stored in the configuration database. If the configuration and state of the VCS One cluster when the Policy Master starts up are different than when the Policy Master went down, the changes are interpreted as a fault and the Policy Master issues commands to bring the VCS One cluster back to the last state stored in the configuration database. GTQ entries remain intact.

To do this, the Policy Master reads the configuration database and replays the logs to bring VCS One cluster configuration and state information to the most current available.

If there are groups that are planned to go online or offline, then those actions are acted upon after the respective host connects to the Policy Master and the agents on those hosts probe the resources.

Note: The Policy Master commands `vcsonclientd` to perform operations at the resource level. The client daemon only knows about resources; service groups are a Policy Master construct.

Cold start up mode

When the Policy Master service group starts after a failover or switch to an alternate system at a DR site, cold mode is the default action.

In cold start mode, the Policy Master enforces the configuration in the configuration database, but does not enforce state information. The Policy Master probes all resources on all systems, determines their current state, and accepts that state as the correct state. Any existing GTQ entries are eliminated.

See [“About the Group Transition Queue”](#) on page 283.

This mode is used when you do not want to treat new state information as a fault. For example, when the state of a service group has changed while the Policy Master was offline.

The following are reasons this could occur:

- While the Policy Master was offline, the configuration changed. For example, a database was taken down and moved to another system using database commands outside of the VCS One cluster environment.
- The Policy Master cluster failed but the systems continued to run.

- You want to restore a previous configuration by loading an archived configuration database snapshot, and ignore the state information present with the snapshot.

See “[Starting the Policy Master in Cold mode](#)” on page 570.

Accepting the result of the probe as the current state of the VCS One cluster means the administrator must manually bring online any service groups that are not running when the probe occurs.

Note: A group brought offline manually by the administrator remains offline on all subsequent start ups for all Policy Master start up modes until the administrator manually brings the group back online.

How the Policy Master loads the VCS One cluster configuration

The VCS One cluster configuration is stored in a database.

VCS One supports the following configuration formats:

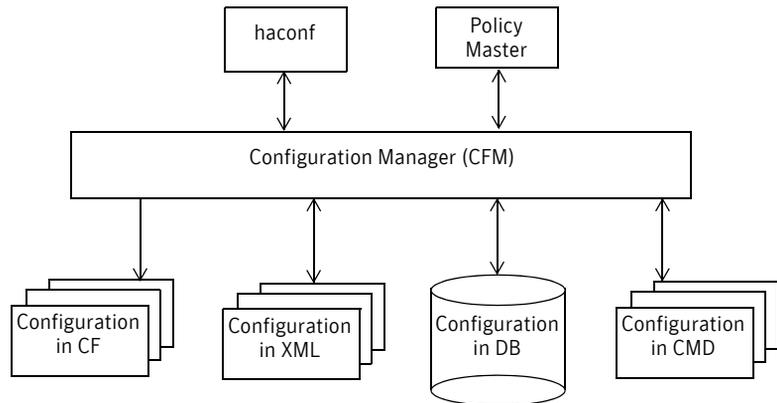
- XML – configuration exists in flat files
- Database – configuration exists in the database
- CMD – configuration exists in CLI (command line interface) format

VCS One provides a Configuration Manager (CFM) as an abstraction layer that provides an interface to load, update, and save the VCS One cluster configuration. You can use `haconf` utility to interface with the Configuration Manager and convert configurations from one format to another.

See *Veritas Cluster Server One Command Reference Guide*.

[Figure 3-1](#) depicts how the Configuration Manager makes the configuration available to the Policy Master.

Figure 3-1 Configuration Manager conversions



Depending on the operation performed in the VCS One cluster, the VCS One configuration flows in the following ways:

- Initial VCS One startup – The configuration is read from the XML files, is written to the database, and an in-memory copy is available with the PM.
XML → DB → PM
- Subsequent VCS One start ups – Once the configuration database is seeded, for all subsequent start ups, the configuration is read from the database and an in-memory copy is available with the PM.
DB → PM
- PM failover – The configuration remains with the database while an in-memory copy is written to the failover PM node.
DB → PM
- Database backup – The configuration is written to an XML file.
DB → XML
- Configuration updates – All configuration updates are written to the database.
PM → DB

VCS One provides utilities `haconf` and `hadb` to interface with the database.

How the Policy Master and client systems resolve failures in communication

The Policy Master and the client systems communicate over one designated TCP/IP-based primary network, and one or more optional secondary networks. If the designated primary network becomes unavailable, the secondary path becomes primary. If the primary path is restored, a heartbeat connection is established over this path as a standby for the current communication path.

The Policy Master uses communication links to the systems to determine membership in the VCS One cluster. Communications over these networks are secured using the Symantec Product Authentication Service authentication and encryption package.

VCS One cluster membership

Membership in the VCS One cluster is determined by the Policy Master receiving a continuous heartbeat signal from a system. Change in membership in the VCS One cluster is determined by the loss of heartbeats across all configured network links.

Policy Master detects loss of heartbeat, ping command responds

If there is a loss of the heartbeat signal from a client system on all connections to the Policy Master, the Policy Master attempts a `ping` command to the physical system to differentiate between a system failure and a `vcsonclientd` daemon failure. If the system replies to the `ping` command, this indicates the rare situation where the daemon has failed or been shutdown and has not been restarted by the `vcsonclientd` shadow.

This special condition is known as *Daemon Dead Node Alive (DDNA)*. In this case, the Policy Master does not take corrective action to failover service groups running on the suspect system because it is not able to determine the state of the resources running on the system. The administrator must intervene to verify the service groups are offline on the failed system and manually failover the service groups.

Policy Master detects loss of heartbeat, ping command fails

If there is a loss of the heartbeat signal from the system on all connections, and the system does not respond to the `ping` command from the Policy Master, the client system is designated `FAULTED`. Any configured policy for that system pertaining to failover of service groups is performed.

System detects loss of connection to Policy Master

If a client system detects a failure of its connection to the Policy Master on all configured network paths, all agents on the system are put in a QUIESCE state. In this state, the agent does not run any entry points, therefore monitoring of resources halts. No further action is taken on any resources in service groups running locally on the system while the connection is down.

The `vcstoneclientd` daemon repeatedly sends connection requests to the Policy Master to attempt a reconnect. Once the daemon reconnects, the following occurs:

The client daemon, `vcstoneclientd`, on the VCS One cluster system sends its configuration version number (CVN) to the Policy Master.

The configuration version number is used to keep track of configuration changes for the system. Whenever there is a configuration change, both the Policy Master and the client system independently increment their configuration version number.

The Policy Master compares the two configuration version numbers.

The Policy Master compares the received CVN to the one the Policy Master has stored. The numbers will be different if the configuration changed on the Policy Master while the connection was down.

Action depends on whether the two configuration version numbers match.

If the CVNs match, `vcstoneclientd` removes the QUIESCE state from the agents and probes all the resources.

If the CVNs do not match, the Policy Master clears the configuration on the system, which stops all running agents. The Policy Master then sends a new configuration snapshot to the system. `vcstoneclientd` starts the new set of agents and probes all the resources.

The latest state of all resources is sent from the client system to the Policy Master.

The Policy Master has the state of all service groups and can take corrective action if needed.

How you can define service group load and system capacity

The Capacity and Load construct allows you to define the amount of assets a system provides (Capacity), and the amount of assets a specific service group is expected to utilize (Load).

When a service group is started on a system, the values attributed to the Load of the service group are subtracted from the values attributed to the Capacity of the system that the service group is placed on.

If a service group has no Load-related values set, that is, they are the default values of zero, then the group can go online on any system for which it is configured, provided the compatibility criteria is met.

If a service group has a Load configured, then it can only go online on a system that has a Capacity value defined and sufficient to accommodate the Load value.

The Load and Capacity construct is configured using the VCS One cluster attribute `PrecedenceOrder`. The attribute enables definition of up to four prioritized keys. The keys are user-configurable, but typically represent CPU, memory, network, and storage (I/O) resources. The keys for Capacity and Load are always identical.

See [“Designing application placement policy”](#) on page 273.

Defining Load and Capacity keys with the `PrecedenceOrder` attribute

The default value of the VCS One cluster attribute `PrecedenceOrder` is:

<code>PrecedenceOrder</code>	CPU MEM STBW NTBW
------------------------------	----------------------------

The names and ranking of the four keys can be customized or eliminated. For example, using all four keys for `PrecedenceOrder` may look like the following:

<code>PrecedenceOrder</code>	CPU MEMORY STORAGE NETBANDWIDTH
------------------------------	--

These keys define a relative ranking of Load and Capacity across the VCS One cluster. For example, if `PrecedenceOrder` is defined with two keys, `cpu` and `memory`, values for the Capacity attribute for two systems in that VCS One cluster could be:

On sys1:	Capacity	CPU: 400 MEM: 200
On sys2:	Capacity	CPU: 200 MEM: 100

These values may indicate that sys1 has four processors, and sys2 has two processors, or they may indicate that sys1 has processors that are twice as fast

as the sys2 processors. These settings could also indicate that sys1 has twice as much memory as sys2. As long as the values are consistently relative, the measurement remains standardized across the VCS One cluster.

Load and Capacity values are hard values, meaning the values are strictly enforced. The total of the Load values of the service groups online on a system can not exceed the system's Capacity value.

The order of precedence of the four attributes affects the calculation of the target system to host a service group as well as the calculation of disruption factor.

See "[PrecedenceOrder](#)" on page 688.

How to control the scheduling class and scheduling priority of agent operations

Symantec has introduced four new attributes—EPClass, EPPriority, OnlineClass, and OnlinePriority—to enable you to control the scheduling class and scheduling priority of the agent operations. Agent operations include online, offline and monitor.

The new attributes OnlineClass and OnlinePriority are used to set the scheduling class and scheduling priority for the online entry point.

The new attributes EPClass and EPPriority are used to set the scheduling class and scheduling priority for all entry points, except the online entry point.

These attributes provide a single interface to tune the scheduling parameters for all entry points. It does not matter if they are implemented as C-based or script-based entry points.

It is usually required that the monitor, clean, offline and the other entry points running on an application have a higher scheduling class and scheduling priority without which they would compete with the application for system resources. However, running the online entry point with a higher scheduling class and scheduling priority may create problems because applications inherit the scheduling parameters from the application vendors, who specify that the applications are run using the default operating system scheduling parameters. Also, the online entry point is usually invoked before you start the application and the system is not very busy.

Hence, you must usually set the values of EPPriority and EPClass attributes to a higher value than the default value. You must usually set the value of the OnlinePriority and OnlineClass attribute to the default operating system scheduling values.

Setting the attribute's values to zero instructs VCS One to take the operating system default value for the particular operating system for which that

application's type is configured. This value accommodates different operating systems that have different default operating system scheduling values.

You may use only one of the following sets of attributes to configure scheduling class and scheduling priority for VCS One:

- AgentClass, AgentPriority, ScriptClass, ScriptPriority
- OnlineClass, OnlinePriority, EPClass, EPPriority

How you can configure automated tasks and group operations

VCS One allows you to automate administrative tasks based on a schedule or an event.

Schedule

These tasks are initiated by a scheduler. A day, date, time of day, or range of time trigger these tasks. Automated tasks based on a schedule may include the following examples:

Trigger	Task
Every Saturday at 9 A.M.	Switch all the applications running on server S1 over to server S2
The first Monday of every month	Run a script that creates a report.
Between the hours of 6 PM and 6 AM	Run the CRM application at a Priority=2

Events

The state of objects, such as resources, groups, users, and systems, trigger these tasks. Automated tasks based on an event may include the following examples:

Event	Task
A system is not available to run an application	Externally connect to a provisioning system to allocate a new server
A service group moves to a new node in the Organization Tree.	Check if it was an AIX system. Send an email notification.

Event

A system is added to the VCS One cluster

Task

Update the SystemList attribute of an application to include that system, if the operating system and extended attributes are appropriate.

How VCS One provides security in communications

Symantec Product Authentication Service (AT) provides services that implement core security mechanisms in VCS One. AT works within the configured authentication policy to perform the following operations:

- Validates the identities of users, as well as the identities of systems, connecting to the Policy Master.
- Gives a credential to any entity whose identity it can validate.
- Sets up secured communications between authenticated entities.

VCS One uses AT to authenticate and secure communications between various VCS One modules (for example, between the client systems and the Policy Master). AT also authenticates users when they log in to the Policy Master or VCS One client systems.

VCS One uses digital certificates for authentication and the secure sockets layer (SSL) protocol to encrypt communications over the network.

Authenticated and encrypted communications exist between the Policy Master and the system, the GUI connection, and the command line interface connection.

Each system obtains a different system identity credential that lets the Policy Master uniquely identify it. The VCS One client daemon (vcsoneclientd) running on the system uses this credential to validate its identity to the Policy Master.

The system identity credential has privileges associated with it that lets the system carry out tasks, such as sending resource state changes to the Policy Master.

The Policy Master has the following explicit checks to make sure the communication is valid, such as:

- The Policy Master only allows messages that originate from a system identity credential.
- The Policy Master checks that the message is valid with respect to the known configuration.

In VCS One, AT runs as a single daemon process on the active Policy Master node. The VCS One Policy Master installer configures AT to run on the active Policy Master node.

When you add a new system to the VCS One cluster, components on the system use secure socket layer (SSL) protocol to validate their identity with Symantec Product Authentication Service in the Policy Master cluster and receive an authentication certificate.

This certificate is a type of electronic passport that vouches for the identity of its holder and binds the holder to their public key. The certificate is then combined with a private key to make a valid credential. The credential allows the establishment of a secure session between the client system component and the Policy Master.

After a credential is established, all communication between the client system and the Policy Master is encrypted by the sender and decrypted by the receiver. Local host communication is not encrypted.

How VCS One global clusters work

This chapter includes the following topics:

- [About VCS One global clusters](#)
- [About global cluster building blocks](#)
- [Typical VCS One global cluster setup](#)
- [How global clusters work](#)

About VCS One global clusters

A VCS One global cluster links the individual VCS One clusters at separate sites, and enables wide-area failover and disaster recovery (DR) for the applications you configured. A VCS One global cluster configuration can have a maximum of two clusters. Clustering on a global level also requires an infrastructure to replicate the application data between these clusters.

Local clustering provides local failover within a site. Large-scale disasters such as major floods, hurricanes, and earthquakes can cause outages for an entire city or region. In such situations, with global clustering you can migrate applications to a different site that is located at a considerable distance away to ensure application and data availability.

In a global cluster environment, VCS One failover behavior is as follows:

- If an application fails on a system within a cluster, VCS One fails over the faulted application to another system within the same cluster.
- If an application fails on all systems within a cluster or if the entire cluster fails, VCS One provides the capability to fail over the application in that cluster to a system in another cluster.

About global cluster building blocks

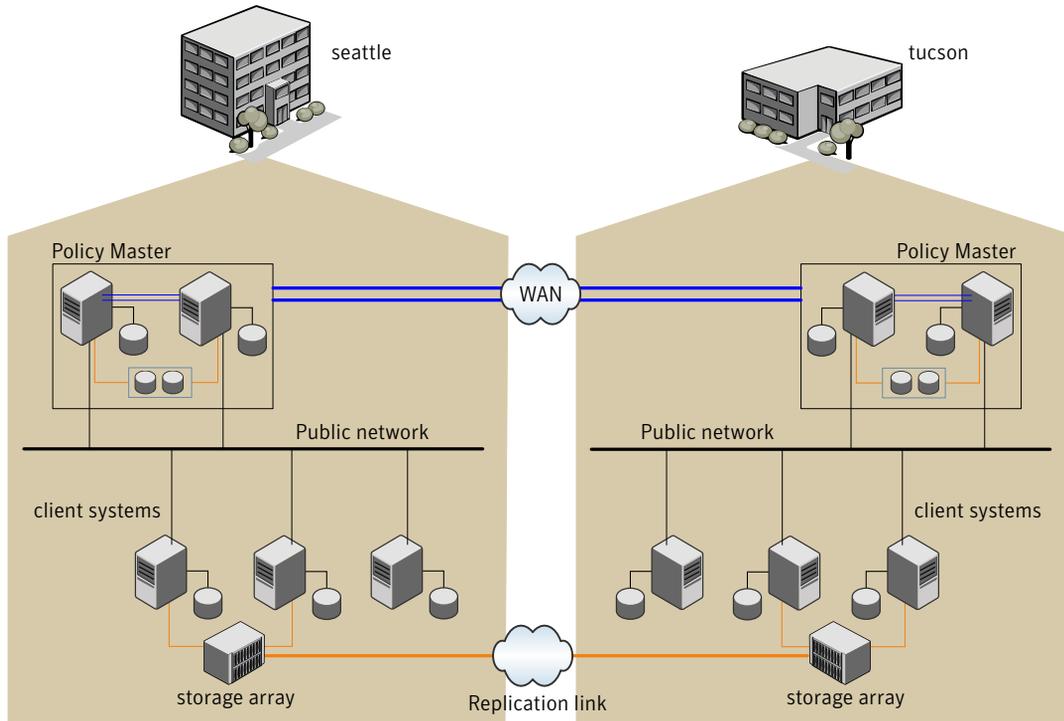
VCS One extends clustering concepts to wide-area high availability and disaster recovery with the following components:

VCS One clusters	Each site must have a VCS one cluster configured with a unique cluster name.
Wide-area network links	The VCS One clusters must have redundant wide-area network (WAN) connections between them for inter-cluster communication.
Storage arrays for data replication	Storage arrays at each site must replicate the application data to the other site using a technology that Symantec supports. The storage arrays must meet the requirements of the corresponding replication technology. For example, you must configure EMC SRDF replication on the symmetrix arrays at each site.
Remote cluster objects	A remote cluster object must be defined at each site to represent the VCS One cluster at the other site.
Global composite service group (CSG)	A global CSG must be defined for each application for which you want to enable disaster recovery. A global CSG is a CSG with additional properties to enable wide-area failover. A global CSG requires that you specify the remote clusters on which the CSG can run in addition to the local cluster. VCS One disaster recovery setup must meet the following conditions: <ul style="list-style-type: none"> ■ A CSG with the same name must exist on all sites. ■ The list of clusters on which the CSG can run must be the same on all sites. <p>See “About composite service groups” on page 40.</p>
VCS One replication agents	The appropriate VCS One replication agent must be installed at each site. For example, if EMC SRDF replication is configured, then the VCS One agent for EMC SRDF is installed at each site. VCS one provides agents for supported replication technologies. These agents are available in the Veritas High Availability Agent Pack software. See the <i>Veritas High Availability Agent Pack Getting Started Guide</i> for a list of replication technologies that VCS One supports. Contact your sales representative for more details.

Typical VCS One global cluster setup

Figure 4-1 depicts a typical VCS One global cluster setup. The example setup shows two VCS One clusters seattle and tucson.

Figure 4-1 Typical two-site VCS One global cluster setup



How global clusters work

Review the following sections to understand how global clusters work:

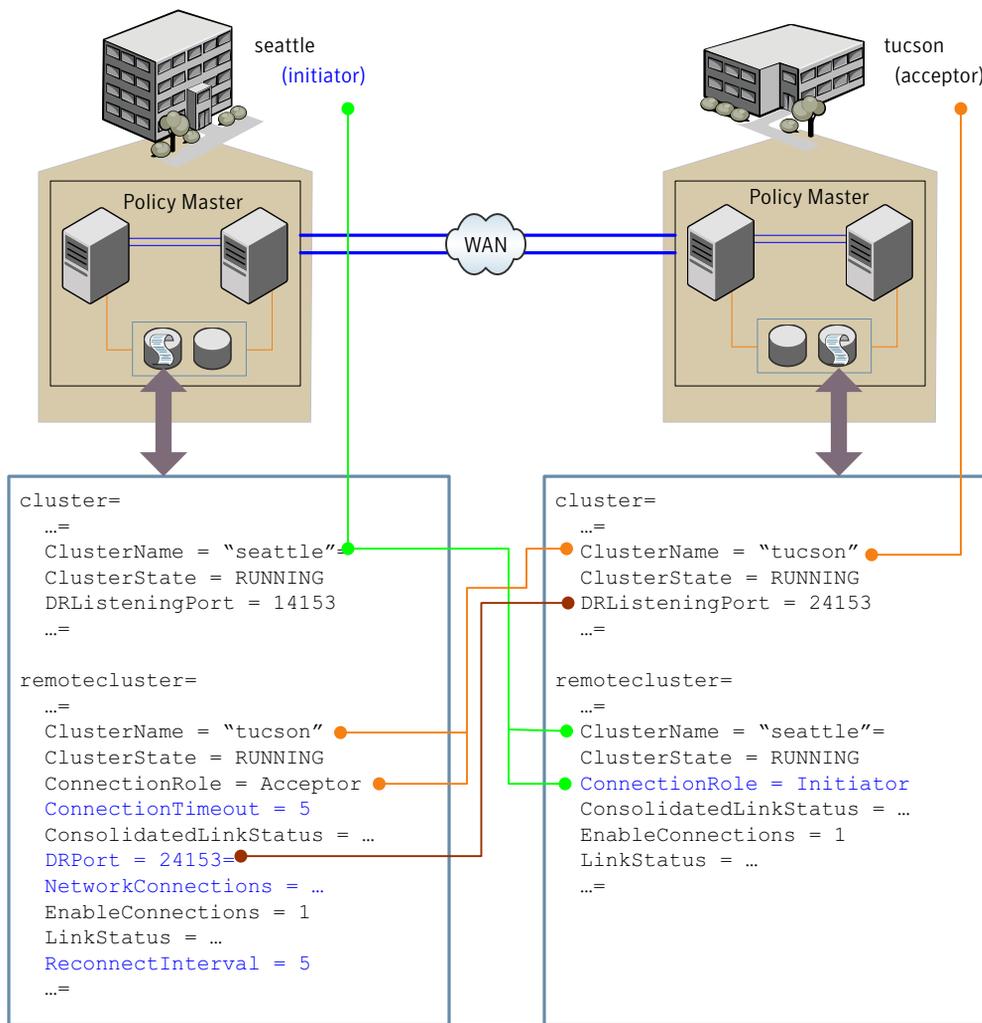
- [How VCS One global clusters communicate with each other](#)
- [How VCS One enables wide-area failover of a multi-tier application](#)
- [How VCS One determines the state of a multi-tier application](#)
- [How VCS One resolves authority for application that spans clusters](#)
- [How VCS One responds to various disasters](#)

How VCS One global clusters communicate with each other

In a VCS One global cluster environment, each cluster must have a remote cluster object that represents the cluster at the remote site. Based on the local and remote cluster names you provide during configuration, VCS One designates one of the clusters as Initiator and the other as Acceptor. The Initiator is responsible to initiate DR connections to the Acceptor. VCS One stores this connection role information of the remote cluster in the ConnectionRole attribute of the remote cluster object at each site.

[Figure 4-2](#) illustrates the correlation between the cluster and the remote cluster objects.

Figure 4-2 Cluster and remote cluster objects in a global cluster setup



VCS One clusters listen for incoming connections from the remote clusters on an IP address and port that are defined in the cluster-level attributes DRAddress and DRListeningPort. If DRAddress attribute is not defined, then VCS One uses the IP addresses defined in the ClusterAddress attribute. If a port is not defined in the attribute DRListeningPort, VCS One uses the default port number 14151 to listen for incoming connections.

VCS One clusters communicate with each other over the wide-area network links that you configure. Symantec recommends that you set up at least two network links for cluster communication in a global cluster environment. This network link information in the form of IP addresses is specified in the

NetworkConnections attribute of the remote cluster. The Initiator connects to the remote cluster (designated as the Acceptor) on IP addresses specified in the NetworkConnections attribute of that remote cluster. Similarly, the Initiator connects to the port specified in the DRPort attribute of the remote cluster.

VCS One uses Symantec Product Authentication Service (AT) for authentication and secure communication. In a global cluster setup, the local and the remote clusters must have an explicit trust relationship for VCS One to successfully establish connection between the clusters.

The EnableConnections attribute of the remote cluster controls the connectivity between the Initiator and Acceptor clusters. After you enable connections between the clusters by setting the EnableConnections attribute, VCS One initiates connections on all IP addresses specified in the NetworkConnections attribute of the remote cluster. The first network connection link that establishes connection with the remote cluster is the primary link. VCS One exchanges snapshots of global cluster objects on the primary link.

VCS One maintains persistent connections on all links and periodically sends heartbeats on all links to monitor the health of the remote cluster. If a primary link fails, VCS One fails over to any available secondary link for primary communications. If all network links fail, VCS One transitions the remote cluster state as `FAULTED`.

How VCS One enables wide-area failover of a multi-tier application

Each multi-tier application for which you want to enable disaster recovery must have a composite service group (CSG) defined. A CSG is a logical representation of a multi-tier application. You can configure each tier in the application as separate service group in the VCS One cluster configuration. The CSG is a collection of such related service groups to enable you to perform operations on the multi-tier application as a whole.

In a VCS One global cluster setup, you must configure the CSG as a global CSG. A global CSG spans multiple clusters. The CSG-level attribute `ClusterList` represents the names of all clusters where a CSG can potentially fail over to.

A CSG is the smallest unit of failover across clusters. The Policy Master exchanges pertinent information about the global CSG only with the other clusters that the CSG is defined on. The attributes in a global CSG that are exchanged between the clusters are `ClusterList`, `Authority`, `CSGState`, and `InTransition`.

See [“Composite service group attributes”](#) on page 692.

How VCS One determines the state of a multi-tier application

The state of a CSG represents the state of the multi-tier application in the cluster. VCS One uses the cluster-wide state of each group in the CSG to determine the state of the CSG. A CSG can have the following states and is stored in the CSG-level attribute `CSGState`:

- **ONLINE**—All groups are online
- **PARTIAL**—Some groups are online or partial
- **OFFLINE**—All groups are offline

VCS One sets the **ATTN** and **PENDING** flags for the CSG in the following situations:

ATTN flag (Requires user intervention)	<ul style="list-style-type: none">■ A group in the CSG is unable to go online on any system in the VCS One cluster.■ A group in the CSG is faulted on all systems in the cluster.■ CSG is online or partially online on more than one cluster.■ CSG state is stale. For example, when the Policy Master restarts in warm mode (normal mode), the state of the groups is not up-to-date because the Policy Master reads the configuration information from the VCS One database.
PENDING flag	<ul style="list-style-type: none">■ A resource or group in the CSG is in transition on any system within the cluster.

The value of the `CSGState` attribute can be a combination of the flags and the state values. For example, `ONLINE | ATTN`, `OFFLINE | PENDING`, or `PARTIAL | PENDING | ATTN`.

See [“Composite service group attributes”](#) on page 692.

How VCS One resolves authority for application that spans clusters

The CSG-level attribute `Authority` designates which cluster has the right to bring a global CSG online in a global cluster setup. VCS One uses this attribute to prevent a multi-tier application from coming online in multiple clusters at the same time.

When you set up global clusters, the clusters initially do not have authority for the CSG. The `Authority` attribute is a non-editable attribute; user-initiated actions seed authority for the CSG. The cluster where you perform an online operation or a request authority operation for the CSG gets the authority for the CSG. The Policy Master negotiates authority for the global CSG with the other clusters it is connected to.

VCS One automatically resolves authority for a global CSG when the CSG state changes on any of the clusters.

When the Policy Master starts up in the warm (normal) mode, it restores the configuration with the state information stored in the database. However, the information in the database might not be up-to-date as a CSG takeover operation could have been initiated at the remote site. So, the Policy Master does the following to reconcile the state changes before it resolves authority for the global CSGs:

- Marks the state of the global CSGs that are not in a clean OFFLINE state as STALE and sets the ATTN flag.
- Waits to establish connection with other remote clusters that the global CSG is defined on.
If a remote cluster is unreachable, the Policy Master waits until the time as defined in the cluster-level attribute DRStaleStateTimeout.
- Clears the STALE state of the global CSGs after the connection is established or the time-out expires.
The Policy Master does not clear the STALE state of the global CSG if it detects a concurrency violation for the global CSG. You must resolve the concurrency violation for the Policy Master to proceed.

See [“Policy Master start up modes”](#) on page 54.

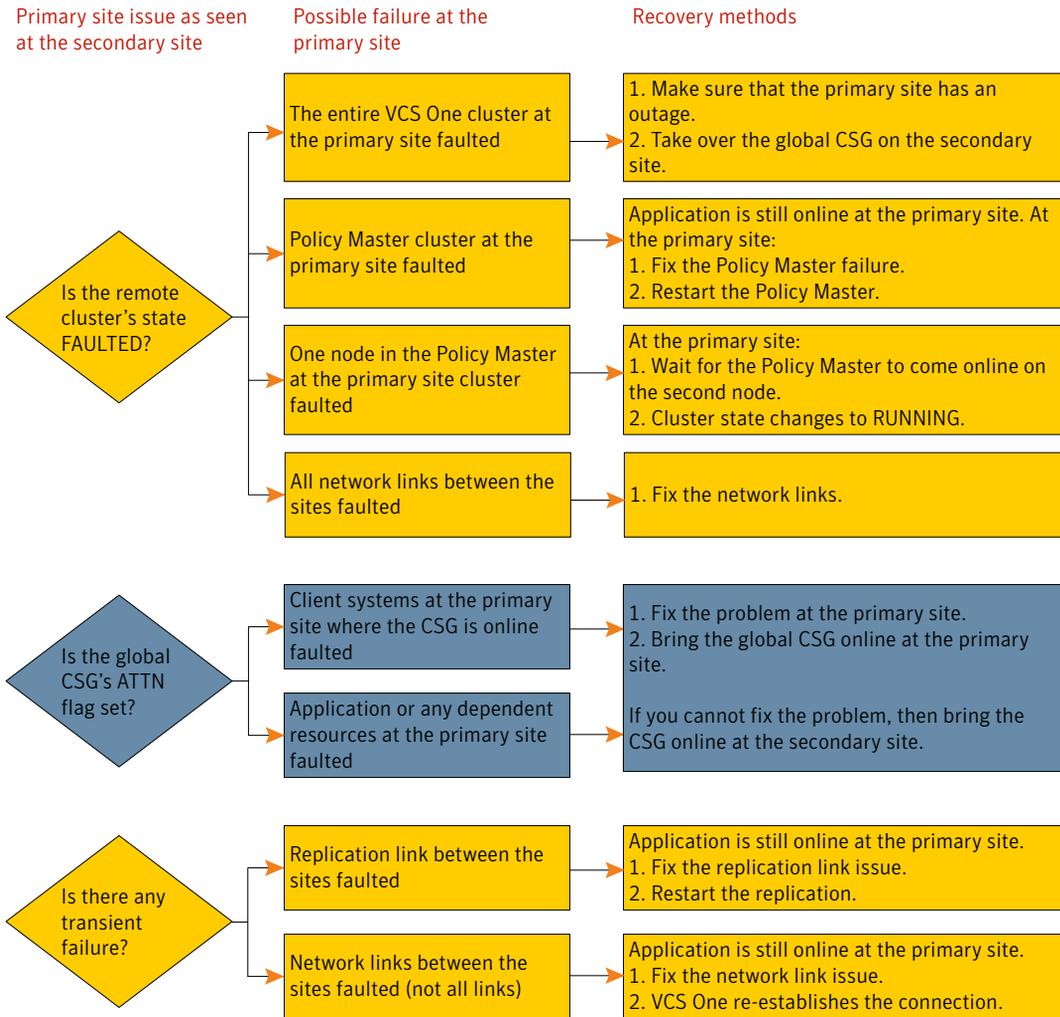
How VCS One responds to various disasters

VCS One triggers a BPA event each time the state of a remote cluster changes from RUNNING. VCS One also triggers a BPA event each time a global CSG faults or requires administrative attention (ATTN flag).

[Figure 4-3](#) presents a diagnosis flow and basic recovery methods for the various disasters.

See [Table 4-1, “Failure scenarios in VCS One global clusters”](#) for detailed failure description, and for the procedures on how to recover and how to fail back.

Figure 4-3 Diagnosing failures and recovering from disasters



[Table 4-1](#) lists the possible failure scenarios and how to recover from these failures in a VCS One global cluster environment.

Table 4-1 Failure scenarios in VCS One global clusters

Failure and description	Recovery and failback procedure
<p>Total site failure: VCS One cluster at the primary site fails:</p> <ul style="list-style-type: none"> ■ The Policy Master cluster at the primary site fails. ■ All client systems and their storage at the primary site fail. 	<p>The Policy Master at the secondary site marks the primary site's VCS One cluster state as FAULTED LINK_DOWN, and triggers a BPA event.</p> <p>To recover from a total site failure</p> <ol style="list-style-type: none"> 1 Verify that the primary site has indeed suffered an outage or disaster. 2 Take over the global CSG at the secondary site. See "Taking over a global CSG" on page 503. <p>To fail back to the primary site after a total site failure</p> <ol style="list-style-type: none"> 1 If you restore the primary site after an extended outage, then restart the Policy Master at the primary site in the cold mode. See "Starting the Policy Master in Cold mode" on page 570. 2 If you restore the primary site after a brief outage, then restart the Policy Master at the primary site in the warm mode. When the primary site has been restored, the Policy Master at the primary site faults all the service groups that were previously online. The service group state is FAULTED and the global CSG state is OFFLINE ATTN. See "Policy Master start up modes" on page 54. See "How VCS One resolves authority for application that spans clusters" on page 72.
<p>Partial site failure (Policy Master cluster failure):</p> <ul style="list-style-type: none"> ■ The Policy Master cluster at the primary site fails. ■ The client systems and their storage at the primary site are functional. 	<p>The Policy Master at the secondary site marks the primary site's VCS One cluster state as FAULTED LINK_DOWN, and triggers a BPA event.</p> <p>Note: Application is still online on the client systems in such a partial failure scenario. So, do not attempt to take over the global CSG at the secondary site.</p> <p>To recover from a Policy Master cluster failure</p> <ol style="list-style-type: none"> 1 Determine the reason for the Policy Master cluster failure. 2 Start the Policy Master cluster in the warm mode at the primary site.

Table 4-1 Failure scenarios in VCS One global clusters

Failure and description	Recovery and fallback procedure
<p>Partial site failure (client systems failure, storage failure, or application failure)</p> <ul style="list-style-type: none"> ■ The Policy Master cluster at the primary site is functional. ■ One or more of the following failures occur at the primary site: <ul style="list-style-type: none"> - Storage for the client systems fails. - The client systems and their storage fail. - Application fails on all the client systems. 	<p>The Policy Master at the primary site sets the ATTN flag for the CSGs, and marks the state of the associated service groups as FAULTED.</p> <p>Note: If the application fails on one of the client systems at the primary site, VCS One fails the application over to another client system within the same VCS One cluster.</p> <p>To recover from a partial site failure</p> <ol style="list-style-type: none"> 1 If the client systems have failed, check if a network partition exists between the Policy Master and the client systems at the primary site. Fix any network issues. 2 For all other failures, fix the problem locally and bring the global CSG online at the primary site. 3 If you cannot succeed in step 2, then bring the global CSG online on the secondary site. See “Bringing a global CSG online” on page 500. <p>To fail back to the primary site after a partial site failure</p> <ol style="list-style-type: none"> 1 If you have set up data replication, then ensure that the data at the primary is up-to-date with the secondary. 2 If the data is not up-to-date, use the replication agent’s update action to synchronize the data. Refer to the replication agent guide for details. 3 Switch back the global CSG to the primary site. See “Switching a global CSG” on page 502.
<p>Policy Master node failure: One of the nodes in the Policy Master cluster at a site fails</p>	<p>When one node in the Policy Master cluster fails, VCS One brings the Policy Master online on the standby node. When the Policy Master is fully up and running on the standby node at the primary site, the cluster state changes to RUNNING.</p> <p>To recover from a Policy Master node failure</p> <ul style="list-style-type: none"> ■ Determine the reason for the Policy Master node failure and fix the issue.

Table 4-1 Failure scenarios in VCS One global clusters

Failure and description	Recovery and fallback procedure
<p>Complete network link failure: All the network links between the two VCS One clusters fail.</p>	<p>During such network partitions, VCS One in each cluster marks the state of the remote cluster as <code>FAULTED LINK_DOWN</code>. The status of each network link is <code>DOWN</code>.</p> <p>To recover from a complete network link failure</p> <ol style="list-style-type: none"> 1 Determine the reason for the network partition. 2 Fix the network links. <p>Note: Symantec recommends you to not take over the CSGs in such a failure.</p>
<p>Partial network link failure: One or more network links to the remote cluster is down.</p>	<p>When a network link to the remote cluster fails, VCS One marks the state of this link as <code>DOWN</code>. The state of the VCS One cluster is <code>RUNNING LINK_PARTIAL</code>.</p> <p>Symantec recommends that you configure multiple network links for resilience. When the primary link fails, VCS One automatically fails over to any active secondary link. VCS One periodically attempts to initiate connection over the network links that you have defined.</p> <p>To recover from a partial network link failure</p> <ul style="list-style-type: none"> ■ Fix the faulted network links. When the link comes up, VCS One automatically establishes the communication link and exchanges heartbeats with the remote cluster.
<p>Replication link failure: Replication link between the storage at the two sites fail</p>	<p>The application is still available at the primary site and so the CSG state does not change.</p> <p>The replication resource's <code>ResourceInfo</code> attribute indicates the replication link failure and that the data replication is not in progress.</p> <p>To recover from a replication link failure</p> <ol style="list-style-type: none"> 1 Fix the replication link. 2 Restart the replication. Refer to the replication agent guide for details.

How the Policy Master cluster protects data

This chapter includes the following topics:

- [About protecting data in the VCS One cluster](#)
- [About communications in the Policy Master cluster](#)
- [About membership in the Policy master cluster](#)
- [About membership arbitration in the Policy Master cluster](#)
- [About data protection in the Policy Master cluster using SCSI-3 storage](#)
- [How I/O fencing works](#)
- [Best practices for Policy Master cluster communications](#)

About protecting data in the VCS One cluster

When systems in the VCS One cluster share storage devices, you can configure a protection mechanism to eliminate multiple simultaneous access to the storage. When failover occurs, the system that is the failover target for the service group blocks access to the shared data resources from other systems.

The default protection mechanism is SCSI-3 Persistent Reservations implemented by Veritas Volume Manager. You may also designate and configure other forms of data protection, such as SAN fabric zoning and LUN masking.

About communications in the Policy Master cluster

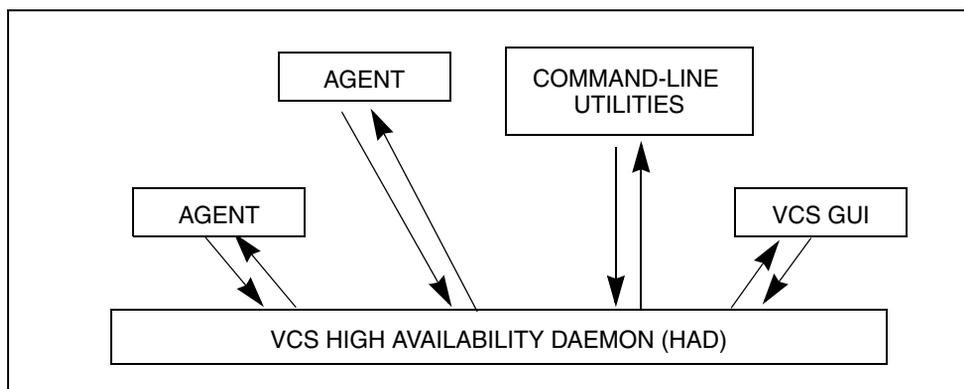
The Policy Master cluster is kept highly available by the use of Veritas Cluster Server (VCS) software. VCS uses local communications on a system and system-to-system communications.

About communications between systems in the Policy Master cluster

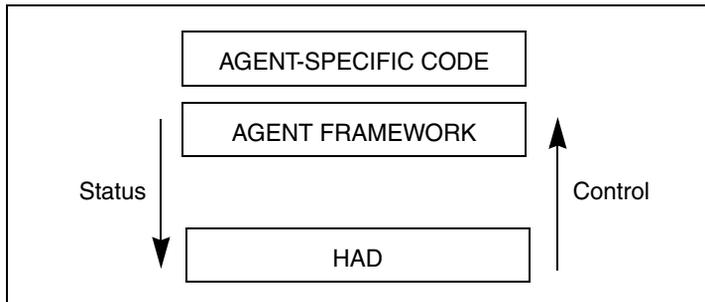
Each system in the Policy Master cluster runs the VCS High Availability Daemon (HAD), which is the decision logic for the Policy Master cluster. HAD uses a VCS-specific communication protocol known as Inter Process Messaging (IPM) to communicate with the GUI, the command line, and the agents in the Policy Master cluster.

[Figure 5-1](#) shows basic communication on a single VCS system.

Figure 5-1 Communication on a single VCS system



[Figure 5-2](#) depicts communication from a single agent to HAD.

Figure 5-2 Communication between HAD and an agent

The agent uses the agent framework, which is compiled into the agent itself. For each resource type configured in a VCS One cluster, an agent runs on each client system. The agent handles all resources of that type. The engine passes commands to the agent and the agent returns the status of command execution. For example, an agent is commanded to bring a resource online. The agent responds back with the success (or failure) of the operation. Once the resource is online, the agent communicates with the engine only if this status changes.

About inter-system Policy Master cluster communications

VCS uses the Policy Master cluster interconnect for network communications between Policy Master cluster systems. Each system runs as an independent operating system and shares information at the Policy Master cluster level. On each system the VCS High Availability Daemon, (HAD), maintains a view of the Policy Master cluster configuration. This daemon operates as a replicated state machine, which means all systems in the Policy Master cluster have a synchronized state of the Policy Master cluster configuration.

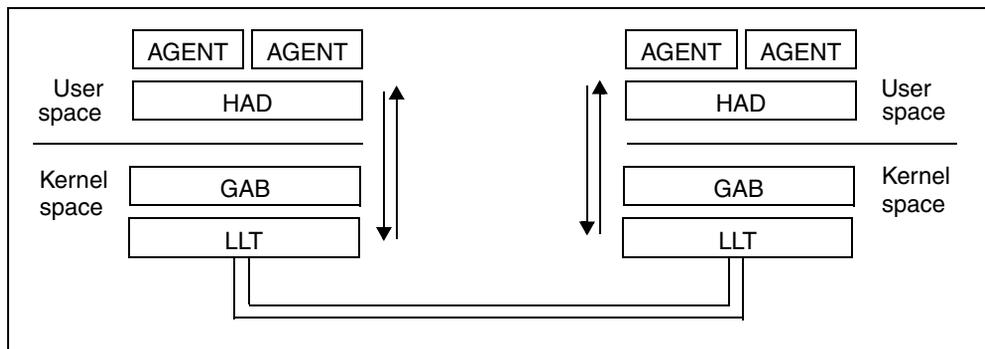
This synchronized state is accomplished by the following design:

- All systems run an identical copy of HAD.
- HAD on each system maintains the state of its own resources, and sends all Policy Master cluster information about the local system to all other machines in the Policy Master cluster.
- HAD on each system receives information from the other Policy Master cluster systems to update its own view of the Policy Master cluster.
- Each system follows the same code path for actions on the Policy Master cluster.

The replicated state machine communicates over a purpose-built communications package consisting of two components, Group Membership

Services/Atomic Broadcast (GAB) and Low Latency Transport (LLT). [Figure 5-3](#) illustrates the overall communications paths between two systems using the replicated state machine model.

Figure 5-3 Policy Master cluster communications with replicated state machine



Group Membership Services/Atomic Broadcast (GAB)

The Group Membership Services/Atomic Broadcast protocol (GAB) is responsible for Policy Master cluster membership and reliable Policy Master cluster communications.

GAB has the following major functions.

- Policy Master cluster membership
GAB maintains Policy Master cluster membership by receiving input on the status of the heartbeat from each system via LLT. When a system no longer receives heartbeats from a Policy Master cluster peer, LLT passes the heartbeat loss to GAB. GAB marks the peer as `DOWN` and excludes it from the Policy Master cluster. In most configurations, membership arbitration is used to prevent network partitions.
- Policy Master cluster communications
GAB provides reliable Policy Master cluster communications with guaranteed delivery of messages to all Policy Master cluster systems. The Atomic Broadcast functionality is used by HAD to ensure that all systems in the Policy Master cluster receive all configuration change messages, or are rolled back to the previous state, much like a database atomic commit. Although the communications function in GAB is known as Atomic Broadcast, no network broadcast traffic is generated. An Atomic Broadcast message is a series of point-to-point unicast messages from the sending

system to each receiving system, with a corresponding acknowledgement from each receiving system.

Low Latency Transport (LLT)

The Low Latency Transport protocol is used for all Policy Master cluster communications as a high-performance, low-latency replacement for the IP stack.

LLT has the following major functions.

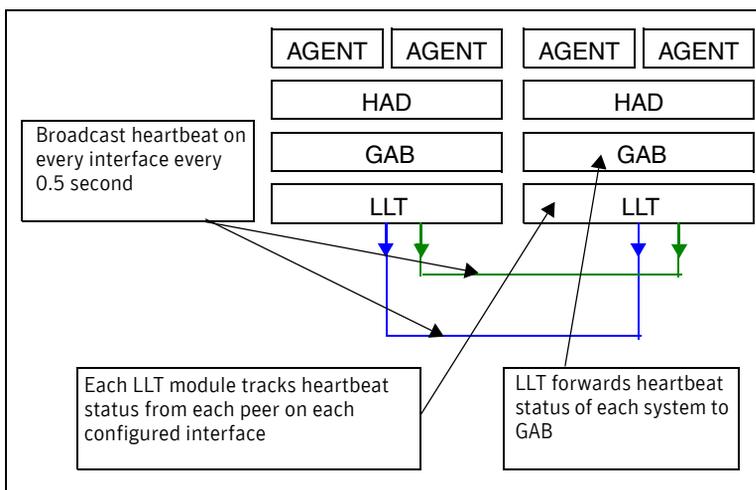
- **Traffic distribution**
LLT provides the communications backbone for GAB. LLT distributes (load balances) inter-system communication across all configured network links. This distribution ensures all Policy Master cluster communications are evenly distributed across all network links for performance and fault resilience. If a link fails, LLT redirects traffic to the remaining links. A maximum of eight network links are supported.
- **Heartbeat**
LLT sends and receives heartbeat traffic over each configured network link. LLT heartbeat is an Ethernet broadcast packet. This broadcast heartbeat method lets a single packet notify all other Policy Master cluster members that the sender is functional, as well as provide necessary address information for the receiver to send unicast traffic back to the sender. The heartbeat is the only broadcast traffic generated by VCS. Each system sends two heartbeat packets per second per interface. All other Policy Master cluster communications, including all status and configuration traffic is point-to-point unicast. This heartbeat is used by the Group Membership Services to determine Policy Master cluster membership.

The heartbeat signal is defined as follows:

- LLT on each system in the Policy Master cluster sends heartbeat packets out on all configured LLT interfaces every half second.
- LLT on each system tracks the heartbeat status from each peer on each configured LLT interface.
- LLT on each system forwards the heartbeat status of each system in the Policy Master cluster to the local Group Membership Services function of GAB.
- GAB receives the status of heartbeat from all Policy Master cluster systems from LLT and makes membership determination based on this information.

Figure 5-4 shows the flow of the heartbeat in the Policy Master cluster

Figure 5-4 Heartbeat in the Policy Master cluster



You can configure LLT to designate specific Policy Master cluster interconnect links as either high priority or low priority. High priority links are used for Policy Master cluster communications to GAB as well as heartbeat signals. Low priority links, during normal operation, are used for heartbeat and link state maintenance only, and the frequency of heartbeats is reduced to 50% of normal to reduce network overhead.

If all configured high priority links fail, LLT switches all Policy Master cluster communications traffic to the first available low priority link. Communication traffic returns to the high priority links when they become available.

While not required, best practice recommends to configure at least one low priority link, and to configure two high priority links on dedicated Policy Master cluster interconnects to provide redundancy in the communications path. Low priority links are typically configured on the public or administrative network.

About membership in the Policy master cluster

The current members of the Policy Master cluster are the systems that are actively participating in the Policy Master cluster. It is critical for HAD to accurately determine current Policy Master cluster membership in order to take corrective action on system failure and maintain overall Policy Master cluster topology.

A change in Policy Master cluster membership is one of the starting points of the logic to determine if HAD needs to perform any fault handling in the Policy Master cluster.

There are two aspects to Policy Master cluster membership: initial joining of the Policy Master cluster and how membership is determined once the Policy Master cluster is up and running.

Initial joining of systems to the Policy Master cluster membership

When the Policy Master cluster initially boots, LLT determines which systems are sending heartbeat signals, and passes that information to GAB. GAB uses this information in the process of seeding the Policy Master cluster membership.

Seeding ensures a new Policy Master cluster starts with an accurate membership count of the number of systems in the Policy Master cluster. This prevents the possibility of one Policy Master cluster splitting into multiple sub-clusters upon initial startup.

The following process seeds a new Policy Master cluster:

- When the Policy Master cluster initially starts, all systems in the Policy Master cluster are not yet seeded.
- GAB checks the number of systems that have been declared to be members of the Policy Master cluster in the `/etc/gabtab` file.

The number of systems declared in the Policy Master cluster is denoted as follows:

```
/sbin/gabconfig -c -n#
```

where the variable `#` is replaced with the number of systems in the Policy Master cluster.

Note: This number should represent 100% of the systems in the Policy Master cluster

- When GAB on each system detects that the correct number of systems are running, based on the number declared in `/etc/gabtab` and input from LLT, it seeds.
- HAD starts on each seeded system. HAD only runs on a seeded system.

Manual seeding of a Policy Master cluster

Seeding the Policy Master cluster manually is appropriate when there are more Policy Master cluster systems declared in `/etc/gabtab` than will join the Policy Master cluster. This could occur if a system is down for maintenance when the Policy Master cluster starts.

Caution: Do not seed the Policy Master cluster manually unless you are aware of the risks and implications of the command.

Before manually seeding the Policy Master cluster, check that systems that will join the Policy Master cluster are able to send and receive heartbeats to each other. Confirm there is no possibility of a network partition condition in the Policy Master cluster.

There is no declaration of the number of systems in the Policy Master cluster with a manual seed. The command seeds all systems that are in communication with the system where the command is run.

Ongoing Policy Master cluster membership

Once the Policy Master cluster is up and running, a system remains an active member of the Policy Master cluster as long as peer systems receive a heartbeat signal from that system over the Policy Master cluster interconnect.

A change in Policy Master cluster membership is determined in the following way:

- When LLT on a system no longer receives heartbeat messages from a system on any of the configured LLT interfaces for a predefined time, LLT informs GAB of the heartbeat loss from that specific system.
This predefined time is 16 seconds by default, but can be configured. It is set with the `set-timer peerinact` command as described in the `/etc/llttab` manual page.
- When LLT informs GAB of a heartbeat loss, the systems that are remaining in the Policy Master cluster coordinate to agree which systems are still actively participating in the Policy Master cluster and which are not. This happens during a 5-second period known as “GAB Stable Timeout.”
VCS has specific error handling that takes effect when the systems do not agree.
- GAB marks the system as DOWN, excludes the system from the Policy Master cluster membership, and delivers the membership change to the fencing module.
- The fencing module performs membership arbitration to ensure that only one functional cohesive Policy Master cluster continues to run.

The fencing module is turned on by default.

About membership arbitration in the Policy Master cluster

Membership arbitration is necessary on a perceived membership change because systems may falsely appear to be down. When LLT on a system does not receive heartbeat messages from another system on any configured LLT interface, GAB marks the system as DOWN. However, if the Policy Master cluster interconnect network fails, a system can appear to be failed when it is not. In most environments when this happens, it is caused by an insufficient Policy Master cluster interconnect network infrastructure, usually one that routes all communication links through a single point of failure.

If all the Policy Master cluster interconnect links fail, one Policy Master cluster can separate into two sub-cluster, each of which does not know about the other. The two sub-cluster could each carry out recovery actions for the departed systems. This is termed split brain.

In a split brain condition, two systems could try to import the same storage and cause damage, have an IP address up in two places, or mistakenly run an application in two places at once.

Membership arbitration prevents split brain conditions.

Components of membership arbitration

The components of membership arbitration are the fencing module and the coordinator disks.

Fencing module

Each system in the Policy Master cluster runs a kernel module called `vxfen`, or the fencing module. This module uses membership arbitration to ensure valid and current Policy Master cluster membership on a membership change.

`vxfen` performs the following actions:

- Registers with the coordinator disks during normal operation
- Races for control of the coordinator disks during membership changes

Coordinator disks

Coordinator disks are special purpose disks that act together as a global lock device. Racing for control of these disks is used to determine Policy Master cluster membership. Control is won by the system that gains control of a majority of the coordinator disks, so there must always be an odd number of disks, with three disks recommended.

You cannot use coordinator disks for any other purpose in the Policy Master cluster configuration, such as data storage or inclusion in a disk group for user data. Any disks that support SCSI-3 Persistent Reservation can be coordinator disks. Best practice is to select the smallest possible LUNs for use as coordinator disks.

How the fencing module starts up

The fencing module starts up in the following way:

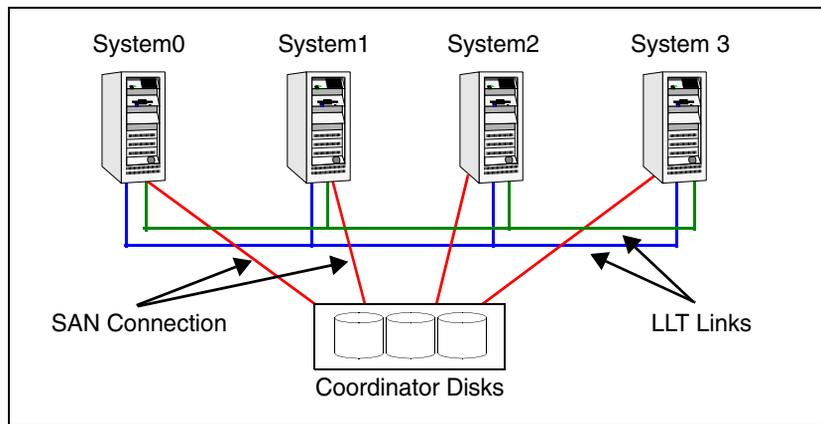
- The coordinator disks are placed in a disk group.
During initial Policy Master cluster configuration, the coordinator disks are placed in a disk group, and the name of the disk group is placed in `/etc/vxfendg`. This set up allows the fencing start up script to use Symantec Veritas Volume Manager (VxVM) commands to easily determine which disks are coordinator disks, and what paths exist to those disks. This disk group is never imported, and is not used for any other purpose.
- The fencing start up script uses the disk group name in `/etc/vxfendg` and VxVM commands to populate the file `/etc/vxfentab` with all paths available to the coordinator disks.
For example, if you configure three coordinator disks with two paths to each disk, the `/etc/vxfentab` file will contain six individual lines, representing the path name to each disk, such as `/dev/rdisk/c1t1d1s2`.
- When the fencing driver is started, it reads the physical disk names from the `/etc/vxfentab` file. These disk names represent the physical paths available on a system to the coordinator disks.
- The fencing driver determines the serial number of the disk represented by a specific path. Using this information, the driver builds an in-memory list of the physical coordinator disks.
- The fencing driver verifies that any other systems in the Policy Master cluster that are already up and running detect the same coordinator disks. The fencing driver examines GAB port B for membership information. If no other systems are up and running, it is the first system up and is considered the correct coordinator disk configuration. When a new member joins, it requests a coordinator disks configuration. The system with the lowest LLT ID responds with a list of the coordinator disk serial numbers. If there is a match, the new member joins the Policy Master cluster. If there is not a match, `vxfen` enters an error state and the new member is not allowed to join. This process ensures that all systems communicate with the same coordinator disks.
- The fencing driver determines if a possible preexisting split brain condition exists.

This is done by verifying that any system that has keys on the coordinator disks can also be seen in the current GAB membership. If this verification fails, the fencing driver prints a warning to the console and system log and does not start.

- If all verifications pass, the fencing driver on each system registers keys with each coordinator disk.

Figure 5-5 shows the topology of the coordinator disks in the Policy Master cluster:

Figure 5-5 Topology of coordinator disks in the Policy Master cluster



How membership arbitration works

When the Policy Master cluster starts, all systems register a unique key on the coordinator disks. The key is based on the LLT system ID, for example LLT ID 0 = A.

When there is a perceived change in membership, the following process is followed for membership arbitration:

- GAB marks the system as DOWN, excludes the system from the Policy Master cluster membership, and delivers the membership change—the list of departed systems—to the fencing module.
- The system with the lowest LLT system ID in the Policy Master cluster races for control of the coordinator disks
 - In the most common case, where departed systems are truly down or faulted, this race has only one contestant.

- In a split brain scenario, where two or more subclusters have formed, the race for the coordinator disks is performed by the system with the lowest LLT system ID of that subcluster. This system races on behalf of all the other systems in its subcluster.
- The race consists of executing a preempt and abort command for each key of each system that appears to no longer be in the GAB membership. The preempt and abort command allows only a registered system with a valid key to eject the key of another system. This ensures that even when multiple systems try to eject other, each race has only one winner. The first system to issue a preempt and abort command wins and ejects the key of the other system. When the second system issues a preempt and abort command, it can not perform the key eject because it is no longer a registered system with a valid key.
- If the preempt and abort command returns success, that system has won the race for that coordinator disk.
Each system repeats this race to all the coordinator disks. The race is won by, and control is attained by, the system that ejects the other system's registration keys from a majority of the coordinator disks.
- On the system that wins the race, the vxfen module informs all the systems that it was racing on behalf of that it won the race, and that subcluster is still valid. This information is passed back to GAB.
- On the system(s) that do not win the race, the vxfen module triggers a system panic. The other systems in this subcluster note the panic, determine they lost control of the coordinator disks, and also panic and restart.
- Upon restart, the systems try to seed into the Policy Master cluster.
 - If the systems that restart can exchange heartbeat with the number of Policy Master cluster systems declared in `/etc/gabtab`, they automatically seed and continue to join the Policy Master cluster. Their keys are replaced on the coordinator disks. This case only happens if the original reason for the membership change has cleared during the restart.
 - If the systems that restart can not exchange heartbeat with the number of Policy Master cluster systems declared in `/etc/gabtab`, they do not automatically seed, and HAD does not start. This is a possible split brain condition, and requires the administrator to intervene.

Note: Forcing a manual seed at this point lets the Policy Master cluster seed. However, when the fencing module checks the GAB membership against the systems that have keys on the coordinator disks, a mismatch occurs. vxfen detects a possible split brain condition, prints a warning, and does not start. In turn, HAD does not start. Administrative intervention is required.

About data protection in the Policy Master cluster using SCSI-3 storage

Membership arbitration alone is not complete data protection because it assumes, similar to quorum solutions, that all systems either participate in the arbitration or are already down.

The following examples are rare situations which much also be protected against:

- A system hang causes the kernel to stop processing for a period of time.
- The system resources were so busy that the heartbeat signal was not sent.
- A break and resume function is supported by the hardware and executed. Dropping the system to a system controller level with a break command can result in the heartbeat signal timeout.
- The OfflineMonitorInterval resource attribute, which controls the monitoring of offline resource, is disabled to avoid extra processing on client nodes.

In the first three types of situations, the systems are not actually down, and may return to the Policy Master cluster after Policy Master cluster membership has been recalculated. This could corrupt data because a system could potentially write to disk before it determines it should no longer be in the Policy Master cluster. In the fourth situation, a concurrency violation could occur if you online resources outside of VCS One control.

Combining membership arbitration with data protection of the shared storage eliminates all of the above possibilities for data corruption.

Data protection fences off (removes access to) the shared data storage from any system that is not a current and verified member of the Policy Master cluster. Access is blocked by the use of SCSI-3 persistent reservations.

SCSI-3 Persistent Reservation (SCSI-3 PR) is an enhancement to the SCSI specification that supports multiple systems, or multiple paths from a single system, accessing a device. At the same time it blocks access to the device from other systems, or other paths.

When a service group comes online on a particular system, if the service group contains a disk group, the disk group is imported. When using SCSI-3 PR, importing the disk group puts registration and reservation on the data disks. Only the system that has imported the storage with SCSI-3 reservation can write to the shared storage. This prevents a system that did not participate in membership arbitration from corrupting the shared storage. SCSI-3 PR ensures persistent reservations across SCSI bus resets.

Note: Use of SCSI III PR protects against all elements in the IT environment that might be trying to write illegally to storage, not only VCS related elements.

Membership arbitration combined with data protection is termed I/O Fencing.

How I/O fencing works

This topic describes the general logic employed by the I/O fencing module along with some specific example scenarios.

About the I/O fencing algorithm

To ensure the most appropriate behavior is followed in both common and rare corner case events, the fencing algorithm works as follows:

- The fencing module is designed to never have systems in more than one subcluster remain current and valid members of the Policy Master cluster. In all cases, either one subcluster survives, or in very rare cases, no systems will.
- The system with the lowest LLT ID in any subcluster of the original Policy Master cluster races for control of the coordinator disks on behalf of the other systems in that subcluster.
- If a system wins the race for the first coordinator disk, that system is given priority to win the race for the other coordinator disks. Any system that loses a race delays a short period of time before racing for the next disk. Under normal circumstances, the winner of the race to the first coordinator disk wins all disks. This ensures a clear winner when multiple systems race for the coordinator disk, preventing the case where three or more systems each win the race for one coordinator disk.
- If the Policy Master cluster splits such that one of the sub-clusters has at least 51% of the members of the previous stable membership, that subcluster is given priority to win the race.

The system in the smaller subcluster(s) delay a short period before beginning the race.

This ensures that as many systems as possible remain running in the Policy Master cluster.

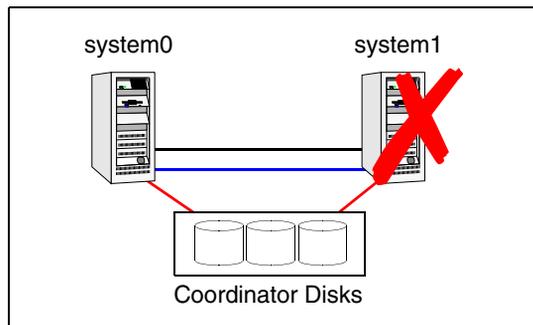
Two system Policy Master cluster where one system fails

System1 fails, and System0 carries out the I/O fencing operation in the following way:

- The GAB module on System0 determines System1 has failed due to loss of heartbeat signal reported from LLT.
- GAB passes the membership change to the fencing module on each system in the Policy Master cluster.
The only system that is still running is System0
- System0 gains control of the coordinator disks by ejecting the key registered by System1 from each coordinator disk.
The ejection takes place one by one, in the order of the coordinator disk's serial number.
- When the fencing module on System0 successfully controls the coordinator disks, HAD carries out any associated policy connected with the membership change.
- System1 is blocked access to the shared storage, if this shared storage was part of a service group that was now taken over by System0 and imported.

Figure 5-6 shows a two system Policy Master cluster where one system fails.

Figure 5-6 I/O Fencing example with system failure



Four system Policy Master cluster where cluster interconnect fails

The Policy Master cluster interconnect fails in such a way as to split the Policy Master cluster from one four-system Policy Master cluster to two two-system Policy Master clusters. The Policy Master cluster performs membership arbitration to ensure that only one subcluster remains.

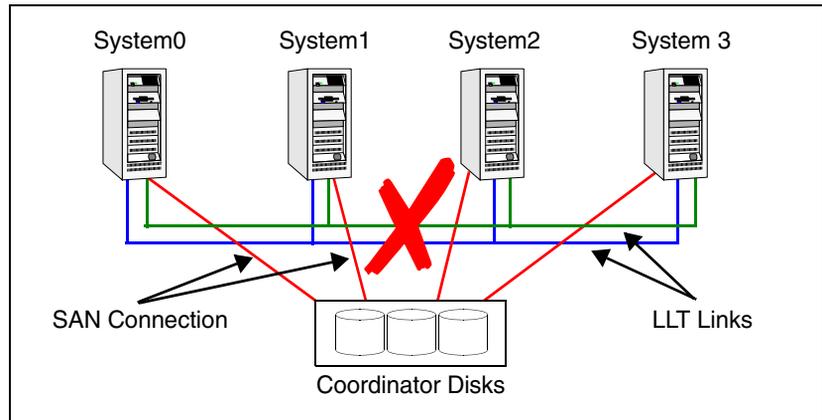
Due to loss of heartbeat, System0 and System1 both believe System2 and System3 are down. System2 and System3 both believe System0 and System1 are down.

I/O fencing operations progress in the following way:

- LLT on each of the four systems no longer receives heartbeat messages from the systems on the other side of the interconnect failure on any of the configured LLT interfaces for the peer inactive timeout configured time.
- LLT on each machine passes to GAB that it has noticed a membership change. Specifically:
 - LLT on System0 passes to GAB that it no longer detects System2 and System3
 - LLT on System1 passes to GAB that it no longer detects System2 and System3
 - LLT on System2 passes to GAB that it no longer detects System0 and System1
 - LLT on System3 passes to GAB that it no longer detects System0 and System1

Figure 5-7 shows a four system Policy Master cluster with a cluster interconnect failure

Figure 5-7 Four system Policy Master cluster where cluster interconnect fails



- After LLT informs GAB of a heartbeat loss, the systems that are remaining perform a 5-second GAB Stable Timeout. In this example:
 - System0 and System1 confirm that both of them do not detect System2 and System3
 - System2 and System3 agree that both of them do not detect System0 and System1
- GAB marks the system as DOWN, and excludes the system from the Policy Master cluster membership. In this example:
 - GAB on System0 and System1 mark System2 and System3 as DOWN and excludes them from Policy Master cluster membership.
 - GAB on System2 and System3 mark System0 and System1 as DOWN and excludes them from Policy Master cluster membership.
- GAB on each of the four systems passes the membership change to the vxfen driver for membership arbitration. Each subcluster races for control of the coordinator disks. In this example:
 - System0 has the lower LLT ID, and races on behalf of itself and System1.
 - System2 has the lower LLT ID, and races on behalf of itself and System3.
- GAB on each of the four systems also passes the membership change to HAD. HAD waits for the result of the membership arbitration from the fencing module before taking any further action.

- Assume System0 wins the race for the coordinator disks, and ejects the registration keys of System2 and System3 off the disks. The result is as follows:
 - System0 wins the race for the coordinator disk. The fencing module on System0 communicates race success to all other fencing modules in the current Policy Master cluster, in this case System0 and System1. The fencing module on each system in turn communicates success to HAD. System0 and System1 remain valid and current members of the Policy Master cluster.
 - System2 loses the race for control of the coordinator disks. The fencing module on System2 calls a kernel panic and the system restarts.
 - System3 detects another membership change from the kernel panic of System2. Because that was the system that was racing for control of the coordinator disks in this subcluster, System3 panics also.
- HAD carries out any associated policy or recovery actions based on the membership change.
- System2 and System3 are blocked access to the shared storage (if the shared storage was part of a service group that was now taken over by System0 or System 1).
- To rejoin System2 and System3 to the Policy Master cluster, you must do the following:
 - Shut down System2 and System3
 - Fix the Policy Master cluster interconnect links
 - Restart System2 and System3

Best practices for Policy Master cluster communications

The following are the recommended best practices for Policy Master cluster communications to best support proper Policy Master cluster membership and data protection.

- Properly seed the Policy Master cluster by requiring all systems are in the GAB membership before the Policy Master cluster automatically seeds. If every system is not present, manual intervention by the administrator must eliminate the possibility of a split brain condition before manually seeding the Policy Master cluster.
- Configure multiple independent communication network links between Policy Master cluster systems.

Networks should not have a single point of failure, such as a shared hub or ethernet card.

- Low-priority LLT links are recommended.
Low-priority LLT links provide an extra path for heartbeat communications in case the main communication links fail.
- Disable the console-abort sequence
Most UNIX systems provide a console-abort sequence that enables the administrator to halt and continue the processor. Continuing operations after the processor has stopped may corrupt data and is therefore unsupported by VCS.
When a system is halted with the abort sequence, it stops producing heartbeats. The other systems in the Policy Master cluster consider the system failed and take over its services. If the system is later enabled with another console sequence, it continues writing to shared storage as before, even though its applications have been restarted on other systems.
Disable the console-abort sequence or create an alias to force the “go” command to perform a restart on systems not running I/O fencing.
- Select the smallest possible LUNs for use as coordinator disks. Use three coordinator disks.
- Do not reconnect the Policy Master cluster interconnect after a network partition without shutting down one side of the split Policy Master cluster.

A common example of this happens during testing, where the administrator may disconnect the Policy Master cluster interconnect and create a network partition. Depending on when the interconnect cables are reconnected, unexpected behavior can occur.



Getting started

This section includes the following chapters:

- [“Starting and stopping Veritas Cluster Server One”](#) on page 101.
- [“Using the VCS One console”](#) on page 107.
- [“Using the Simulator”](#) on page 173.

Starting and stopping Veritas Cluster Server One

This chapter includes the following topics:

- [About VCS One user interfaces](#)
- [Setting the PATH variable to use the CLI](#)
- [Before starting the VCS One console](#)
- [Logging off from the VCS One console](#)

About VCS One user interfaces

VCS One provides efficient and centralized control of numerous mission critical applications that run on multiple systems in the VCS One cluster. VCS One provides a command line interface (CLI), and a management console to perform administrative tasks on the VCS One cluster. The management console is a Web-based interface, which uses the Symantec Web server. The Symantec Web Server and the Policy Master must reside on the same system.

Setting the PATH variable to use the CLI

Use this procedure to set the PATH variable to use the CLI (command line interface) with VCS One.

Note that on the Policy Master, both VCS and VCS One are installed. In some instances, the same command exists in both these products, such as halog and haclus. Be aware of the order of your PATH variable. To avoid confusion, use the full path name when executing a command.

To set the PATH variable to use the command line interface (CLI)

- ◆ At the command prompt, type the following command:

```
PATH=$PATH:/opt/VRTSvcsonone/bin
export PATH
```

More information is available about VCS One commands. See the *Veritas Cluster Server One Command Reference Guide*.

Before starting the VCS One console

Before starting the VCS One console, ensure that you perform the following tasks:

- Install a supported browser.
- Install a supported Macromedia Flash plug-in.
- Install and configure VCS One.
See the *Veritas Cluster Server One Installation Guide*.
- Configure the ports that the Symantec Web server uses.
- Enable the Web browser cookies and JavaScript, and disable the pop-up blocker.

For supported software versions, see the *Veritas Cluster Server One Release Notes*.

Changing Web browser settings

This section describes how to change the Web browser settings for Microsoft Internet Explorer 7.0 to accurately view the VCS One console. These steps disable browser caching, and set the ActiveX and cookie settings as required by VCS One. You may need to follow the equivalent steps given in the browser's documentation.

To change Web browser settings

- 1 Start Microsoft Internet Explorer.
- 2 In the Tools menu, select **Internet Options**.
- 3 In the Internet Options dialog box, click the **General** tab.
- 4 Under Browsing history, click **Settings**.
- 5 In the Temporary Internet Files and History Settings dialog box, select the **Every time I visit the webpage** option, and then click **OK**.
- 6 In the Internet Options dialog box, click the **Security** tab, click **Local intranet**, and then click **Custom Level**.
- 7 In the Security Settings dialog box, under **ActiveX controls and plug-ins**, enable the following settings:
 - **Download signed ActiveX controls**
 - **Run ActiveX controls and plug-ins**
 - **Script ActiveX controls marked safe for scripting**
- 8 In the Security Settings dialog box, click **OK**.
- 9 In the **Internet Options** dialog box, click the **Privacy** tab. Under Settings, click **Advanced**.
- 10 In the **Advanced Privacy Settings** dialog box, perform the following tasks:
 - Select the **Override automatic cookie handling** check box.
 - Under **First-party Cookies**, select the **Accept** option.
 - Under **Third-party Cookies**, select the **Accept** option.
 - Select the **Always allow session cookies** check box.
 - Click **OK**.
- 11 In the **Internet Options** dialog box, click **Apply**.
- 12 Click **OK**.

Starting and logging on to the VCS One console

To start and log on to the VCS One console

- 1 Open a Web browser and enter the following URL:

`http://PM_cluster_virtual_IP_address:14171`

It is recommended that you use the virtual IP address of the Policy Master cluster instead of the name of the active Policy Master cluster node. If you use the virtual IP address, the VCS One console maintains a connection with the Policy Master after a Policy Master cluster failover operation.

Note: When you start the VCS One web console for the first time, a Web page might appear with a `Secure Connection Failed` message. Follow the steps provided in the browser to add and permanently store a trusted security certificate as an exception. After the security certificate is added, the VCS One Web console login page appears in the browser.

- 2 In the web browser, click the **VCS One Web Console** link.
- 3 In the **Log on** page, specify the following details:
 - In the **Select Language** box, select the appropriate language. In this release, only English is supported.
 - In the **User Name** field, enter the name of the user.
 - In the **Password** field, enter the password.
 - In the **Domain** field, enter the domain name.
You must specify a domain name for all domain types except `unixpwd` (which is the default domain type) and `pam`. To view a list of all the domains on the Policy Master system, enter the following command:

```
# /opt/VRTSvcsone/bin/haat showallbrokerdomains
```

If the **Domain** field is left blank and the domain type is `unixpwd` or `pam`, VCS One assumes that the domain type is the same as the Policy Master system's domain type.
 - In the **Domain Type** field, select a domain type (`unixpwd`, `nt`, `nis`, `nisplus`, `pam`, `vx`, or `ldap`).
 - In the **Broker:Port** field, enter the authentication broker name and the port number separated by a colon (:). This field is optional and is populated automatically.
- 4 Click **Log On**.

The web console is best viewed at 1024x768 screen resolution.

More information is available about the VCS One console.

See [“Using the VCS One console”](#) on page 107.

More information is available about how to troubleshoot authentication issues.

See “[Troubleshooting authentication issues](#)” on page 616.

Logging on to VCS One using the command line

The `halogin` command authenticates users in the VCS One environment and sets up a valid user profile. Authentication is required to execute VCS One commands.

To log on to VCS One using the command line

- ◆ At the command prompt, type the following command:

```
# /opt/VRTSvcsone/bin/halogin [-forclient] [-passwd password] \  
-user user@domain -domaintype domaintype
```

Use the optional `-forclient` option to ensure that the user profile is used when “ha” commands are executed within script-based entry points inside local zones so that they can connect to the Policy Master via the VCS One client daemon (`vcsoeclientd`). If you do not supply a password, the command prompts you for it.

The `-user user@domain` option is the fully qualified user name and the `-domaintype domaintype` option is the relevant domain type. Accepted values for the domain type include `unixpwd`, `nt`, `nis`, `nisplus`, `ldap`, `pam`, and `vx` (which is the Symantec Private Domain). These values are case sensitive.

If you do not use the `halogin` command to log on to VCS One, you must use the `-user` and `-domaintype` switches each time you issue a VCS One command.

The VCS One client system root user (localhost root user) is an exception, and has the user privileges that are associated with the VCS One client daemon. For the root user, VCS One commands ignore the profile that is created by the `halogin` command on the active Policy Master cluster node.

For more information about VCS One commands, refer to the *Veritas Cluster Server One Command Reference Guide*.

Logging off from the VCS One console

This section describes how to log off from the VCS One console.

To log off from the VCS One console

- ◆ In the VCS One console, click **Logout**.
After you successfully log off from the VCS One console, the following information message is displayed:

```
VCS One INFO V-97-11-10 You have been successfully logged out.
```

Note: If you use the Firefox Web browser and have multiple open browser connections to the VCS One console, when you log off from one console, VCS One simultaneously logs you off from all the other open browser connections.

Using the VCS One console

This chapter includes the following topics:

- [About the VCS One console](#)
- [Managing SSL certificates](#)
- [VCS One console layout](#)
- [Summary information on the Home tab](#)
- [Manage tab options](#)
- [Logs tab options](#)
- [Administration tab options](#)
- [Summary information on the Search tab](#)

About the VCS One console

The VCS One console enables you to configure, manage, and monitor the VCS One cluster. You can use the console to perform various operations on one or more VCS One objects, such as service groups, systems, and sets.

You can use the VCS One Simulator to familiarize yourself with the console and simulate tasks and functionality of VCS One.

See [“About the Simulator”](#) on page 174.

Note: Before starting the VCS One console ensure that pop-up blockers are disabled in the Web browser.

About VCS One console ports

By default, the VCS One console serves HTML content on port 14171 and 14172. Be sure to enable these ports. These ports are used as follows:

- 14171 (HTTPS): Secure SSL port. VCS One console presents a self-signed SSL certificate (issued by Symantec) to the browser. You must accept the certificate before accessing the secure Web consoles. The SSL protocol prevents malicious users from sniffing Web console data from the network.
- 14172: Administrative port.
- 14173: Webservices communication port.

If you use these ports for another application on the system, configure VCS One console to use different ports.

Managing SSL certificates

This section points you to the tools and files you need to perform SSL-related tasks, such as installing and managing certificates signed by a Certificate Authority (CA). For more detailed information about certificate management, see the Apache Tomcat 6.0 SSL Configuration instructions available on the Internet.

You can use the self-signed certificate that VCS One provides, or you can optionally obtain a certificate from a third-party certificate authority (CA).

The self signed certificate is stored in the key store located at:

`/opt/VRTSvcsone/web/tomcat/cert`

Configuring and Managing SSL certificates (optional)

You do not need to perform any tasks to manage the SSL certificate that Symantec provides. However, you can optionally configure and manage SSL certificates using Java Keytool, or another tool of your choice.

After you make any modifications to your SSL configuration, you must stop and restart the server using:

```
/opt/VRTSvcsone/bin/hastop -web  
/opt/VRTSvcsone/bin/hastart -web
```

Locating the Java Keytool utility

For your convenience, the Java Keytool utility is included in the VCS One installation, and is located at:

```
/opt/VRTSvcsone/jre/bin
```

Changing the key store password

The default password that protects the key store is *changeit*. If you change the key store password, you need to update the server.xml file with the new password. The server.xml file is located at:

```
/opt/VRTSvcsone/web/tomcat/conf
```

VCS One console layout

The VCS One console area consists of the following elements:

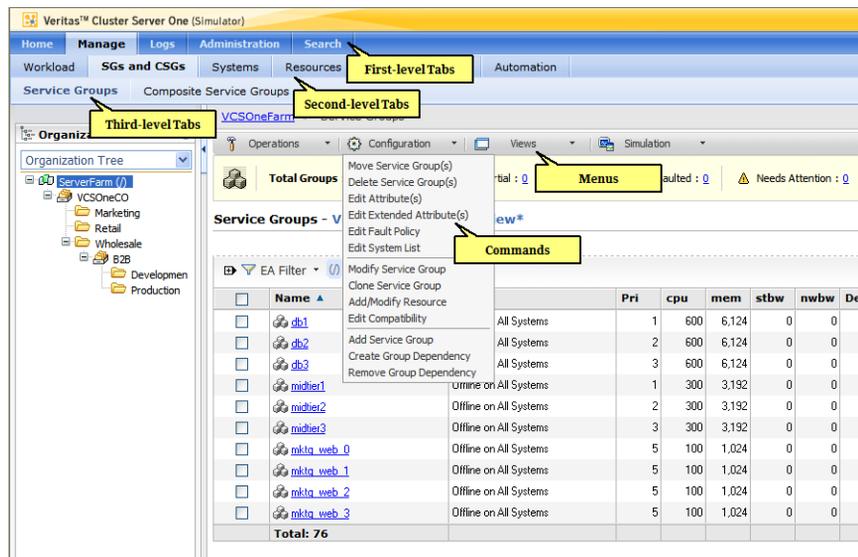
- The tab bar, which contains first-level, second-level, and third-level tabs. See [“About the tab bar”](#) on page 110.
- The left and right panes, which display the navigation hierarchy and object information respectively. See [“About panes”](#) on page 111.
- The history icon, which provides access to recently visited objects. See [“About the History menu bar”](#) on page 117.
- The wizards, which provide access to configuration settings. See [“About wizards”](#) on page 117.
- The Help link, which displays help information. See [“About VCS One Help”](#) on page 117.
- The Log Out link, which logs you out of the VCS One console. See [“Logging off from the VCS One console”](#) on page 118.

About the tab bar

The tab bar is located in the top area of the VCS One console and contains three levels of tabs. The first-level tabs are visible from all the views in the console. Clicking any of these tabs displays the second-level tabs. The second-level tabs contain menu commands. The third-level tabs are available only for certain second-level tabs such as the **SGs and CSGs** tab. The third-level tabs are used to group objects by type. For example, clicking the **Composite Service Groups** third-level tab displays the list of all composite service groups for the selected OU.

Figure 7-1 shows the location of the tab bar and the menus in the VCS One console.

Figure 7-1 Tab bar and menus



The first-level tabs provide access to the following functionality:

- The **Home** tab enables you to perform VCS One cluster operations. See “[Summary information on the Home tab](#)” on page 118.
- The **Manage** tab enables you to perform operations on VCS One cluster objects such as service groups, composite service groups, systems, resources, jobs, and rules. See “[Manage tab options](#)” on page 120.
- The **Logs** tab enables you to view, search, and delete log server messages. See “[Logs tab options](#)” on page 156.

- The **Administration** tab enables you configure users and roles, manage organization units and sets, define extended attributes, and configure global and automation settings.
See “[Administration tab options](#)” on page 162.
- The **Search** tab enables you to search for specific VCS One cluster objects.
See “[Summary information on the Search tab](#)” on page 172.

About disabled menu items

None of the menu items are disabled or grayed out; however, in certain cases where the pre-conditions for the operation are not met, an operation might not complete after you click the menu item. The reasons for non-completion of the command display as messages on the screen. You can take corrective action based on these messages. The operation will complete only after all the pre-conditions for the operation are met.

About panes

The area below the tab bar is divided into two panes. The left pane contains navigation hierarchies. The right pane displays various views which depend on the tab, command, or object selected.

[Figure 7-2](#) shows the location of the right pane, the left pane, the navigation bar, the menu bar, and the tables.

Figure 7-2 Panes, navigation bar, and menu bar

The screenshot shows the Veritas Cluster Server One (Simulator) interface. The left pane displays the Organization Tree with a hierarchy including VCSOneCO, Marketing, Retail, Wholesale, Development, and Production. The right pane displays the Service Groups view, showing a table of service groups with their status and resource usage. The table is as follows:

Name	Status	Pri	cpu	mem	stbw	nwbw	Dependency
db1	Offline on All Systems	1	600	6,124	0	0	0..1
db2	Offline on All Systems	2	600	6,124	0	0	0..1
db3	Offline on All Systems	3	600	6,124	0	0	0..1
midtier1	Offline on All Systems	1	300	3,192	0	0	1..2
midtier2	Offline on All Systems	2	300	3,192	0	0	1..2
midtier3	Offline on All Systems	3	300	3,192	0	0	1..2
mkta_web_0	Offline on All Systems	5	100	1,024	0	0	0:0
mkta_web_1	Offline on All Systems	5	100	1,024	0	0	0:0
mkta_web_2	Offline on All Systems	5	100	1,024	0	0	0:0
mkta_web_3	Offline on All Systems	5	100	1,024	0	0	0:0
Total: 76							

The left pane of the VCS One console contains a list box. The list box provides access to the organization tree nodes and object sets. You can right-click a node or set and access the related operations.

In the list box, you can select one of the following options:

- My Objects or a custom view name to select the default set (My Objects) or a custom view that is associated with the service group or system.
See [“About administrating sets of objects”](#) on page 550.
- Organization Tree to navigate to a specific organization tree node to which the service group or system is attached.
See [“How you manage users using the Organization Tree”](#) on page 221.

The right pane contains the navigation bar, the menu bar, and tables. For most of the second-level tabs and all the third-level tabs, if you click any of the tabs, a navigation bar and a menu bar appears. The navigation bar shows a list of the objects that you selected to navigate to this view. The menu bar has drop-down commands for operations and tasks that are related to the selected tab. Most of the console information is displayed in the form of tables.

About console refresh

As you use the console, the status of the various VCS One cluster objects, such as systems, changes. Service groups go online and offline, alerts are generated, and object data changes. The information in the console updates (refreshes) automatically to reflect the latest data.

For information that is displayed in tables, only the relevant cells of the rows are updated – the complete page does not reload. This behavior of the console is known as partial page refresh. This feature prevents refresh issues for systems that have a large number of objects or have slow connections. Additionally, user activity is not disrupted due to continuous updates to the systems and applications under management.

Tip: To manually refresh the current view, use the browser refresh command.

About tables

Most of the information in the right pane is displayed in the form of tables. A table can also contain another table which is known as a nested table. The information in the tables is updated automatically to reflect the latest data.

You can configure most of the tables to suit your viewing preferences. You can perform the following configuration tasks:

- Select objects in a table

See [“About selecting objects in a table”](#) on page 113.

- Sort the table contents
See [“Sorting the contents of a table”](#) on page 113.
- View multiple pages
See [“Viewing multiple pages of a data table”](#) on page 114.
- Change table settings such as column order and number of rows displayed
See [“Changing the table settings”](#) on page 114.
- Configure table views
See [“Configuring table views”](#) on page 115.
- Filter results in a table
See [“Filtering results in a table”](#) on page 115.

About selecting objects in a table

You can select an object in a table by selecting the check box next to the object’s name or by clicking anywhere on the object’s row. You can also select multiple objects by using the CTRL and SHIFT keys. To select multiple objects that are contiguous, click the first object, press the SHIFT keys, then select the last object in the series. To select multiple objects that are non-contiguous, select the first object, press the CTRL key, then select the second object, and so on.

Sorting the contents of a table

In some of the VCS One console tables, you can sort the rows by the data in a column. Some columns are not sortable.

To sort rows in a table by data in a column

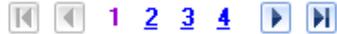
- 1 In the table, locate the column which you want to use to sort the data.
- 2 Click the column heading.
The table refreshes with the list sorted by the values in that column in ascending order. A triangle icon (pointed up) displays in that column heading.
- 3 To sort the table in the descending order, click the column heading again.
The table refreshes with the list sorted by the values in descending order. A triangle icon (pointed down) displays in that column heading.

Viewing multiple pages of a data table

Tables can contain multiple pages. You can view subsequent pages of a table using the go-to-page bar. This bar is located in the right corner below the table.

Figure 7-3 shows the go-to-page bar.

Figure 7-3 Go-to-page bar



To access pages in the table

- 1 In a table with multiple pages, locate the go-to-page bar below the table.
- 2 Click the controls on the go-to-page bar to move forward and backward through the table pages.

Changing the table settings

Tables can be configured to change the columns that are displayed, the order of columns, and the number of rows displayed.

To change the table settings

- 1 In the top right corner of the table, click the **Table Settings** icon.
- 2 In the Table Settings dialog box, in the Available Columns area, check the box for each column that you want to display.
- 3 Click **>>**.
- 4 To change the position of the column in the table, in the Selected Columns area, check the column name check box.
- 5 Click **Move Up** or **Move Down**.
- 6 To arrange the information in the ascending or descending order, in the Sort column, click the arrow against the column name.
- 7 Select **Up** or **Down**.
- 8 To change the number of rows displayed, select the appropriate value in the **Rows Per Page** box.
- 9 Click **OK**.

Configuring table views

A view is a snapshot of the current table settings. The view that is displayed before any new views are created is called the default view. You can change the table settings, such as the columns displayed and the number of rows, and save these settings as a view. You can also delete a view; however, the default view cannot be removed.

To select a saved view, in the top right corner above the table, click the view drop-down arrow, and select the view name. The page refreshes and displays the new view.

To save a view

- 1 Change the table settings as per your preference.
See [“Changing the table settings”](#) on page 114.
- 2 In the top right corner of the table, next to the view drop-down box, click the **Save View** icon.
- 3 In the View Manager dialog box, click the Action drop-down arrow, and select **Save As**.
- 4 In the Name and Description text boxes, enter a name for the view and its description respectively.
- 5 Click **Save As**.

To remove a view

- 1 In the top right corner of the table, click the view drop-down box arrow and select the view that you want to remove.
- 2 In the top right corner of the table, next to the view drop-down box, click the **Delete View** icon.
- 3 In the confirmation dialog box, click **OK**.

Filtering results in a table

Within a table, you can use the **Filter** option to search for a specific VCS One object. You can filter objects by entering a keyword or by selecting an extended attribute value. You can apply multiple filters to narrow your search.

To filter objects by entering a keyword

- 1 In the right pane above the table, click the plus sign next to the EA Filter icon. The Keyword box displays.
- 1 In the **Keyword** box, enter the keyword. The keyword can be a string that matches part of the object names that you want to locate.

2 Click **Go**.

If the search is successful, the specified objects matching the keyword string display in the table.

To filter objects by selecting an extended attribute value

- 1 Click the **EA Filter** drop-down arrow, and select the desired extended attribute value. The table is refreshed and only objects matching the selected filter display.
- 2 Repeat the preceding step to add more filters.
- 3 To save the list of filtered objects as a set, click **Save as Set**.

To remove filters

- 1 To remove a filter, click the cross mark next to the filter name.
- 2 To remove all filters, click **Clear All**.

About selecting menu commands

The commands used to perform various operations can be invoked in any of the following ways:

- Click the menu bar in the right pane and select the command.
- Right-click an object name in the table and select the command from the context-sensitive menu.
- In the left pane, right-click an OU name and select the command from the context-sensitive menu.

About filtering objects using the organization tree

The organization tree, which is located in the left pane of the console, can be used to filter objects displayed in the right pane. Using the organization tree, you can filter objects such as systems, service groups, composite service groups, resources, users, extended attributes, rules, and jobs.

To filter objects, in the list page of the object, select the appropriate Organization Tree Node (OU Name node or OU Value node). For example, to filter systems, use the following procedure.

To filter systems using the organization tree

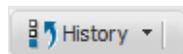
- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Systems** tab.

- 3 In the left pane, if the organization tree is not displayed, select **Organization Tree** from the list.
- 4 In the left pane, select the appropriate Organization Tree Node (OU Name node or OU Value node). All the systems associated with the selected Organization Tree node are listed in the right pane under **Systems**.

About the History menu bar

Figure 7-4 shows the History menu bar.

Figure 7-4 History menu bar



The History menu bar contains a list of recently visited VCS One cluster objects such as service groups, systems, and resources. Each object in the History menu bar has an icon associated with it which indicates the type of the object. Each object also has links to related operations and tasks. For example, for a recently visited service group the following links are available: Group Details, Resource Dependencies, Group Dependencies, Workload, Map View, and All Attributes.

When you navigate to object-specific pages such as the details page for an object the object name gets added to the History menu bar. The most recently visited object is placed at the top of the list. The History menu bar holds 10 objects. You cannot configure this value. The list is cleared after you log off.

Click the arrow on the History menu bar to view the list of recently visited objects.

About wizards

Many of the VCS One commands use wizards that help you configure various settings. You can navigate through the wizard screens either by using a pointing device such as a mouse or by using the keyboard. You can use the TAB key to move between the various screen elements such as buttons. To select a button, use the SPACEBAR key. Note that the ENTER key does not work when selecting a button.

About VCS One Help

The Help link is located on the right top corner of the VCS One console area. The Help is context-sensitive – when you click the Help link you see the help for the current page in a separate window.

Logging off from the VCS One console

To log off from the VCS One console

- ◆ Click the **Logout** link located at the top-right corner of the VCS One console area.

Summary information on the Home tab

When you log on to the VCS One console or click the **Home** tab, the console displays the summary information about the VCS One cluster.

The summary information includes a comprehensive view of all the service groups, composite service groups, and systems present in the VCS One cluster. You can check the status of all the service groups and systems at a glance and determine the health of the VCS One cluster.

[Table 7-1](#) describes the console details that are displayed in the right pane.

Table 7-1 VCS One cluster summary console elements

Element	Description
Composite Service Groups	The numerical distribution of composite service groups in the online, offline, and partial states is displayed in the Composite Service Groups graph. To view the composite service groups that are currently in a particular state, click the number or the state name or the bar that corresponds to each state.
Service Groups	The numerical distribution of service groups in the online, offline, faulted, and partial states is displayed in the Service Groups graph. To view the service groups that are currently in a particular state, click the number or the state name or the bar that corresponds to each state.
Systems	The numerical distribution of systems in the running, offline, and faulted states is displayed in the Systems graph. To view the systems that are currently in a particular state, click the number or the state name or the bar that corresponds to each state.
Remote Clusters' Summary	The numerical distribution of remote clusters in the running, offline, faulted, and disabled states is displayed in this table. To view the respective remote clusters that are currently in a particular state, click the number that corresponds to each state.

Table 7-1 VCS One cluster summary console elements

Element	Description
Global CSGs' Summary on Remote Clusters	The numerical distribution of global composite service groups in the online, offline, and partial states and which are located on remote clusters is displayed in this table. To view the respective composite service groups that are currently in a particular state, click the number that corresponds to each state.
Service Groups' Summary: By Priority	The numerical distribution of service groups in the online, offline, faulted, and partial states and categorized by the service group's priority value, is displayed in this table. To view the respective service groups that are currently in a particular state, click the number that corresponds to each state.
Systems' Summary: By OS	The numerical distribution of systems in the running, offline, and faulted states and categorized by the operating system, is displayed in this table. To view the respective systems that are currently in a particular state, click the number that corresponds to each state.
Needs Attention	The Needs Attention table lists all the service groups and systems that are currently in the faulted state or which otherwise need attention. This table also lists the faulted remote clusters and those composite service groups which have a concurrency violation. Each object is displayed as a link. You can click an object to view its details and perform operations on it.

Manage tab options

All VCS One cluster objects such as service groups, systems, and resources are created, configured, and managed from the **Manage** tab. You can use the second-level tabs to perform various operations on VCS One cluster objects.

[Table 7-2](#) describes the second-level tabs under the **Manage** tab.

Table 7-2 Second-level tabs under the Manage tab

Tab	Description
Workload	Displays a graphical view of service groups and systems. This view also contains options to configure the view and locate specific objects. See “Workload tab menus” on page 121.
SGs and CSGs	Provides access to the service group and composite service group-related menu commands. This tab has the following third-level tabs: Service Groups and Composite Service Groups . Click the respective third-level tabs to access the menu commands. See “Service Groups tab operations” on page 130. See “Composite Service Groups tab operations” on page 139.
Systems	Provides access to the system-related menu commands. See “Systems tab operations” on page 142.
Resources	Provides access to the resources-related menu commands. See “Resources tab operations” on page 145.
Disaster Recovery	Provides access to the disaster recovery-related menu commands. See “Disaster Recovery tab operations” on page 148.
Automation	Provides access to the jobs and rules-related menu commands. See “Jobs tab operations” on page 151. See “Business Rules tab and Notification Rules tab operations” on page 153.

Workload tab menus

The **Workload** tab displays the service groups and systems in a graphical view. This view is called the Workload view.

The **Workload** tab has various menus which are located in the right pane below the navigation bar. Each menu contains commands which you can use to perform service group and system operations.

[Table 7-3](#) describes the **Workload** tab menus.

Table 7-3 Workload tab menus

Menu	Description
Configuration	Contains commands to perform operations such as adding or deleting a system, adding or deleting a service group, and creating or removing a group dependency. See “Workload configuration menu commands” on page 121.
Views	Contains the command to view the GTQ (Group Transition Queue). See “Workload view menu commands” on page 122.

Workload configuration menu commands

In the Workload view, the **Configuration** menu provides commands to manage systems and service groups.

[Table 7-4](#) describes the **Configuration** menu commands.

Table 7-4 Workload view Configuration menu commands

Command	Description
Add System	Adds a system to the VCS One cluster using the Add System Wizard. See “Adding a system to the VCS One cluster” on page 292.
Delete System	Deletes a system from the VCS One cluster. See “Deleting a system from the VCS One cluster” on page 298.
Add Service Group	Adds a service group using the Service Group Configuration Wizard. See “Adding a service group” on page 315.
Delete Service Group	Deletes a service group. See “Deleting a service group” on page 326.

Table 7-4 Workload view Configuration menu commands

Command	Description
Create Group Dependency	Defines the dependencies among service groups. See “Performing operations from the Group Dependency View” on page 323.
Remove Group Dependency	Removes the dependencies among service groups. See “Performing operations from the Group Dependency View” on page 323.

Workload view menu commands

In the Workload view, you can click **Views** to select the following view:

- GTQ View
 Displays the GTQ view in a separate window.
 See [“About the GTQ view”](#) on page 124.

About the Service Group Workload view

The Service Group Workload view displays the service group and system information in a bar graph form. Each vertical rectangle represents a system in the VCS One cluster. When no service groups are online on the system, the rectangle has a uniform solid color. When a service group is online on a system, a part of the vertical rectangle is shaded. The shaded area represents a service group that is online. The size of the shaded area represents the load of the service group as a percentage of the capacity of the system.

The numbers that are displayed above each rectangle indicate the load of the service group and the capacity of the system. If the system capacity exceeds six digits, only the load of the service group is displayed. A blinking area around a number indicates that the load dimensions of one of the service group has exceeded 80 percent of the capacity of the system. Move the mouse pointer over the numbers to view the eighty-percent mark for a particular system.

The bar graph under each system represents all the defined Load attribute key values for the service groups on the respective system. A small orange triangle in the shaded area indicates that a service group is a partially online on the system.

How to view service group information

In the Workload view, you can click a shaded area to select a service group. A dotted line is displayed around the shaded area and information about the service group is displayed under the **Group Overview** box. Information about the

systems that are part of the service group's SystemList attribute is displayed under the **SystemList** box. The **Other Info** box contains information such as the incompatible groups, parent groups, and child groups for the selected service group.

You can also move the mouse pointer over a service group to view the name, the priority, and the current load values of the service group.

How to view system details

In the Workload view, you can click the entire rectangle to view information about the system itself. The information also shows service groups that are online or faulted on the selected system. This information is displayed under the **System Overview** and **Groups Configured** boxes respectively. You can view service group information only if you have privileges for the service group.

About service groups that are not online

In the right side of the Workload view, you can view in a tabular form the service groups that are currently not online. Service groups that are not online can be in the waiting, offline, or faulted state. Click the respective table caption to display the service groups in that state. You can right-click a group name and perform the relevant operation.

[Table 7-5](#) describes the various states of service groups that are not online.

Table 7-5 States of the service groups that are not online

Service group state	Description
Waiting Groups	<p>The Waiting Groups table lists the service groups that are placed in the Group Transition Queue (GTQ). The action ID, service group name, priority, current operation, and the target system is also displayed for each service group. You can change the width of these columns. If IN is displayed as the current operation, the service group is in the INTENT ONLINE state.</p> <p>From the Waiting Groups table, you can right-click a service group to perform any of the following operations:</p> <ul style="list-style-type: none"> ■ Abort action Aborts the selected action. ■ Flush All Groups Removes all the service groups currently in the GTQ.

Table 7-5 States of the service groups that are not online

Service group state	Description
Offline Groups	<p>The Offline Groups table lists the service groups which are currently offline in the VCS One cluster. The service group name and priority is displayed for each service group.</p> <p>From the Offline Groups table, you can right-click a service group to perform any of the following operations:</p> <ul style="list-style-type: none"> ■ Online Group Anywhere Brings the service group online on any available system that is defined in the system list of the service group. ■ Show member systems Displays only those systems that are defined in the system list of the service group.
Faulted Groups	<p>The Faulted Groups table lists the service groups currently faulted in the VCS One cluster. The service group name and priority is displayed for each service group.</p> <p>From the Faulted Groups table, you can right-click a service group to perform any of the following operations:</p> <ul style="list-style-type: none"> ■ Clear Group Fault Clears the service group fault and brings the service group online. ■ Show member systems Displays only those systems that are defined in the system list of the service group.

How to view host system details

In the Workload view, you can click the any of the load bar graph rectangles to view information about the host system itself.

About the GTQ view

The GTQ (Group Transition Queue) view displays the service groups that are currently in the GTQ in a separate window. You can abort the current action for selected service groups or flush all groups from the queue.

See [“About the Group Transition Queue”](#) on page 283.

See [“Stopping the current action for a service group in the GTQ”](#) on page 339.

See [“Flushing the plan of action on all service groups in the GTQ”](#) on page 338.

Workload view service group operations

You can use the Workload view to perform service group operations. For example, you can bring a service group online or take it offline, switch the service group to another system, freeze or unfreeze a service group, or clear a service group fault. From the Workload view, you can select the shaded area that represents a service group, then right-click it to select an operation.

Service group operations are also available from the Service Groups third-level tab located under the **Manage > SGs and CSGs** tab.

See [“Service Groups tab operations”](#) on page 130.

[Table 7-6](#) describes the service group commands that are accessible from the Workload view.

Table 7-6 Service group commands that are accessible from the Workload view

Command	Description
Offline Group	Takes the service group offline but does not cause the service group to fail over. See “Taking a service group offline” on page 333.
Fault Group	Faults the service group on a system. If the service group is configured to fail over and a failover target is available, the service group is brought online on another system. This option is available only with the VCS One Simulator and not in real-time product deployment. See “Faulting a service group in the Simulator” on page 343.
Switch Group	Switches the service group to another system that is listed in the system list of the service group. See “Switching a service group” on page 336.
Freeze Group	Freezes a service group. A frozen service group cannot be moved to another system. Diagonal lines identify a frozen service group. See “Freezing a service group” on page 339.
Unfreeze Group	Unfreezes a currently frozen service group. An unfrozen service group lets you perform online or offline operations on it. See “Unfreezing a service group” on page 340.

Table 7-6 Service group commands that are accessible from the Workload view

Command	Description
Clear Group Fault	Clears a service group fault. When a service group faults on a system, first clear the service group fault. After you clear the fault, you should bring the service group online on the same system. See “Clearing a service group fault” on page 344.
Edit Attributes	Edits the service group attributes. See “Editing service group attributes” on page 324.
Show member systems	Displays only those systems in the Workload section that are part of the system list for a particular service group. The values that are set in the View box limits this view.
Go to group details	Displays the details for the selected service group.
Go to Map View	Displays the object relationship of a service group in a graphical way. See “Summary information on the map view” on page 137.
Zoom Host System	Displays the details of the host system in a Zoom Window. The Zoom Window is located in the right pane of the Workload section.

Workload view system operations

You can use the Workload view to perform system operations. For example, stop or start a system, pin or unpin a system, or freeze or unfreeze a system. The type of operation that you can perform depends on user privileges. From the Workload view, you can select the bar graph rectangle that represents a system, then right-click it to select an operation.

System operations are also available from the **Manage > Systems** tab.

See [“Systems tab operations”](#) on page 142.

[Table 7-7](#) describes the system commands that are accessible from the Workload view.

Table 7-7 System commands accessible from the Workload view

Command	Description
Pin System	Fixes a system in the Workload view. You can pin up to four systems. A pinned system is always visible in the Workload view. Pin a system that requires continuous monitoring, such as one that hosts critical service groups.
Zoom System	Displays the system's details in a zoom window. The zoom window is located in the right pane of the Workload section.
Unpin System	Releases a system that is currently pinned.
Freeze System	Freezes a system. You can freeze a system to prevent service groups from coming online on it. Diagonal lines identify a frozen system. See “Freezing a system” on page 300.
Unfreeze System	Unfreezes a currently frozen system. You may need to unfreeze a frozen system to enable service groups to come online on the system. See “Unfreezing a system” on page 302.
Stop System	Takes a system offline. An offline system is displayed in gray. This option is available only with the VCS One Simulator and not in real-time product deployment. See “Putting a system in the offline state” on page 309.
Start System	Starts an offline or a faulted system. This option is available only with the VCS One Simulator and not in real-time product deployment. See “Repairing a system using the Simulator” on page 306.
Simulate Daemon Dead	Simulates a system state in which the client daemon process stops functioning on the system, but the system itself is still up-and-running. This option is available only with the VCS One Simulator and not in real-time product deployment. See “Simulating a system in DDNA state” on page 309.
Simulate System Fault	Simulates a system fault. A faulted system is displayed with red lines around it. This option is available only with the VCS One Simulator and not in real-time product deployment. See “Faulting a system using the Simulator” on page 305.

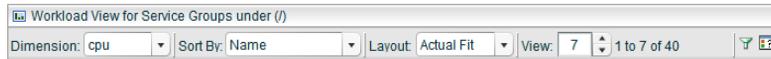
Table 7-7 System commands accessible from the Workload view

Command	Description
Edit Attributes	Edits the system attributes. See “Editing system attributes” on page 297.
Go to system details	Displays the detail system information.
Go to Map View	Displays the system’s object relationship in a graphical way. See “Summary information on the map view” on page 137.
Reset system filter	Resets the system filters.

Workload view options

You can use the Workload view options to configure the graphical view. [Figure 7-5](#) shows the various options found in the Workload view.

Figure 7-5 Workload view options



[Table 7-8](#) describes the Workload view options.

Table 7-8 Workload view options

Option	Description
The Dimension box	Click the arrow to change the load dimension that is displayed for all the systems. For example, if you want to view the memory consumption, change the load dimension to mem . The color changes for each load dimension.
The Sort By box	Click the arrow to arrange the systems in the order of their System Names, Total Load, Available Capacity, and Total Capacity. Systems are displayed from left to right with increasing values.
The Layout box	Click the arrow to toggle between the Best Fit, Actual Fit, and Uniform Fit views.
The View box	Enter the number of systems that you want to view. The default value is seven. You can expand the view by clicking the gray rectangle in the pane divider. Note that up to 32 systems can be viewed without using the slider.

Table 7-8 Workload view options

Option	Description
The Navigator tab	Click the tab to view a snapshot of all systems in the VCS One cluster. Systems that are currently displayed in the workload section are displayed in a shaded rectangle in the Navigator. Move the rectangle or the slider in the appropriate direction to select systems.
The Find tab	Use the Find tab to search for service groups and systems. See “Finding a system or a service group” on page 130.
The Filter Systems icon 	Click the icon to launch the Filter Systems dialog box. The dialog box enables you to select the systems that you want to display based on their name and their operating system. See “Filtering systems in the Workload view” on page 129.
The Legend icon 	Click the icon to view a legend that represents the colors and patterns that are used to depict various states and load capacity dimensions.

Filtering systems in the Workload view

In the Workload view, you can filter systems based on their name and their operating system.

To filter systems in the Workload view

- 1 Click the Filter Systems icon.
- 2 In the Filter Systems dialog box, perform the following steps:
 - a In the Select Platform box, select an operating system. All the systems that run the specified operating system are listed.
 - b Check the box that corresponds to each system that you want to view in the Workload section. Check **Select All** to select all the systems in the list.
- 3 Click **OK**.

Finding a system or a service group

In the Workload view, you can search for service groups and systems.

To find a system or a service group

- 1 Under Find, in the **Name** box, enter the name of the system or service group that you want to locate.
- 2 Check **Exact Match**, if you want to find the service group or system that exactly matches the search criteria.
- 3 Select either the **System** or the **Group** option to search for systems or service groups respectively.
- 4 Click **Find**.
 If the search is successful the respective system or service group is displayed with a dotted rectangle border.

Service Groups tab operations

The **Service Groups** tab located under the SGs and CSGs tab has various menus which are located in the right pane below the navigation bar. Each menu contains commands which you can use to perform service group operations.

[Table 7-9](#) describes the **Service Group** tab menus.

Table 7-9 Service Groups tab menus

Menu	Description
Operations	Contains commands to perform operations such as bringing a service group online or taking it offline, freezing or unfreezing a service group, and enabling or disabling a service group. See “Service group operations menu commands” on page 131.
Configuration	Contains commands to perform operations such as adding, modifying, and moving a service group. See “Service group configuration menu commands” on page 132.
Views	Contains commands to view the service groups in a variety of views such as the workload view or map view. See “Service group view menu commands” on page 134.
Simulation	Contains commands to perform simulation operations such as inducing a service group fault. See “Service group simulation menu commands” on page 138.

Summary information on the Service Groups tab default view

The **Service Groups** tab default view displays a tabular list of service groups for a selected OU node or set.

For each service group, the table contains the following information:

- The name of the service group.
- The current status of the service group.
- The priority value that is assigned to the service group.
- The load dimension values specified for the service group.
- The dependency details of the service group.
- The name of the OUValue to which the service group belongs.
- Other relevant service group information.
- The operating system of the system to which the service group belongs.

You can display additional information such as the fault policy and the date of creation by changing the table settings.

See [“To change the table settings”](#) on page 114.

Service group operations menu commands

In the right pane of the Service Groups view, the **Operations** menu has commands for managing service groups.

[Table 7-10](#) describes the service group **Operations** menu commands.

Table 7-10 Service group Operations menu commands

Command	Description
Online Anywhere/ Everywhere	Brings one or more service groups online on any or all available systems. See “Bringing a service group online” on page 329.
Offline Everywhere	Takes one or more service groups offline on all systems. See “Taking a service group offline” on page 333.
Clear Fault	Clears one or more faulted service groups. See “Clearing a service group fault” on page 344.
Freeze	Freezes one or more service groups. See “Freezing a service group” on page 339.

Table 7-10 Service group Operations menu commands

Command	Description
Unfreeze	Unfreezes one or more service groups. See “Unfreezing a service group” on page 340.
Enable All Resources	Enables all resources of one or more service groups. See “Enabling service group resources” on page 347.
Disable All Resources	Disables all resources of one or more service groups. See “Disabling service group resources” on page 348.
Refresh System List	Refreshes the system list of the selected service groups. Run this command whenever you modify the SystemListExpr attribute.
Online on system	Brings the selected service group online. See “Bringing a service group online” on page 329.
Offline on system	Takes the selected service group offline. See “Taking a service group offline” on page 333.
Enable	Enables the selected service group. See “Enabling a service group” on page 342.
Disable	Disables the selected service group. See “Disabling a service group” on page 342.
Switch	Switches a selected service group to a different system. See “Switching a service group” on page 336.
Probe All Resources	Probes all resources of the selected service group. See “Probing service group resources” on page 349.
Clear All Faults	Clears all faults of a service group. See “Clearing a service group fault” on page 344.

Service group configuration menu commands

In the right pane of the Service Groups section, the **Configuration** menu has commands for configuring service groups.

[Table 7-11](#) describes the service group **Configuration** menu commands.

Table 7-11 Service group Configuration menu commands

Command	Description
Move Service Group(s)	Moves one or more service groups to another node in the organization tree. See “Moving a service group to another organization tree node” on page 327.
Delete Service Group(s)	Deletes one or more service groups. See “Deleting a service group” on page 326.
Edit Attribute(s)	Edits the attributes of the selected service groups. Use this command to edit common attributes of multiple service groups in a single batch operation. See “Editing service group attributes” on page 324.
Edit Extended Attribute(s)	Edits the extended attributes of the selected service groups. Use this command to edit common extended attributes of multiple service groups in a single batch operation. See “Assigning an extended attribute a value” on page 519.
Edit Fault Policy	Configures the fault policy for the selected service group. See “Configuring a service group’s fault policy” on page 356.
Edit SystemList	Changes the system list of the selected service group. See “Configuring a service group’s SystemList with a list of systems” on page 353.
Modify Service Group	Changes the resource values of the selected service group using the Service Group Configuration Wizard. See “Modifying a service group” on page 327.
Clone Service Group	Clones the selected service group. See “Cloning service groups” on page 350.
Add/Modify Resource	Adds or changes resources of the selected service group. See “Adding a resource to a service group” on page 380.
Edit Compatibility	Specifies the compatible or incompatible service groups for the selected service group. See “Configuring a service group’s compatibility list” on page 355.

Table 7-11 Service group Configuration menu commands

Command	Description
Add Service Group	Adds a service group using the Service Group Configuration Wizard. See “Adding a service group” on page 315.
Create Group Dependency	Defines the dependencies among service groups. See “Linking service groups” on page 345.
Remove Group Dependency	Removes the dependencies among service groups. See “Unlinking service groups” on page 346.

Service group view menu commands

In the right pane of the Service Group view, the **Views** menu has commands for managing service group views.

[Table 7-12](#) describes the service group **Views** menu commands.

Table 7-12 Service group Views menu commands

Command	Description
Resource Dependencies	Displays the resource dependencies for a selected service group in a separate window. See “Summary information on the dependency view” on page 135.
Group Dependencies	Displays the service group dependencies for a selected service group in a separate window. See “Summary information on the dependency view” on page 135.
Workload	Displays the workload view for a selected service group. See “About the Service Group Workload view” on page 122.
Map View	Displays the object relationship of a service group in a graphical way. See “Summary information on the map view” on page 137.
All Attributes	Displays all attributes of the selected service group in a separate window.
GTQ View	Displays the Group Transition Queue in a separate window. See “About the GTQ view” on page 124.

Summary information on the dependency view

The dependency view is a graphical representation of a service group's dependency with other service groups as well as the dependency of the resources for a selected service group.

The VCS One console provides two types of dependency views:

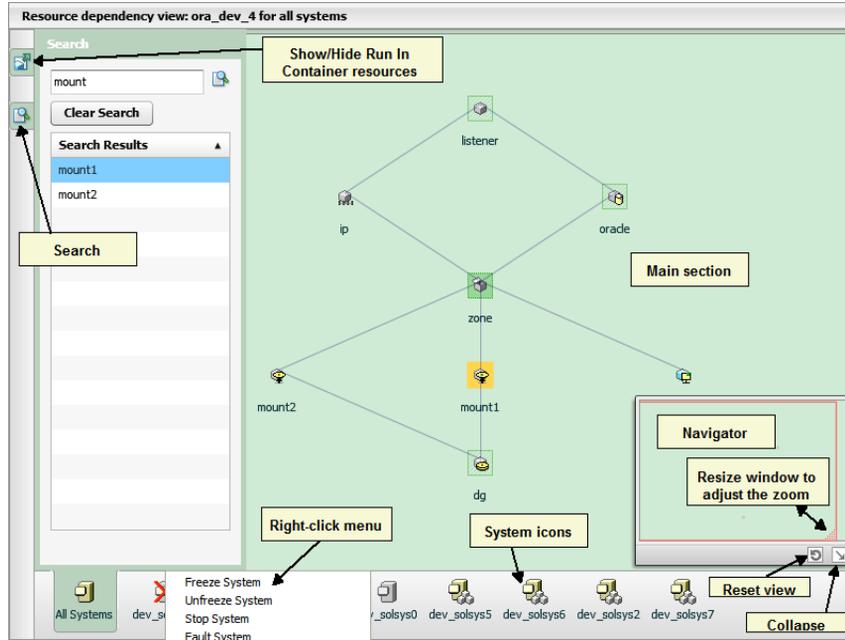
- **Group dependency view**
Displays the dependency of the selected service group with other service groups.
See [“About service groups and service group dependencies”](#) on page 38.
- **Resource dependency view**
Displays the dependency of resources for a selected service group.
See [“About resources and resource dependencies”](#) on page 37.

The dependency view window area contains the following elements:

- **Main section**
See [“About the main section of the dependency view”](#) on page 136.
- **Search and other icons**
See [“About the icons in the dependency view”](#) on page 136.
- **System icons**
See [“About the system icons in the dependency view”](#) on page 137.
- **Navigator**
See [“About the Navigator”](#) on page 137.

[Figure 7-6](#) illustrates the resource dependency view.

Figure 7-6 Resource dependency view



About the main section of the dependency view

The main section of the dependency view is located in the center of the dependency view window. To pan or move the view in any direction, click and drag the mouse in the desired direction. You can also move the view by using the Navigator.

See [“About the Navigator”](#) on page 137.

About the icons in the dependency view

The dependency view contains the following icons in the left side of the window:

Search



Enables you to search for a service group or resource.

Click the icon to open the search panel. Enter the search string in the text box and click the **Search** icon. The results display in the Search Results pane. Click the object name in the Search Results pane to locate it in the dependency view. The selected object is highlighted in the dependency view with a yellow rectangle.

Show/Hide Run In Container resources Shows or hides the run-in container resources.

This icon is available only in the resource dependency view. The container resource icons are marked with a shaded green rectangle in the dependency view.



About the system icons in the dependency view

The bottom area of the resource dependency view contains icons representing the systems present in the system list of the selected service group. The icon indicates the current state of each system. You can right-click on any icon to perform operations related to that system.

About the Navigator

You can use the Navigator to pan or zoom the dependency view. The Navigator is located in the lower right corner of the **Dependency View** window. The Navigator itself cannot be resized, though it can be collapsed.

The Navigator contains a window with a red border which can be resized or moved around. You can use the window to pan the dependency view or to zoom in or out of the dependency view.

The Navigator also has two icons located on the lower right side of the Navigator window. Click the round arrow to reset the dependency view to its original size. Click the diagonal arrow to collapse the Navigator.

To pan (or move around) in the dependency view

- ◆ Click and hold anywhere in the red window, then move the window while still holding the mouse button.

To zoom in or zoom out of the dependency view

- ◆ Click and hold the lower right corner of the red window, then move the mouse in the desired direction to stretch the window. To zoom in, make the window smaller. To zoom out, make the window bigger.

The window can be stretched in any direction. You might have to move the window around to stretch it in a better way.

Summary information on the map view

The map view is a graphical representation of an object's relationship with other objects. These objects can be service groups or systems. The object connection is represented by lines of various colors. The colors indicate the status of the main object with respect to the connected object. For example, in the case of a service group, a red line indicates that the service group is faulted on the connected system, a blue line indicates that the service group is online on the connected

system, and a gray line indicates that the service group is offline on the connected system.

The map view contains five icons which are located on the left side of the map view page. The first four icons provide access to panels. The panels provide access to additional information and map view settings. Click an icon to hide or display the respective panel.

[Table 7-13](#) describes the map view icons.

Table 7-13 Map view icons

Icon	Description
	<p>Details panel</p> <p>This panel displays information about the service group and status of the service group on various systems.</p>
	<p>Filters panel</p> <p>The filter panel has options for controlling the types of groups displayed. Use the Expand All option to expand all the objects that are displayed in the map.</p>
	<p>Settings panel</p> <p>The Settings panel has options to control the information that is displayed in the map. The panel also contains a slider bar which you can use to adjust the space between the map objects. Adjust the object spacing if the map view appears cluttered because of too many objects.</p>
	<p>Legend</p> <p>The legend panel depicts the icons that are used to represent objects in the map view. In the Legend panel, you can click the arrow icon next to the object icon to display the legend for that object.</p>
	<p>Pause Graph</p> <p>You can click this icon to pause the movement of the graph.</p>

Service group simulation menu commands

Simulation operations are available only in the VCS One Simulator and not in real-time product deployment. In the right pane of the Service Groups section, the **Simulation** menu contains the **Fault Service Groups** command. This command enables you to simulate a fault in one or more service groups.

More information is available about how to induce a service group fault.

See [“Faulting a service group in the Simulator”](#) on page 343.

Composite Service Groups tab operations

The **Composite Service Groups** tab, which is located under the **SGs and CSGs** tab, has various menus which are located in the right pane below the navigation bar. Each menu contains commands which you can use to perform composite service group operations.

[Table 7-14](#) describes the **Composite Service Group** tab menus.

Table 7-14 Composite Service Groups tab menus

Menu	Description
Operations	Contains commands to perform operations such as bringing a composite service group online or taking it offline, flushing a composite service group, and switching a composite service group. See “Composite service group operations menu commands” on page 140.
Configuration	Contains commands to perform operations such as adding, modifying, and moving a composite service group. See “Composite service group configuration menu commands” on page 140.
Views	Contains the command to view all attributes of the composite service group. See “Composite service group view menu commands” on page 141.

Summary information on the Composite Service Groups tab default view

The **Composite Service Groups** tab default view displays a tabular list of composite service groups for a selected OU node or set.

For each composite service group, the table contains the following information:

- The name of the composite service group. The name can be expanded to see the list of the service groups that make up the composite service group. You can perform operations on the service groups by selecting them inline, then right-clicking to select the appropriate command.
- The current status of the composite service group.
- The OU to which the composite service group belongs.
- The information about whether the composite service group needs attention.
- The status of the composite service group on the remote cluster.

- The authority of the composite service group.
 You can control the display of the columns by changing the table settings.
 See [“To change the table settings”](#) on page 114.

Composite service group operations menu commands

In the right pane of the Composite Service Groups view, the **Operations** menu has commands for managing composite service groups.

[Table 7-15](#) describes the composite service group **Operations** menu commands.

Table 7-15 Composite service group Operations menu commands

Command	Description
Online CSG(s)	Brings the selected composite service group online. See “Bringing a composite service group online” on page 373.
Offline CSG(s)	Takes the selected composite service group offline. See “Taking a composite service group offline” on page 374.
Flush CSG(s)	Cancel the online or offline operation that is currently being performed on the composite service group. See “Flushing a pending action on a composite service group” on page 375.
Request Authority	Requests authority for a global composite service group. See “Requesting authority for a global CSG” on page 499.
Switch	Brings a global composite service group online on another system in a different VCS One cluster site. See “Switching a global CSG” on page 502.

Composite service group configuration menu commands

In the right pane of the Composite Service Groups section, the **Configuration** menu has commands for configuring composite service groups.

[Table 7-16](#) describes the composite service group **Configuration** menu commands.

Table 7-16 Composite service group Configuration menu commands

Command	Description
Move CSG(s)	Moves one or more composite service groups to another node in the organization tree. See “Moving a local composite service group in the organization tree” on page 372.
Delete CSG(s)	Deletes one or more composite service groups. See “Deleting a composite service group” on page 371.
Configure Global CSG	Changes the VCS One cluster list of the selected composite service group. The VCS One cluster list determines whether the composite service group is local or global. See “Configuring a global CSG” on page 498.
Edit GroupList	Changes the group list of the selected composite service group. See “Modifying the group list of the CSG” on page 369.
Add CSG	Adds a composite service group using the Composite Service Group Configuration wizard. See “Creating a composite service group” on page 364.

Composite service group view menu commands

In the right pane of the Composite Service Group view, the **Views** menu has commands for managing composite service group views.

[Table 7-17](#) describes the composite service group **Views** menu commands.

Table 7-17 Composite service group Views menu commands

Command	Description
All Attributes	Displays all attributes of the selected composite service group. See “Editing a composite service group’s attributes” on page 371.

Systems tab operations

The **Systems** tab has various menus which are located in the right pane below the navigation bar. Each menu contains commands which you can use to perform system operations.

[Table 7-18](#) describes the **Systems** tab menus.

Table 7-18 Systems tab menus

Menu	Description
Operations	Contains commands to perform operations such as freezing or unfreezing a system, and stopping the system. See “System operations menu commands” on page 143.
Configuration	Contains commands to perform operations such as moving and deleting a system. See “Systems configuration menu commands” on page 143.
Views	Contains commands to view the service groups in a map view. See “Systems view menu commands” on page 144.
Simulation	Contains commands to perform simulation operations such as inducing a system fault. See “Systems simulation menu commands” on page 144.

Summary information on the Systems tab default view

The **Systems** tab default view displays the list of systems for a selected OU node or set in a table form.

For each system, the table contains the following information:

- The name of the system.
- The current status of the system.
- The capacity dimension values specified for the system.
- The platform that the system runs.
- The name of the virtual machine on which the system is configured.
- The name of the OUValue to which the system belongs.
- Other relevant system information. This information includes special conditions, such as whether a system is in the FROZEN state or DDNA state.

You can display additional information such as the date of creation and IP address by changing the table settings.

See [“To change the table settings”](#) on page 114.

System operations menu commands

In the right pane of the Systems view, the **Operations** menu has commands for managing systems.

[Table 7-19](#) describes the system **Operation** menu commands.

Table 7-19 System Operations menu commands

Command	Description
Freeze	Freezes one or more systems. See “Freezing a system” on page 300.
Unfreeze	Unfreezes one or more systems. See “Unfreezing a system” on page 302.
Stop System(s)	Stops the selected systems. See “Putting a system in the offline state” on page 309.
Fault System	Faults the selected system. See “Faulting a system” on page 305.

Systems configuration menu commands

In the right pane of the Systems view, the **Configuration** menu has commands for configuring systems.

[Table 7-20](#) describes the system **Configuration** menu commands.

Table 7-20 System Configuration menu commands

Command	Description
Move System(s)	Moves one or more systems to another node in the organization tree. See “Moving a system to another organization tree node” on page 306.
Delete System(s)	Deletes one or more systems. See “Deleting a system from the VCS One cluster” on page 298.
Edit Attributes	Edits the system attributes. Use this command to edit common attributes of multiple systems in a single batch operation. See “Editing system attributes” on page 297.

Table 7-20 System Configuration menu commands

Command	Description
Edit Extended Attribute(s)	Edits the extended attributes of the selected systems. Use this command to edit common extended attributes of multiple systems in a single batch operation. See “Assigning an extended attribute a value” on page 519.
Add System	Adds a system to the VCS One cluster. See “Adding a system to the VCS One cluster” on page 292.

Systems view menu commands

In the right pane of the Systems view, the **Views** menu has commands for managing system views.

[Table 7-21](#) describes the system **Views** menu commands.

Table 7-21 System Views menu commands

Command	Description
Map View	Displays the object relationship of a system in a graphical way. See “Summary information on the map view” on page 137.
All Attributes	Displays all attributes of the selected system in a separate window.

Systems simulation menu commands

Simulation operations are available only in the VCS One Simulator and not in real-time product deployment. In the right pane of the Systems view, the **Simulation** menu has commands for simulating system operations.

[Table 7-22](#) describes the system **Simulation** menu commands.

Table 7-22 Systems Simulation menu commands

Command	Description
Simulate System Fault	Simulates a system fault. See “Faulting a system using the Simulator” on page 305.
Simulate Daemon Dead	Simulates a daemon dead node alive (DDNA) situation. See “Simulating a system in DDNA state” on page 309.

Table 7-22 Systems Simulation menu commands

Command	Description
Start Systems	Starts a faulted system. See “Repairing a system using the Simulator” on page 306.

Resources tab operations

The **Resources** tab has various menus which are located in the right pane below the navigation bar. Each menu contains commands which you can use to perform resource operations.

[Table 7-23](#) describes the **Resources** tab menus.

Table 7-23 Resources tab menus

Menu	Description
Operations	Contains commands to perform operations such as enabling or disabling a resource, bringing the resource online or offline, and clearing a resource fault. See “Resource operations menu commands” on page 146.
Configuration	Contains the command for removing a resource. See “Systems configuration menu commands” on page 143.
Views	Contains commands to view the resource types and all attributes of a selected resource. See “Systems view menu commands” on page 144.
Simulation	Contains commands to perform simulation operations such as inducing a resource fault and clearing a simulated fault and bringing the resource online. See “Systems simulation menu commands” on page 144.

Summary information on the Resources tab default view

The **Resources** tab default view displays the list of resources for a selected OU node or set in a table form. The list of displayed resources also depends on your privileges.

For each resource, the table contains the following information:

- The name of the resource.
- The current state of the resource.
- The resource type.

- The name of the service group to which the resource belongs.
- The date when the resource state was last updated.

You can display additional information such as the date of creation by changing the table settings.

See [“To change the table settings”](#) on page 114.

Resource operations menu commands

In the right pane of the Resources view, the **Operations** menu has commands for managing resources.

[Table 7-24](#) describes the resource **Operations** menu commands.

Table 7-24 Resource Operations menu commands

Command	Description
Enable Resources	Enables a resource. See “Enabling resources in a service group” on page 383.
Disable Resources	Disables a resource. See “Disabling resources in a service group” on page 384.
Online	Brings the selected resource online. See “Bringing a resource online” on page 384.
Offline	Takes the selected resource offline. See “Taking a resource offline” on page 385.
Offline Propagate	Takes the selected resource and all its children offline. See “Taking parent and child resources offline concurrently” on page 386.
Probe	Probes the selected resource. See “Probing a resource” on page 386.
Clear Fault	Clears the resource fault. See “Clearing a resource fault” on page 388.
Clear Admin Wait	Clears a resource having the ADMIN_WAIT state. See “Clearing resources in the ADMIN_WAIT state” on page 389.

Resources configuration menu commands

In the right pane of the Resources view, the **Configuration** menu has commands for configuring resources.

[Table 7-25](#) describes the resource **Configuration** menu command.

Table 7-25 Resource Configuration menu command

Command	Description
Delete Resource	Removes the selected resource. See “Deleting a resource from a service group” on page 381.

Resources view menu commands

In the right pane of the Resources view, the **Views** menu has commands for viewing resource types and resource attributes.

[Table 7-26](#) describes the resource **Views** menu command.

Table 7-26 Resource Views menu command

Command	Description
Resource Types	View the resource types available in the configuration and related detailed information. See “Viewing resources in the configuration by resource type” on page 392.
All Attributes	Displays all attributes of the selected resource in a separate window. You can edit the attributes from this window. See “Editing resource attributes” on page 381.

Resources simulation menu commands

Simulation operations are available only in the VCS One Simulator and not in real-time product deployment. In the right pane of the Resources view, the **Simulation** menu has commands for simulating resource operations.

[Table 7-27](#) describes the resource **Simulation** menu commands.

Table 7-27 Resources Simulation menu commands

Command	Description
Fault Resource	Simulates a resource fault. See “Faulting a resource using the Simulator” on page 387.
Clear Fault and Online	Repairs a faulted resource and brings it online. See “Repairing a resource using the Simulator” on page 388.

Disaster Recovery tab operations

The **Disaster Recovery** tab has various menus which are located in the right pane below the navigation bar. Each menu contains commands which you can use to perform disaster recovery operations.

[Table 7-28](#) describes the **Disaster Recovery** tab menus.

Table 7-28 Disaster Recovery tab menus

Menu	Description
Operations	Contains commands to perform operations such as enabling or disabling a connection, taking over a composite service group, bringing a CSG online, taking a CSG offline, and requesting authority. See “Disaster Recovery operations menu commands” on page 149.
Configuration	Contains commands for adding a remote cluster, modifying a remote cluster, removing a remote cluster, and configuring global CSGs. See “Disaster Recovery configuration menu commands” on page 150.
Views	Contains the command to view all attributes of a selected resource. See “Disaster Recovery view menu command” on page 150.
Simulation	Contains commands to perform simulation operations such as inducing a fault in the remote cluster, faulting one or more links, and clearing one or more simulated link faults. See “Disaster Recovery simulation menu commands” on page 151.

Summary information on the Disaster Recovery tab default view

The **Disaster Recovery** tab default view displays the list of remote clusters in a table form. The list of displayed remote clusters also depends on your privileges.

For each remote cluster, the table contains the following information:

- The name of the remote cluster.
- The state of the remote cluster.
- Whether the remote cluster is enabled or not.
- The connection details of the remote cluster.
- The link status of the remote cluster.
- The port of the remote cluster.

You can choose which columns display by changing the table settings.

See [“To change the table settings”](#) on page 114.

Disaster Recovery operations menu commands

In the Disaster Recovery view, the **Operations** menu has commands for managing connections and composite service groups.

[Table 7-29](#) describes the disaster recovery **Operations** menu commands.

Table 7-29 Disaster Recovery Operations menu commands

Command	Description
Enable Connection(s)	Enables connections between VCS One clusters. See “Enabling connections between clusters” on page 485.
Disable Connection(s)	Disables connections between VCS One clusters. See “Disabling connections between clusters” on page 485.
Take Over CSG(s)	Takes over a global composite service group. A takeover operation brings the global CSG online on the local VCS One cluster. See “Taking over a global CSG” on page 503.
Online CSG(s)	Brings the selected global CSGs online. See “Bringing a global CSG online” on page 500.
Offline CSG(s)	Takes the selected global CSGs offline. See “Taking a composite service group offline” on page 374.

Table 7-29 Disaster Recovery Operations menu commands

Command	Description
Request Authority	Requests authority for a global CSG. See “Requesting authority for a global CSG” on page 499.

Disaster Recovery configuration menu commands

In the Disaster Recovery view, the **Configuration** menu has commands for configuring remote VCS One clusters.

[Table 7-30](#) describes the disaster recovery **Configuration** menu command.

Table 7-30 Disaster Recovery Configuration menu command

Command	Description
Add Remote Cluster	Adds a remote VCS One cluster. See “Adding remote clusters” on page 478.
Modify Remote Cluster	Modifies a remote VCS One cluster. See “Modifying remote cluster configuration” on page 488.
Delete Remote Cluster(s)	Deletes one or more remote VCS One clusters. See “Deleting remote clusters” on page 484.
Configure Global CSG	Configures a global CSG. See “Configuring a global CSG” on page 498.

Disaster Recovery view menu command

In the Disaster Recovery view, the **Views** menu has the command for viewing remote cluster attributes.

[Table 7-31](#) describes the disaster recovery **Views** menu command.

Table 7-31 Disaster Recovery Views menu command

Command	Description
All Attributes	Displays all attributes of the selected resource in a separate window. You can edit the attributes from this window. See “Editing resource attributes” on page 381.

Disaster Recovery simulation menu commands

Simulation operations are available only in the VCS One Simulator and not in real-time product deployment. In the Disaster Recovery view, the **Simulation** menu has commands for simulating remote VCS One cluster operations.

[Table 7-32](#) describes the disaster recovery **Simulation** menu commands.

Table 7-32 Disaster Recovery Simulation menu commands

Command	Description
Fault Remote Cluster(s)	Simulates a fault in the remote VCS One cluster. See “Faulting a remote cluster using the Simulator” on page 492.
Fault Link(s)	Simulates a link fault. See “Simulating a link fault” on page 493.
Clear Link Fault(s)	Clears a link fault. See “Clearing a simulated link fault” on page 494.

Jobs tab operations

The **Jobs** tab located under the **Automation** tab has various menus which are located in the right pane below the navigation bar. Each menu contains commands which you can use to perform job operations.

[Table 7-33](#) describes the **Jobs** tab menus.

Table 7-33 Jobs tab menus

Menu	Description
Operations	Contains commands to perform operations such as exporting or importing a job. See “Job operations menu commands” on page 152.
Configuration	Contains commands to perform operations such as adding and deleting a job. See “Job configuration menu commands” on page 153.
Views	Contains commands to view event types that are associated with a job. See “Job view menu commands” on page 153.

Summary information on the Jobs tab default view

The **Jobs** tab default view displays the list of jobs for a selected OU node. The list of displayed jobs also depends on your privileges.

For each job, the table contains the following information:

- The name of the job.
- The rules count.
- The OU value to which the job belongs.
- The name of the user who created the job.
- The job description.

You can hide or show columns by changing the table settings.

See [“To change the table settings”](#) on page 114.

The complete information for a particular job can be viewed by clicking the job name on the jobs listing page. From the job details page, you can perform operations such as running the job, modifying the job, cloning the job, and deleting the job.

More information is available about how to perform job operations.

See [“Managing automated tasks”](#) on page 409.

Job operations menu commands

In the right pane of the Jobs view, the job **Operations** menu has commands for managing jobs.

[Table 7-34](#) describes the job **Operations** menu commands.

Table 7-34 Job Operations menu commands

Command	Description
Export Job(s)	Exports one or more jobs. See “Exporting a rule or a job to an XML file” on page 428.
Run Job	Runs a job. See “Running a job” on page 424.
Import Job	Imports an existing job. See “Importing a rule or a job from an XML file” on page 429.

Job configuration menu commands

In the right pane of the Jobs view, the job **Configuration** menu has commands for configuring jobs.

[Table 7-35](#) describes the job **Configuration** menu commands.

Table 7-35 Job Configuration menu commands

Command	Description
Delete Job(s)	Deletes one or more jobs. See “Deleting a job” on page 424.
Modify Job	Modifies the selected job. See “Modifying a job” on page 423.
Clone Job	Creates one or more copies of the selected job. See “Cloning a job” on page 423.
Add Job	Adds a new job. See “Creating a job” on page 421.

Job view menu commands

The job **Views** menu contains the following command:

- Event Types
Displays the event types that are associated with a job.

Business Rules tab and Notification Rules tab operations

The **Business Rules** tab and the **Notification Rules** tab are located under the **Automation** tab. Both tabs have various menus which are located in the right pane below the navigation bar. Each menu contains commands which you can use to perform rule operations. Although rules are classified under the business and notification categories, most of the commands and wizards are common to both types of rules.

[Table 7-36](#) describes the Business Rules tab and the Notification Rules tab menus.

Table 7-36 Business Rules tab and Notification Rules tab menus

Menu	Description
Operations	Contains commands to perform operations such as enabling or disabling a rule. See “Rule operations menu commands” on page 154.
Configuration	Contains commands to perform operations such as adding and deleting a rule. See “Rule configuration menu commands” on page 155.
Views	Contains commands to view event types that are associated with a rule. See “Rule view menu commands” on page 156.

Summary information on the Business Rules tab and Notification Rules tab default view

Based on the organization tree node that is selected in the left pane, the relevant information is displayed for all the rules that are defined for that node. You can display additional information by changing the table settings.

See [“To change the table settings”](#) on page 114.

The complete information for a particular rule can be viewed by clicking the rule name on the rules listing page. From the rule details page, you can perform operations such as modifying the rule, cloning the rule, and deleting the rule.

More information is available about how to perform rule operations.

See [“Managing automated tasks”](#) on page 409.

Rule operations menu commands

In the right pane of the Business Rules and Notification Rules view, the rule **Operations** menu has commands for managing rules.

[Table 7-37](#) describes the rule **Operations** menu commands.

Table 7-37 Rule Operations menu commands

Command	Description
Enable Rule(s)	Enables one or more rules. See “Enabling a rule” on page 425.

Table 7-37 Rule Operations menu commands

Command	Description
Disable Rule(s)	Disables one or more rules. See “Disabling a rule” on page 426.
Export Rule(s)	Exports one or more rules. See “Exporting a rule or a job to an XML file” on page 428.
Take Rule Ownership	Changes rule ownership. See “Changing the owner of a rule” on page 425.
Import Rule	Imports an existing rule. See “Importing a rule or a job from an XML file” on page 429.

Rule configuration menu commands

In the right pane of the Business Rules and Notification Rules view, the rule **Configuration** menu has commands for configuring rules.

[Table 7-38](#) describes the rule **Configuration** menu commands.

Table 7-38 Rule Configuration menu commands

Command	Description
Delete Rule(s)	Deletes one or more rules. See “Deleting a rule” on page 428.
Modify Rule	Modifies the selected rule. See “Modifying a rule” on page 427.
Add/Modify Conditions	Adds or modifies conditions for the selected business rule. See “Adding or modifying conditions and filters for the rule” on page 417.
Clone Rule	Creates one or more copies of the selected rule. See “Cloning a rule” on page 420.
Add Rule	Adds a new rule. See “Creating a business rule” on page 411.

Rule view menu commands

The Business Rules and Notification Rules **Views** menu contains the following command:

- **Event Types**
 Displays the event types that are associated with a rule.

Logs tab options

The **Logs** tab provides access to various types of VCS One log messages. The log messages, time-stamped and labeled by severity, are displayed in the right pane.

[Table 7-39](#) describes the second-level tabs under the **Logs** tab.

Table 7-39 Second-level tabs under the Logs tab

Tab	Description
Policy Master Logs	Contain messages that are generated on the Policy Master by the Policy Master daemon, VCS One console, and VCS One commands.
Command Logs	Contain messages that are generated by running commands from the VCS One console.
Event Logs	These logs are associated with Business Policy Automation (BPA) and contain messages that are related to events.
Rule Execution Logs	These logs are associated with Business Policy Automation (BPA) and contain messages that are related to business rules and notification rules. The default view displays business rule log messages. To view notification rule log messages, click the Show drop-down arrow, and select the rule type.

About log message filters

You can use various types of filters to filter the log messages. The log message filters are available in the left pane. You can use either a single filter or a combination of multiple filters. The filters vary according to the log message type.

You can view the following types of filters from the VCS One console:

- [Policy Master log message filters](#)
- [Event log message filters](#)
- [Rule execution log message filters](#)

About Policy Master log message filters

You can view specific Policy Master log messages using the following filters:

- **Severity**
The severity filter uses the severity level which includes critical, error, warning, notice, and information.
See [“Viewing log messages based on severity”](#) on page 157.
- **Time**
The time filter uses a period which includes the date and time.
See [“Viewing log messages based on time”](#) on page 157.
- **Data**
The data filter uses a text filter or an object filter which filters messages using various object types such as systems, service groups, resources, users, composite service groups, and remote VCS One clusters. You can also choose to sort the results by relevance to the filter. You also have the option of filtering the messages using either all the filter keywords or at least one of the keywords.
See [“Viewing log messages based on data”](#) on page 158.

Viewing log messages based on severity

To view log messages based on severity

- 1 In the left pane, under **Severity Filter**, do one of the following:
 - Click **All** to view log messages for all severities.
 - Click **None** to clear all the currently selected log message severities. If you select this option, go to step 3.
 - Check the box that corresponds to the log message severity level that you want to view. Severity levels include Critical, Error, Warning, Notice, and Information.
- 2 If required, under **Time Based Filter** and **Data Based Filter**, enter the relevant search criteria.
- 3 Click **Apply**.
All log entries for the specified severity and time are displayed.

Viewing log messages based on time

To view log messages based on time

- 1 In the left pane, under **Time Based Filter**, enter the start and the end date and time.
- 2 Click **Apply**.

All log entries for the specified time period are displayed.

Viewing log messages based on data

To view log messages based on data

- 1 In the left pane, under **Data Based Filter**, select either the **Text Filter** or **Object Filter** option.
- 2 If you select **Text Filter**, enter the text string to be used as the filter.
- 3 If you select **Object Filter**, enter the relevant information against each of the object type boxes.
- 4 Click **Apply**.
All log entries that match the specified data are displayed.

About event log message filters

You can view specific event log messages using the following filters:

- **Event category**
The category filter uses the event source which includes events generated by the Policy Master and the scheduler, and manual events.
See [“Viewing log messages based on event category”](#) on page 158.
- **Event status**
The status filter uses the event status which includes missed, in-process, and processed events.
See [“Viewing log messages based on event status”](#) on page 159.
- **Event severity**
The severity filter uses the message type which includes critical, error, warning, and information.
See [“Viewing log messages based on severity”](#) on page 159.
- **Time**
The time filter uses a period which includes the date and time.
See [“Viewing log messages based on time”](#) on page 160.
- **Data**
The data filter uses objects and event names to filters messages.
See [“Viewing log messages based on data”](#) on page 160.

Viewing log messages based on event category

To view log messages based on event category

- 1 In the left pane, under **Event Category**, do one of the following:

- Click **All**, to view log messages for all event categories.
 - Click **None**, to clear all the currently selected log message event categories. If you select this option, go to step 3.
 - Check the box that corresponds to the log message event category that you want to view. Category types include PM, Scheduler, and Manual.
- 2 If required, under **Event Category, Event Severity, Time Based Filter**, and **Data Based Filter**, enter the relevant search criteria.
 - 3 Click **Apply**.
All log entries for the specified filter information are displayed.

Viewing log messages based on event status

To view log messages based on event status

- 1 In the left pane, under **Event Status**, do one of the following:
 - Click **All**, to view log messages for all event status types.
 - Click **None**, to clear all the currently selected log message event status types. If you select this option, go to step 3.
 - Check the box that corresponds to the log message event status that you want to view. Status types include Missed, In Process, and Processed.
- 2 If required, under **Event Category, Event Severity, Time Based Filter**, and **Data Based Filter**, enter the relevant search criteria.
- 3 Click **Apply**.
All log entries for the specified filter information are displayed.

Viewing log messages based on severity

To view log messages based on severity

- 1 In the left pane, under **Event Severity**, do one of the following:
 - Click **All**, to view log messages for all severities.
 - Click **None**, to clear all the currently selected log message severities. If you select this option, go to step 3.
 - Check the box that corresponds to the log message severity level that you want to view. Severity levels include Critical, Error, Warning, Notice, and Information.
- 2 If required, under **Event Category, Event Status, Event Severity**, and **Data Based Filter**, enter the relevant search criteria.
- 3 Click **Apply**.

All log entries for the specified severity and time are displayed.

Viewing log messages based on time

To view log messages based on time

- 1 In the left pane, under **Time Based Filter**, enter the start and the end date and time.
- 2 Click **Apply**.
All log entries for the specified time period are displayed.

Viewing log messages based on data

To view log messages based on data

- 1 In the left pane, under **Data Based Filter**, select either the **Event name Filter** or **Object Filter** option.
- 2 If you select **Event name Filter**, enter the event name.
- 3 If you select **Object Filter**, enter the object name.
- 4 Click **Apply**.
All log entries that match the specified data are displayed.

About rule execution log message filters

You can view specific rule execution log messages using the following filters:

- **Status**
The status filter uses the event status which includes scheduled, successful, failed, running, and missed events.
See [“Viewing log messages based on status”](#) on page 160.
- **Time**
The time filter uses a period which includes the date and time.
See [“Viewing log messages based on time”](#) on page 161.
- **Data**
The data filter uses owners, objects, rules, and jobs to filters messages.
See [“Viewing log messages based on data”](#) on page 161.

Viewing log messages based on status

To view log messages based on status

- 1 In the left pane, under **Status Filter**, do one of the following:
 - Click **All**, to view log messages for all status types.

- Click **None**, to clear all the currently selected log message status types. If you select this option, go to step 3.
 - Check the box that corresponds to the log message status type that you want to view. Status types include Scheduled, Success, Failure, Running, and Missed Events.
- 2 If required, under **Time Based Filter** and **Data Based Filter**, enter the relevant search criteria.
 - 3 Click **Apply**.
All log entries for the specified filter information are displayed.

Viewing log messages based on time

To view log messages based on time

- 1 In the left pane, under **Time Based Filter**, enter the start and the end date and time.
- 2 Click **Apply**.
All log entries for the specified time period are displayed.

Viewing log messages based on data

To view log messages based on data

- 1 In the left pane, under **Data Based Filter**, enter the relevant information in the data text boxes.
- 2 Click **Apply**.
All log entries that match the specified data are displayed.

About log message deletion

You can delete command, rule, and job log messages to recover disk space or improve message retrieval performance. More information is available about deleting log messages.

See [“Deleting event and rule log entries”](#) on page 586.

See [“Deleting job log entries”](#) on page 586.

Administration tab options

All VCS One cluster users, roles, extended attributes, sets, and organization tree objects are configured and administered from the **Administration** tab. You can use the second-level tabs to perform various operations and tasks on these objects.

[Table 7-40](#) describes the second-level tabs under the **Administration** tab.

Table 7-40 Second-level tab under the Administration tab

Tab	Description
User	Provides access to the user-related menu commands. See “Users tab operations” on page 162.
Roles	Provides access to the roles-related menu commands. See “Roles tab operations” on page 164.
Organization Units	Provides access to the organization units-related menu commands. See “Organization Units tab operations” on page 165.
Extended Attributes	Provides access to the extended attributes-related menu commands. See “Extended Attributes tab operations” on page 166.
Sets	Provides access to the sets-related menu commands. See “Sets tab operations” on page 168.
Settings	Provides access to the settings-related menu commands. See “Settings tab operations” on page 169.

Users tab operations

The **Users** tab has the **Configuration** menu which is located in the right pane below the navigation bar. The **Configuration** menu contains commands which you can use to perform user and user group operations such as adding, deleting, moving, and enabling or disabling users and user groups.

See [“Users and user groups configuration menu commands”](#) on page 163.

Summary information on the Users tab default view

The **Users** tab default view displays a tabular list of users and user groups for a selected OU node or set.

For each user or each user group, the table contains the following information:

- The name of the user or user group.
- The type of user. VCS One supports both users and user groups.
- The organization unit to which the user or the user group is attached.
- The first name and last name of the user.
- The date and time when the user last logged on to the console.
- The logon status of the user.
- The email address of the user or user group.
- The SNMP details of the user or user group.

How to locate specific users

You can use the organization tree to view users or user groups. To view all users and user groups that are attached to a specific Organization Tree node, navigate to that node.

You can click the **Show all users** link in the right pane to display all the VCS One users. This display also includes the users that VCS One uses internally.

Users and user groups configuration menu commands

In the right pane of the Users view, the **Configuration** menu has commands for configuring users and user groups.

[Table 7-41](#) describes the user and the user group **Configuration** menu commands.

Table 7-41 User and user group Configuration menu commands

Command	Description
Delete Users/User Groups	Deletes one or more users or user groups. See “Deleting a user or usergroup” on page 532.
Disable Users/User Groups	Disables currently enabled users or user groups. See “Disabling a user or usergroup” on page 540.
Enable Users/User Groups	Enables currently disabled users or user groups. See “Enabling a user or usergroup” on page 539.

Table 7-41 User and user group Configuration menu commands

Command	Description
Move Users/User Groups	Moves one or more users or user groups to another node in the organization tree. See “Moving a user to another Organization Tree node:” on page 539.
Add Users/User Groups	Adds a user or a user group to an organization tree node. See “Adding a user or usergroup” on page 531.
Clone Users/User Groups	Clones a user or a user group to an organization tree node. See “Cloning a user or user group” on page 532.
Assign/Unassign Roles	Assigns or unassigns a role to one or more users or user groups. See “Assigning or unassigning a role and objects to a user or usergroup” on page 533.

Roles tab operations

The **Roles** tab has the **Configuration** menu which is located in the right pane below the navigation bar. The **Configuration** menu contains commands which you can use to perform role operations such as adding, deleting, and assigning or unassigning roles.

See [“Roles configuration menu commands”](#) on page 164.

Summary information on the Roles tab default view

The **Roles** tab default view displays a tabular list of predefined and user-defined roles for a selected OU node or set.

For each roles, the table contains the following information:

- The name of the role.
- The type of VCS One objects that can be assigned to the role.
- The description of the role.

Roles configuration menu commands

In the right pane of the Roles view, the **Configuration** menu has commands for configuring roles.

[Table 7-42](#) describes the role **Configuration** menu commands.

Table 7-42 Role Configuration menu commands

Command	Description
Delete Role	Deletes an existing role from the VCS One cluster. See “Deleting a role” on page 537.
Clone Role	Clones an existing role. See “Cloning a role” on page 536.
Add Role	Adds a new role to the VCS One cluster. See “Adding custom roles” on page 534.

Organization Units tab operations

The **Organization Units** tab has the **Configuration** menu which is located in the right pane below the navigation bar. The **Configuration** menu contains commands which you can use to perform organization unit operations such as adding and deleting OUName and OUValue.

See [“Organization units configuration menu commands”](#) on page 165.

How to locate organization units

In the left pane of the Organization Units section, you can use the organization tree to locate organization units. Select the organization tree, and then navigate to a specific organization tree node to view the organization units that are associated with it.

If you select an OUName node from the organization tree, the associated OUValues are displayed in the right pane, under OUValues applicable for this OUName. The fully qualified name is also displayed for each OUValue.

If you select an OUValue node from the organization tree, the associated OUNames are displayed in the right pane, under OUNames applicable for this OUValue. The fully qualified name is also displayed for each OUName.

Organization units configuration menu commands

In the right pane of the Organization Units view, the **Configuration** menu has commands for configuring organization units.

Table 7-43 describes the organization units **Configuration** menu commands.

Table 7-43 Organization units Configuration menu commands

Command	Description
Add OUName	Adds an organization unit name to the organization tree. See “How to build an organization tree” on page 508.
Delete OUName	Deletes an organization unit name from the organization tree. See “Deleting an OUName node from the organization tree” on page 512.
Add OUValue	Adds an organization unit value to the selected organization unit name node. See “How to build an organization tree” on page 508.
Delete OUValue	Deletes an organization unit value from the organization tree. See “Deleting OUValue nodes from the organization tree” on page 513.

Extended Attributes tab operations

The **Extended Attributes** tab has the **Configuration** menu which is located in the right pane below the navigation bar. The **Configuration** menu contains commands which you can use to perform extended attribute operations such as adding and deleting extended attributes.

See [“Extended attributes configuration menu commands”](#) on page 167.

Summary information on the Extended Attributes tab default view

The **Extended Attributes** tab default view displays a tabular list of all the VCS One cluster extended attributes for a selected OU node.

For each extended attribute, the table contains the following information:

- The name of the extended attribute.
- The extended attribute category. Categories include common, system, and group.
- The extended attribute type. Extended attributes can be of type enumerated or freeform.
- The valid values that can be applied to the extended attribute.

- The default value of the extended attribute. This value is assigned to the object if no other value is specified.
- The path of the organization tree node that is associated with the default value of the extended attribute.
- The description of the extended attribute.

How to view extended attributes

In the left pane of the Extended Attributes section, you can use the organization tree to locate extended attributes. In the organization tree, navigate to a specific OUValue node to view the extended attributes that are associated with it.

All the extended attributes are displayed in the right pane under the following:

- **Locally-defined Extended Attributes**
All the extended attributes that are defined specifically for the selected organization tree node are displayed under Locally-defined Extended Attributes. The name, category, type, valid values, default values, and description of the extended attribute is displayed.
- **Inherited Extended Attributes**
All the extended attributes that the selected organization tree node inherits from its preceding organization tree nodes are displayed under Inherited Extended Attributes. The name, category, type, valid values, default values, organization unit name where it is defined, and description of the extended attribute is displayed.

Extended attributes configuration menu commands

In the right pane of the Extended Attributes view, the **Configuration** menu has commands for configuring extended attributes.

[Table 7-44](#) describes the extended attributes **Configuration** menu commands.

Table 7-44 Extended attributes Configuration menu commands

Command	Description
Add Extended Attribute	Adds an extended attribute. See “Defining an extended attribute” on page 518.
Delete Extended Attribute(s)	Deletes one or more extended attribute. See “Deleting an extended attribute” on page 521.

Sets tab operations

The **Sets** tab has the **Configuration** menu which is located below the navigation bar. The **Configuration** menu is also available on the sets details page. The **Configuration** menu contains commands which you can use to perform set operations such as adding, deleting, and modifying sets, and adding a custom view.

See [“Sets list page configuration menu commands”](#) on page 168.

See [“Sets details page configuration menu commands”](#) on page 169.

Summary information on the Sets tab default view

The **Sets** tab default view displays a tabular list of sets. Each VCS One user has a default set called My Objects. This set comprises all the VCS One objects that the user has privileges to view. This set cannot be edited or deleted.

For each set, the table contains the following information:

- The name of the set.
- The description of the set.

You can also create custom views for each set from the default view or from the details page of a set. You can add, delete, or modify custom views from the details page.

Sets list page configuration menu commands

In the sets list page the **Configuration** menu has commands for adding, modifying, removing sets, and for adding a custom view.

[Table 7-45](#) describes the sets list page **Configuration** menu commands.

Table 7-45 Sets list page Configuration menu commands

Command	Description
Delete Set(s)	Deletes one or more sets. See “Deleting a set” on page 552.
Modify Set	Modifies the selected set. See “Modifying a set” on page 553.
Add Custom View	Adds a custom view. See “Configuring a custom view of the organization tree and extended attributes” on page 553.

Table 7-45 Sets list page Configuration menu commands

Command	Description
Add Set	Adds a set. See “Building a set” on page 550.

Sets details page configuration menu commands

Click the name of a set to view the sets details page.

In the sets details page the **Configuration** menu has commands for configuring and removing sets, and for adding and removing custom views.

[Table 7-46](#) describes the sets details page **Configuration** menu commands.

Table 7-46 Sets details page Configuration menu commands

Command	Description
Modify Set	Modifies the selected set. See “Modifying a set” on page 553.
Delete Set	Deletes the selected set. See “Deleting a set” on page 552.
Add Custom View	Adds a custom view. See “Configuring a custom view of the organization tree and extended attributes” on page 553.
Delete Custom View	Removes a custom view.

Settings tab operations

The **Settings** tab provides access to two types of VCS One settings – global settings and automation settings. The links for both these settings are located in the left pane.

The global settings are available in the form of individual attributes which you can edit.

See [“Editing VCS One cluster attributes”](#) on page 516.

The global settings page also has the **Configuration** menu which is located in the right pane below the navigation bar. The **Configuration** menu contains the commands which you can use to modify the precedence order and refresh the catalog files.

See [“Global settings configuration menu commands”](#) on page 170.

The automation settings include the SMTP settings, SNMP settings, syslog notifications, and the script settings. The automation settings page also has the **Operations** and **Configuration** menus which are located in the right pane below the navigation bar. The **Operations** menu contains commands which you can use to enable or disable notifications. The **Configuration** menu contains commands which you can use to edit and test the settings.

See “[Automation settings operations menu commands](#)” on page 171.

See “[Automation settings configuration menu commands](#)” on page 171.

Summary information on the Settings tab default view

The **Settings** tab default view depends on the privileges of the logged-in user. For users having privileges at the VCS One cluster level the default view displays a tabular list of all the attributes of the VCS One cluster. For other users who have lesser privileges the default view displays the automation settings.

For global settings, the table contains the following information:

- The name of the attribute.
- The value of the attribute.
- The indication about whether the attribute must be configured or not.

Values of attributes which are editable can be changed by clicking the icon in the Edit column.

Global settings configuration menu commands

In the right pane of the Global Settings view, the **Configuration** menu has commands for configuring the global settings.

[Table 7-47](#) describes the global settings **Configuration** menu commands.

Table 7-47 Global settings Configuration menu commands

Command	Description
Modify Precedence Order	Changes the precedence order of the existing load dimensions that are defined in the VCS One cluster. You can also add or delete new load dimensions, if required. See “ Defining the VCS One cluster’s load and capacity keys ” on page 404.
Refresh Catalog Files	Reloads the catalog files. The catalog files have the .bmc and .bmcmmap extensions and contain the attribute definitions. Use this command whenever the catalog files are updated or added; for example, after you install a new agent.

Automation settings operations menu commands

In the right pane of the Automation Settings view, the **Operations** menu has commands for enabling notifications and script execution.

[Table 7-48](#) describes the automation settings **Operations** menu commands.

Table 7-48 Automation settings Operations menu commands

Command	Description
Enable SMTP Notifications	Enables the SMTP notifications. See “Enabling notification settings” on page 525.
Enable SNMP Notifications	Enables the SNMP notifications. See “Enabling notification settings” on page 525.
Enable Syslog Notifications	Enables the syslog notifications. See “Enabling syslog notifications” on page 526.
Enable Script Execution	Enables the script execution. See “Enabling script execution” on page 527.

Automation settings configuration menu commands

In the right pane of the Automation Settings view, the **Configuration** menu has commands for editing and testing the settings.

[Table 7-49](#) describes the automation settings **Configuration** menu commands.

Table 7-49 Automation settings Configuration menu commands

Command	Description
Edit Settings	Changes SMTP and SNMP settings. See “Modifying notification settings” on page 523.
Test Settings	Tests the SMTP notification settings. See “Testing notification settings” on page 528.

Summary information on the Search tab

The **Search** tab enables you to search for any object in the VCS One cluster such as systems, service groups, composite service groups, and resources. The search functionality is useful to locate specific objects in a densely populated VCS One cluster.

To search for an object

- 1 Click the **Search** tab.
- 2 In the Search text box, enter the search string.
- 3 Click the **show options** link to change search options. You can search for an exact match, or search for all or at least one of the words that is specified in the search string.
- 4 Click **Search**.

The objects that match the search criteria display in the Results table.

The links that are located below the search options enable you to view the search results for specific categories such as cluster, groups, composite service groups, and so on. The links also show information about the number of hits for that particular object type. For example, to view the search results for all service groups, click the **Groups** link.

The search operation scans both attributes and their values. For example, if you specify "State = online" as the search criteria, a search is performed on the State attribute as well as its value ("online").

For composite service groups, in addition to the list of matching composite service groups for the given string, the service groups contained inside the composite service groups also display.

Note: If the **Search** tab is not displayed in the console, it is possible that the search functionality has been disabled by the VCS One administrator. See "[Webserversubsystems](#)" on page 691.

Using the Simulator

This chapter includes the following topics:

- [About the Simulator](#)
- [About the Simulator's start-up modes](#)
- [About multiple Simulator instances](#)
- [About Simulator scripts and commands](#)
- [Starting the default Simulator instance](#)
- [Adding a Simulator instance](#)
- [Starting a Simulator instance](#)
- [Loading or changing a configuration in the Simulator](#)
- [About logging on to the Simulator](#)
- [Accessing the GUI for a Simulator instance](#)
- [Accessing the command line for a Simulator instance](#)
- [Creating and saving a custom configuration in the Simulator](#)
- [Displaying the status of a Simulator instance](#)
- [Listing Simulator instances](#)
- [Listing port information for a Simulator instance](#)
- [Setting up a disaster recovery configuration in the Simulator](#)
- [Simulating disaster recovery operations using the Simulator](#)
- [Stopping a Simulator instance](#)
- [Removing a Simulator instance](#)

About the Simulator

The VCS One Simulator is available for Windows. You can install the VCS One Simulator on one or more Windows systems.

The Simulator lets you simulate a VCS One cluster. It lets you view, modify, and test the VCS One cluster configuration and behavior.

The Simulator includes the following features:

- Runs a simulated version of the same Policy Master that is used in a real VCS One cluster. The simulated Policy Master behaves the same as the one in an real VCS One cluster.
- Lets you import the configuration from a real VCS One cluster into the Simulator to troubleshoot configuration issues and perform root cause analysis without impacting the production environment.
- Lets you induce faults and view the resulting behavior to create and fine-tune the VCS One cluster configuration, including the failover policy, without using a production environment. Then, you can import the simulated configuration into your production environment.
- Lets you test configurations from different operating systems. For example, you can run the VCS One Simulator on a Windows system and test configurations for Linux and Solaris VCS One clusters.
- Lets you train and educate VCS One users in a protected environment. The Simulator has the same look and feel as the actual VCS One software. You can reproduce your own environment for realistic lab scenarios.
- Supports multiple Simulator instances.
 - Use the `hamultisim` command to add, remove, start, and stop a specific Simulator instance. You can also use this command to open the GUI or command line for a specific Simulator instance.
 - Use the `hasim` command to perform command line operations on a specific Simulator instance.
- Lets you simulate disaster recovery operations within and across sites.
- Runs on a stand-alone system.

The Simulator does not require any additional storage or networking hardware.
- Runs in non-secure mode only.
- Lets you perform operations from either the GUI or the command line. You can start the Simulator from the Windows command line by either running the `startsim` batch file script that is located where you installed the Simulator or using the `hamultisim -startsim` command.

The difference between a real and a simulated VCS One cluster

A real VCS One cluster is based on a client-server model. The Policy Master is the server-side center of logic that is hosted on independent hardware. Systems in a VCS One cluster connect to the Policy Master through a client-side process. This process is named `vcstoneclientd` and it runs locally on each system in a VCS One cluster.

In a simulated VCS One cluster, the client-side connections with the Policy Master are simulated. For every simulated system in a VCS One cluster, a `vcstonesim` process opens two communication channels: one for communication and the other for establishing a heartbeat with other systems. As a result, the Simulator can simulate the load of real clients on the Policy Master.

All code paths and logic decisions in the Simulator are the same as those in an actual VCS One cluster installation.

Choosing a configuration for the Simulator

To use the VCS One Simulator to simulate a VCS One environment, perform one of the following tasks to create the configuration in the Simulator:

- Create a custom configuration using the Simulator.
- Import an existing configuration into the Simulator.

When the Simulator starts, select one of the following configurations:

- The default configuration
If you do not specify a configuration, the Simulator loads the default configuration when you start the database. The Simulator starts the database, loads the default configuration in the database, and starts the Policy Master, the proxy Simulator, and the Web server.
- A specific configuration
Discards all configuration and state changes from the previous session and uses the specified configuration. If you want to save the existing configuration, export it before you use this option.
See [“Backing up and restoring VCS One data”](#) on page 575.
The specified configuration can be either a sample or a custom configuration that you create.

- Sample configuration
VCS One includes sample configurations. These sample configurations are in the following directory:

```
installation_location\VCSOne\Simulator\conf
```

The *installation_location* is the location where you installed the Simulator. If you installed the Simulator in the default location, the sample configurations are on your desktop under:

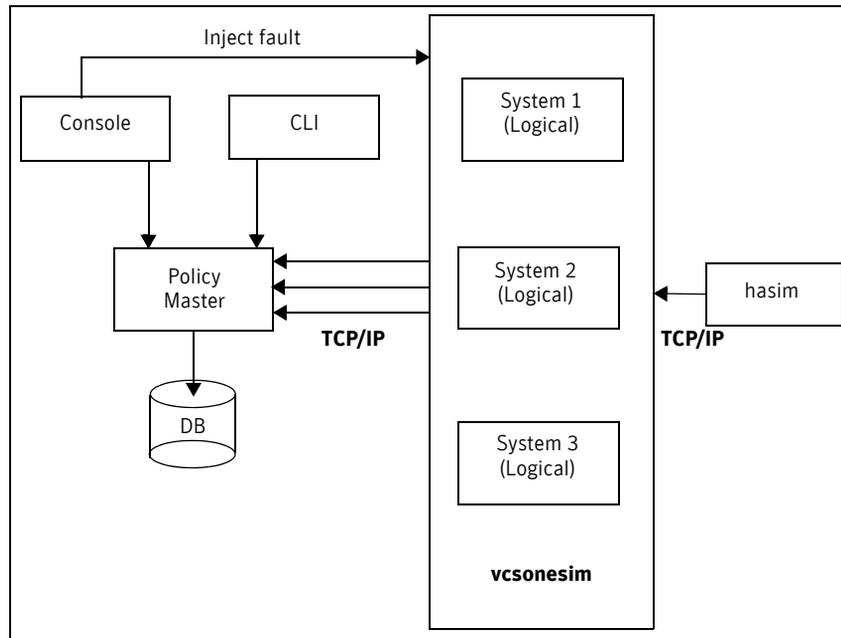
```
\VCSOne\Simulator\conf
```

- Custom configuration that you create
You can create a custom configuration that simulates your VCS One cluster configuration.
Use the configuration named “emptyconf” as a starting point for creating a custom configuration.
Use the configurations named “emptyDR_Site1” and “emptyDR_Site2” as a starting point for creating custom configurations to simulate disaster recover operations within and across sites.
See “[Loading or changing a configuration in the Simulator](#)” on page 186.

Components of the Simulator

Figure 8-1 depicts the Simulator’s components and how they interact.

Figure 8-1 The Simulator’s components



The Simulator has the following main components:

vcsonesim	The Simulator process. It simulates real systems in a simulated VCS One cluster, and simulates system faults.
hasim	The command line interface to vcsonesim.
Policy Master	The Policy Master runs the same code in a real or simulated VCS One cluster.

About the Simulator's start-up modes

The Simulator has three start-up modes. In all start-up modes, the Simulator reads state information from the specified configuration. The modes differ in what happens after the Simulator reads the configuration.

[Table 8-1](#) describes the command options to start the Simulator in each of the start-up modes.

Table 8-1 Simulator start-up modes

No command option (default mode)	Starts the Simulator from the specified configuration. The Simulator automatically moves all service groups and resources to an OFFLINE state and moves systems to a RUNNING state regardless of their stored state. Starts the Policy Master in cold start-up mode.
-extended	Starts the Simulator from the specified configuration. The Simulator preserves the systems, resources, and groups' states/istates defined in the configuration. You can see the state/istate information for all objects in the database. The Simulator completes commands that involve systems, resources, and groups that have an outstanding intended online state (such as INTENT_ONLINE or WAITING_FOR_ONLINE).

Table 8-1 Simulator start-up modes

<code>-extended -no_operation</code>	<p>Using <code>-no_operation</code> with <code>-extended</code> starts the Simulator from the specified configuration in read-only mode. You cannot perform write operations.</p> <p>Starting the Simulator in read-only mode is useful for debugging.</p> <p>The Simulator preserves the systems, resources, and groups' states/istates defined in the configuration. You can see the state/istate information for all of the objects in the database.</p> <p>The Simulator does not complete commands that involve systems, resources, and groups that have outstanding intended states.</p>
--------------------------------------	--

To change between these modes, you must stop the Simulator and then restart it in the chosen mode.

About multiple Simulator instances

You can create and run any number of VCS One Simulator instances at the same time.

A Simulator instance consists of a set of processes (such as the database, Policy Master, ProxySim, and WebServer processes) that are required to simulate VCS One.

Multiple Simulator instances let you:

- Simulate disaster recovery operations within a site.
You can use the Simulator to fault and repair a remote cluster. You can also simulate a link fault and clear it.
For more information, see [“Managing remote clusters”](#) on page 477.
- Simulate disaster recovery operations across sites.
A VCS One global cluster links individual VCS One clusters at separate sites, and enables wide-area failover and disaster recovery for applications.
You can create a Simulator instance for each VCS One cluster to simulate a global cluster.
If you create multiple Simulator instances to simulate global clusters, you must manually change the ClusterName attribute. By default, the Simulator assigns VCSOneFarm as the cluster name.
For more information, see [“Setting up VCS One global clusters”](#) on page 469.
- Simulate failover behavior before and after a configuration change.

- Simulate different Organization Tree set ups.
- Simulate multiple clusters with separate configurations.

About Simulator scripts and commands

The following batch file scripts are in the `VCSOne` directory where the Simulator is installed:

<code>startsim.bat</code>	Starts the default Simulator instance.
<code>stopsim.bat</code>	Stops the default Simulator instance.
<code>cli_prompt.bat</code>	Opens a command prompt for the default Simulator instance.
<code>hamultisim.bat</code>	Adds, removes, starts, and stops Simulator instances. Opens the GUI or Windows command line for a specific Simulator instance. Use this command to control multiple Simulator instances.

In addition, the `hasim` command is in the `installation_location\VCSOne\Simulator\bin\` directory:

<code>hasim</code>	Performs operations on a Simulator instance from the Windows command line for that instance.
--------------------	--

Viewing Simulator command usage

Use the following procedure to view the command usage for `hamultisim`.

To view the command usage for `hamultisim`

- 1 Open the Windows command prompt by selecting **Start > Run**.
- 2 In the field, enter `cmd` and click **OK**.
- 3 Change directories to the following location:

```
cd installation_location\VCSOne
```

where `installation_location` is the directory where you installed the Simulator.

- 4 Enter the following command:

```
hamultisim -help
```

To view the command usage for hasim

- 1 Open the Windows command prompt by selecting **Start > Run**.
- 2 In the field, enter `cmd` and click **OK**.
- 3 Change directories to the following location:

```
cd installation_location\VCSOne
```

where *installation_location* is the directory where you installed the Simulator.

- 4 At the Windows command prompt, run the following command to list Simulator instances:

```
hamultisim -list
```
- 5 At the Windows command prompt, run the following command to open the command line for the specifies Simulator instance:

```
hamultisim -cliprompt instance_name
```

where *instance_name* is the name of the Simulator instance.
- 6 At the new Windows command prompt, enter the following command:

```
hasim -help
```

Starting the default Simulator instance

Starting a Simulator instance consists of starting the configuration database, loading the configuration, and starting the Web server (GUI) and Policy Master.

You can only start and stop the Simulator from the system on which it is installed. You can connect to the Simulator from a remote system. If you connect remotely, some options may not be available to you.

VCS One includes one default Simulator instance. The name of the default Simulator instance is `default`.

You can start the Simulator by running a script or entering a command.

To start the default Simulator instance by running a script

- ◆ Double click on the following batch file script to start the default Simulator instance:

```
installation_location\VCSOne\startsim.bat
```

where *installation_location* is the directory where you installed the Simulator.

The script asks you if you want to use the default configuration. If you do not want to use the default configuration, the script asks you to enter the directory for the XML configuration files you want to use.

The Simulator launches in your Web browser.

To start the default Simulator instance using a command

- ◆ At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -startsim default \  
[-d xml_dir]
```

If you want to load a configuration other than the default configuration, use `-d xml_dir` to specify the configuration you want to load. *xml_dir* is the directory that contains the XML configuration files.

The Simulator includes different sample configurations. They are in the following directory:

```
installation_location\VCSOne\Simulator\conf
```

The Simulator launches in your Web browser.

Adding a Simulator instance

Before you can start a Simulator instance, you must add it.

To add a new Simulator instance

- ◆ At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -addsim [-hosts] \  
instance_name
```

where *installation_location* is the directory where you installed the Simulator and *instance_name* is the name of the Simulator instance.

Use the `-hosts` option to enable more than one Simulator instance to be open in the same Web browser. This option adds a hosts entry for the specific Simulator instance in the hosts file on the system. The host entry format is:

```
127.0.0.1 vcstone_instance_name
```

Adding a hosts entry lets you access the GUI for the Simulator instance using a URL that contains the instance name:

```
https://vcstone_instance_name:ssl_port
```

where *instance_name* is the name of the Simulator instance and *ssl_port* specifies the SSL port.

If you do not specify a hosts entry, the URL for connecting to the GUI for a Simulator uses a DNS number and has the following format:

```
https://127.0.0.1:ssl_port
```

A hosts entry for each specific Simulator instance is required because Web browsers store cookies based on the DNS name part of the URL. As a result, it is not possible to log onto multiple Simulator instances simultaneously

with 127.0.0.1 as the DNS part of the URL. The hosts entry for a specific Simulator instance is deleted from the hosts file when you remove the Simulator instance with the `hamultsim -removesim` command.

Starting a Simulator instance

Before you can start a new Simulator instance, you must add it. If you have not already added the Simulator instance that you want to start, add it.

See “[Adding a Simulator instance](#)” on page 181.

Starting a Simulator instance

Use the following procedure to start a Simulator instance.

To start a Simulator instance

- ◆ At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultsim -startsim \  
instance_name [-d xml_dir]
```

where *installation_location* is the directory where you installed the Simulator, *instance_name* is the name of the Simulator instance, and *xml_dir* is the configuration directory that you want to load in the Simulator. If you do not provide a configuration directory, the Simulator starts with the default configuration or the previously loaded configuration.

Starting a Simulator instance with the same state information that is in the database

Use the following procedure to start a Simulator instance with the same state information that is in the database.

To start a Simulator instance with the same state information that is in the database

- ◆ At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultsim -startsim \  
instance_name -extended
```

where *installation_location* is the directory where you installed the Simulator and *instance_name* is the name of the Simulator instance. When you start the Simulator with the `-extended` option, the Simulator preserves the systems, resources, and groups' states/istates defined in the configuration. You can see the state/istate information for all objects in the

database. The Simulator completes commands that involve systems, resources, and groups that have an outstanding intended online state (such as INTENT ONLINE or WAITING FOR ONLINE).

Starting a Simulator instance in read-only mode

Read-only mode is useful for debugging.

To start a Simulator instance in read-only mode

- ◆ At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -startsim \  
instance_name -extended -no_operation
```

where *installation_location* is the directory where you installed the Simulator and *instance_name* is the name of the Simulator instance.

When you start the Simulator with both the `-extended` and the `-no_operation` options, the Simulator starts in read-only mode. You cannot perform write operations.

The Simulator preserves the systems, resources, and groups' states/istates defined in the configuration. You can see the state/istate information for all objects in the database.

The Simulator does not complete commands that involve systems, resources, and groups that have outstanding intended states.

Starting a Simulator instance with non-default ports

A Simulator instance uses certain ports by default. When you start a new Simulator instance, the ports are set up automatically. If a Simulator instance is already using the default port and you start up another Simulator instance, it starts on the next available port.

After you start two Simulator instances, the ports look similar to the following example.

```
installation_location\VCSOne\hamultisim -list -ports  
Instances: dbport  pmport  proxysimport  sslport  adminportwsslport  
sim1         14157  14151  14156          14171  14172      14173  
sim2         14158  14152  14159          14174  14175      14176
```

Because the ports are set up automatically, there is typically no reason for you to specify the Simulator ports. Setting the ports automatically is recommended. If, however, you have another application that is already using one of the ports required by a Simulator instance, you can manually specify alternate ports for the instance when you start it. The ports a Simulator instance uses should not be used by any other process.

If you set non-default ports when you start a Simulator instance and a port is not available, the Simulator instance starts on the next available port.

Caution: If you set non-default ports for a Simulator instance, it is not possible to reset the ports to default values. In addition, disaster recovery configurations will not work if you start Simulator instances in a different order than that indicated by their port number assignments.

To start a Simulator instance with non-default ports

- 1 At the command prompt, enter the following command to display the port information for each process:

```
installation_location\VCSOne\hamultisim -list -ports
```

where *installation_location* is the directory where you installed the Simulator.

- 2 Enter the following command to start a Simulator instance with non-default ports:

```
installation_location\VCSOne\hamultisim -startsim \  
-instance_name [-d xml_dir] [-dbport port] [-pmpport port] \  
[-proxysimport port] [-sslport port] [-adminport port] \  
[-wssslport wsssl_port]
```

where *installation_location* is the directory where you installed the Simulator. Use the `-d xml_dir` option to load a specific XML configuration into the database and start it.

Table 8-2 shows the port-related options for `hamultisim -startsim`.

Table 8-2 hamultisim port options

Option	Default port	Description
<code>-dbport port</code>	14157	Starts the database on the port provided. If you do not specify a port, the database starts on port 14157 by default. If this port is not available, it starts on the next available port.
<code>-pmpport port</code>	14151	Starts the Policy Master on the port provided. If you do not specify a port, the Policy Master starts on port 14151 by default. If this port is not available, it starts on the next available port.
<code>-proxysimport port</code>	14156	Starts the proxysimport on the port provided. If you do not specify a port, The proxysimport starts on port 14156 by default. If this port is not available, it starts on the next available port.
<code>-sslport port</code>	14171	Used for secure and encrypted https communication between the Web server and the browser. If you do not specify an SSL port, the Web server starts on port 14171 by default. If this port is not available, it starts on the next available port.
<code>-admin port</code>	14172	Starts the Web server on the admin port provided. If you do not specify a port, the Web server starts on port 14172 by default. If this port is not available, it starts on the next available port.
<code>-wssslport port</code>	14173	Used by the Web server for secure and encrypted communication for Web services. If you do not specify an wssslport port, the Web server starts on port 14173 by default. If this port is not available, it starts on the next available port.

Loading or changing a configuration in the Simulator

You can load a sample or custom configuration into a Simulator instance or change the configuration.

Loading a sample configuration and starting a Simulator instance

The Simulator includes sample configurations. They are in the following directory:

```
installation_location\VCSOne\Simulator\conf
```

To load a sample configuration and start a Simulator instance

- ◆ At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -startsim \  
instance_name -d xml_dir
```

where *installation_location* is the directory where you installed the Simulator, *instance_name* is the name of the Simulator instance, and *xml_dir* is the directory that contains the XML configuration files.

Loading a custom configuration and starting a Simulator instance

Use the following procedure to load a custom configuration into a Simulator instance.

To load a custom configuration and start a Simulator instance

- ◆ At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -startsim \  
instance_name -d xml_dir
```

where *installation_location* is the directory where you installed the Simulator, *instance_name* is the name of the Simulator instance, and *xml_dir* is the directory that contains the XML configuration files.

Loading the real Policy Master configuration into a Simulator instance

Use the following procedure to load the real Policy Master configuration into a Simulator instance.

To load a the real Policy Master configuration into a Simulator instance

- 1 At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -startsim \  
instance_name -d xml_dir
```

where *installation_location* is the directory where you installed the Simulator, *instance_name* is the name of the Simulator instance, and *xml_dir* is the directory that contains the real Policy Master configuration files.

- 2 Open a Windows command prompt for the specified instance using the following command:

```
installation_location\VCSOne\hamultisim -cliprompt \  
instance_name
```

- 3 Because the real Policy Master configuration does not contain the user `simuser`, manually add `simuser`. Run the following command at the command prompt that you opened in the previous step.

```
hauser -add simuser@domain
```

- 4 Add the `ServerFarmAdministrator` and `ServerFarmObjectAdministrator` roles for `simuser`:

```
hauser -addrole simuser@domain ServerFarmAdministrator  
hauser -addrole simuser@domain ServerFarmObjectAdministrator
```

You may now log on to the Simulator as `simuser`.

Changing the configuration that is loaded in a Simulator instance

To change the configuration that is loaded in a Simulator instance, you must stop the Simulator instance and restart it, specifying the configuration to load.

To change the configuration that is loaded in a Simulator instance

- 1 Check if the Simulator instance is running by entering the following command:

```
installation_location\VCSOne\hamultisim -status
```

where *installation_location* is the directory where you installed the Simulator.

- 2 If the Simulator instance is running, stop it by using one of the following methods:

- Double click on the following batch file script to stop the default Simulator instance:

```
installation_location\VCSOne\stopsim.bat
```

This script is in the directory where you installed the Simulator.

- At the Windows command prompt, enter the following command to stop a Simulator instance other than the default instance:

```
installation_location\VCSOne\hamultisim -stopsim \  
instance_name
```

where *instance_name* is the name of the Simulator instance. Use `default` as the instance name to specify the default instance.

- 3 Restart the Simulator instance by using one of the following methods:

- Double click on the following batch file script to start the default Simulator instance:

```
installation_location\VCSOne\startsim.bat
```

This script is in the directory where you installed the Simulator.

When you are prompted, enter the name of the configuration you want to load.

- At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -startsim \  
instance_name -d xml_dir
```

where *instance_name* is the name of the Simulator instance and *xml_dir* is the directory of the XML configuration files. Use `default` as the instance name to specify the default instance.

The Simulator includes different sample configurations. They are in the following directory:

```
installation_location\VCSOne\Simulator\conf\confxml
```

The Simulator launches in your Web browser.

About logging on to the Simulator

When the Simulator launches in your Web browser, it prompts you to enter the following information to log on to the Simulator in non-secure mode:

User Name	<p>The word <code>simuser</code> is entered by default. You may use <code>simuser</code> or enter an alternate valid VCS One user name.</p> <p>To use the Simulator fully, assign other users <code>ServerFarmAdministrator</code> and <code>ServerFarmObjectAdministrator</code> privileges.</p> <p>The user <code>simuser</code> is part of the predefined Simulator configurations and has <code>ServerFarmAdministrator</code> and <code>ServerFarmObjectAdministrator</code> privileges.</p>
Password	<p>You do not need to enter a password to log on to the Simulator.</p>
Domain	<p>The word <code>domain</code> is entered by default. You may use <code>domain</code> or enter an alternate valid domain name.</p>

Accessing the GUI for a Simulator instance

Use the following procedures to access the GUI for the default Simulator or to access the GUI for a specific Simulator instance.

Accessing the GUI for the default Simulator

Use the following procedure to access the GUI for the default Simulator.

To access the GUI for the default Simulator

- ◆ Do one of the following:
 - Start the default Simulator by running the `startsim` script. The GUI automatically opens in the Web browser.
 - Access the GUI for the default Simulator by going to the following URL:
`https://127.0.0.1:14171`

To access the GUI if the default Simulator uses a port other than the default port (14171)

- 1 At the Windows command prompt, get the SSL port (`sslport`) for the default Simulator instance:

```
installation_location\VCSOne\hamultisim -list -ports
```

where *installation_location* is the directory where you installed the Simulator.

- 2 Go to the following URL:

```
https://127.0.0.1:sslport
```

where *sslport* is the SSL port you obtained in step 1.

Accessing the GUI for a Simulator instance

Use the following procedure to access the GUI for a Simulator instance.

To access the GUI for a Simulator instance

- 1 Display the SSL port (*sslport*) of the Simulator instance you want to access:

```
installation_location\VCOne\hamultisim -list -ports
```

where *installation_location* is the directory where you installed the Simulator.

- 2 Do one of the following:

- If you used the `-hosts` option when you added the Simulator instance, go to the following URL:

```
https://vc_sone_instance_name:sslport
```

where *sslport* is the name of SSL port that you obtained in step 1 for that instance.

- If you did not use the `-hosts` option, go to the following URL:

```
https://127.0.0.1:sslport
```

where *sslport* is the name of SSL port that you obtained in step 1 for that instance.

Accessing the command line for a Simulator instance

Use the following procedures to access the command line for the default Simulator or a specific Simulator instance.

Accessing the command line for the default Simulator instance

Use the following procedure to access the command line for the default Simulator.

To access the command line for the default Simulator

- ◆ Do one of the following:
 - Double click on the following batch file script to start the default Simulator instance:

```
installation_location\VCSOne\cli_prompt.bat
```

where *installation_location* is the directory where you installed the Simulator.

- At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -cliprompt default
```

where *installation_location* is the directory where you installed the Simulator.

The VCS One “ha” commands that you run from this command line apply to the default Simulator instance. After you access the command line for the default Simulator instance, you may use the `hasim` command to perform operations on that Simulator instance. To see all `hasim` operations, use `hasim -help`.

Accessing the command line for a Simulator instance

Use the following procedure to access the command line for a specific Simulator instance.

To access the command line for a Simulator instance

- ◆ At the command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -cliprompt \  
instance_name
```

where *installation_location* is the directory where you installed the Simulator and *instance_name* is the name of the Simulator instance.

The VCS One “ha” commands that you run from this command line apply to the specified Simulator instance. After you have accessed the command line for this Simulator instance, you may use the `hasim` command to perform operations on that Simulator instance. To see all `hasim` operations, use `hasim -help`.

Creating and saving a custom configuration in the Simulator

Configuration files that you load into the Simulator must be in XML.

To create a custom configuration

- 1 Start with a sample configuration that is included with the Simulator.

The sample configurations are in the following directory:

```
installation_location\VCSOne\Simulator\conf
```

- 2 Use the Simulator to modify the configuration.

To save the custom configuration

- ◆ Save the new configuration with a new name. To save the configuration, you must export the information in the VCS One cluster's configuration database before you stop the Simulator. After you have opened a command prompt for a Simulator instance, enter the following command:

```
installation_location\VCSOne\Simulator\bin\haconf -dbtoxml \  
xml_dir
```

where *installation_location* is the directory where you installed the Simulator and *xml_dir* is the directory that contains the XML configuration files.

See [“Backing up and restoring VCS One data”](#) on page 575.

Displaying the status of a Simulator instance

You can use `hamultisim -status` to display the status of the specified Simulator instance. If you do not specify an instance name, the status is displayed for all Simulator instances. You can also use the command to display the status of all the processes of individual Simulator instances.

A Simulator instance has one of the following statuses:

RUNNING	All the processes for the specified instance are up and the instance is running.
NOT RUNNING	All the processes for the specified instance are down and the instance is not running.
PARTIAL	Some of the processes for the specified instance are up and the instance is in a PARTIAL state.

The `hamultisim -processes` command displays the status of each process for the specified instance. If no instance is specified, the `-processes` option displays the status of all the processes for all instances.

The process status of a Simulator instance can be one of the following states:

UP The process is running.

DOWN The process is not running.

To display the status of a Simulator instance

- ◆ At the command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -status [-processes] \  
instance_name
```

where *installation_location* is the directory where you installed the Simulator.

Use `-processes` to display the status of all processes for a specific Simulator instance.

To display the status of all Simulator instances

- ◆ At the command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -status [-processes]
```

where *installation_location* is the directory where you installed the Simulator.

Use `-processes` to display the status of the processes for all instances.

Listing Simulator instances

To list Simulator instances

- ◆ At the command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -list
```

where *installation_location* is the directory where you installed the Simulator.

Listing port information for a Simulator instance

Use the following procedure to list port information for a Simulator instance.

To list port information for a Simulator instance

- ◆ At the command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -list -ports
```

where *installation_location* is the directory where you installed the Simulator.

This command lists the port information for each process. The `-ports` option lists the instances, processes, and ports on which the process is configured.

Setting up a disaster recovery configuration in the Simulator

To simulate a disaster recovery operations using the VCS One Simulator, you must first set up a disaster recovery configuration. In a disaster recovery configuration, two simultaneous instances of the Simulator are running on the same system.

The steps for setting up a disaster recover configuration in the Simulator are the same as the steps for setting up a real disaster recovery configuration, except that you need to use 127.0.0.1 as the IP address and you do not need to set up trust between the two Simulator instances.

In this procedure, `seattle` is the name of the primary VCS One cluster and `tucson` is the name of the secondary VCS One cluster.

To set up a disaster recovery configuration in the Simulator

- 1 If you have a single configuration that you want to use, make two copies of the configuration files in two separate directories.
- 2 Open the first `main.xml` file and edit it as follows:
 - a Find the following line:

```
<cluster name="name1">
```
 - b Note the cluster name.
 - c Change all occurrences of this cluster name to another name. This VCS One cluster is the primary one. In this procedure, `seattle` is used as the name of the primary VCS One cluster.

```
<cluster name="seattle">
```

3 Open the second main.xml file and edit it as follows:

a Find the following line:

```
<cluster name="clus2">
```

b Note the cluster name.

c Change all occurrences of this cluster name to another name. This VCS One cluster is the secondary one. In this procedure, tucson is used as the name of the secondary VCS One cluster.

```
<cluster name="tucson">
```

4 Add two Simulator instances using the `-hosts` option:

```
installation_location\VCSOne\hamultisim -addsim -hosts seattle
```

```
installation_location\VCSOne\hamultisim -addsim -hosts tucson
```

The Simulator instance's name do not need to match the cluster names, but it is helpful if they do.

5 List the ports for the Simulator instances:

```
installation_location\VCSOne\hamultisim -list -ports
```

The output looks similar to the following:

```
Instances: dbport  pmport  proxysimportsslportadminport  wssslport
default      14157  14151  14156      14171  14172      14173
seattle      14157  14151  14156      14171  14172      14173
tucson       14157  14151  14156      14171  14172      14173
```

The ports for the two instances are the same before you start the Simulator instances.

6 Start the first Simulator instance:

```
installation_location\VCSOne\hamultisim -startsim seattle -d \  
xml_dir
```

7 Start the second Simulator instance:

```
installation_location\VCSOne\hamultisim -startsim tucson -d \  
xml_dir
```

8 List the ports for the Simulator instances to see that the ports for the second Simulator instance have been changed from the original default values:

```
installation_location\VCSOne\hamultisim -list -ports
```

The output looks similar to the following:

```
Instances: dbport  pmport  proxysimportsslportadminport  wssslport
default      14157  14151  14156      14171  14172      14173
seattle      14157  14151  14156      14171  14172      14173
tucson       14158  14152  14159      14174  14175      14176
```

- 9 Open command prompts for both Simulator instances:

```
installation_location\VCSOne\hamultisim -cliprompt seattle  
installation_location\VCSOne\hamultisim -cliprompt tucson
```

- 10 View the cluster name on the first Simulator instance:

```
installation_location\VCSOne\haclus -list
```

- 11 View the cluster name on the second Simulator instance:

```
installation_location\VCSOne\haclus -list
```

- 12 Add the second cluster to the first Simulator instance:

```
installation_location\VCSOne\haclus -add tucson  
installation_location\VCSOne\haclus -list
```

The output looks similar to the following:

```
seattle*  
tucson
```

The asterisk denotes the local cluster.

- 13 Add the first cluster to the second Simulator instance:

```
installation_location\VCSOne\haclus -add seattle  
installation_location\VCSOne\haclus -list
```

The output looks similar to the following:

```
seattle  
tucson*
```

The asterisk denotes the local cluster.

- 14 Display the second cluster on the first Simulator instance:

```
installation_location\VCSOne\haclus -display tucson
```

The output looks similar to the following:

```
#Attribute          Value  
ClusterName        tucson  
ClusterState       INIT  
ConnectionRole     Acceptor  
ConnectionTimeout  5  
ConsolidatedLinkStatus  
DRPort             14151  
EnableConnections  0  
LinkStatus  
MaxHeartbeatInterval  5  
MissedHeartbeatThreshold 5  
NetworkConnections  
RClusterUUID  
ReconnectInterval  5  
RunningDRVersion   0  
SourceFile         main.xml  
TransitionTimeout  300
```

- 15 Display the first cluster on the second Simulator instance:

```
installation_location\VCSOne\haclus -display seattle
```

The output looks similar to the following:

#Attribute	Value
ClusterName	seattle
ClusterState	INIT
ConnectionRole	Initiator
ConsolidatedLinkStatus	
EnableConnections	0
LinkStatus	
MaxHeartbeatInterval	5
MissedHeartbeatThreshold	5
RClusterUUID	
RunningDRVersion	0
SourceFile	main.xml
TransitionTimeout	300

The Initiator and Acceptor are determined by the alphabetical order of the two cluster names. The first cluster name becomes the Initiator.

- 16 For the cluster that initiates the connection request (seattle), perform the following steps:

- a Type the following command:

```
installation_location\VCSOne\haclus -modify \  
NetworkConnections 127.0.0.1 -clus tucson
```

- b Type the following command:

```
installation_location\VCSOne\haclus -modify \  
DRPort 14152 -clus tucson
```

The DRPort is the Policy Master port (pmport) number for the remote (*tucson*) Simulator instance. The pmport number is displayed in the output for `hamultisim -list -ports`.

- c Type the following command:

```
installation_location\VCSOne\haclus -modify \  
EnableConnections 1 -clus tucson
```

- 17 For the cluster that accepts the connection (tucson), type the following command:

```
installation_location\VCSOne\haclus -modify \  
EnableConnections 1 -clus seattle
```

- 18 Display cluster information for the first cluster:

```
installation_location\VCSOne\haclus -display seattle
```

The output looks similar to the following:

#Attribute	Value
ClusterName	rc1
ClusterState	RUNNING
ConnectionRole	Initiator
ConsolidatedLinkStatus	LINK_UP
EnableConnections	1
LinkStatus	127.0.0.1 UP
MaxHeartbeatInterval	5

```

MissedHeartbeatThreshold 5
RClusterUUID              8b18e8c4-1dd2-11b2-8f0b-aaf14f23bc3d
RunningDRVersion          1.0
SourceFile                 main.xml
TransitionTimeout         300

```

- 19 On the first Simulator instance, display cluster information for the second cluster:

```
installation_location\VCSOne\haclus -display tucson
```

The output looks similar to the following:

```

#Attribute                Value
ClusterName               rc2
ClusterState              RUNNING
ConnectionRole            Acceptor
ConnectionTimeout         5
ConsolidatedLinkStatus    LINK_UP
DRPort                    14152
EnableConnections         1
LinkStatus                127.0.0.1 UP
MaxHeartbeatInterval     5
MissedHeartbeatThreshold 5
NetworkConnections        127.0.0.1
RClusterUUID              8b18e8c4-1dd2-11b2-8f0b-aaf14f23bc3d
ReconnectInterval         5
RunningDRVersion          1.0
SourceFile                 main.xml
TransitionTimeout         300

```

The link is now up and running. If you have loaded the same configuration into both Simulator instances, you can set up global composite service groups (CSGs), bring service groups online, and switch them from one cluster to the other with the Simulator.

In a real disaster recovery configuration, the clusters would have different storage locations and definitions for running the applications on the disaster recovery site.

- 20 Save the configuration to the same or a new location to preserve the disaster recovery configuration settings so that you can reload the databases in the future.

Perform the following steps for the first Simulator instance:

- a Change directories to the location where the configuration is located.
- b Save the configuration by running the following command:
haconf -dbtoxml .

Perform the following steps for the second Simulator instance:

- a Change directories to the location where the configuration is located.

- b Save the configuration by running the following command:

```
haconf -dbtoxml .
```

See the following chapters for information about configuring clusters for disaster recovery and setting up global CSGs:

- “[Setting up VCS One global clusters](#)” on page 469
- “[Managing global composite service groups](#)” on page 497.

Simulating disaster recovery operations using the Simulator

See the following sections for information about simulating disaster recovery operations:

- “[Faulting a remote cluster using the Simulator](#)” on page 492
- “[Clearing a simulated cluster fault using the Simulator](#)” on page 493
- “[Simulating a link fault](#)” on page 493
- “[Clearing a simulated link fault](#)” on page 494

Stopping a Simulator instance

Use the following procedures to stop the default Simulator or a specific Simulator instance.

Stopping the default Simulator instance

Use the following procedure to stop the default Simulator.

To stop the default Simulator instance

- ◆ Do one of the following:
 - Double click on the following batch file script to stop the default Simulator instance:

```
installation_location\VCSOne\stopsim.bat
```

where *installation_location* is the directory where you installed the Simulator.

- At the Windows command prompt, enter the following command:

```
installation_location\VCSOne\hamultisim -stopsim default
```

Stopping a Simulator instance

Use the following procedure to stop a specific Simulator instance.

To stop a Simulator instance

- ◆ At the command prompt, enter the following command:

```
installation_location\VCSOne\hamultsim -stopsim instance_name
```

where *installation_location* is the directory where you installed the Simulator and *instance_name* is the name of the Simulator instance.

This command stops all the processes for the Simulator instance.

Removing a Simulator instance

Use the following procedure to remove a Simulator instance.

To remove a specific Simulator instance

- ◆ At the command prompt, enter the following command:

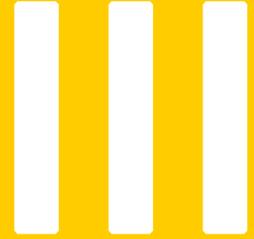
```
installation_location\VCSOne\hamultsim -removesim \  
instance_name
```

where *installation_location* is the directory where you installed the Simulator and *instance_name* is the name of the Simulator instance.

If you used the `-hosts` option with `hamultsim -addsim` when you created the Simulator instance, this command removes the Simulator instance and deletes its entry from the hosts file.

For instructions on how to uninstall the Simulator, see the *Veritas Cluster Server One Installation Guide*.

Section



Design

This section includes the following chapters:

- [“Design overview”](#) on page 203
- [“Designing roles and privileges for users”](#) on page 217.
- [“Designing actions taken after a fault”](#) on page 227.
- [“Designing attribute values using variables”](#) on page 233.
- [“Designing service groups”](#) on page 241
- [“Designing application placement policy”](#) on page 273.

Design overview

This chapter includes the following topics:

- [Introduction](#)
- [Planning](#)
- [Preparing](#)
- [Implementing](#)
- [Configuring and verifying](#)

Introduction

The purpose of the implementation checklist is to make sure the administrator considers all aspects of the VCS One implementation, and no steps are inadvertently missed. The checklist does not attempt to explain all the steps, but instead offers references of where to go for more information.

Note: These instructions assume the tasks are performed by an administrator with full permissions to all aspects of the VCS One cluster and applications.

Before designing and implementing your VCS One installation, be familiar with the architecture and concepts of VCS One.

Planning

Planning the VCS One cluster consists of determining your goals, your current environment and the differences between the two. In addition, coordination of the implementation is an important task.

Define your goals

The first step in planning is to define your goals. There are two ways to accomplish this. Either approach the question from a hardware perspective or approach the question from a software perspective. With the hardware perspective, first evaluate the existing IT hardware infrastructure to decide which systems will be part of the VCS One cluster, and note the applications running on them. With the software perspective, first evaluate what applications are going to be managed by VCS One, and note the systems those applications are running on. With either approach, the result is that you have the following:

- The set of systems that will be controlled by VCS One
- The list of applications that will be managed by VCS One

Remember to list any systems that will be included as spares for maintenance, expansion, or mobility of the managed applications.

Note: Often the end goal changes over the course of planning because of hardware requirements or available resources. It is a best practice to estimate the priority of your goals in case adjustments must be considered later in the process.

Determine the current environment

The second step in planning is a process of discovery of what currently exists in your environment.

Collect system information

You will need information about both the Policy Master cluster nodes and the client systems. For each system that will be controlled by VCS One, collect the following information:

- **Systems:** Document the name, OS, OS version, number of CPUs, speed of CPUs, and memory available on the system(s).
- **Network requirements:** Determine the network connectivity of the systems. Document the NICs available on each system and what subnets they are on.
- **Storage requirements, if applicable:** Determine the storage topology of the systems. Document the HBA(s) available on each system. Also document which systems have shared storage between them if you are considering a VCS One cluster configuration that has application failover capability, either manual or automated.

For example, all VCS One cluster systems may be connected to shared storage, or subsets of the VCS One cluster systems may be connected to their own storage.

Collect application information

For each application that will be controlled by VCS One, collect the following information:

- **Failover capability:** Determine if the application will have failover capability, either manual or automated.
- **Hardware requirements:** Determine the hardware architecture and version of the operating system that the application requires.
- **Resource requirements:** Determine the logical and physical components that are used by the application, and how they depend on each other. These components will become your list of VCS One resources, and will determine the start and stop order of the resources.

See [“About resources and resource dependencies”](#) on page 37.

- **Application dependencies:** Determine if this application is dependent on other applications.

For example, a web based application may require an Oracle application backend database.

Plan organizational tasks

Depending on the practices and procedures of the environment, you may need to get approvals, schedule down time in advance or request change orders.

Determine the difference between goals and current environment

The third step in planning is to contrast your current environment with your goal. This allows you to establish a plan for what needs to be accomplished.

System requirements and recommendations

The *Veritas Cluster Server One Release Notes* lists supported hardware architecture and operating system versions. This topic gives required and recommended components to run VCS One.

Every VCS One production environment requires a highly available Policy Master connected to client systems. Use the information collected about the systems in your current environment and [Table 9-1](#) to determine if you must upgrade any of your systems to meet the following requirements.

Table 9-1 Hardware requirements and recommendations for the Policy Master cluster

	Requirements	Additional Recommendations
Policy Master Cluster (Two to four systems)	Linux PM: Intel-based systems running Opteron® or Extended Xeon® 64-bit processors (not Itanium®) Solaris PM: SPARC-based systems 1 GHz minimum CPU CD-ROM drive for installation from a software disc Check the <i>Veritas Cluster Server One Release Notes</i> or the technical support web site to make sure the system hardware and software is supported	Dual processor systems
Memory	512 megabytes minimum	Eight gigabytes of memory for large numbers of systems, service groups or application resources in the VCS One cluster

Table 9-1 Hardware requirements and recommendations for the Policy Master cluster

	Requirements	Additional Recommendations
Local storage	<p>With Storage Foundation: 520 megabytes local disk space minimum.</p> <p>Without Storage Foundation: 350 megabytes local disk space minimum.</p> <p>1 built-in SCSI adapter per system to access the local disks</p>	
Shared storage	<p>1 SCSI or Fibre channel attached array-based storage shared between the Policy Master cluster systems</p> <p>One data disk at least 2 GB in size for Policy Master configuration database. Disk must be protected by mirroring or RAID technology.</p> <p>At least 3 coordinator disks for I/O fencing</p> <p>All disks must be SCSI-3 compliant</p> <p>Check the hardware compatibility list (HCL) to make sure the storage is supported</p>	<p>Fibre channel attached array-based storage recommended</p> <p>Two host bus adapters to eliminate the HBA as a single point of failure</p>
Network	<p>Three 100BaseT network interface cards (NIC)</p> <ul style="list-style-type: none">■ One public network■ Two cluster interconnect links	<p>Use gigabit network interface cards</p> <p>Additional separate NIC(s) for Policy Master to client communications</p> <p>Configure a low priority heartbeat link for the Policy Master cluster using one of the links between the Policy Master and the VCS One cluster.</p>

Caution: Not using SCSI-3 compliant shared storage in the Policy Master cluster can lead to data corruption issues. This can be due to loss of communications between the Policy Master cluster system, manual actions by the operator or other instances where the Policy Master does not have complete control of the environment.

Table 9-2 Hardware requirements and recommendations for client system

	Requirements	Additional Recommendations
VCS One cluster systems	1 GHz minimum CPU Check the <i>Veritas Cluster Server One Release Notes</i> or the technical support web site to make sure the system hardware and software is supported	
Memory	256 megabytes minimum	
Local Storage	300 megabytes local disk space minimum.	
Shared storage	Disk space as needed for application, Check the hardware compatibility list (HCL) to make sure the storage is supported SCSI-3 compliant shared storage between systems if application movement (manual or automatic) is configured	
Network	One network interface card connecting the system to both the Policy Master cluster and the customer systems	Separate NIC(s) to connect to the Policy Master cluster and the customer systems

Caution: Not using SCSI-3 compliant shared storage in the VCS One cluster can lead to data corruption issues. This can be due to loss of communications between the Policy Master and the client systems.

Planning your user privilege model

Determine if the predefined roles for users match to the requirements of your environment.

See “[Pre-defined roles in VCS One](#)” on page 628.

Planning the names of your VCS One cluster objects and attributes

The following criteria describe the requirements of VCS One object names.

- The space character and the following special characters are not allowed in names of systems, service groups, resources, and agents:
` ' \ " / \ = * + ? () { } [] \$ # ^ ! % & , . : ; < > | ~ @
- User names and user group names can not contain a space character or the following special characters:
` ' \ " / \ = * + ? () { } [] \$ # ^ ! % & , . : ; < > | ~
- User and user group names are case insensitive. For example, `username@domain.com` is treated the same as `USERNAME@DOMAIN.COM`. This could have an impact if there are two distinct users that have the same names except for the case. If one user has been added to VCSOne ServerFarm, the other user would gain the same privileges.
- Attribute and object names are case-insensitive.
- Attribute values are case-sensitive by default but can be configured otherwise.
- The description text of any VCS One object can not use a single quotation mark.
- An attribute value that contains an escape sequence for a special character must be enclosed in double quotation marks.
- A group extended attribute can not have the same name as an already existing group attribute or common extended attribute.
- A system extended attribute can not have the same name as an already existing system attribute or common extended attribute.
- A set name is local to a user. Set names do not have to be unique across the VCS One cluster.
- A fully qualified resource name is in the format `group.resource`. For example, `oracle_group.ip_resource`

[Table 9-3](#) lists the maximum permissible size for various VCS One objects.

Table 9-3 Size of VCS One objects

Object	Maximum permissible size
VCS One cluster name	128 characters
System name	128 characters
Group name	128 characters
OUName node name	128 characters
OUValue node name	128 characters
Depth of the Organization Tree	512 OUname=OUvalue pairs
Length of the fully qualified path of a OUNode (from root of the tree to the node)	4096 characters
Resource name	128 characters
Resource type name	128 characters
Fully qualified resource name	Group name + Resource name + 2
User name	64 characters
User group name	64 characters
Fully qualified user name (name@domain)	128 characters
Domain name	64 characters
Role name	128 characters
String attribute name	32 characters

Including special characters in attribute values

To include special characters in attribute values in the XML configuration file, use standard XML escape sequences. This pertains when manually editing the XML configuration file.

Enclose attribute values that have XML escape sequences in double-quotation marks. For example:

```
<attribute name="StartProgram"><scalar>"start in bg -- &amp;"
</scalar></attribute>
```

Special character	Escape sequence
" (double quotes)	"
& (ampersand)	&
< (less than)	<
> (greater than)	>
' (single quote)	'

The escape character for a resource attribute variable is the caret character (^).

Caution: Symantec recommends using the escape sequences instead of the special characters. If you use the special character, you may encounter errors depending on the location of the special character.

Preparing

Now that you have identified what you need, in this phase you use that knowledge to prepare for installation and implementation. In this step, do the following:

- Gather reference material.
Product documentation and other reference material can help implementation go more smoothly when questions arise.
- Validate agent requirements.
Determine if the agents bundled with VCS One meet your resource management requirements.
If you have a resource that can not be managed by existing agents, it may be necessary to create a custom agent, or to use the application agent with custom start and stop scripts.
- Collect agent specific attributes.
Most agents required specific information at the individual resource level in order to control the resource. For example, the Mount agent requires a specific file system name, and the IP agent requires a specific IP address.
- Set up your Policy Master cluster hardware.
See *Veritas Cluster Server One Installation Guide*.

- Collect information about the Policy Master cluster for the installation scripts.
 - Identify the names of the systems in the Policy Master cluster.
 - Choose a number (0-65535) to represent the Policy Master cluster ID. If there are other Veritas Cluster Server (VCS) clusters in the environment, choose a unique cluster ID to differentiate this Policy Master cluster.
- Verify network connectivity, and collect network information for the installation scripts.
 - Test the Policy Master can connect to the client systems with operating system tools, such as the `ping` command.
 - Identify the names of the two Policy Master cluster interconnect NICs on each Policy Master system.
 - Identify the virtual IP address for the Policy Master cluster systems.

Implementing

This phase summarizes the steps for implementation and installation of VCS One. This phase should occur only after planning is complete and all preparations have been completed.

See *Veritas Cluster Server One Installation Guide*.

The following are the general steps for implementation:

- Enable secure shell communications on each client system.

This is one of the few tasks that may require accessing every system of the VCS One cluster.
- Configure shared storage on the Policy Master nodes, and test the disks for SCSI-3 compliance.

Before installation, collect the storage information you will need to configure shared storage:

 - Identify the name of the mount point for the shared storage.

If you need a mount point for the Network Appliance Filer (NetApp Filer), mount the NFS point on a local directory on the system where you will install the Policy Master.
 - Identify the type of file system used on the shared storage.
 - Identify the name of the disk group to store the database (if Storage Foundation configuration is not performed by the installer).

- Identify the name of the disk that will be part of the disk group to store the database (if Storage Foundation configuration is not performed by the installer). Use short disk names.
- Identify the name and size of the volume where the database is to be created on external storage (if Storage Foundation configuration is not performed by the installer).
- Set up I/O fencing on the Policy Master nodes.

Note: A response file can be used to allow for unattended installations on multiple client systems.

- **Install the Policy Master**
The installation names the Policy Master cluster `vcstone_cluster`.
If you do not already have Veritas Storage Foundation installed, you will be prompted to install it when you install the VCS One Policy Master. There is no need to separately install Storage Foundation.
If you will use the Network Appliance Filer (NetApp Filer), you will be prompted to configure this during the installation of the VCS One Policy Master.
- Install the VCS One client daemon software on the client systems.
- Install the high availability agents.
- Verify the installation.
- [Optional] Configure shared storage hardware as appropriate if the managed applications will be configured to move between systems.

Configuring and verifying

This topic outlines the process the administrator can follow in configuring the Policy Master cluster and the VCS One cluster.

Configuring the Policy Master cluster

Make the following considerations to configure the Policy Master cluster:

- The `VCSONeWeb` resource in the Policy Master service group is not set as a critical resource by default. This means that if the `VCSONeWeb` resource crashes, VCS One does not initiate failover of the of the Policy Master service group.
- ◆ Type the following commands when the VCS cluster is up and running to make the `VCSONeWeb` resource a critical resource

```
/opt/VRTSvcs/bin/haconf -makerw  
/opt/VRTSvcs/bin/hares -modify VCSOneWeb Critical 1  
/opt/VRTSvcs/bin/haconf -dump -makero
```

- Tune attributes of the Policy Master service group.
See [“Tuning attributes of the Policy Master service group”](#) on page 562.

Configuring the VCS One cluster

The VCS One cluster configuration can be modified via the following methods:

- Graphical user interface, also known as the console.
- Command line interface
- XML files edit followed by importing the new files into the database.
If you edit the XML files directly, the `vcsonencrypt` command can be used to generate encrypted passwords.

Each step should be verified as it is completed.

- Start VCS One.
 - Start the VCS One Web Console.
 - Log in to the VCS One software.
- Configure VCS One cluster level attributes.
 - Set or accept the default value of the `PrecedenceOrder` attribute.
 - Set or accept the default value of the `FragmentationPolicy` attribute.
 - Add systems.
 - [Optional] Set system `Capacity` attribute.
 - [Optional] Set `DefaultPlatform` attribute.
See [“DefaultPlatform”](#) on page 684.
 - [Optional] Define the organizational units and extended attributes, if needed.
 - In a VCS One cluster that contains more than a few thousand resources, you may decide to change the default monitoring of the PMSG
See [“Tuning attributes of the Policy Master service group”](#) on page 562.
- Configure the VCS One cluster systems.
 - [Optional] Define `Capacity` for each client system.
 - Start `vcsonclientd` on each client system. Verify it is running.
- Configure the managed applications.
 - Add resources.
 - Define resource dependencies.

- Create service groups and then add resources.
- [Optional] Define Load for each service group.
- [Optional] Define Priority for each service group.
- [Optional] Define Compatibilities or Incompatibilities for each service group.
- [Optional] Link service groups as necessary for service group dependencies.
- [Optional] Define the organizational unit and extended attribute values, if you have not already done so, and move them under the pre-defined Organization Tree.

Note: It is a best practice to manually move the application outside of VCS One control before testing movement under VCS One control.

- Configure Notification.
 - SMTP
 - SNMP
- Assign User Permissions.
 - Designate privileges to users based on their job tasks, such as operator level privileges.
- Customized Management: Sets
 - [Optional] Assign this application to the proper department or line of business.
- Configure Log Files
 - Configure the level of logs to collect.
- Custom configuration tasks for your environment.

Designing roles and privileges for users

This chapter includes the following topics:

- [About designing roles and privileges for users](#)
- [About users and the Organization tree](#)
- [How you manage users using the Organization Tree](#)
- [About user permissions in the organization tree](#)

About designing roles and privileges for users

When a user is created, the user must be assigned a role. A role is a named collection of privileges. Privileges define what actions the user can perform, such as adding a system to the VCS One cluster or modifying a service group.

When a user tries to perform an operation, VCS One authorizes the user's action against the privileges associated with the user's role.

VCS One has both predefined roles and the ability to create custom roles. A reference is available of all the VCS One cluster privileges and pre-defined roles.

See "[Reference of privileges](#)" on page 627.

Roles and user privileges that correspond to virtualization may be visible to the user. This capability is not supported in the current release, but is planned for a future release.

About user groups

VCS One allows existing groups of users already configured in the data center, such as with NIS or LDAP, to be represented by a user group object. VCS One identifies the membership of the external user to a VCS One user group using Symantec Authentication Services (AT). Roles and privileges are assigned to a user group in the same manner as they are assigned to an individual user.

The association of a user with a user group is dynamic. The user is implicitly associated with all the groups specified in the user credentials. The credentials of the user includes the credentials of the user group to which the user belongs.

About privileges

Because every action in VCS One requires a privilege, the privileges are organized into privilege categories for ease of administration. The privilege categories sort the individual actions the role can perform by the type of object the action is related to.

For example, the System Privilege category contains privileges to freeze a system or change the value of the SystemList attribute; the Notifier Privilege category contains the privilege to change the notification settings.

The user's total privileges are a union of the privileges explicitly granted to the user and the privileges granted to any user group of which the user is a member.

To give a user every available privilege, assign the user both the ServerFarmAdministrator and ServerFarmObjectAdministrator roles.

For business policy automation rules, note the following guidelines:

- A user can own a rule if that user or at least one of that user's user groups are explicitly added to the VCS One configuration.

This holds true even if the user is root on the Policy Master node, that user or its user groups should be added explicitly.

- Assign explicit privileges to that user to perform the actions the rule invokes.

A user with sufficient privileges may disable a user or user group. A disabled user or any user belonging to a disabled user group has the following characteristics:

- Will have all privileges revoked.
- Will not be able to perform any of the actions associated with the user or user group.
- Will not be able to log in through the VCS One console.

At the point the effective privileges of the user is zero, the user is logged out of the console.

A user with sufficient privileges may re-enable a disabled user to reinstate privileges.

What information identifies a user or user group

When an administrator adds a user or user group to the VCS One cluster, the following information is configured:

- Username - identifies a specific user in the format name@domain
- First name and last name of the user
- Email address - allows a user to be notified by email
- SNMP IP address - allows the user to receive notification of VCS One events

Additionally each user has an associated role and is attached to an organization unit node in the Organization Tree.

About roles

A role signifies a set of privileges for a user. You may assign predefined roles or create new custom roles. A user may be assigned various roles. The privileges contained in the role provide the ability to perform an operation, such as add, modify or delete, on an object, such as a group, resource or organization tree node.

The following roles are predefined in VCS One.

ServerFarmAdministrator

ServerFarmObjectAdministrator ServerFarmObjectOperator ServerFarmObjectGuest

SystemAdministrator	SystemOperator	
VObjectAdministrator	VObjectOperator	
VFrameAdministrator	VFrameOperator	
PFrameAdministrator	PFrameOperator	
ContainerUserFarm	ContainerUserGroup	
GroupAdministrator	GroupOperator	
CSGAdministrator	CSGOperator	
ResourceAdministrator	ResourceOperator	
UserAdministrator	UserOperator	
ZoneUserFarm	ZoneUserGroup	
VCOneClientFarm	VCOneClientSystem	VCOneClientGroup
VCOneClientPFrame	VCOneClientVFrame	

You may update the operations that can be performed by the following roles:

VCOneClientFarm	VCOneClientSystem	VCOneClientGroup
ZoneUserFarm	ZoneUserGroup	VCOneClientPFrame
ContainerUserFarm	ContainerUserGroup	VCOneClientVFrame
ServerFarmObjectAdministrator	ServerFarmObjectGuest	

You may not update the operations that can be performed by the other predefined roles, but you can develop a custom role to accommodate the needs of your environment.

Privileges are sorted into privilege categories, also called role types, which describe to what type of object the privileges correspond. The following privilege categories exist:

Farm	Object	System
Group	Composite Service Group	
VObject	PFrame	VFrame
Resource	User	Organization tree
Automation	Notifier	

In order to receive notification about an object, a user must have both Notifier privileges and some other privilege on that object. A user that has only the Notifier privilege on an object will not receive notifications.

About users and the Organization tree

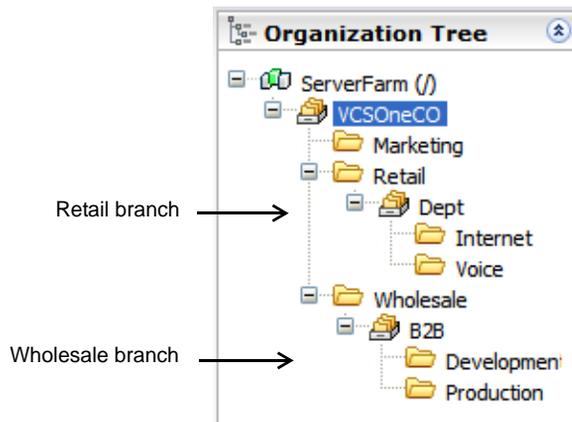
An Organization Tree is a logical hierarchical structure of the VCS One cluster that is used to delineate user views and privileges.

Systems, service groups, and users are placed into particular areas of the Organization Tree. The user privileges for those systems and service groups depend on where they are in the tree. As the tree changes, privileges are dynamically updated.

For example, in the sample Organization Tree in [Figure 10-1](#), an operator can have the privilege to online or offline a service group on any system in the Wholesale branch of the tree. If additional systems are added to the Wholesale branch, that user's privileges are automatically updated to include the new systems.

Additionally, a user in the Wholesale branch of the tree has no visibility into the Retail branch of the tree, unless privileges are explicitly granted.

Figure 10-1 Sample Organization Tree

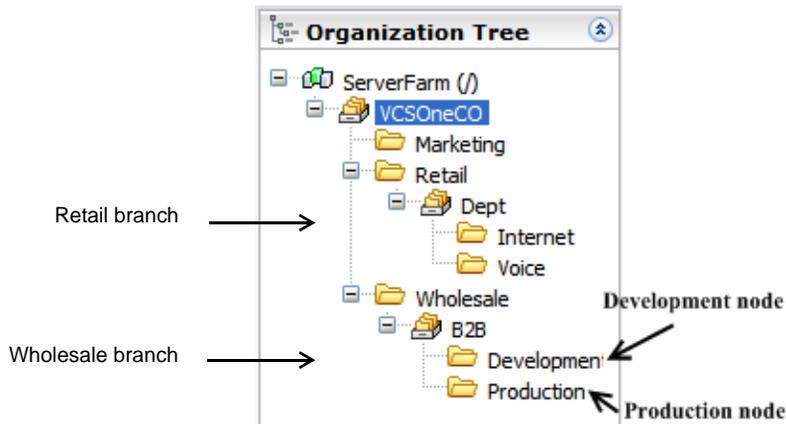


How you manage users using the Organization Tree

The following structure of the Organization Tree help you manage what a user can see and do in the VCS One cluster:

- The Organization Tree subdivides the VCS One cluster into OUNames (branches) and OUValues (nodes).
The sample Organization Tree in Figure 10-2 has three top-level division branches, Marketing, Retail, and Wholesale. Inside the Wholesale division branch, there are two projects under the B2B branch called Development and Production.

Figure 10-2 Organization Tree branches and nodes



- Objects are attached to the Organization Tree at particular nodes. In this example, some systems and service groups are attached to the Development node, and other systems and service groups are attached to the Production node.
 - Attach a user to the organization tree at the node that corresponds to the level of privilege you want them to have to view and perform operations in the VCS One cluster.
 - A user can be assigned privileges over objects and OUs at or below the node where the user or user group is attached.
 - The operations the user is able to perform are in accordance with the role and corresponding privileges assigned to the user.
 - A user is able to view the direct path back to the top of the tree, the ServerFarm (/) node.
- For example, if you want UserA to have privileges only on systems attached to the Production node, you must ensure the following:
- Attach UserA at the Production node.
 - Assign related system privileges to UserA.

- Determine UserA is not a member of a user group that is attached at or above the Development node.

UserA would not be able to see that the Development node exists. You may want this type of configuration if a user has the role of GroupOperator, and you only want to user to be able to online or offline the service groups running on the production systems.

If you want UserB to have privileges on both the Production and the Development systems, you must attach the user to the Wholesale node and assign relevant system privileges for UserB on the Wholesale node.

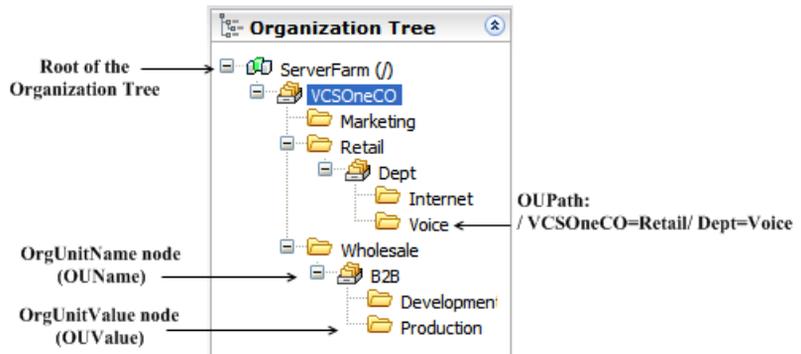
An example of this configuration is a user that has the role of ServerFarmObjectAdministrator. UserB can move systems from Development to Production if there is a business need.

In this case, UserB privileges would be dynamically updated to have SystemOperator privileges on any new systems attached at or below the Wholesale node.

About the architecture of the Organization Tree

Figure 10-3 shows the architecture of an Organization Tree.

Figure 10-3 Architecture of the Organization Tree



About organization units

Each VCS One cluster may have one Organization Tree, which is built in the order of a tree hierarchy. The tree hierarchy is made up of multiple organization units that form the nodes of the Organization Tree.

Each organization unit node in the Organization Tree is one of the following types:

- OrgUnitName (OUName)

OUNames define the branches or categorization of the Organization Tree. An OUName has one or more OUValues as child objects in the Organization Tree. An OUName can not have another OUName as a direct child object. In the sample Organization Tree the OUName nodes are **VCSOneCO**, **Dept**, and **B2B**.

- OrgUnitValue (OUValue)

An OUValue denotes the value of an OUName. An OUValue can have at most one OUName node as a child object in the Organization Tree.

In the sample Organization Tree the OUValue nodes are **Marketing**, **Retail**, **Wholesale**, **Internet**, **Voice**, **Development**, and **Production**.

Users, user groups, systems, and service groups are attached only at OUValue nodes in the Organization Tree.

The number of OUName and OUValue nodes appropriate for your environment is determined by how you want to limit user privileges on systems and service groups:

Use the following guidelines to help you decide whether to create an Organization tree hierarchy.

- If you want to have all administrators in your organization have ServerFarmAdministrator privileges on all systems and service groups, you can attach all systems and service groups at the ServerFarm(/) level.
- If you want to compartmentalize a user to only have privileges on a specific set of systems, you must create an organization unit structure.

In VCS One, the Serverfarm(/) is an implied OUValue. To build an organization unit structure, create an OUName as the first object under this OUValue. Add additional OUValues as needed to the first level OUName. In [Figure 10-3](#), VCSOneCO is the first level OUName under the implicit OUValue of (/).

More information is available on building an Organization Tree.

See [“How to build an organization tree”](#) on page 508.

About paths in the Organization Tree

An Organization Tree path is denoted by a list of OUName=OUValue pairs, separated by a forward slash (/).

The following examples are valid paths in the Organization Tree in [Figure 10-3](#).

- /VCSOneCO=Retail
- /VCSOneCO=Wholesale
- /VCSOneCO=Wholesale/B2B=Development

About user permissions in the organization tree

User permissions operate with the following criteria:

- A user's permissions are relevant to the node in the organization tree where the user, or a user group that the user is a member of, is attached.

The level of privileges assigned is for the node the user is attached at and all the nodes below that node in the organization tree.

In [Figure 10-4](#), if a user is attached at the Production node, then privileges can be assigned only to objects and OUs at or under the Production node. So, the user can be made a GroupAdministrator for the Production node but not the Development node. Similarly, a user attached at the Wholesale node can be made a GroupAdministrator for either the Development node or the Production node or the Wholesale node, or for all the three nodes.

Figure 10-4 Sample organization tree



- Movement of objects in the organization tree from one node to another can change the users that have permission to perform actions on those objects.
- A user's view of the organization tree is filtered by where they are attached. A user can view all of the organization tree below where they are attached. Above the user, the only part of the organization tree a view will view is the direct line back to the root of the tree. In [Figure 10-4](#), a user attached at Development node will see following path /VCSOneCO=Wholesale/B2B=Development. This same user would not be able to view the Retail branch of the tree or even the Production node unless given separate specific permissions.

Designing actions taken after a fault

This chapter includes the following topics:

- [About designing the actions taken after a fault](#)
- [Configuration examples of fault handling behavior](#)

About designing the actions taken after a fault

Controlling the actions of VCS One when a fault occurs is configurable with attributes of the following objects:

- Resource
- Service Group
- System

When a fault occurs these settings control the immediate offline actions. The related subsequent online actions and any necessary kick out actions can be controlled manually or be automatically executed.

See [“About designing application placement policy”](#) on page 274.

You can use the VCS One Simulator to simulate actions that are taken after a fault.

See [“About the Simulator”](#) on page 174.

Resource level control

The resource level attribute ResFaultPolicy controls the behavior of a resource in the event of a fault.

You can set a fault policy uniformly on all resources in a service group or set fault policy for each individual resource.

[Table 11-1](#) lists the possible values for ResFaultPolicy:

Table 11-1 ResFaultPolicy values for resource level control of fault behavior

Value	Behavior of resource when faults
FaultPropagateAll	<p>Default value of ResFaultPolicy.</p> <p>Agent calls clean entry point. The value of the resource attribute RestartLimit is checked:</p> <p>If RestartLimit is zero (default value), the resource state is marked as <code>FAULTED</code>. The fault is propagated and all group resources transition to the <code>OFFLINE</code> state. The service group changes to the <code>OFFLINE FAULTED</code> state.</p> <p>If RestartLimit is greater than zero, VCS One attempts to restart the resource RestartLimit number of times.</p> <p>If the resource does not successfully restart, the fault is propagated and all group resources transition to the <code>OFFLINE</code> state. The service group changes to the <code>OFFLINE FAULTED</code> state.</p> <p>The value of the GrpFaultPolicy attribute determines failover of the group</p>
FaultPropagateParent	<p>If RestartLimit is greater than 0, VCS One attempts to restart the resource RestartLimit number of times.</p> <p>If the resource does not successfully restart, the fault is propagated to the parent resources. Parent resources are the resources that are higher up in the resource dependency tree.</p> <p>Fault is propagated to parent resources in the <code>ONLINE</code> state. If there are any parent resources in the <code>OFFLINE</code> state, the fault is not propagated beyond that resource.</p> <p>If the fault is propagated to a resource where ResFaultPolicy = FaultPropagateAll, then all group resources transition to the <code>OFFLINE</code> state, and the service group changes to the <code>OFFLINE FAULTED</code> state.</p>
FaultHold	<p>Agent calls clean entry point.</p> <p>If RestartLimit is greater than 0, VCS One attempts to restart the resource RestartLimit number of times.</p> <p>If RestartLimit is 0, the resource is reported as faulted to the Policy Master. The service group state changes to <code>PARTIAL</code>. The fault is not propagated further.</p>

Table 11-1 ResFaultPolicy values for resource level control of fault behavior

Value	Behavior of resource when faults
FaultNone	<p>Agent does not call the clean entry point. The resource state is marked as ADMIN_WAIT, and the group waits for administrative action.</p> <p>The service group does not failover until the resource fault is removed and the ADMIN_WAIT state is cleared.</p> <p>Exception: If the parent resource has the value FaultPropagateAll and the service group the resource is in has the GrpFaultPolicy attribute set to Failover, the agent overrides the ADMIN_WAIT state and invokes the clean entry point.</p> <p>See “Clearing resources in the ADMIN_WAIT state” on page 389.</p>

If two resources in the same service group have different values for ResFaultPolicy, the value of the most recently faulted resource determines the behavior of all of the group’s resources.

- Assume the policy for the child resource is FaultPropagateAll and for the parent resource is FaultHold. If the child faults, VCS One brings the service group offline, whereas if the parent faults, the FaultHold policy prevails.
- If resourceA with ResFaultPolicy=FaultNone faults, it goes into ADMIN_WAIT state, and waits for action by an administrator. If resourceB in the same service group faults with ResFaultPolicy=FaultPropagateAll, VCS One automatically clears the ADMIN_WAIT state of resourceA. This logic enables VCS One to take action that is based on the FaultPropagateAll setting.

Service group level control

The group level attribute GrpFaultPolicy controls whether or not a service group attempts to fail over to another system. This policy is active only after the resource level policy setting of ResFaultPolicy=FaultPropagateAll concludes with a faulted group.

[Table 11-2](#) lists the possible values for GrpFaultPolicy:

Table 11-2 GrpFaultPolicy values for group level control of fault behavior

Value	Behavior of group when faults
Failover	Default value of GrpFaultPolicy. The service group attempts to failover to the next best target system. Target choice is based on Advanced Workload Management policy.
NoFailover	The service group does not attempt to failover to another server.

In case of a group fault, the process to take the faulted group offline is initiated only after all of its firm and hard parent groups are taken offline.

System level control

The service group attribute NodeFaultPolicy controls whether or not a service group attempts to fail over in the event of a system fault.

[Table 11-3](#) lists the possible values for NodeFaultPolicy:

Table 11-3 NodeFaultPolicy values for system level control of fault behavior

Value	Behavior of group when system faults
Failover	Default value of NodeFaultPolicy. Set the state of the group as offline and fail over the group.
NoFailover	Set the state of the groups as offline, but do not attempt failover

The NodeFaultPolicy supersedes GrpFaultPolicy. For example, if a service group is taken offline or faults on a system and does not fail over because the value of GrpFaultPolicy=NoFailover, that group is still be targeted for failover if the system faulted.

Configuration examples of fault handling behavior

The following examples outline attribute values to be set to accomplish the wanted behavior:

Table 11-4 Attribute values to configure fault handling behavior

To configure this behavior...	Set these attribute values...
To configure a group in the VCS One cluster to not failover without manual intervention.	Set the following attributes: <ul style="list-style-type: none"> ■ GrpFaultPolicy=NoFailover ■ NodeFaultPolicy=NoFailover
To configure a group to not fail over a group in the event of a fault, but if the system faults fail over all groups on that system.	Set the following attributes: <ul style="list-style-type: none"> ■ GrpFaultPolicy=NoFailover ■ NodeFaultPolicy=Failover
To configure that when a resource faults, the group is taken offline but not failed over	Set the following attributes: <ul style="list-style-type: none"> ■ ResFaultPolicy=FaultPropogateAll ■ GrpFaultPolicy=NoFailover or <ul style="list-style-type: none"> ■ ResFaultPolicy=FaultPropogateAll and have only one system designated in the group's SystemList attribute.

Designing attribute values using variables

This chapter includes the following topics:

- [About designing attribute values using variables](#)
- [Examples of using a resource variable](#)
- [What can be defined using a resource variable](#)
- [Where a variable can be used](#)
- [Resource variable syntax](#)
- [Where a variable cannot be used](#)
- [Design implications of resource variables](#)

About designing attribute values using variables

VCS One allows you use a variable to define an attribute value. This variable is called a resource variable.

The use of variables in attribute definitions has the following benefits:

- You can use extended attributes with predefined mandatory values as variables to obtain standardization and consistency of terminology.
- You can more easily manage resources by decreasing the number of localized attributes.

Examples of using a resource variable

This topic includes three examples for how you might use resource variables in your environment to reduce the need to enter the same information multiple times, minimize the risk of typographical errors, and simplify configuration edits.

Example 1

A typical service group contains one disk group with multiple volume resources and mount resources. When you set up this configuration, you must provide the name of the disk group several times.

[Table 12-1](#) shows an example of this configuration:

Table 12-1 Typical service group configuration example

Type of resource	Attribute of resource	Sample value of attribute
DiskGroup	DiskGroup	exmpldg
Volume	DiskGroup	exmpldg
Mount	BlockDevice	/dev/vx/dsk/exmpldg/volume

To improve your efficiency, you can define an extended attribute for a group that contains a DiskGroup resource. Use a resource variable in place of the disk group name in each of the resource definitions. The disk group name is entered once for the extended attribute. As you create new volume resources and mount resources, you do not need to retype the disk group name. Additionally, if the disk group name changes, you only need to make one update at common extended attribute definition. Without using this method, you would have to update each of the DiskGroup, Volume and Mount resources.

Table 12-2 shows the same example using resource variables and the following common extended attribute:

DGName = exmpldg

Table 12-2 Service group example using resource variables

Type of resource	Attribute of resource	Sample value of attribute
DiskGroup	DiskGroup	@{DGName}
Volume	DiskGroup	@{DGName}
Mount	BlockDevice	/dev/vx/dsk/{DGName}/ <i>volume</i>

Example 2

When you use localized attributes, the attributes become harder to maintain as the number of objects grow. Resource variables can make localized attributes easier to maintain.

This example is of a service group that has a Mount resource that runs on the Solaris operating system.

In a non-failover environment, you may define the required resource attributes of the Mount resource using the following definitions:

```
Mount resource name = mount_app01
Block device = /dev/hda
FscckOpt = -y
FSType = vxfs
MountPoint = /mnt/solaris/10
```

In an environment where the application may move between systems, you may want the value of the MountPoint attribute to be different on different systems. In this case, you can localize the MountPoint attribute.

To localize the MountPoint attribute means that you make a local value for the MountPoint attribute for each system on which the service group may be online. When you localize the attribute, the value of the MountPoint attribute can change depending on which system the service group is online on.

In this environment, you may define the required attributes using the following definitions:

```
Mount resource name = mount_app01
Block device = /dev/hda
FscckOpt = -y
FSType = vxfs
MountPoint = /mnt/solaris/10 (definition on sys1)
MountPoint = /mnt/solaris/9 (definition on sys2)
```

When there are many systems that the Mount resource may run on, the list of localized resource attributes becomes long and hard to manage.

When you add the use of resource variables to this example, you may define an system extended attributes that is named OS_VERSION on each system. Then you may define the attributes using the following definitions:

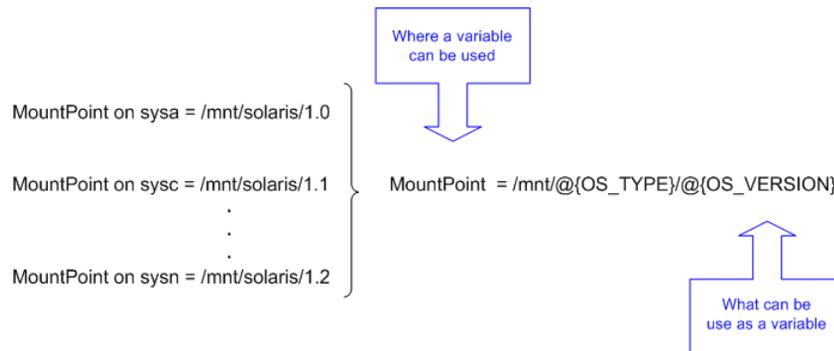
```
Mount resource name = mount_app01  
Block device = /dev/hda  
FsockOpt = -y  
FSType = vxfs  
MountPoint = /mnt/solaris/@{OS_VERSION}
```

In this example, on each system where the Mount resource runs, the value of the extended attribute OS_VERSION would replace the variable @{OS_VERSION} when the MountPoint value is parsed.

When a new system is added to the SystemList, you only need to set the extended attribute values for the system. You do not need to edit the Mount resources.

Figure 12-1 shows how the multiple values of the MountPoint attribute can be converted into one value that uses resource variables.

Figure 12-1 Example of using resource variables



Example 3

Consider a parallel service group containing NIC resources that may run on five different systems.

Table 12-3 shows an example of this configuration:

Table 12-3 NIC resource configuration example

Type of resource	Attribute of resource	System	Sample value of attribute
NIC	Device	System1	en0
NIC	Device	System2	en1
NIC	Device	System3	en0
NIC	Device	System4	en2
NIC	Device	System5	en1

The next added system requires that you edit the Device attribute for each NIC resource to add to the localized attribute. The configuration is simplified if you define a system level extended attribute and use a resource variable inside the NIC resource definition.

Define the following system extended attribute:

ProdNIC = en0

Table 12-4 shows an example of how to use the resource variable in this configuration:

Table 12-4 NIC resource variable configuration example

Type of resource	System	Attribute and Value of attribute
NIC	SystemN	Device = @{ProdNIC}

When a new system is added to the SystemList of the parallel service group, you only need to set the extended attribute value for the system. You do not need to edit the NIC resources.

What can be defined using a resource variable

The following attributes can be defined using a resource variable instead of a static value:

- System built-in attributes
Must be of type-dimension: string-scalar or string-association.
- Service group built-in attributes
Must be of type-dimension: string-scalar or string-association

- System extended attributes.
- Service group extended attributes
- Common extended attributes that pertain to system or service group values.
See “[About extended attributes](#)” on page 517.

Attribute values have one of the following dimensions:

scalar	A scalar has only one value. If the data-type is string, you may define this value using a resource variable.
association	An association is an unordered list of key-value pairs. If the data-type is string, the value field of the association may be defined using a resource variable. The key (name) field may not be a variable. If the value field is defined using a resource variable, then the value may not be deleted until the reference to the variable is removed.

Attribute values may not use the following dimensions:

vector	A vector is an ordered list of values. Each value is indexed using a positive integer [zero or higher].
keylist	A keylist is an unordered list of unique strings in that list.

See “[System attributes](#)” on page 702.

Where a variable can be used

A variable can be used in the definition of a resource value if the resource attribute is type=string.

The type and dimension of predefined resources in VCS One can be found in reference tables in the following documents:

- Engine resources.
See “[Attributes reference](#)” on page 677.
- Resources that are part of the agents that are shipped with VCS One
See [Veritas Cluster Server One Bundled Agent’s Reference Guide](#).

Resource variable syntax

The following syntax forms denote a resource variable:

- `@{object.attribute_name}`
- `@{object.ea}`

Use the following information to replace the appropriate variables:

object	<p>The type of object. Options are system or group.</p> <p>The default value is system. When using a system object, you may leave off the object classification and use the syntax <code>@{attribute_name}</code>.</p>
attribute_name	<p>The name of the built-in system or group attribute whose value this variable replaces.</p> <p>If the attribute is of dimension association, the format of this variable is <code>attribute_name%association_key</code>.</p> <p>For example, <code>@{system.SysInfo%OsVersion}</code></p>
ea	<p>The name of the extended attribute whose value this variable replaces. Must be one of the following types of extended attributes:</p> <ul style="list-style-type: none"> ■ System extended attribute ■ Group extended attribute ■ Common extended attribute <p>If it is a common extended attribute, it must pertain to a system or service group value.</p>

You can use the `^` symbol as an escape character in the VCS One console and command-line interfaces. To escape a variable in the resource attribute value, place the `^` symbol before the variable.

For example, in the following command, SysName not treated as a variable.

```
hares -modify r1 pathname /tmp/^{SysName}

hares -value r1 pathname
/tmp/^{SysName}
```

More information is available on how to configure resource variables.

See [“Defining an attribute value with a resource variable”](#) on page 393.

Where a variable cannot be used

A variable cannot be used in the following ways:

- You cannot use a variable in the definition of a resource type attribute value. Specifically, you cannot use a variable in the types.xml file or in an agent's version of a types.xml file, such as oracletype.xml.

- You cannot use a variable in specifying the default value of a resource attribute.
- You cannot use a variable in localized resource attributes.

Design implications of resource variables

When a static value of a resource is replaced with a resource variable, some operations affect the value of the variable.

For example, you define an extended attribute at a node in the organization tree. The definition of the extended attribute applies to objects, such as systems and service groups, that are attached at that node and below in the organization tree.

If an extended attribute is used as part of a resource variable definition, operations that change or invalidate the value of the extended attribute also change or invalidate the value of the resource.

If an extended attribute is used as part of a resource variable definition, the following rules apply:

- You may not delete any organization tree node that has that an extended attribute defined using a resource variable.
To delete, you must remove the reference to the resource variable.
- You may not move a group or a system between nodes in the organization tree unless the extended attribute is defined at both nodes.
- If you move a group or a system between nodes in the organization tree where the extended attribute is defined, you must also explicitly update the value of the resource variable to ensure the value reflects the move.
See [“Updating the value of a resource variable”](#) on page 395.
- Using variables in association keys and keylists may lead to duplicate or empty keys. After you modify the values, you may use the following command to verify the issue is fixed.

```
hares -verifyvars resource attribute
```

Designing service groups

This chapter includes the following topics:

- [About designing service groups](#)
- [About bringing running applications under VCS One control](#)
- [Designing the name of a service group](#)
- [Designing the Priority of a service group](#)
- [Designing application movement within a local site](#)
- [Designing multi-tier applications](#)
- [Design rules of composite service groups](#)
- [Designing service groups that use off-host resources](#)
- [Designing service groups that run in Solaris zones](#)
- [Designing service groups that run in AIX WPARs](#)

About designing service groups

A service group is a virtual container that contains all the hardware resources and software resources that are required to run the managed application.

A composite service group is a collection of objects. Use composite service groups to control several objects as one managed business service.

In this release, service groups are the only CSG-supported object.

Managed applications planning

Use the information collected from the applications in your current environment and this topic to outline the plan for your managed applications.

For each application that will be managed by VCS One, do the following:

- Determine the list of system(s) the application will run on. The following considerations will determine this list:
 - System configuration.
Choose the appropriate operating system, number and speed of CPUs, and memory requirements of the application. Consider any performance criteria or service level agreements (SLA) that must be met.
 - The capability of the application to move between systems for maintenance or availability.
If the application is to be managed locally on one server, for start, stop, and monitor activities, this list will be one system. If there are additional systems that will be included as spares for the managed application (the application will be capable of movement, either manual or automated), there will be multiple systems identified. Choose systems that have shared storage between them if the application has movement capability, either manual or automated.

Note: This list of systems will become the value for the SystemList attribute of the managed application's service group.

- Use the application resource requirements information you collected to build a resource dependency tree.
See [“Collect application information”](#) on page 205..
- Determine the resource type of each VCS One resource.

Note: The list of resource types necessary for each resource will become the list of agents required to support the managed application.

See [“Designing service groups”](#) on page 241.

Defining a service group

Once you have figured out your resource dependency tree, you are ready to move to the next step to create your service group. When you create a service group, you define the following items:

- A unique name of the service group across the VCS One cluster
- The list of systems on which the group is allowed to run
- Definitions of the key service group attributes that define, for example, its priority, its compatibility with other service groups, and its load requirements
- The list of resources that establish the managed application, and any specific configuration information that is required for those resources
- The dependency relationship between the resources
- The dependency relationship with other service groups, if applicable

Consider the following design principles when building your service groups:

- A service group can have multiple resources of the same type. For example, two different disk resources can exist in the same service group.
- Resource names must be unique within a service group. However, it is not necessary for them to be unique across service groups in the same VCS One cluster. Two different service groups can have resources with the same name.
- If there is more than one service group that is defined on a system, one group may fail over without affecting the others.

Defining service group dependencies

Use the application dependency information you collected to build an service group dependency tree. For example, a web based application may require that an Oracle application backend database is running before it starts up.

Consider the following design principles when designing your service groups dependencies:

- The type of the service group dependency affects how the service group may start, stop, and move to another system.

See [“Types of service group dependencies”](#) on page 249.

Service group dependencies have the following general characteristics:

- Five tiers of service group dependencies are supported.
- A service group can depend on up to five child service groups.
- A service group can have any number of parent service groups.

Shared storage

A service group can only be started on a client system that has access to its associated data files.

If application movement is configured in the VCS One cluster, the associated data files needed by the managed application must be available from any system configured to host service group. Typically, this requires some form of shared storage. VCS One supports shared storage on NAS and SAN. To provide the best possible data integrity, configure shared storage to allow VCS One to restrict access to only the active node hosting an application. On NAS based storage, VCS One provides the ability to control NFS exports from a NetApp based NAS filer. On SAN based storage, VCS One uses Veritas Storage Foundation to control SCSI-III reservations at the disk group level.

Additional planning for applications in failover environments

The following attributes may be independently set for a service group:

- Load
- Compatibility
- Priority

One or more of the following tasks may be appropriate if the application is configured to be able to move between servers for maintenance or availability:

- Determine the resources required by the application (Load) with respect to the resources available on the servers (Capacity).

Typically the Load of an application represents the number of CPUs and the amount of physical memory required for the application.

See [“About service group Load and system Capacity for physical systems”](#) on page 280.

Note: These settings become the values of the Load attribute of the service group and the Capacity attribute of the client systems.

- Determine the compatibility of each application with other applications in the VCS One cluster. Compatibility is defined with one of the following criteria:
 - Compatible with all other applications

- Compatible with no other applications
- Compatible with a specific list of other applications
- Not Compatible with a specific list of other applications

See [“Application relationships through service group compatibility”](#) on page 278.

Note: Group compatibility privilege is effective only at the root (/) of the Organization Tree. This means that compatibility privilege granted at other OU nodes does not have any effect. You may not modify group compatibility at OUValues other than / even if you have the privileges at those OUValues unless you also have the privilege at /.

- Determine the fault behavior of the resources, service groups and systems. See [“Designing actions taken after a fault”](#) on page 227.

About bringing running applications under VCS One control

You can bring applications that are currently up-and-running under the control of VCS One without stopping the application or incurring additional application downtime.

Once you create and configure the appropriate service groups and resources for the application, VCS One starts the respective application agents, detects that the application is currently running, and brings the service group and its resources online.

If certain resources are not brought online, check the resource attributes and probe the resources. The probe operation restarts the agent monitor cycle, which detects that the resource is running and marks the resource as online.

Designing the type of service group

You must decide what type of service group your application requires. All VCS One service groups are one of the following types:

- **Failover service groups**
Failover service groups are brought online on only one system at a time. They are used with applications that do not support simultaneous application data access by multiple systems.
- **Parallel service groups**
Parallel service groups are brought online on multiple systems simultaneously. They are used with applications that manage multiple application instances, which run at the same time without data corruption.

The service group attribute called `Parallel` defines the type of service group. See [“Parallel”](#) on page 716.

Designing the name of a service group

The following criteria describe the requirements of VCS One service group and composite service group names:

- The space character and the following special characters are not allowed in names of service groups or composite service groups:
`` ' \ " / \ = * + ? () { } [] $ # ^ ! % & , . . ; < > | ~ @`
- Service group names and composite service group names must be unique with in the VCS One cluster in which they run.
- Service group and composite service group names are case-insensitive.
- The description text of any VCS One object can not use a single quotation mark.

Note the definition of the composite service groups is placed after the definition of all other service groups in the `main.xml` file. This information is only important if you are a very experienced VCS One administrator and you edit the configuration file directly.

Designing the Priority of a service group

The `Priority` of the service group is a value that reflects the importance of the application to the business.

The `priority` of the service group is considered for allocation of VCS One cluster resources and failover target policy.

The service group attribute called `Priority` defines the priority of the service group. The `Priority` attributes uses a scale of 1 to 5, where `Priority = 1` is the highest priority.

See [“About Priority”](#) on page 277.

Designing application movement within a local site

Local application mobility considers whether or not the application will move between multiple systems in the same site.

Edit the `SystemList` attribute to configure the systems on which the service group may run.

- If the application will start and stop on one system, the SystemList attribute will have one system listed.
- If the application has failover or migrate capability, the SystemList attribute contains a list of all the systems on which the service group may run.

Several service group attributes provide the capability to custom design your failover policy.

See [“Designing actions taken after a fault”](#) on page 227.

Designing multi-tier applications

Multi-tier application design considers whether or not the application is dependent on other applications. If one application depends on another application’s state, you need to design service group dependencies between the service groups that represent each application.

A composite service groups does not have dependencies. Service group dependencies remain at the individual service group level.

See [“Defining service group dependencies”](#) on page 243.

About designing service group dependencies

A service group can be dependent on one or more other service groups.

Service group dependencies are used to configure multi-tier, inter-dependent stacks of applications. A common service group dependency is to have a web front-end application dependent on a finance application. If that same finance application is dependent on a database application, that comprises a three-tier service group dependency.

Because the service group is the complete stack of hardware and software components that are required to provide an application service to an end user, service group dependencies create more complex design and failover configurations.

Design rules of service group dependencies

Design rules of service group dependencies vary by the type of service group dependency configuration you use.

Table 13-5 depicts supported and unsupported service group dependency configurations.

Table 13-5 Supported service group dependency configurations

Parent	Child	Local			Global		
Failover	Failover	<i>Soft</i>	<i>Firm</i>	<i>Hard</i>	SOFT	<i>Firm</i>	<i>Hard</i>
Failover	Parallel	SOFT	FIRM	<i>Hard</i>	SOFT	<i>Firm</i>	<i>Hard</i>
Parallel	Failover	<i>Soft</i>	<i>Firm</i>	<i>Hard</i>	SOFT	FIRM	<i>Hard</i>
Parallel	Parallel	SOFT	FIRM	<i>Hard</i>	<i>Soft</i>	<i>Firm</i>	<i>Hard</i>
Legend							
SOFT	Bold text with green background dependencies are allowed under any condition						
<i>Soft</i>	Plain text with red background dependencies are not allowed under any condition						
<i>Soft</i>	<i>Italics</i> text with yellow background dependencies are allowed with restrictions.						

Rules that apply to all service group dependencies:

- Five levels of service group dependencies are supported.
- A parent service group can depend on up to five child service groups.
- A child service group can have unlimited parent service groups.
- A service group can be both a parent service group and a child service group, creating a multi-tier configuration.
- If a child service group has a hard service group dependency between itself and one parent, all the parent dependencies must be of type hard. A child must have all hard group dependencies or all non-hard group dependencies. See “[Types of service group dependencies](#)” on page 249.
- If a parent service group has a hard service group dependency between itself and a child service group, the parent service group may have only one child service group.
- Parallel parent service groups cannot be dependent on a global parallel child service group.
- Parallel parent service groups cannot be dependent on a local failover child service group. Cyclic service group dependencies can not exist.

- The following attributes should be the same for both child and parent groups when there is a local dependency between them:
 - CompatibleGroups
 - IncompatibleGroups
- The following attributes should always be the same for both child and parent groups:
 - Priority
 - Evacuate
 - Frozen
 - NodeFaultPolicy
 - GroupFaultPolicy
- The following attributes should be the same for both child and parent groups when the child and parent are of the same service group type [Failover or Parallel]:
 - SystemList
 - SystemZones
- The child group's SystemList attribute must always include all the systems in the parent group's SystemList attribute.

More information is available about service groups, service group dependencies, and how to design service group failover policy.

See [“About service groups and service group dependencies”](#) on page 38.

See [“About designing the actions taken after a fault”](#) on page 228.

See [“Mapping an application placement decision”](#) on page 282.

See [“Managing service groups”](#) on page 313.

See [“Service group attributes”](#) on page 712.

Types of service group dependencies

The dependency relationship between a parent service group and a child service group is called a link. The link between a parent service group and a child service group is characterized by the location of the service groups and the type of dependency.

- A dependency can be local or global.
- A dependency can be soft, firm, or hard with respect to the rigidity of the constraints that exist between parent and child service groups when they

are brought online or taken offline. A soft dependency specifies minimum constraints. A hard dependency specifies maximum constraints.

Local and global dependencies

The relative location of the parent service group and child service group determines whether the dependency between them is local or global.

Local dependency

In a local dependency, the parent service group depends on the child service group being online on the same system.

Global dependency

In a global dependency, an instance of the parent service group depends on one or more instances of the child service group being online on any system.

Soft, firm, and hard dependencies

The type of dependency defines the rigidity of the link between parent and child service groups.

Soft dependency

A soft dependency specifies minimum constraints while bringing the parent and child service groups online. The only constraint imposed by a soft dependency, whether the dependency is local or global, is that the child service group must be brought online before the parent service group is brought online. For example, in a local soft dependency, an instance of the child service group must be brought online on the same system before the parent service group can be brought online.

A soft dependency has the following characteristics:

- If the child service group faults, VCS One does not immediately take the parent service group offline. If the child service group cannot fail over, the parent service group remains online.
- When both service groups are online, either the child service group or the parent service group, can be taken offline, while the other remains online.
- If the parent service group faults, the child service group can remain online.
- When a link is created, the child service group need not be online if the parent service group is online. However, when both the service groups are online, their online state must not conflict with the type of link created.

Firm dependency

A firm dependency specifies more constraints when VCS One brings the parent or child service groups online or takes them offline. In addition to the constraint that the child service group must be online before the parent service group is brought online, the other constraints include the following:

A firm dependency has the following characteristics:

- If the child service group faults, the parent service group is taken offline, unless it is frozen at the time of the fault, in which case, it remains in its original state. If the child service group cannot fail over to another system, the parent service group remains offline.
- If the parent service group faults, the child service group can remain online.
- The child service group cannot be taken offline if the parent service group is online. The parent service group can be taken offline while the child service group is online.
- When a link is created, if both the parent and child service groups are online, their online state must not conflict with the type of link created.

Hard dependency

A hard dependency specifies maximum constraints when VCS One brings the parent or child service groups online or takes them offline.

A hard dependency has the following characteristics:

- If the child service group faults, the parent service group is taken offline before the child service group is taken offline. If the child service group fails over, the parent service group fails over to another system (or the same system for a local dependency). If the child service group cannot fail over, the parent service group remains offline.
- If the parent service group faults, the child service group is taken offline. If the child service group fails over, the parent service group fails over to another system (or the same system for a local dependency). If the child service group cannot fail over, the parent service group remains offline.

Service group dependency configurations

This section discusses service group dependency configurations. In the following tables, the term instance applies to parallel service groups only. For example, if a parallel service group is online on three systems, an instance of the service group is online on each system.

For failover service groups, only one instance of a group is online at any time. The default dependency type is Firm.

Failover parent / Failover child

Table 13-6 depicts the failover behavior for a failover parent and a failover child.

Table 13-6 Failover parent/Failover child

Link	Failover parent depends on ...	Failover parent is online if ...	If failover child faults ...	If failover parent faults ...
local soft	Failover child online on the same system.	Child must be online in order to online the parent. Once the parent is online, child group can migrate	Parent stays online. If child cannot fail over, parent remains online.	Child stays online.
local firm	Failover child online on the same system.	Child is online on the same system.	Parent taken offline. If child fails over to another system, parent migrates to the same system. If child cannot fail over, parent remains offline.	Child stays online.
local hard	Failover child online on the same system.	Child is online on the same system.	Parents taken offline before the child is taken offline. If child fails over to another system, parent migrates to another system. If child cannot fail over, parent remains offline.	Child taken offline. If child fails over, parent migrates to the same system. If child cannot fail over, parent remains offline.

Table 13-6 Failover parent/Failover child

Link	Failover parent depends on ...	Failover parent is online if ...	If failover child faults ...	If failover parent faults ...
global soft	Failover child online somewhere in the VCS One cluster.	Child is online somewhere in the VCS One cluster.	Parent stays online. If child fails over to another system, parent remains online. If child cannot fail over, parent remains online.	Child stays online. Parent fails over to any available system. If no system is available, parent remains offline.
global firm	Failover child online somewhere in the VCS One cluster.	Child is online somewhere in the VCS One cluster.	Parent taken offline before the child is offline. If child fails over to another system, parent is brought online on any system. If child cannot fail over, parent remains offline.	Child stays online. Parent fails over to any available system. If no system is available, parent remains offline.
global hard	Failover child online somewhere in the VCS One cluster.	Child is online somewhere in the VCS One cluster.	Parents taken offline before the child is taken offline. If child fails over to another system, parent is brought online on any system. If child cannot fail over, parent remains offline.	Child taken offline. If child fails over, parent migrates to another system. If child cannot fail over, parent remains offline.

Failover parent / Parallel child

Table 13-7 depicts the failover behavior for a failover parent and a parallel child.

Table 13-7 Failover parent/Parallel child

Link	Failover parent depends on ...	Failover parent is online if ...	If parallel child faults on a system ...	If failover parent faults ...
local soft	Instance of parallel child service group on the same system.	Child instance must be online to online the parent group.	Parent does not failover.	Parent fails over to another system and depends on the child instance there. Child instance remains online where the parent faulted.
local firm	Instance of parallel child service group on the same system.	Instance is online on same system.	Parent fails over to another system and depends on the child instance there.	Parent fails over to another system and depends on the child instance there. Child instance remains online where the parent faulted.
global soft	All online instances of parallel child service group remaining online.	One or more instances of the child service group are online somewhere in the VCS One cluster.	Parent remains online if child faults on any system.	Parent fails over to another system, maintaining dependence with all child instances.

Table 13-7 Failover parent/Parallel child

Link	Failover parent depends on ...	Failover parent is online if ...	If parallel child faults on a system ...	If failover parent faults ...
global firm	All online instances of parallel child service group remaining online.	One or more instances of the child service group are online somewhere in the VCS One cluster.	<p>Parent remains online if there are other instances of parallel child that are online.</p> <p>Parent is brought offline if no instances of child are online.</p> <p>Parent fails over if child fails over to any system.</p>	Parent fails over to another system, maintaining dependency with all child instances.

Parallel parent / Failover child

[Table 13-8](#) depicts the failover behavior for a parallel parent and a failover child.

Table 13-8 Parallel parent/Failover child

Link	Parallel parent instances depend on ...	Parallel parent instances are Online if ...	If failover child faults on a system ...	If parallel parent faults ...
global soft	Failover child service group somewhere in the VCS One cluster.	Failover child must be online somewhere in the VCS One cluster to online the parent group.	Parent remains online if child faults on any system. If faulted child fails over to another system, parent remains online. If child cannot fail over to another system, parent remains online.	Child stays online.
global firm	Failover child service group somewhere in the VCS One cluster.	Failover child is online somewhere in the VCS One cluster.	All instances of the parent are brought offline. If child fails over then all instances of the parent are brought online.	Child stays online.

Parallel parent / Parallel child

Table 13-9 depicts the failover behavior for a parallel parent and a parallel child.

Table 13-9 Parallel parent/Parallel child

Link	Parallel parent depends on ...	Parallel parent is online if ...	If parallel child faults ...	If parallel parent faults ...
local soft	Parallel child instance online on the same system.	Child must be online to online the parent.	If child cannot fail over, parent remains online.	Child instance stays online. Parent instance can fail over only to a system where the child instance is running and another parent instance is not running.
local firm	Parallel child instance online on the same system.	Parallel child instance is online on same system.	Parent taken offline. If child fails over to another system, VCS One brings an instance of the parent online on the same system as child. If child cannot fail over, parent remains offline.	Child stays online. Parent instance can fail over only to a system where the child instance is running and another parent instance is not running.

Table 13-9 Parallel parent/Parallel child

Link	Parallel parent depends on ...	Parallel parent is online if ...	If parallel child faults ...	If parallel parent faults ...
local hard	Parallel child instance online on the same system.	Parallel child instance is online on the same system.	<p>Parent instance taken offline before the child is taken offline.</p> <p>If child instance fails over to another system, VCS One brings an instance of the parent online on the same system as the child.</p> <p>If child cannot fail over, parent remains offline.</p>	<p>Child taken offline.</p> <p>If child fails over, parent migrates to the same system.</p> <p>If child cannot fail over, parent remains offline.</p>

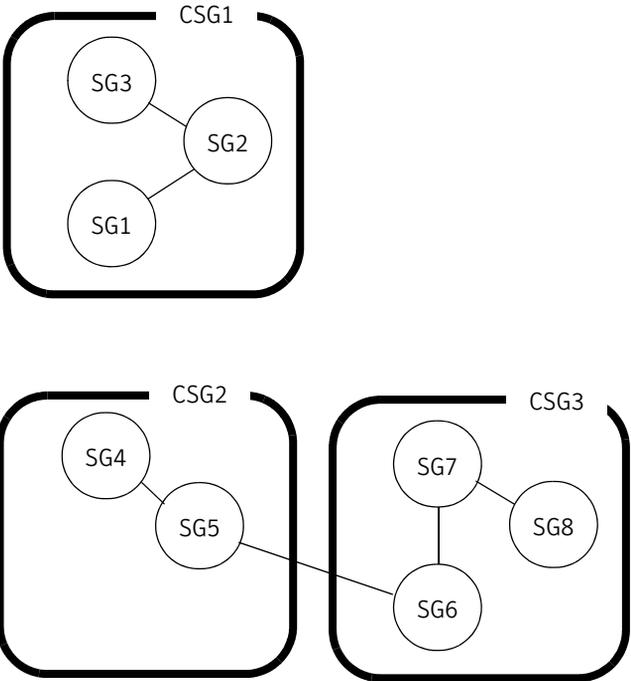
Design rules of composite service groups

The following design rules apply to composite service groups:

- A composite service group contains one or more service groups.
 A composite service group may not contain a composite service group.
- A group may only be part of one composite service group.
- The service groups contained in a composite service group may or may not have dependencies between them.
- A service group in a composite service group may have a dependency on a service group in a different composite service group.
 - If this dependency exists, and disaster recovery is setup for both CSGs, then both CSGs must fail over to the DR location at the same time.
 - If this dependency exists, and DR is setup of one CSG but not the other, then cross-site failover will not occur.
- Composite service groups and service groups can not have any dependency relationship.
 A service group can not have a dependency on a composite service group, and a composite service group can not have a dependency on a service group.

Figure 13-2 displays valid composite service group design.

Figure 13-2 Valid composite service group design



Designing service groups that use off-host resources

Off-host resource design considers whether or not your service group uses local resources.

About off-host resources in service groups

VCS One enables you to create local and off-host resources.

A local resource satisfies the following conditions:

- The resource, the agent that monitors the resource, and the respective service group reside on the same physical or local system. The resource is controlled (brought online, taken offline, and monitored) on the same system where the service group is brought online or configured.
- The resource's ControlGroup attribute value is empty.

An off-host resource satisfies the following conditions:

- The resource and its respective service group reside on the local system, but the agent that monitors it is located on a remote or control system. The resource is controlled (brought online, taken offline, and monitored) from a different system (where the control group is online), and not the system on which its service group is brought online or configured.
- The resource's ControlGroup attribute value is set to the name of the control group located on a remote system.
- Only a resource of type NetAppExport can be configured as an off-host resource.

In other words, an off-host resource is a resource that is defined and located on the local system but is monitored and operated from a remote system.

The remote system that hosts the agent, which monitors the off-host resource is called the control system. The control system also hosts a service group called the control group, which primarily consists of the agent that monitor the off-host resource. The control group can only be a FailOver service group and can be online or partially online on one control system at a time.

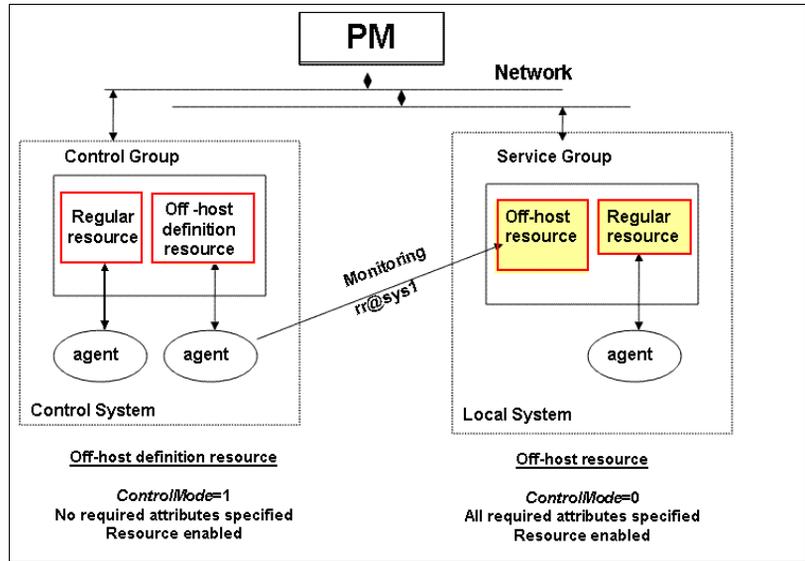
A local resource is converted into an off-host resource by setting its ControlGroup attribute value to the control group name, which is located on the control system. If the ControlGroup attribute value is empty, the resource is a local resource.

Off-host resources enable resource sharing and at the same time restricts local users from gaining administrative access on the remote system, which monitors the off-host resource.

How off-host resources work

Figure 13-3 depicts the off-host resource architecture.

Figure 13-3 Off-host resource architecture



As illustrated in the figure, the off-host resource is part of a local service group, which resides on the local system. The local service group, in addition to the off-host resource can contain other local resources.

The control or remote system hosts the control group. The control group contains an off-host definition resource. The resource type of the off-host definition resource must be the same as the off-host resource. The **ControlMode** attribute of the off-host definition resource must be set to 1. You do not need to specify any other required attributes. After setting the **ControlMode** attribute, you must enable the off-host definition resource. Note that it is mandatory to first set the **ControlMode** attribute and then enable the resource.

The sole purpose of the off-host definition resource is to start the respective agent on the control system. The off-host resource reference is a hidden resource name with the *resource_name@system_name* format. *resource_name* is the fully qualified resource name, which also includes the group name in the *group.resource* format. It is used by the agents on the control system to monitor the respective off-host resources.

You can not delete the off-host definition resource if it is the last resource type in the control group. This is because at least one off-host definition resource is required to keep the agent running.

On the local system, the off-host resource's ControlGroup attribute value is set to control group name that resides on the control system. All online, offline, and monitor commands issued by users, on the local system, are performed by the agent located on the control system. The off-host resource's ControlMode attribute must be set to 0, all the required resource attributes should be specified, and it must be enabled.

If the control group faults, the local service group does not failover, and the off-host resource status is displayed as UNKNOWN. If the control system faults, the status of the off-host resource in the local service group is displayed as either SYSTEM FAULT, AGENT FAULT, NETWORK DISCONNECTED, or DDNA.

The local service group and the control group can be failed over or switched to another system, similar to regular service groups. The off-host resource displays the same behavior in the VCS One Simulator.

The online, offline, and probe operations cannot be performed on the off-host resource if the control group is not online on any system. Similarly, the online and offline operations cannot be performed on the local service group if the control group is not online on any system. In the event of a control group concurrency violation, take the control group offline on all nodes and bring the control group online or partially online on only one node.

More information is available about how to create an off-host resource.

See [“Creating an off-host resource in a service group”](#) on page 357.

Counting off-host resources managed by an agent

The agent on the control system monitors the off-host resources when the control group is either in the ONLINE or PARTIAL state. The agent monitors the off-host resource on each system, which is listed in the SystemList of the service group, for which the off-host resource is configured.

If multiple service groups have off-host resources of the same resource type, and each off-host resource specifies the same control group, the number of off-host resources monitored by the agent is equal to the total number of systems listed in the SystemList of all the service groups.

For example, consider the off-host resources R1, R2, and R3, which are of the same resource type, and belong to the service groups SG1, SG2, and SG3 respectively. Each of these service groups have five systems listed in their SystemList. If all the off-host resources that belong to these service groups specify the same control group, the total number of off-host resources managed by the agent is 15 (5 + 5 + 5).

In other words, the agent monitors all the off-host resources on all the systems, which are listed in the SystemList attribute of all the service groups.

Optimizing the off-host resource setup

The number of off-host resources monitored by an agent is directly proportional to the number of systems, which are listed in the SystemList of the service groups, for which off-host resources are configured. In large VCS One cluster environments, the number of off-host resources that are managed by a single agent can be large.

Hence, it is imperative that you perform the following tasks to ensure optimum resource utilization:

- Calculate the actual and projected number of off-host resources that a single agent manages.

See [“Counting off-host resources managed by an agent”](#) on page 262.

- Select a system with adequate capability and resources.

The control system must be able to provide sufficient CPU and memory resources, for the agent, to effectively manage a large number of off-host resources.

- Set the value of the NumThreads attribute for the off-host resource.

The NumThreads attribute specifies the number of threads that an agent can create and use to schedule the agent entry points. Specify a large value if the agent monitors a large number of off-host resources. This ensures that more worker threads are available to schedule the agent entry points. More information is available about the NumThreads attribute.

See [“Resource type attributes”](#) on page 720.

It is recommended that an agent must not manage more than 600 resources. This number is deduced based on the maximum permissible NumThreads value, which is 30. This translates into each worker thread managing not more than 20 resources.

Note that the value for NumThreads must be set as per the available system resources (CPU, memory) on the system that hosts the control group. The optimal configuration for the NumThreads attribute and the number of off-host resources that use the same control group, differ on each system, and must be set appropriately.

Using multiple control groups to improve scalability

In order to maximize system resources, it is recommended that off-host resources must be split across multiple control groups. This facilitates better off-host resource load management and distributes the off-host resources across multiple systems. Consequently, agent responsiveness is also improved.

Off-host resources: user privileges

In order to perform various operations on the off-host resource, you require the following privileges:

- You require Read and Modify privileges on the service group in order to assign or unassign the service group as a control group for an off-host resource.
- You require Modify privileges on the control group, to modify an off-host resource, after a valid ControlGroup value is specified.
- You do not need to have any privileges on the control group to delete an off-host resource from a local service group. However, you require appropriate Delete privileges on the local service group to delete an off-host resource from a local service group.
- You require Online, Offline, and Probe privileges on the local service group in order to perform operations on an off-host resource.

Designing service groups that run in Solaris zones

Solaris zones provide multiple independent isolated environments for running applications in the same Solaris instance. Zones provides resource management, fault isolation, and security isolation.

Overview of how VCS One works with zones

VCS One provides application management and high availability to applications running in zones by extending its management and failover capability to zones.

Configuration options for using zones with VCS One include the following:

- Manage a local zone, including start, stop, monitor, and failover.
- Manage an application running inside a zone.

The Solaris zone must be installed and configured before it can be brought under VCS One control.

Create the service group with the standard managed application resource types (Application, Storage, Networking) with the addition of a Zone resource.

Configure the service group's ContainerInfo attribute, and each resource's ContainerOpts attribute.

The VCS One client daemon, `vcsonelientd`, and the necessary agents run in the global zone. Agents may execute commands in both the global and the local zones. For applications running within zones, agents run entry points inside the zones.

VCS One runs in a secure environment using Symantec Product Authentication Service, therefore communication from non-global zones to global zones is secure.

See the *Veritas Cluster Server One Bundled Agents Reference Guide* and Enterprise agent guides for more information on agents that are zone-aware and support applications running in non-global zones.

Designing attributes values for zone support

The service group level attribute ContainerInfo specifies information about the zone. VCS One defines this information at the service group level to avoid each resource in the service group having to define it at the resource level.

The ContainerInfo attribute has the following keys:

- **Name**
The name of the zone. Indicates to the resources in the group the name of the zone to act upon.
- **Type**
Type = Zone for a Solaris zone.
Type = WPAR for an AIX Workload Partition.
The XRM option is not supported.
- **Enabled**
Enabled = 1 enables the zone.
Enabled = 0 disables the zone.

The resource level attribute ContainerOpts specifies information that can be passed to the agent controlling the resources. These values are only effective if the ContainerInfo:Enabled attribute enables the zone.

- **RunInContainer**
RunInContainer = 1 specifies the resource will run in the local zone.
RunInContainer = 0 specifies the resource runs in the global zone.
- **PassCInfo**
PassCInfo = 1 specifies to pass the container information, defined in the service group's ContainerInfo attribute, to the resource. An example use of this value would be to pass the agent the name of the zone to act upon.
PassCInfo = 0 specifies to not pass the container information to the resource.
- **PassLoadInfo**
The service group's Load attribute sets values that indicate the amount of system resources the service group requires.

PassLoadInfo = 1 specifies to pass the service group's Load values to the resource. Use this value to pass the Load values to the Zone agent, which will use the values to set the resources available in Solaris Resource Manager.

Note: Load values must be set or changed when service group is in the OFFLINE state for a zone-enabled service group. Specifically, you may not use the `hagrp -changeload` command unless the zone-enabled service group is in the OFFLINE state.

PassLoadInfo = 0 specifies to not pass the service groups load dimensions to the resource.

Table 13-10 displays the agents available in zones and the associated default attribute values that are set for each application and resource type.

Each resource type also contains the [WorkLoad](#) attribute, which is a non-static attribute. The value for this attribute is populated from the service group's Load attribute, when the resource's ContainerOpts: PassLoadInfo key is set to 1.

Table 13-10 Zones capable agents and associated default attribute values

Resource Type	RunInContainer	PassCInfo	PassLoadInfo
Application	1	0	0
Mount	1	0	0
IP	0	1	0
IPMultiNICB	0	1	0
Process	1	0	0
Zone	0	1	1
Oracle	1	0	0
Netlsnr	1	0	0

Designing resource dependencies

The following diagrams illustrates different examples of resource dependencies.

Figure 13-4 depicts the dependency diagram when the zone root is set up on local storage with the loop back file system.

Figure 13-4 Zone root on local disks with loop back file system

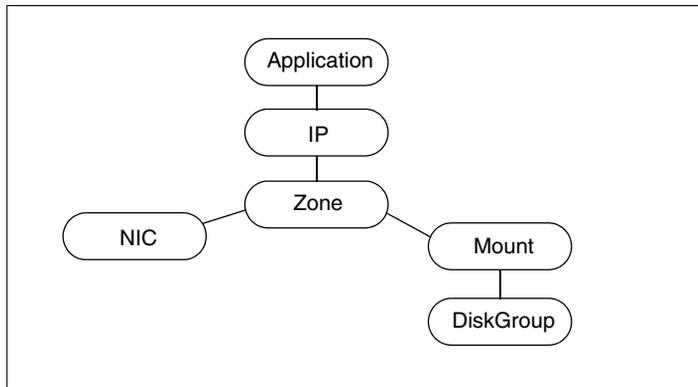


Figure 13-5 depicts the dependency diagram for a zone root on is set up on local storage with the direct mount file system.

Figure 13-5 Zone root on local disks with direct mount file system

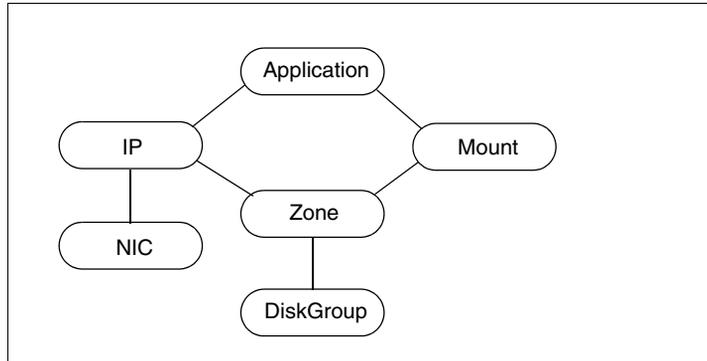


Figure 13-6 depicts the dependency diagram for a zone root is set up on shared storage with the loop back file system.

Figure 13-6 Zone root on shared disks with loop back file system

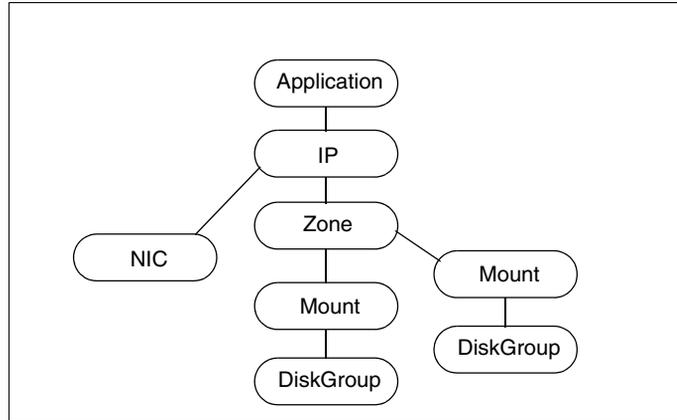
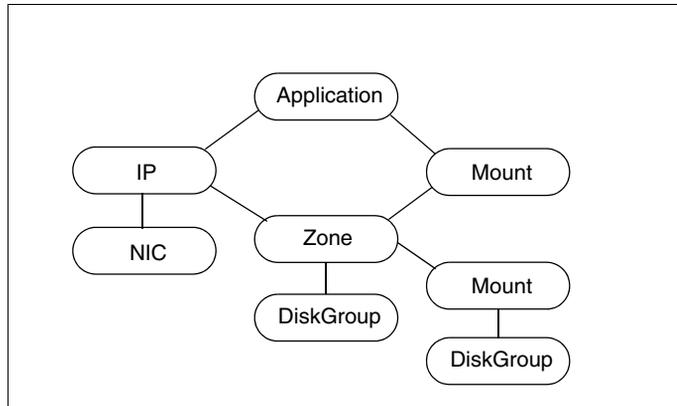


Figure 13-7 depicts the dependency diagram for a zone root is set up on shared storage with the direct mount file system.

Figure 13-7 Zone root on shared disks with direct mounted file system



Use the following principles when you create the service group:

- Set the MountPoint attribute of the Mount resource to the mount path.
- If the application requires an IP address, configure the IP resource in the service group.
- If the zone root file system is on shared storage, you can configure separate mounts for the zone and the application (as shown in the illustration), but you can configure the same disk group for both.

Designing service groups that run in AIX WPARs

An AIX workload partition (WPAR) is a virtualized operating system environment within an instance of the AIX operating system. AIX WPARs provide an isolated and secure environment for running applications.

VCS One provides application management and high availability to applications running in WPARs.

See [“About managing service groups in AIX Workload Partitions”](#) on page 454.

Note: VCS One provides support for system WPARs. VCS One does not provide support for application WPARs.

Overview of how VCS One works with WPARs

Configuration options for using WPARs with VCS One include the following:

- Manage a WPAR, including start, stop, monitor, and failover.
- Manage an application running inside a WPAR.

If a WPAR faults, VCS One fails over the entire service group that contains the WPAR to another system.

While applications may run in a WPAR, system resources are managed only at the global partition level. These system resources included CPUs, I/O, and adapters. The VCS One client daemon, `vcsonclientd`, and the necessary agents run in the global partition.

VCS One runs in a secure environment using Symantec Product Authentication Service, therefore communication from the global partition to the WPAR is secure.

See the *Veritas Cluster Server One Bundled Agents Reference Guide* and VCS One Enterprise agent guides for more information on agents that are WPAR-aware and support applications inside WPARs.

About the WPAR agent

The WPAR agent monitors WPARs, brings WPARs online, and takes them offline. For more information about the agent, see the *Veritas Cluster Server Bundled Agents Reference Guide*.

Designing attributes values for WPAR support

The service group level attribute `ContainerInfo` specifies information about the WPAR. VCS One defines this information at the service group level to avoid each resource in the service group having to define it at the resource level.

The `ContainerInfo` attribute has the following keys:

- **Name**
The name of the WPAR where you want the application to run. Indicates to the resources in the group the name of the WPAR to act upon.
- **Type**
Type = WPAR runs the application in the AIX WPAR specified in the Name key.
- **Enabled**
 - Enabled = 1
Enables the WPAR resource.
 - Enabled = 0
Disables the WPAR resource.

The resource level attribute `ContainerOpts` specifies information that can be passed to the agent controlling the resources. These values are only effective if the `ContainerInfo:Enabled` attribute enables the WPAR.

- **RunInContainer**
RunInContainer = 1 specifies the resource will run in the WPAR.
RunInContainer = 0 specifies the resource runs in the global partition.
- **PassCInfo**
PassCInfo = 1 specifies to pass the container information, defined in the service group's `ContainerInfo` attribute, to the resource. An example use of this value would be to pass the agent the name of the WPAR to act upon.
PassCInfo = 0 specifies to not pass the container information to the resource.
- **PassLoadInfo**
PassLoadInfo = 0. This key is not used with WPAR technology.

Designing resource dependencies for WPAR-enabled service groups

The following diagrams illustrates different examples of resource dependencies. In one case the WPAR root is set up on local storage. In the other, WPAR root is set up on shared storage.

Resource dependency diagrams: WPAR root on local disks

Figure 13-8 WPAR root on local disks (with direct mount file system)

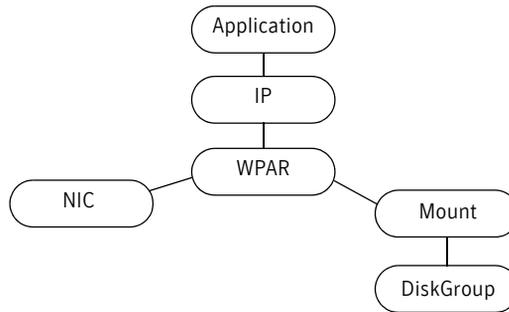
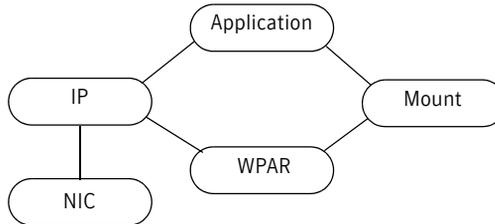
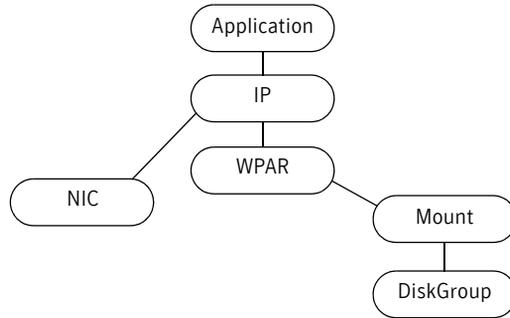


Figure 13-9 WPAR root on local disks (file system mounted from inside WPAR)



Resource dependency diagrams: WPAR root on shared storage

Figure 13-10 WPAR root on shared storage (with namefs file system)



Designing application placement policy

This chapter includes the following topics:

- [About designing application placement policy](#)
- [About managing applications](#)
- [Application start and stop configuration](#)
- [Manual application switch configuration](#)
- [About automated failover configurations](#)
- [About Priority](#)
- [About disruption factor and kickout](#)
- [Application relationships through service group compatibility](#)
- [About service group Load and system Capacity for physical systems](#)
- [Breaking the tie: the FragmentationPolicy attribute](#)
- [Mapping an application placement decision](#)

About designing application placement policy

You can configure resource, service group, and cluster attributes to control where a managed application runs.

You can use the VCS One Simulator to test and simulate where an application runs given certain circumstances and configurations.

See [“About the Simulator”](#) on page 174.

If you configure a managed application to be able to move between systems, the movement can be controlled in the following ways.

- Operator-initiated process
An operator or administrator can perform the move.
- VCS One-initiated process
The Policy Master initiates the process automatically. The Policy Master determines and executes the plan without administrative interaction.

The more attributes that are configured, the more sophisticated the control of where the application runs.

See [“Designing actions taken after a fault”](#) on page 227.

See [“About automated failover configurations”](#) on page 275.

Service group dependencies are considered when the Policy Master determines where a service group runs.

See [“About designing service group dependencies”](#) on page 247.

About managing applications

You can individually configure managed applications in the VCS One cluster to run in the configuration most appropriate to them, such as the following:

- Basic configurations, in which the application runs on one system.
- Manual switch configurations, in which multiple systems may host an application.
- Advanced highly-available configurations. In these configurations multiple systems may host an application and multiple criteria are dynamically considered when choosing a failover host.

Application start and stop configuration

This configuration uses VCS One to start, stop, and monitor applications, but does not switch or failover them between systems.

The group level attribute, `SystemList` defines the systems in the VCS One cluster on which the service group can come online. In a basic application management configuration, there is only one system defined in the `SystemList`.

In a basic configuration, there is no reason to define other application management related attributes such as `Load`, `Priority`, `Compatibility`, or `FragmentationPolicy`. These attributes may remain at their default values.

Manual application switch configuration

This configuration is similar to application start and stop management, with the addition of switchover capability. A switch is an administrator-initiated movement of the object for maintenance or availability purposes.

In this configuration, for a service group running on a physical system, the `SystemList` attribute lists each system where the application may potentially come online. During startup, a service group will attempt to come online on each system in the order they are listed in the `SystemList`.

Additionally, the service group `GrpFaultPolicy` and `NodeFaultPolicy` attributes should be set to `NoFailover`. This allows an operator initiated switch instead of an VCS One initiated failover.

Advanced management configurations options, such as `Load` and `Capacity`, can also be configured with a manual switch configuration.

About automated failover configurations

The most simple of the highly-available configurations has multiple systems listed in the `SystemList`. In this configuration, you can configure a service group that faults to attempt to come online on a system without manual intervention. The service group `GrpFaultPolicy` attribute default value of `Failover` is appropriate for this configuration.

More advanced management configurations use one or more components of VCS One's Advanced Workload Management (AWM) feature to determine on which system a service group will come online.

AWM is an integrated policy-based mechanism that automates placement both when a group is brought online, and in the event of a failover in response to a resource fault, group fault, or system fault. AWM's core functionality is to make the best effort to keep high priority applications up and running.

You may also configure the following attributes to control where a service group may run.

SystemList	The list of systems the application is approved to run on.
ResFaultPolicy	The fault policy of the resources in the service group.
GrpFaultPolicy	The fault policy of the service group, if the service group fails.
NodeFaultPolicy	The fault policy of the service group, if the system fails.
Load, Capacity	The amount of system resources the application requires with respect to the amount of resources available on a given system.
CompatibleGroups, IncompatibleGroups	The compatibility or incompatibility of the application with respect to other managed applications.
Priority	The priority of the application as compared to other managed applications.

The following factors contribute to AWM application placement decisions:

- The priority of the service group and the related level of disruption it will cause if it is failed over.
- The compatibility of the application's service group with other service groups.
- The load of the service group in relation to the capacity, or available resources, defined on the physical system.
- The value of the cluster's FragmentationPolicy attribute, if set to BiggestAvailable or BestFit.
- Any relevant local service group dependencies that are defined, if the value of the FragmentationPolicy attribute is set to Heuristic.

At the highest level, the AWM algorithm will choose the target system for the service group that has the following elements:

- Enough value in the capacity-related attributes to support the values needed for the service group's load-related attributes.
- The least disruption factor.
- No incompatible service groups that have equal or higher priority.

If the elements are equal, the value of the cluster level attribute, FragmentationPolicy, will determine the target system.

If the FragmentationPolicy attribute does not determine a unique system, the target system will be the first system listed in the SystemList that meets all the requirements.

About Priority

The Priority attribute enables you to ensure the most important service groups have the greatest opportunity to remain online in the VCS One cluster.

Each service group has an assigned Priority value. The Priority value is set in the following manner.

Service group Set by the administrator with appropriate permissions. Priority value should be set to reflect the level of importance of that group relative to other groups in the VCS One cluster.

There are five levels of priority. The highest priority value is 1. The default priority value is the lowest priority value, which is 5.

Higher priority objects can be configured to take over the resources used by lower priority objects. Failure to define different levels of priority will result in every object of that type having equal access to VCS One cluster resources.

[Table 14-11](#) shows the possible values for the Priority attribute and the associated disruption values.

Table 14-11 Priority levels and associated disruption values

Priority level	Disruption value
Priority = 1 (highest priority)	No value, service group can not be kicked out
Priority = 2	1000
Priority = 3	100
Priority = 4	10
Priority = 5 (default)	1

About disruption factor and kickout

Lower priority groups may be taken offline or switched to make room for higher priority groups. Taking lower priority groups offline or switching them is referred to as kickout. Each service group has an associated disruption value based on its priority level. The Disruption Factor (DF) for a system is the sum of the disruption values of all groups that will be kicked out in order to make room for higher priority service groups.

The system that can host the object and has the lowest disruption factor will be chosen as the target for bringing the object online. If equal candidate systems

have identical disruption factors, the system is chosen based on the value of the cluster-level attribute `FragmentationPolicy`.

See [“About service group Load and system Capacity for physical systems”](#) on page 280.

See [“Breaking the tie: the `FragmentationPolicy` attribute”](#) on page 281.

Equal priority service groups will never kickout one another. For a kickout to occur, one service group must be of higher priority. Service groups that have the highest priority, 1, can never be kicked out.

Application relationships through service group compatibility

Application relationships refer to the compatibility or incompatibility of two applications online on the same system at the same time. You can configure one of the following relationships between two service groups:

- **Compatible** – two applications can be online on the same system at the same time.
- **Incompatible** – two applications can not be online on the same system at the same time.

The service group level attribute `CompatibleGroups` can be defined to list the service groups that can co-exist with a particular group. Similarly, the attribute `IncompatibleGroups` can be defined to list the service groups that cannot co-exist with a particular service group. Only one of these two attributes can be defined for a group.

The following service group compatibility examples are valid:

- **Compatible with all other service groups in the VCS One cluster, including those that will be added in the future (default):**
`CompatibleGroups = {ALLGROUPS}`
- **Not compatible with any other service groups in the VCS One cluster, and will not be compatible with service groups added in the future:**
`IncompatibleGroups = {ALLGROUPS}`
- **Compatible with the service groups named G2 and G3, and incompatible with all other groups, including any groups added in the future:**
`CompatibleGroups = {G2, G3}`
- **Not compatible with the service groups named G2 and G3, but compatible with all other groups, including any groups added to in the future:**
`IncompatibleGroups = {G2, G3}`

The following service group compatibility examples are invalid:

- The ALLGROUPS value should not be defined with any other group name.
CompatibleGroups = {ALLGROUPS, G2}
- CompatibleGroups and IncompatibleGroups are mutually exclusive attributes. Both can not be set for a particular service group. The following definition will give an error when loading the configuration:
CompatibleGroups = {G2, G3}
IncompatibleGroups = {G4, G5}

In an environment that has four service groups, named G1, G2, G3, and G4, the following two examples are not equal in the definition of service group G1:

CompatibleGroups = {G2}
 IncompatibleGroups = {G3, G4}

The first definition indicates that G1 is compatible only with G2; the second definition means that G1 is compatible with G2 and all future groups.

Take the following considerations into account when planning service group compatibility definitions:

- Service groups named in the definition must already exist in the VCS One cluster, and cannot include the name of the service group being defined (can not self-reference.)
- All service groups that share a local group dependency must be compatible with each other as well as compatible or incompatible with the same set of groups.
- Consistent compatibility definitions across all service groups in the VCS One cluster are verified and enforced.
For example, if a modification to the compatibility of a group in a local service group dependency is made, the Policy Master ensures that all service groups in the dependency tree are changed accordingly.
- When changing the value of CompatibleGroups or IncompatibleGroups:
 - The service groups must not be in transition, it must be completely online or completely offline.
 - Two service groups must be completely offline on a system before they can be defined to be incompatible.
- Empty brackets in the definition imply an ALLGROUPS value. The following two examples are equal:
CompatibleGroups = {}
CompatibleGroups = {ALLGROUPS}

About service group Load and system Capacity for physical systems

The Load and Capacity construct allows the administrator to define a fixed amount of resources a system provides (Capacity), and a fixed amount of resources a specific service group is expected to utilize (Load).

The Load and Capacity construct is configured using the cluster attribute `PrecedenceOrder`, which enables definition of up to four prioritized keys, typically representing CPU, memory, network, and storage (I/O) resources.

These attributes define both Load and Capacity, and the two values are always considered in tandem. When a service group is started on a system, the values attributed to the Load of the service group are subtracted from the values attributed to the Capacity of the system that the service group is placed on.

If a service group has no Load related attributes values set, then the group can go online on any system for which it is configured, provided the compatibility criteria is met. If a service group has a Load configured, then it can only go online on a system that has a Capacity value defined and sufficient to accommodate the Load value.

Defining Load and Capacity

The default keys of the cluster attribute `PrecedenceOrder` is:

PrecedenceOrder	CPU
	MEM
	STBW
	NTBW

The names and ranking of the four keys can be customized or eliminated. For example, using all four keys for `PrecedenceOrder` may look like the following:

PrecedenceOrder	CPU
	MEMORY
	STORAGE
	NETBANDWIDTH

These keys define a relative ranking of Load and Capacity across the VCS One cluster. For example, if `PrecedenceOrder` is defined with two keys, CPU and

MEM, values for the Capacity attribute for two systems in that VCS One cluster could be:

On sys1:	Capacity	CPU: 400 MEM: 200
On sys2:	Capacity	CPU: 200 MEM: 100

These values may indicate that sys1 has four processors, and sys2 has two processors, or they may indicate that sys1 has processors that are twice as fast as the sys2 processors. These settings could also indicate that sys1 has twice as much memory as sys2. As long as the values are consistently relative, the measurement remains normalized across the VCS One cluster.

Load and Capacity values are hard values, meaning the values are strictly enforced. The total of the Load values of the service groups online on a system can not exceed the systems’s Capacity value.

The order of precedence of the four attributes affects the calculation of the target system to host a service group as well as the calculation of disruption factor.

See “[PrecedenceOrder](#)” on page 688.

Breaking the tie: the FragmentationPolicy attribute

If two systems have an equivalent Disruption Factor, the best target system to run the service group is chosen based on the value set for the cluster wide attribute FragmentationPolicy.

This attribute can have the following values:

- **BiggestAvailable** – The system chosen is the one with the largest value for the first key in the PrecedenceOrder attribute, by default CPU, as defined in the Capacity attribute of the system.

For example, if the cluster attribute PrecedenceOrder is defined with two keys, named CPU and MEM, and three systems have the value of their Capacity attribute are as follows:

On sys1:	Capacity	CPU: 400 MEM: 300
On sys2:	Capacity	CPU: 200 MEM: 100
On sys3:	Capacity	CPU: 100 MEM: 100

and the service group Load attribute is:

Load	CPU: 200
	MEM: 200

FragmentationPolicy set to BiggestAvailable would choose sys1 because it has the largest value for CPU.

- BestFit – The system chosen is the one with the value for the first key of the PrecedenceOrder attribute that is at least equal to as well as closest to the value for the corresponding Load attribute of the service group. In the above example, FragmentationPolicy set to BestFit would choose sys2, because the CPU value of 200 in the Load attribute of the service group is the closest match to the CPU value of 200 in the Capacity attribute of sys2.
- Heuristic – The system chosen is based on whether or not the service group has a local service group dependency with another service group:
 - If it does not, then choose target system as if BestFit was set.
 - If it does, then choose target system as if BiggestAvailable was set.The Heuristic option increases the chances for both the parent and child groups with a local service group dependency to meet the load requirements on the same system.

The default setting for the FragmentationPolicy attribute is BiggestAvailable.

Mapping an application placement decision

The search for a system to host a service group can happen for the following reasons:

- A service group is configured for failover faults.
- A system faulted that was hosting a service group configured for failover.
- You issue a command to online a service group but do not indicate a specific system to target.

Fault policy determines if a group will failover. More information on fault policy is available.

See [“Designing actions taken after a fault”](#) on page 227.

In any of these cases, the following high level steps occur.

- The object enters the Group Transition Queue (GTQ).
- Advanced Workload Management policy determines a plan for the best target system to run every object in the GTQ before it directs any actions to be taken. More than one object may be in the GTQ at the same time because:

- An entire system went down and there were multiple objects that failed simultaneously.
- An object was not able to be placed in the VCS One cluster, and is waiting for placement.
- After the plan is finalized for all GTQ entries all objects are automatically brought online and taken offline according to the plan.
 If entries remain in the GTQ because no eligible target systems are identified, these entries are designated as intent-online GTQ entries. The corresponding state for the service groups is INTENT ONLINE.
- Intent-online GTQ entries are re-evaluated to see if a target system can be identified when certain events occur:
 See “[Events that re-examine intent-online GTQ entries](#)” on page 286.

About the Group Transition Queue

The Group Transition Queue (GTQ) is an internal structure that keeps track of planned online and offline actions for groups, as well keeps track of which groups are intended to be online in the VCS One cluster.

The Group Transition Queue is the heart of the AWM placement decision. You can perform actions on service groups inside the GTQ.

See “[Stopping the current action for a service group in the GTQ](#)” on page 339.

See “[Flushing the plan of action on all service groups in the GTQ](#)” on page 338.

The GTQ is stored in the Policy Master configuration database and consists of the following items:

- List of service groups that need to be brought online
- Service group planned actions
- Service group action dependencies
- Service group action status

Even though the terminology is that a service group *enters* the GTQ, a service group never actually moves to the GTQ, but rather an entry is made of an action planned on the service group.

Service groups are prioritized as they enter the Group Transition Queue, in the following order:

- Priority attribute value with the higher priority value given precedence. Priority = 1 is placed ahead of Priority = 2.
- Load attribute value with the smaller value given precedence.
- If child-parent service group dependency exists between two service groups in a GTQ, the child is given precedence over the parent.

- Time order of entry in the GTQ. Newer entries are added after existing entries, when everything else is equal.

Choosing the best target system for groups without dependencies

The best target system selection process for a service group without service group dependencies is as follows:

- Consider a system in the service group's SystemList attribute. A system must be present in the system list to be a valid failover target. A sample system list would be:

```
<SystemList>  
  <val key="SystemA">0</val>  
  <val key="SystemB">1</val>  
  <val key="SystemC">2</val>  
</SystemList>
```

Each system in the system list is considered based on the FragmentationPolicy setting.

- Check if the system meets the basic criteria to run the service group. Basic criteria include the following:
 - The system is in a RUNNING state.
 - The system is not in the FROZEN state.
 - The service group is enabled on the system.
 - The service group is probed on the system.
 - Agents for the resources in the group have not failed on the system.
 - Another instance of the service group is not already running on the system.
 - All defined Capacity attribute values of the system meet or exceed the related Load attribute values of the service group.
- Check if the system is running any incompatible service groups that have equal or higher priority values. If so, eliminate the system from consideration and return to considering the next system in the system list.
- Check if the system has adequate available resources on all defined system Capacity attribute values for the corresponding Load attribute values of the service group.
 - If a target system selection process is initiated due to a service group or system fault, this step determines if lower priority groups need to be kicked out either for compatibility conflicts or to make available system capacity resources to run a higher priority service group.
 - If a target system selection process is initiated due to a normal service group online operation, no service group kickout is considered. In this

case, the only acceptable target system is one that provides adequate capacity and compatibility without kickout (DF=0).

The normal service group online operation can be changed to behave as if in response to a fault with the following command:

```
hagrps -online [-ejectlowpri] <group> -sys <system>
```

- Calculate Disruption Factor of system.
- Determine the current best target system.
 - Lowest disruption factor is always the determining factor for choice of best target system.
 - If the least disruption factor is 0, and more than one system offers a 0 disruption factor, the system is selected based on the FragmentationPolicy attribute setting.
 - If least disruption factor is non-zero, and more than one system has the same least disruption factor, then the first system in the SystemList that has that disruption factor value is selected.
- If no systems exist that meet the criteria, the service group will not go online, and will remain as a persistent action in the GTQ.

Choosing the best target system for groups with dependencies

The best target system selection process for a service group with local service group dependencies is the following:

- Equal priority groups of same group type (failover or parallel)
 Groups are placed in a single GTQ entry for processing. The service group load calculation is evaluated as a combined total. The best target system must accept the entire set of groups bounded by the local group dependency as a single requirement.
 If no such target system can be identified, AWM attempts to find a target system for every group individually. For example, a child service group may online and the parent service group may remain in the GTQ with an intent online entry.
- Parent groups have lower priority than child groups
 Groups are placed in the GTQ as multiple entries for processing, with the child group always ahead of the parent group. The best target system is planned for the child group as usual except that the FragmentationPolicy attribute BiggestAvailable is applied. This provides the highest probability for adequate capacity to remain for the parent group to come online.
- Child groups have lower priority than parent groups
 This configuration is not supported in VCS One.

- Child group is of a different type (failover or parallel) than parent group. Groups are placed in the GTQ as multiple entries for processing, with the child group always ahead of the parent group. The best target system is planned for the child group as usual except that the FragmentationPolicy attribute BiggestAvailable is applied. This provides the highest probability for adequate capacity to remain for the parent group to come online.

The best target system selection process for a service group with global service group dependencies is the following:

- AWM evaluates each group independently. The decision for a child service group and the decision for a global parent group are not considered together.
- Groups are placed in the GTQ as multiple entries for processing, with the child group always ahead of the parent group. If a target system can not be determined for the child, and another instance of the child group is not online in the VCS One cluster, then a target system for the parent will not be identified.

Events that re-examine intent-online GTQ entries

If entries remain in the GTQ because no eligible target systems are identified, these entries are designated as intent-online GTQ entries.

Intent-online GTQ entries are re-evaluated to see if a target system can be identified when the following events occur:

- The value of the Capacity attribute is increased.
- The value of the Load attribute is decreased
- A service group, that is incompatible with another group, is taken offline.
- A child group is brought online.
- All the groups on a system are probed.
- A service group is enabled on one or more systems.
- A persistent resource recovers from a fault.
- A faulted resource is cleared.
- A system is added to the SystemList attribute of a service group.
- A new system joins the VCS One cluster.
- A system rejoins the VCS One cluster after reboot.
- A system is unfrozen.
- An agent registers with the Policy Master.

Any potential target system for an intent-online GTQ entry must have the service group completely offline.

The intent-online entry is removed for a failover service group if either of the following is true:

- If the service group is not completely offline on all systems in the VCS One cluster, and there is a reconnect of the Policy Master to the VCS One environment.
- If the service group is partially online on a system as the system joins the VCS One environment. In this case the Policy Master will not fully online the service group in case you want the group to remain in the partially online state.

Tasks: Managing components

This section includes the following chapters:

- [“Managing systems”](#) on page 291
- [“Managing service groups”](#) on page 313
- [“Managing composite service groups”](#) on page 363
- [“Managing resources”](#) on page 377
- [“Managing application placement”](#) on page 397
- [“Managing automated tasks”](#) on page 409

Managing systems

This chapter includes the following topics:

- [Adding a system to the VCS One cluster](#)
- [Locating a system](#)
- [Viewing system attributes](#)
- [Editing system attributes](#)
- [Adding a system to the VCS One cluster using the Simulator](#)
- [Deleting a system from the VCS One cluster](#)
- [Freezing a system](#)
- [Unfreezing a system](#)
- [Faulting a system using the Simulator](#)
- [Repairing a system using the Simulator](#)
- [Moving a system to another organization tree node](#)
- [Viewing a selected list of systems](#)
- [Displaying system information](#)
- [Putting a system in the offline state](#)
- [Simulating a system in DDNA state](#)
- [Simulating a system heartbeat failure](#)
- [Simulating a system heartbeat recovery](#)

Adding a system to the VCS One cluster

This topic describes how to add a physical system to the VCS One cluster. Adding a system to the VCS One cluster involves physically connecting the system to the VCS One cluster network and installing the VCS One client software. The VCS One installation program configures the system as part of the VCS One cluster.

Checking installation prerequisites

Before installing the VCS One client, you must ensure that the following prerequisites are met:

- The target installation system runs one of the supported platforms as listed in the *Veritas Cluster Server One Release Notes*.
- The target installation system is physically connected to the VCS One network using at least one TCP/IP connection. The system's IP address is known.
- The clocks are in sync between the Policy Master and the system to be added.
- The Policy Master daemon is running. Execute the following command on the active Policy Master cluster node, to ensure that the Policy Master daemon is running:
haadmin -state
- You have the virtual IP address of the Policy Master cluster.
- Symantec Product Authentication Service is functional on the Policy Master systems and the authentication broker is running.
- ssh or rsh communication is configured and functional.
More information is available about setting up ssh or rsh communication. See the *Veritas Cluster Server One Installation Guide*.
- You have logged on to the system (which runs the installation process) with root user credentials.
- You have mounted the VCS One installation disc on a system connected to the same network as the target installation system.
- If the system on which you are installing the VCS One client daemon uses a DHCP IP address, ensure that the address has a long-term lease and is not relinquished while the VCS One client daemon is running. Loss of network connectivity results in VCS One client daemon failures.

Installing the VCS One client

See the *Veritas Cluster Server One Installation Guide* for instructions on how to install the VCS One client.

After the installation process completes, the VCS One client daemon (vcsoneclientd) starts on the system, and the system is part of the VCS One cluster.

Adding a configured system to the VCS One cluster

This section describes how to add a system to the VCS One cluster, which has the VCS One client daemon installed, but is not currently part of the VCS One cluster.

Such a situation may arise if the system was previously configured and added to the VCS One cluster, but was removed from the VCS One cluster.

Prior to adding the system to the VCS One cluster, ensure that it meets the following prerequisites:

- The system runs a platform that VCS One supports.
- The VCS One client software is installed.
- The system is connected to the VCS One cluster by a TCP/IP network.
- If the system on which you are installing the VCS One client daemon uses a DHCP IP address, ensure that the address has a long-term lease and is not relinquished while the VCS One client daemon is running. Loss of network connectivity results in VCS One client daemon failures.

To add a system using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 In the right pane, click the **Systems** tab.
- 3 In the right pane, from the **Configuration** menu, click **Add System**.
- 4 In the **Add System Wizard** screen, click **Next**.
- 5 In the **Add System** screen, perform the following steps in the order presented:
 - In the **Name** box, enter the name of the system. The name of the system cannot exceed 128 characters.
 - In the **Platform** box, select the platform the system runs.
If you do not specify a platform, the system is added with the default platform.
See “[DefaultPlatform](#)” on page 684.
See “[PlatformName](#)” on page 708.

- Check **Configure advanced workload management** if you want to configure AWM.
Advanced workload management is a feature that allows you to define the amount of resources a system has (Capacity) with respect to the amount of resources that a service group needs (Load).
Enter the values that correspond to the amount of resources that this service group needs.

Note: It is strongly recommended that you understand the AWM feature before entering values. You need to define Capacity on a system as well as Load on a service group for this feature.

See [“How you can define service group load and system capacity”](#) on page 59.

- Click **Next** or **Finish**.
Clicking **Finish** in any intermittent screen of the **Add System Wizard** results in adding the system to the default organization unit node for the logged on user. The system inherits the default extended attribute values, which are defined at the default organization unit node.
- 6 In the **Organization Unit Selection** screen, under **Organization Tree**, expand the **ServerFarm** node, and then select the organization unit node where you want the system to reside.
 - 7 Click **Next**.
 - 8 In the **Assign Values to Extended Attributes** screen, perform the following steps in the order presented, for each extended attribute:
 - Under **Extended Attributes**, select the extended attribute.
 - In the **Value** box, select or enter a value for the extended attribute.
 - 9 In the **Assign Values to Extended Attributes** screen, click **Finish**.
 - 10 In the **Summary** screen, click **Close**.

To add a system from the command line

- 1 Add the system to the VCS One cluster. At the command prompt, type the following:

```
hasys -add system [-platform platform] [ouvaluepath]  
[-user user@domain] [-domaintype domaintype]
```

If you do not specify a platform, the system is added with the default platform.

See [“DefaultPlatform”](#) on page 684.

Once the system is added, a message is displayed that prompts you to set the system’s capacity before configuring any service groups on it.

If you do not specify an OUvaluepath, the system is added to the root (/) of the Organization Tree.

- 2 List and display information about the system, which you have added. At the command prompt, type the following:

```
hasys -display system
```

To modify the system's capacity attribute from the command line

- ◆ At the command prompt, type the following:

```
hasys -modify [refreshvars] system Capacity -update key value  
key value ...
```

Example

```
hasys -modify solsys20 Capacity -update cpu 8 memory 3096
```

Locating a system

Use this procedure to locate a system.

You can use one or more of the following structures to locate a system in VCS One:

- Organization Tree
- Extended Attributes
- Sets

To locate a system using the organization tree

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Systems** tab.
- 3 In the left pane, select **Organization Tree** from the drop-down list.
- 4 In the left pane, select the appropriate Organization Tree Node (OU Name node or OU Value node).
- 5 In the right pane, view all the system associated with the selected organization tree node.

To locate a system using extended attributes

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Systems** tab.
- 3 In the right pane, use the **EA Filter** to view system by extended attribute. See [“Filtering results in a table”](#) on page 115.

To locate a system using sets

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Systems** tab.
- 3 In the left pane, select either **My Objects** or a user-defined set from the list.
- 4 In the right pane, view all the systems associated with the selected set.

To locate a system using multiple filtering methods

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Systems** tab.
- 3 In the left pane, select **Organization Tree** from the drop-down list
- 4 Click a node in the organization tree.
- 5 In the right pane, view all the systems associated with that organization tree node.
- 6 In the right pane, use the **EA Filter** box to further filter the systems. Click the down arrow next to **EA Filter** to choose extended attributes.
- 7 Enter text in the **Keyword** text box to further limit the search within the systems currently displayed.
To display the Keyword text box, click the **+** next to **EA Filter**.
- 8 Click **Go**.
- 9 In the right pane, view all the systems that match the search criteria.

Viewing system attributes

This topic describes how to view system attributes.

To view system attributes using the VCS One console

- 1 In the VCS One console, locate the system that you want to view. See [“Locating a system”](#) on page 295.
- 2 In the right pane, under **Systems**, click the appropriate system.
- 3 In the right pane, click **All Attributes**. The **All Attributes** page is displayed, which lists all the system’s attributes. Click the arrow symbol in the **Attribute Name** column to sort the list in ascending or descending alphabetical order.

To view system attributes from the command line

- ◆ At the command prompt, type the following:

```
hasys -value system attribute [-user user@domain] [--domaintype  
domaintype]
```

Editing system attributes

This section describes how to edit system attributes.

To edit system attributes using the VCS One console

- 1 In the VCS One console, locate the system that you want to edit.
See [“Locating a system”](#) on page 295.
- 2 In the right pane, under **Systems**, select the check box corresponding to the system that you want to edit.
- 3 In the right pane, from the **Configuration** menu, click **Edit Attribute**.
- 4 In the The **Edit Attribute** dialog box, perform the following steps for each system attribute that you want to modify:
 - In the **Attribute Name** box, select the system attribute that you want to modify. Only attributes that can be modified are displayed in this list.
 - In the **Value** box, enter or select a value for the specified attribute.
- 5 In the The **Edit Attribute** dialog box, click **OK**.
- 6 Click **Close**.

To edit a system attribute from the command line

- ◆ At the command prompt, type the following:

```
hasys -modify [refreshvars] system attribute value [-user  
user@domain]  
[--domaintype domaintype]
```

More information is available about system attributes.

See [“System attributes”](#) on page 702.

Adding a system to the VCS One cluster using the Simulator

This task is only available using the Simulator, to simulate a system add operation.

To simulate adding a system to the VCS One cluster

Note: Clicking **Finish** in any intermittent screen of the **Add System Wizard** adds the system to the default organization unit node for the logged on user. The system inherits the default extended attribute values, which are defined at the default organization unit node.

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Systems** tab.
- 3 In the right pane, in the **Configuration** menu, click **Add System**.
- 4 In the **Add System Wizard** screen, click **Next**.
- 5 In the **Add System** screen, perform the following steps in the order presented:
 - In the **Name** box, enter the name of the system. The name of the system cannot exceed 128 characters.
 - In the **Platform** box, select the system platform.
 - Under **Capacity**, enter values for the system's capacity dimensions. These dimensions are based on the capacity dimensions that are specified in the VCS One cluster.
 - In the **Add System** screen, click **Next**.
- 6 In the **Organization Unit Selection** screen, under **Organization Tree**, expand the **ServerFarm** node, and select the organization unit node where you want the system to reside. Click **Next**.
- 7 In the **Assign values to Extended Attributes** screen, for each extended attribute perform the following steps in the order presented:
 - Under **Extended Attributes**, select the extended attribute.
 - In the **Value** box, select or enter a value for the extended attribute.
- 8 In the **Assign Values to Extended Attributes** screen, click **Finish**.
- 9 In the **Summary** screen, click **Close**.

Deleting a system from the VCS One cluster

This topic describes how to remove a system from the VCS One cluster. To remove a system, perform the following tasks in the order presented:

- Ensure no service groups are online on the system.
- Stop the `vcsonclientd` daemon on the system

- Delete the system using the VCS One console or the CLI.
 Deletion of the system removes it from the configuration database.

To ensure no service groups are online on the system

- 1 In the VCS One console, locate the system on which you want to take the service groups offline.
 See [“Locating a system”](#) on page 295.
- 2 In the right pane, under **Systems**, click the appropriate system.
- 3 In the right pane, under **Details of Privileged Groups Configured in this system**, check the status of each service group and determine the service groups that are online on the system. The **Status** column displays the status of the service group.
- 4 For each online service group, perform the following steps in the order presented:
 - Under **Service Group Name**, click the name of the service group.
 - In the right pane, from the **Operations** menu, do one of the following:
 - Click **Offline** to take the service group offline.
 - Click **Switch**, to move and bring the service group online on another system.
 - In the corresponding dialog box, click **OK**.
- 5 In the Web browser, click **Back**, to return to the system details page.

To stop the vcsoneclientd from the command line

- 1 Log on to the system that you want to delete with root user credentials.
- 2 At the command prompt, type the following:
`hastop -client -local`

To delete a system using the VCS One console

- 1 In the VCS One console, locate the system that you want to delete.
 See [“Locating a system”](#) on page 295.
- 2 In the right pane, check the box corresponding to the system that you want to delete.
- 3 In the right pane, from the **Configuration** menu, click **Delete System(s)**.
- 4 In the **Delete System(s)** dialog box, click **OK**.
- 5 Click **Close**.

To delete a system from the command line

- ◆ From the active Policy Master cluster node, at the command prompt, type the following:

```
hasys -delete system [-user user@domain] [-domaintype  
domaintype]
```

Freezing a system

Freezing a system enforces the following conditions:

- A service group hosted on the system can not failover to another system.
- A service group hosted on another system can not come online on the frozen system through a failover operation.
- A manual switch of a service group to or from the frozen system is not allowed.

Freezing a system is useful when you want to stop your operations, such as maintenance activities, from triggering a service group failover.

To freeze a system

- 1 In the VCS One console, locate the system that you want to freeze. See [“Locating a system”](#) on page 295.
- 2 In the right pane, under **Systems**, click the system that you want to freeze.
- 3 In the right pane, from the **Operations** menu, click **Freeze**.
- 4 In the **Freeze System** dialog box, select the **Evacuate all online service groups** check box, if you want to move all the existing online service groups to other systems in the VCS One cluster.
- 5 In the **Freeze Systems** dialog box, click **OK**.

To freeze multiple systems

- 1 In the VCS One console, locate the systems that you want to freeze. See [“Locating a system”](#) on page 295.
- 2 In the right pane, under **Systems**, select the check box corresponding to the systems that you want to freeze.
- 3 In the right pane, from the **Operations** menu, click **Freeze**.
- 4 In the **Freeze Systems** dialog box, select the **Evacuate all online service groups** check box, if you want to move all the existing online service groups to other systems in the VCS One cluster. Click **OK**.
- 5 In the **Freeze Systems** dialog box, click **Close**.

To freeze multiple systems using the organization tree

- 1 In the VCS One console, click the Manage tab.
- 2 In the right pane, click the Systems tab.
- 3 In the left pane, select **Organization Tree** from the list. Select the appropriate OU Value node associated with the systems that you want to freeze.
- 4 Right-click the selected OU Value node, and then click **Freeze**.
- 5 In the **Freeze OU** dialog box, click **OK**.
- 6 In the **Results** dialog box, click **Close**.

To freeze multiple systems using sets

- 1 In the VCS One console, click the Manage tab.
- 2 In the right pane, click the Systems tab.
- 3 In the left pane, select the set associated with the systems that you want to freeze.
- 4 Right-click the set, and then click **Freeze**.
- 5 In the **Freeze Set** dialog box, click **OK**.

To freeze multiple systems using custom views

- 1 In the VCS One console, click the Manage tab.
- 2 In the right pane, click the Systems tab.
- 3 In the left pane, select the set associated with the custom view. A set can contain one or more custom views. Expand the appropriate custom view, and then select the extended attribute value associated with the systems that you want to freeze.
- 4 Right-click the extended attribute value, and then click **Freeze**.
- 5 In the **Freeze System(s)** dialog box, click **OK**.

To freeze a system from the command line

- ◆ At the command prompt, type the following:

```
hasys -freeze [-evacuate] {system | -ou expression | -ea  
expression | -ou expression -ea expression | -setname setname}  
[-user user@domain] [-domaintype domaintype] [-info]
```

Unfreezing a system

Unfreeze a frozen system to allow service groups to failover and be brought online on the system.

To unfreeze a system

- 1 In the VCS One console, locate the system that you want to unfreeze. See [“Locating a system”](#) on page 295.
- 2 In the right pane, under **Systems**, click the system that you want to unfreeze.
- 3 In the right pane, from the **Operations** menu, click **Unfreeze**.
- 4 In the **Unfreeze System** dialog box, click **OK**.

To unfreeze multiple systems

- 1 In the VCS One console, locate the systems that you want to unfreeze. See [“Locating a system”](#) on page 295.
- 2 In the right pane, under **Systems**, select the check box corresponding to the systems that you want to unfreeze.
- 3 In the right pane, from the **Operations** menu, click **Unfreeze**.
- 4 In the **Unfreeze Systems** dialog box, click **OK**.
- 5 In the **Unfreeze Systems** dialog box, click **Close**.

To unfreeze multiple systems using the organization tree

- 1 In the VCS One console, click the Manage tab.
- 2 In the left pane, select **Organization Tree** from the list. Select the appropriate OU Value node associated with the systems that you want to unfreeze.
- 3 Right-click the selected OU Value node, and then click **Unfreeze**.
- 4 In the **Unfreeze OU** dialog box, click **OK**.
- 5 In the **Results** dialog box, click **Close**.

To unfreeze multiple systems using sets

- 1 In the VCS One console, click the Manage tab.
- 2 In the right pane, click the Systems tab.
- 3 In the left pane, select the set associated with the systems that you want to unfreeze.

- 4 Right-click the set, and then click **Unfreeze**.
- 5 In the **Unfreeze System** dialog box, click **OK**.

To unfreeze multiple systems using custom views

- 1 In the VCS One console, click the Manage tab.
- 2 In the right pane, click the Systems tab.
- 3 In the left pane, select the set associated with the custom view. A set can contain one or more custom views. Expand the appropriate custom view, and then select the extended attribute value associated with the systems that you want to unfreeze.
- 4 Right-click the extended attribute value, and then click **Unfreeze**.
- 5 In the **Unfreeze System(s)** dialog box, click **OK**.

To unfreeze a system from the command line

- ◆ At the command prompt, type the following:

```
hasys -unfreeze {system | -ou expression | -ea expression | -ou
expression -ea expression | -setname setname}
[-user user@domain] [-domaintype domaintype]
```

Starting and stopping the VCS One client daemon on a system

This section describes how to start and stop the VCS One client daemon (`vcsonelientd`) processes using the `hastart` and `hastop` commands. Use this procedure for maintenance and before you delete a system from the VCS One configuration.

This procedure does not stop the service groups that are online on the system. You can stop the `vcsonelientd` processes on one or more systems in the VCS One cluster. However, the `vcsonelientd` processes must be started on each system locally.

To start the `vcsonelientd` processes on a local system

- ◆ At the command prompt, type the following:

```
hastart -client
```

To stop the `vcsonelientd` processes on a local system and take the service groups offline

- ◆ At the command prompt, type the following:

```
hastop -client -local
```

See the *Veritas Cluster Server One Command Reference Guide*.

To stop the `vcsonelientd` processes on a local system, take the service groups offline, and offline any service groups connected with a global parent service group dependency

- ◆ At the command prompt, type the following:
`hastop -client -local -propagate [-user user@domain] [-domaintype domaintype]`

The `-propagate` option propagates the offline action to the parent service groups.

To stop the `vcsonelientd` processes on a local system and keep the service groups online

- ◆ At the command prompt, type the following:
`hastop -client -local -force [-user user@domain] [-domaintype domaintype]`

The `-force` option ensures that the currently online service groups continue to remain online on the same system.

To stop the `vcsonelientd` processes on a local system and move the online service groups to another system

- ◆ At the command prompt, type the following:
`hastop -client -local -evacuate [-user user@domain] [-domaintype domaintype]`

The `-evacuate` option moves all the online service groups to another system.

To stop the `vcsonelientd` processes on a local system, move the online service groups to another system, and move any online global parent service group to another system

- ◆ At the command prompt, type the following:
`hastop -client -local -propagate -evacuate [-user user@domain] [-domaintype domaintype]`

The `-evacuate` option moves all the online service groups to another system. The `-propagate` option propagate the action to the parent service groups.

To stop the `vcsonelientd` processes on one or more remote systems and failover the online service groups after a system fault

- ◆ At the command prompt, type the following:

```
hastop -client -sys systems [[-actonnodefault] -force|-evacuate]  
[-user user@domain] [-domaintype domaintype]
```

If the system faults after the VCS One client daemon is stopped, and you want the currently online service groups to failover to another system, specify the `-actonnodefault` option. The online service groups are failed over only after the system faults and not when the VCS One client daemon stops.

To stop the `vcsonclientd` processes on all systems in the VCS One cluster

- ◆ On the Policy Master, at the command prompt, type the following:

```
hastop -client -all
```

Faulting a system

Use this procedure to change the state of the system from DDNA or UNKNOWN to FAULTED.

In the DDNA state, the system on which the VCS One client daemon is installed is functional (up and running), however, the VCS One client daemon process has stopped.

If a system is in the DDNA state or the UNKNOWN state, the Policy Master does not failover service groups that are running on the system. The administrator must manually failover the service groups.

Use this procedure to move a system to the FAULTED state, and allow VCS One to respond with automated fault policy.

- 1 In the VCS One console, locate the systems that you want to fault.
See [“Locating a system”](#) on page 295.
- 2 In the right pane, under **Systems**, select the check box that corresponds to the systems that you want to fault.
- 3 In the right pane, in the **Simulation** menu, click **Simulate System Fault**.
- 4 Click **OK**.
- 5 Click **Close**.

Faulting a system using the Simulator

This operation changes the state of the system to FAULTED to simulate a system fault in the Simulator.

To simulate a fault for one or more systems

- 1 In the VCS One console, locate the systems that you want to fault.

See “[Locating a system](#)” on page 295.

- 2 In the right pane, under **Systems**, select the check box that corresponds to the systems that you want to fault.
- 3 In the right pane, in the **Simulation** menu, click **Simulate System Fault**.
- 4 Click **OK**.
- 5 Click **Close**.

To simulate a system fault from the command line

- ◆ At the command prompt, type the following:

```
hasim -faultsys system(s) [-user user@domain -domaintype  
domaintype]
```

Repairing a system using the Simulator

This task is only available using the Simulator, to simulate a system repair operation.

To simulate a repair operation for one or more systems

- 1 In the VCS One console, locate the faulted systems that you want to repair. See “[Locating a system](#)” on page 295.
- 2 In the right pane, under **Systems**, select the check box that corresponds to the faulted systems.
- 3 In the right pane, in the **Simulation** menu, click **Start Systems**.
- 4 Click **OK**.
- 5 Click **Close**.

To simulate a repair operation from the command line

- ◆ At the command prompt, type the following:

```
hasim -startsys system(s) [-user user@domain -domaintype  
domaintype]
```

Moving a system to another organization tree node

You may move a system to any OUvalue node in the organization tree if you have appropriate privileges.

See “[Modify OU](#)” on page 633.

If the system has an extended attribute that is a variable, and that attribute value is invalid at the new organization tree location, the move operation is rejected and an error message is generated.

To override this behavior and move the system, use the `–refreshvars` option. Doing so will update value of the resource attribute.

To move one or more systems to another organization tree node

- 1 In the VCS One console, locate the systems that you want to move. See [“Locating a system”](#) on page 295.
- 2 Select the located system or systems. Click **Configuration > Move System(s)**.
- 3 In the **Organization Unit Selection** dialog box, perform the following steps in the order presented:
 - Under **Organization Tree**, expand the **ServerFarm** node, and select the OU Value node to which you want to move the system.
 - Consider the **Allow changes even if any EA’s are used in attribute values of resources** check box.
 Check this option to confirm to allow the move of the system even if it changes the resource attribute values due to the use of resource variables.
 When a system is moved to another OU, it is possible that the value of an extended attribute which is attached to the system is no longer valid. In this case the extended attribute value for the object changes. If the extended attribute is used as resource variable, then the change in value of the extended attribute can also change a resource attribute value.
 - Consider the **Modify Privileges if move violates the assigned Roles** check box.
 Consider this option in the use case when the user moves to an OUvalue node that is not in the subtree of his original organization tree node. In this case, you must check this option to remove privileges from the user that are no longer valid due to the move, or the move is rejected. This option is equivalent to the `-updateroles` option in the command line.
 - Click **Next**.
- 4 In the **Assign Values to Extended Attributes** dialog box, assign extended attribute values for the system. This dialog box is displayed only if extended attributes are defined for the selected node or any other preceding nodes in the organization tree hierarchy.
- 5 Click **Finish**.

To move a system to another organization tree node from the command line

- ◆ At the command prompt, type the following:

```
hasys -move [-updateroles] [-refreshvars] systems -ou  
ouvaluepath [-user username@domain] [-domaintype domaintype]
```

Viewing a selected list of systems

This section describes how to filter systems based on status.

To filter systems based on status

- 1 In the VCS One console, click the **Manage** tab.
- 2 In the right pane, click the **Systems** tab.
- 3 In the left pane, select **Organization Tree** from the list, and then select the **ServerFarm** node or any other organization tree unit node. Note that you can also select an extended attribute or a set.
- 4 In the right pane, in the **Status of all systems** area, do one of the following to filter systems based on status:
 - Click the number corresponding to **Running**, to view all the systems that are currently in the `RUNNING` state.
 - Click the number corresponding to **Offline**, to view all the systems that are currently in the `OFFLINE` state.
 - Click the number corresponding to **Faulted**, to view all the systems that are currently in the `FAULTED` state.
 - Click the number corresponding to **Deploying**, to view all the systems that are currently in the `DEPLOYING` state.

You can sort systems in ascending or descending alphabetical order by clicking any of the column headings under **Systems**.

Displaying system information

This section describes the VCS One commands that are used to view system information. The `hasys` command provides several options to display system information.

To list all the systems by name

- ◆ At the command prompt, type the following:

```
hasys -list
```

To list all the systems using a common attribute

- ◆ At the command prompt, type the following:

```
hasys -list PlatformName==linux
```

You can use a conditional statement. For example, to list all the systems where the PlatformName attribute value contains linux.

To display system specific attribute information

- ◆ At the command prompt, type the following:

```
hasys -display system
```

To display the value of a specific attribute for a specific system

- ◆ At the command prompt, type the following:

```
hasys -display system -attribute Capacity
```

More information is available about VCS One commands.

See the *Veritas Cluster Server One Command Reference Guide*.

Putting a system in the OFFLINE state

In the Simulator, this task simulates a system state change to OFFLINE. In an actual VCS One cluster, this task takes the VCS One client daemon offline on that system.

You require Stop System privileges to offline a system.

To simulate the offline operation for one or more systems

- 1 In the VCS One console, locate the systems which you want to take offline. See [“Locating a system”](#) on page 295.
- 2 In the right pane, under **Systems**, select the check box that corresponds to the systems that you want to take offline.
- 3 In the right pane, in the **Operations** menu, click **Stop Systems**.
- 4 Click **OK**.
- 5 Click **Close**.

Simulating a system in DDNA state

This task is only available using the Simulator to simulate the Daemon Dead Node Alive state (DDNA) of a system. In the DDNA state, the system on which the VCS One client daemon is installed is functional (up-and-running), however, the VCS One client daemon process has stopped.

If a system is in the DDNA state, the Policy Master does not failover service groups that are running on the system. The administrator must manually failover the service groups.

To simulate the DDNA state for one or more systems

- 1 In the VCS One console, locate the systems for which you want to simulate the DDNA state.
See [“Locating a system”](#) on page 295.
- 2 In the right pane, under **Systems**, select the check box that corresponds to the systems for which you want to simulate the DDNA state.
- 3 In the right pane, in the **Simulation** menu, click **Simulate Daemon Dead**.
- 4 Click **OK**.
- 5 Click **Close**.

To simulate the DDNA state for a system from the command line

- ◆ At the command prompt, type the following:

```
hasim -killclient system(s) [-user user@domain -domaintype
domaintype]
```

To restore a system that is currently in the DDNA state, you must perform a system repair operation.

More information is available about how to simulate a system repair operation. See [“Repairing a system using the Simulator”](#) on page 306.

Simulating a system heartbeat failure

This task is only available using the Simulator to simulate a system heartbeat failure. You must use the command line to simulate a heartbeat failure.

To simulate a system heartbeat failure

- ◆ At the command prompt, type the following:

```
hasim -disablelink system [-hb]
[-user user@domain -domaintype domaintype]
```

The simulator creates two links for each simulated system; one for communication and the other for heartbeats. This command simulates a hardware failure by stopping data flow over the communication link. Use the `-hb` option to stop the data flow on the heartbeat link.

Simulating a system heartbeat recovery

This task is only available using the Simulator to simulate a system heartbeat recovery. You must use the command line to simulate a heartbeat recovery.

To simulate a system heartbeat recovery

- ◆ At the command prompt, type the following:

```
hasim -enablelink system [-hb]  
[-user user@domain -domaintype domaintype]
```

This command restarts data flow on the faulted link and simulates a heartbeat recovery operation.

Managing service groups

This chapter includes the following topics:

- [About service groups](#)
- [Adding a service group](#)
- [Locating a service group](#)
- [Using the Group Dependency View](#)
- [Viewing service group attributes](#)
- [Editing attributes using the All Attributes link](#)
- [Refreshing a service group's SystemList](#)
- [Deleting a service group](#)
- [Modifying a service group](#)
- [Moving a service group to another organization tree node](#)
- [Bringing a service group online](#)
- [Taking a service group offline](#)
- [Switching a service group](#)
- [Flushing a pending action on a service group](#)
- [Flushing the plan of action on all service groups in the GTQ](#)
- [Stopping the current action for a service group in the GTQ](#)
- [Freezing a service group](#)
- [Unfreezing a service group](#)
- [Enabling a service group](#)
- [Disabling a service group](#)
- [Faulting a service group in the Simulator](#)

- Clearing a service group fault
- Linking service groups
- Unlinking service groups
- Enabling service group resources
- Disabling service group resources
- Probing service group resources
- Bringing service group resources online
- Taking service group resources offline
- Cloning service groups
- Changing a service group's priority value
- Changing a service group's load value
- Configuring a service group's SystemList with a list of systems
- Configuring a service group's compatibility list
- Configuring a service group's fault policy
- Creating an off-host resource in a service group

About service groups

A service group is a virtual container that contains all the hardware resources and software resources that are required to run the managed application.

See [“About service groups and service group dependencies”](#) on page 38.

Service groups can be dependent on each other to create more complex managed applications.

See [“About designing service group dependencies”](#) on page 247.

Service groups can run inside a Solaris Zone.

See [“Designing service groups that run in Solaris zones”](#) on page 264.

More information is available about service groups.

See [“About designing application placement policy”](#) on page 274.

See [“About designing the actions taken after a fault”](#) on page 228.

See [“Service group attributes”](#) on page 712.

Adding a service group

Use this procedure to add a service group.

Note that the GrpFaultPolicy attribute and the NodeFaultPolicy attribute determine the VCS One functional mode.

See [“About Veritas Cluster Server One”](#) on page 32.

To add a service group using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the right pane, from the **Configuration** menu, click **Add Service Group**.
- 4 Click **Next**.
- 5 In the **Service Group Configuration** screen, perform the following steps in the order presented:
 - In the **Name** box, enter the name of the service group. The name of the service group cannot not exceed 128 characters. It can not start with a number or contain special characters.
 - In the **Type** section, select either **Failover** or **Parallel**. A failover service group is brought online on only one system at a time. A parallel service group is simultaneously brought online on multiple systems.
 - In the **Priority** box, select the priority for the service group. 1 denotes highest priority while 5 denotes lowest priority.

- In the **Platform** box, select the platform on which the service group will run. Platform comprises the operating system and the recommended hardware architecture. For example, Solaris/SPARC.

Note: For the Solaris/x64 platform, select the solaris/x86 entry.

See [“PlatformName”](#) on page 717.

See [“About the configuration files”](#) on page 567.

- Check **Configure advanced workload management** if you want to configure AWM.
Advanced workload management is a feature that allows you to define the amount of resources a system has (Capacity) with respect to the amount of resources that a service group needs (Load).
Enter the values that correspond to the amount of resources that this service group needs.

Note: It is strongly recommended that you understand the AWM feature before entering values. You need to define Capacity on a system as well as Load on a service group for this feature.

See [“How you can define service group load and system capacity”](#) on page 59.

You can modify the service group’s load dimensions after the service group is created.

See [“Changing a service group’s load value”](#) on page 352..

- In the **Service Group Configuration** screen, do one of the following:
 - Click **Finish > Close**, to create an empty service group with no systems and resources.
You can add systems and resources to the service group at a later stage.
See [“Configuring a service group’s SystemList with a list of systems”](#) on page 353..
See [“Adding a resource to a service group”](#) on page 380.
 - Click **Next** to proceed.
- 6 In the **Organization Unit Selection** panel, under **Organization Tree**, expand the **ServerFarm (/)** node, and then select an organization unit node which will contain the service group. Service groups can be assigned to only Organization Unit Values (OU Values) and not Organization Unit Names (OU Names). Click **Next** to proceed to the **Assign Values to Extended Attributes** screen.
This panel will not appear if there is only one node, the root node, in your Organization tree.

- 7 In the **Assign Values to Extended Attributes** panel, select an extended attribute from the **Extended Attributes** box, and then in the **Value** box, select or enter a value for the extended attribute. Repeat this step for each extended attribute that you want to change. This screen is displayed only if extended attributes are defined for service groups. Click **Next** to proceed to the **System List Configuration** screen.

This panel will not appear if extended attributes are not configured.

- 8 In the SystemList Configuration panel, build the SystemList of the service group. Use the following information to perform this task.

Arrange the order of the systems	Click the table heading to arrange the systems in ascending or descending alphabetical order.
----------------------------------	---

Move a system between the Available System table and the SystemList table	Click the single right arrow or left arrow.
---	---

Move all systems between the Available System table and the SystemList table	Click the double right or left arrow.
--	---------------------------------------

- 9 To determine the list of systems in the Available Systems table, use one of the following filters. Depending on your selection, the appropriate screen is displayed. The following table illustrates the steps that need to be performed for each filter criteria.

Filter Criteria	Procedure
Name	Enter the name of a service group. Click Search .
Extended Attributes	<p>In the Select box, select Extended Attributes.</p> <p>Under Extended Attributes, select an extended attribute, and then select a value for the extended attribute. For free form extended attributes, select a node from the Extended Attributes tree and enter a value in the EA Expression: text box.</p> <p>You can select only one value per extended attribute. However, you can use multiple extended attributes.</p> <p>The appropriate EA expression is built and displayed in the EA Expression box. You can edit this expression.</p> <p>Click Apply.</p>

Filter Criteria	Procedure
Organization Tree	<p>In the Select box, select Organization Tree.</p> <p>Under OU Tree, select an organization tree node. The appropriate OU expression is displayed in the OU Expression box. You can edit this expression.</p> <p>Click Apply.</p>
Sets	<p>In the Select box, select Sets.</p> <p>Under Sets, select either Default or a custom view.</p> <p>In the OU Expression box, enter an OU Expression, if required.</p> <p>In the EA Expression box, enter an EA Expression, if required.</p> <p>Click Apply.</p>
Expression	<p>In the Select box, select Expression.</p> <p>In the OU Expression box, enter an OU Expression, if required.</p> <p>In the EA Expression box, enter an EA Expression, if required.</p> <p>Click Apply.</p>
Attribute	<p>In the Select box, select Attribute.</p> <p>Under Capacity, select either Total or Available.</p> <p>Enter values for the load dimensions defined in the VCS One cluster, and then click Apply.</p>

Systems displayed under **Available Systems** with an asterisks sign (*) indicate that they were selected as part of the previous expression.

- 10 Click **Next**.
- 11 Skip to [step 13](#) if the service group does not run on a container-enabled platform.
- 12 In the **Specify the container type for the service group** screen, do one of the following:
 - Click **Next**, if you do not want to specify a container resource for the service group.
 - Select the **Associate Service Group with a Container** check box, if you want to specify a container resource.

A container resource is used when you configure a service group that is associated with a Solaris Zone or an AIX WPAR. VCS One manages the container as part of the service group and propagates the service group's load dimension values to the respective resource so that limits can be set at the container level. In the **Specify container type for the**

service group screen, perform the following steps in the order presented:

- In the **Type** box, select either **Zone** or **WPAR**.
The XRM option refers to directly using Solaris projects without using Solaris containers. This support has been deprecated in this release.
- In the **Name** box, enter the name of the container.
- In the **Enabled** box, select **Yes** to enable the container association or select **No** to disable the container association.
- Click **Add Container resource to Service Group**.
- In the **Resource Name** box, enter the name of the container resource.
- Click **Next**.

More information is available on Solaris zones.

See [“Managing objects in Solaris zones”](#) on page 433.

- 13 In the **Add Resources** screen, perform the following steps for each resource that you want to add:
 - In the **Type** box, select the resource type.
 - In the **Name** box, enter the name of the resource.
 - Select the **Enable Resource** check box, if you want to enable the resource.
 - Click **Add Resource**, to add the resource to **Resource List**.
 - Under **Resource List**, select the resource, and then click the **Edit** icon.
 - In the **Edit Resource** screen, under **Attribute List**, click a resource attribute and do one of the following:
 - Under **Apply to**, select the **All systems in the systemlist** option, and then in the **Value** box enter a value for the resource attribute. The resource attribute value is global and is the same on all systems defined in the service group’s SystemList attribute. Click **OK** to return to the **Add Resources** screen.
 - Under **Apply to**, select the **Selected systems** option, select a system, then in the **Value** box enter a value for the resource attribute. The resource attribute value is local and is applicable only to the selected system. Repeat this step for each system. Click **OK** to return to the **Add Resources** screen.
 - In the **Add Resource** screen, click **Next** to proceed to the **Link/Unlink Resources** screen.

- 14 In the **Link/Unlink Resources** screen, perform the following steps for each resource dependency that you want to create:
 - In the **Parent Resource** box, select the parent resource.
 - In the **Child Resource** box, select the child resource. Only available child resources that can be linked are displayed.
 - Click **Add Link** to create a dependency link between the parent and child resources.
 - After a resource dependency is created, the parent and child resources are displayed under **Currently linked**. To remove the resource dependency, click the corresponding Remove icon.
- 15 In the **Link/Unlink Resources** screen, click **Finish**.
- 16 In the Result panel, click **Finish** or **Advanced**.

Advanced will allow you to configure service group compatibility and service group fault policy.

See [“Application relationships through service group compatibility”](#) on page 278.

See [“About designing the actions taken after a fault”](#) on page 228.
- 17 Click **Close**.
- 18 In the **Results** screen, do one of the following:
 - Click **Close**, to exit the **Service Group Configuration Wizard**. If errors are encountered while creating the service group, click **Error Details** for more information about the errors.
 - Click **Advanced**, to configure the service group’s compatibility list and failover policy. You can configure the service group’s compatibility list and failover policy at a later stage.

See [“Configuring a service group’s compatibility list”](#) on page 355.

See [“Configuring a service group’s fault policy”](#) on page 356.
- 19 After you configure the service group’s compatibility list and failover policy, in the **Configure Fault Policy** screen, click **Finish**.
- 20 Click **Close**.

To add a service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -add service_group [-platform platform] [ouvaluepath]
[-user user@domain] [-domaintype domaintype]
```

To specify the service group’s SystemList from the command line

- ◆ At the command prompt, type the following:

```
hagrp -modify service_group SystemList -add system_1 0 system_2  
1 ... system_n (n-1)
```

where 0, 1, are the priorities for the systems.

To specify the service group type (parallel or failover) from the command line

- ◆ At the command prompt, type the following:

```
hagrp -modify service_group Parallel 0
```

A failover service group runs only on one system at a time; a parallel service group runs concurrently on multiple systems.

To specify the service group's load dimensions from the command line

- ◆ At the command prompt, type the following:

```
hagrp -modify service_group Load -update cpu 2 memory 2 stbw 2  
nwbw 2
```

To specify the service group's compatibility list from the command line

- ◆ At the command prompt, type the following:

```
hagrp -incompatible service_group1 service_group2 [-user  
user@domain] [-domaintype domaintype]
```

For example, if group SG1 cannot co-exist with group SG2, type the following:

```
hagrp -incompatible SG1 SG2
```

To specify the failover policy for the service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -modify service_group GrpFaultPolicy policy
```

where, *policy* can be either Failover or NoFailover.

After the service group is created, you need to add resources to the service group.

Locating a service group

Use this procedure to locate a service group.

You can use one or more of the following structures to locate a service group in VCS One:

- Organization Tree
- Extended Attributes
- Sets

To locate a service group using the organization tree

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select **Organization Tree** from the drop-down list.
- 4 In the left pane, select the appropriate organization tree node (OU Name node or OU Value node).
- 5 In the right pane, view all the service groups associated with the selected organization tree node.

To locate a service group using extended attributes

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the right pane, use the **EA Filter** to view service groups by extended attribute.
See [“Filtering results in a table”](#) on page 115.

To locate a service group using sets

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select either **My Objects** or a user-defined set from the drop-down list.
- 4 In the right pane, view all the service groups associated with the selected set.

To locate a service group multiple filtering methods

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select **Organization Tree** from the drop-down list
- 4 Click a node in the organization tree.
- 5 In the right pane, view all the service groups associated with that organization tree node.
- 6 In the right pane, use the **EA Filter** box to further filter the service groups. Click the down arrow next to **EA Filter** to choose extended attributes.
- 7 Enter text in the **Keyword** text box to further limit the search within the service groups currently displayed.
To display the Keyword text box, click the **+** next to **EA Filter**.

- 8 Click **Go**.
- 9 In the right pane, view all the service groups that match the search criteria.

Using the Group Dependency View

The VCS One console provides various views to effectively manage the VCS One cluster. This section provides information about the different views related to service group administration.

Additional information is available about how to use the dependency view.

See [“Summary information on the dependency view”](#) on page 135.

Locating the Group Dependency View

Use this procedure to locate the group dependency view. You require at least Read privileges on the service group to view its dependencies.

To locate the group dependency view

- 1 In the VCS One console, locate the service group, which you want to view.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, check the service group.
- 3 Click **Views > Group Dependencies**.

Performing operations from the Group Dependency View

The group dependency view displays the dependencies for the selected service group.

You can perform the following operations in the service group dependency view:

- Bring a service group online
See [“Bringing a service group online”](#) on page 329.
- Take a service group offline
See [“Taking a service group offline”](#) on page 333.
- Switch service groups
See [“Switching a service group”](#) on page 336.
- Link service groups
See [“Linking service groups”](#) on page 345.
- Unlink service groups
See [“Unlinking service groups”](#) on page 346.
- Freeze the service group

See “[Freezing a service group](#)” on page 339.

- Unfreeze the service group
See “[Unfreezing a service group](#)” on page 340.
- Enable the service group
See “[Enabling a service group](#)” on page 342.
- Disable the service group
See “[Disabling a service group](#)” on page 342.
- Flush the service group
See “[Flushing a pending action on a service group](#)” on page 337.
- Clear a service group fault
See “[Clearing a service group fault](#)” on page 344.

Viewing service group attributes

Use this procedure to view service group attributes.

To view service group attributes using the VCS One console

- 1 In the VCS One console, locate the service group that you want to view.
See “[Locating a service group](#)” on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the right pane, click **All Attributes**.
- 4 Click the arrow symbol in the **Attribute Name** column to sort the list in ascending or descending alphabetical order.

To view service group attributes from the command line

- ◆ At the command prompt, type the following:

```
hagrp -display [service_group(s) | -ou expression | -ea  
expression | -ou expression -ea expression | -setname setname]  
[-attribute attribute(s) [-sys system(s)] [-user user@domain] [-  
domaintype domaintype]
```

Editing service group attributes

Use this procedure to edit service group attributes.

To edit service group attributes using the VCS One console

- 1 Locate the service group that you want to modify.
See “[Locating a service group](#)” on page 321.

- 2 In the right pane, select the check box corresponding to the service group that you want to edit.
- 3 In the right pane, from the **Configuration** menu, click **Edit Attribute(s)**.
- 4 In the **Edit Attribute** dialog box, perform the following steps for each service group attribute that you want to edit:
 - In the **Attribute(s)** column, select the attribute that you want to modify. Only attributes that can be modified are displayed in this list.
 - Click **For all Group(s)** to configure the same value for all the selected groups, or click **For selected Group(s)** if you want to configure different values for each selected group.
 - Click the pencil icon to edit the value.
 - Check **Propagate** to propagate the change to all service groups in the local dependency tree. Note that the **Propagate** check box is displayed only for specific attributes.
- 5 Click **Next > Finish > Close**.

Editing attributes using the All Attributes link

To edit attributes using the All Attributes link

- 1 In the **All Attributes** page, click the **Edit** icon corresponding to the attribute, which you want to edit.
 You may only edit attributes of global scope from this page.
- 2 In the **Edit Attribute** dialog box, perform the following steps:
 - In the **Value** box, enter or select a value for the specified attribute.
 - Select the **Propagate** check box to propagate the change to all service groups in the local dependency tree. Note that the **Propagate** check box is displayed only for specific attributes.
- 3 In the **Edit Attribute** dialog box, click **OK**.

Refreshing a service group's SystemList

The SystemList attribute of a service group denotes the list of systems on which the service group is configured to run. The SystemList value may be an explicit list of systems. The SystemList value can also be derived from an expression containing either or both of extended attributes and an OUValue node.

See "[SystemListExpr](#)" on page 719.

This operation is used to refresh the system list of a service group by evaluating the system list expression. This operation results in addition of systems to the system list of the service group which satisfy the system list expression, and removal of systems which do not satisfy the expression.

Invoke this operation after changing the system list expression attribute of a service group.

To refresh a service group's SystemList

- 1 In the VCS One console, locate the service group that you want to bring online.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, click **Operations > Refresh System List**.
- 3 Click **OK > Close**.

Deleting a service group

Use this procedure to delete a service group. You may not delete a service group that is online.

More information is available about deleting resources from a service group. See [“Deleting a resource from a service group”](#) on page 381.

To delete a service group using the VCS One console

- 1 In the VCS One console, locate the service group that you want to delete.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group that you want to delete.
- 3 In the right pane, from the **Configuration** menu, click **Delete Service Group**.
- 4 In the **Delete Service Group** dialog box, click **OK**.

To delete multiple service groups using the VCS One console

- 1 In the VCS One console, locate the service groups that you want to delete.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, select the check box corresponding to the service groups that you want to delete.
- 3 In the right pane, from the **Configuration** menu, click **Delete Service Group(s)**.
- 4 Select the **Forcefully remove group dependencies** check box, to remove the service group dependencies before it is deleted.

- 5 In the **Delete Service Group(s)** dialog box, click **OK**.

To delete a service group from the command line

- ◆ At the command prompt, type the following:
`hagrp -delete service_group`

To delete a service group and its resources from the command line

- ◆ At the command prompt, type the following:
`hagrp -delete -force service_group`

Modifying a service group

Use this procedure to modify a service group. Using this wizard, you may not modify the name, the platform, or the type of this service group.

To modify a service group using the VCS One console

- 1 In the VCS One console, locate the service group that you want to modify. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, select the service group that you want to modify.
- 3 In the right pane, from the **Configuration** menu, click **Modify Service Group**. The **Service Group Configuration Wizard** is used for adding and modifying a service group. An in-depth explanation of this wizard is covered in the [Adding a service group](#) section. See [“Adding a service group”](#) on page 315.

To modify a service group from the command line

- ◆ At the command prompt, type the following:
`hagrp -modify [-propagate] [-refreshvars] group attribute {key value} ... [-sys system] [-user user@domain] [-domaintype domaintype]`

Moving a service group to another organization tree node

You may move a service group to any OUvalue node in the organization tree if you have appropriate privileges.

See [“Modify OU”](#) on page 634.

If the service group has an extended attribute that is a variable, and that attribute value is invalid at the new organization tree location, the move operation is rejected and an error message is generated.

To override this behavior and move the service group, use the `–refreshvars` option. Doing so will update value of the resource attribute.

To move one or more service groups to another organization tree node

- 1 In the VCS One console, locate the service groups that you want to move. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, select the check box corresponding to the service groups that you want to move.
- 3 In the right pane, from the **Configuration** menu, click **Move Service Group(s)**.
- 4 In the **Organization Unit Selection** dialog box, perform the following steps in the order presented:
 - Under **Organization Tree**, expand the **ServerFarm** node, and select the OU Value node to which you want to move the service groups.
 - Consider the **Modify Privileges if move violates the assigned roles of users** option. Consider this option in the use case when the service group moves to an OUValue node that is not in the subtree of the original organization tree node. In this case, you must check this option to remove privileges from users attached at the original node that are no longer valid due to the move of the service group. Otherwise, the move is rejected. This option is equivalent to the `-updateroles` option in the command line.
 - Click **Next**.
 - Click **Close**.
- 5 In the **Assign Values to Extended Attributes** dialog box, assign extended attribute values for the service groups. This dialog box is displayed only if extended attributes are defined for the selected node or any preceding nodes in the organization tree hierarchy.
- 6 Click **OK**.

To move one or more service groups to another organization tree node from the command line

- ◆ At the command prompt, type the following:


```
hagrp -move [-updateroles] service_groups -ou ouvaluepath [-user user@domain] [-domaintype domaintype]
```

Bringing a service group online

Use this procedure to bring a service group online.

To bring a service group online

- 1 In the VCS One console, locate the service group that you want to bring online.
 See [“Locating a service group”](#) on page 321.
- 2 In the right pane, from the **Operations** menu, click one of the following options:
 - **Online on system:** To bring the service group online on a single system
 - **Online Any/Everywhere:** To either bring a failover service group online on any valid system or to bring a parallel service group online on all valid systems.
- 3 In the Online Service Group panel, use the following information to fill in the fields:

Select the system you want to online this service group	<i>System_Name:</i> To online the service group on that system.
	Anywhere: To online a failover service group on any valid system.

	Everywhere: To online a parallel service group on all valid systems.
--	---

Evacuate lower priority service group	Check if you want service groups with a lower Priority attribute value to go offline if their resources are needed in order to bring this service group online.
---------------------------------------	---

Low priority service groups are evacuated if the total Load of all service groups exceeds the system's Capacity.

Do not add Intent Online entries	Check if you do not want the state of the service group set to INTENT-ONLINE in the GTQ if this group can not be brought online.
----------------------------------	--

See [“Mapping an application placement decision”](#) on page 282.

Propagate	If you want this online action to apply to all service groups in the same service group dependency tree.
-----------	--

For example, to bring a parent service group online and propagate the command to child service groups.

Ignore the standby relationship while onlining	The online operation will fail if the service group has a standby group running on a different system than the target system. Check this option to change this behavior and ignore the standby group relationship.
--	---

4 Click **OK**.

To bring a Parallel service group online on all configured systems using the command line

◆ At the command prompt, type the following:

```
hagrp -online [-ejectlowpri][-nointent] group -everywhere  
[-user user@domain] [-domaintype domaintype]
```

To bring a service group online from the Group Dependency view

- 1 In the VCS One console, locate the service group that you want to bring online.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, check the service group that you want to bring online.
- 3 In the left pane, under **Views**, click **Group Dependencies**.
- 4 In the **Service Group dependency view**, right-click the service group to be brought online, and then click **Online**.
- 5 In the **Online Service Group** dialog box, select the system where the service group will be brought online. To bring the service group online on any system in the SystemList, select **Anywhere**. In case of parallel service groups, the **Anywhere** option is replaced by the **All Systems** option.
- 6 Select the **Evacuate lower priority service group** check box, if you want to evacuate other low priority service groups on the specified system. Low priority service groups will be evacuated if the total load of all service groups exceeds the system’s capacity.
- 7 Select the **Do not add intent Online entries** check box, if you do not want to mark the service group as INTENT ONLINE until it comes online. A service group enters the INTENT ONLINE state when it is waiting to come online on a specific system.
- 8 In the **Online Service Group** dialog box, click **OK**.

To online multiple service groups

- 1 In the VCS One console, locate the service groups that you want to bring online.
See “[Locating a service group](#)” on page 321.
- 2 In the right pane, under **Service Groups**, select the check box corresponding to the service groups that you want to bring online.
- 3 In the right pane, from the **Operations** menu, click **Online Anywhere**. The **Online Service Group(s)** dialog box is displayed.
- 4 In the **Online Service Group(s)** dialog box, click **OK**.
- 5 In the **Online Service Group(s)** dialog box, click **Close**.

To online multiple service groups using the organization tree

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select **Organization Tree** from the list. Select the appropriate OU Value node associated with the service groups that you want to bring online.
- 4 Right-click the selected OU Value object, and then click **Online**. The **Online OU** dialog box is displayed. If you are using the Firefox Web browser on a Linux computer, right-click the OU Value node, keep the right mouse button pressed, point to **Online**, and then release the right mouse button.
- 5 In the **Online OU** dialog box, click **OK**.
- 6 In the **Results** dialog box, click **Close**.

To online multiple service groups using sets

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select the set associated with the service groups that you want to bring online.
- 4 Right-click the set, and then click **Online**. The **Online Set** dialog box is displayed.
 - In the **Online Set** dialog box, perform the following steps in the order presented:
 - Select the system where you want to bring the set online.
 - Select the **Evacuate lower priority service groups** check box, if you want to evacuate lower priority service groups in case of a system capacity overflow.

- Select the **Do not add Intent Online entries** check box, if you do not want the service groups that are associated with the set to be marked as INTENT ONLINE until they come online. A service group enters the INTENT ONLINE state when it is waiting to come online on a specific system.
- 5 In the **Online Set** dialog box, click **OK**.

To online multiple service groups using custom views

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select the set associated with the custom view. A set can contain one or more custom views. Expand the appropriate custom view, and select the extended attribute value associated with the service groups that you want to bring online.
- 4 Right-click the selected extended attribute value, and then click **Online**. The **Online Service Group(s)** dialog box is displayed.
- 5 In the **Online Service Group(s)** dialog box, click **OK**.
- 6 In the **Online Service Group(s)** dialog box, click **Close**.

To bring a service group online on a specific system from the command line

- ◆ At the command prompt, type the following:

```
hagrpg -online [-ejectlowpri] group -sys system  
[-user user@domain] [-domaintype domaintype]
```

To bring the service group online on any system from the command line

- ◆ At the command prompt, type the following:

```
hagrpg -online [-ejectlowpri][-nointent] group -any  
[-user user@domain] [-domaintype domaintype]
```

To bring all the service groups online from the command line

- ◆ At the command prompt, type the following:

```
hagrpg -online [-ejectlowpri][-nointent] -all [-user user@domain]  
[-domaintype domaintype]
```

To bring parent and child service groups online concurrently from the command line

- ◆ At the command prompt, type the following:

```
hagrpg -online [-ejectlowpri | -propagate] group -sys system  
[-user user@domain] [-domaintype domaintype]
```

Taking a service group offline

Use this procedure to take a service group offline.

To take a service group offline using the VCS One console

- 1 In the VCS One console, locate the service group that you want to take offline.
 See [“Locating a service group”](#) on page 321.
- 2 In the right pane, from the **Operations** menu, click one of the following options:
 - **Offline on system:** To take the service group offline on a single system
 - **Online Everywhere:** This command takes the specified service group and all its dependent service groups offline from all the systems on which they are currently online.
- 3 In the Offline Service Group panel, use the following information to fill in all relevant fields:

Select the system you want to offline this group from	Click the name of the system on which you want the service group to be offline.
---	---

Forcefully offline the group if the system is in DDNA state.	Check to offline the service group on a system in the DDNA state. Daemon Dead Node Alive state indicates the vcsoneclientd process on the system, which is still alive, does not send heartbeats to the Policy Master.
--	---

Propagate	Check if you want this offline action to apply to all service groups in the same service group dependency tree. For example, to take a parent service group offline and propagate the command to all child service groups.
-----------	---

- 4 Click **OK**.

To take a service group offline from the group dependency view

- 1 In the VCS One console, locate the service group that you want to take offline.
 See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, check the service group that you want to take offline.

- 3 In the left pane, under **Views**, click **Group Dependencies**. The **Service Group dependency view** is displayed.
- 4 In the **Service Group dependency view**, right-click the service group that you want to take offline, and then click **Offline**. The **Offline Service Group** dialog box is displayed.
- 5 In the **Offline Service Group** dialog box, click **OK**.

To take multiple service groups offline

- 1 In the VCS One console, locate the service group that you want to take offline.
See “[Locating a service group](#)” on page 321.
- 2 In the right pane, under **Service Groups**, select the check box corresponding to the service groups that you want to take offline.
- 3 In the right pane, from the **Operations** menu, click **Offline**. The **Offline Service Group(s)** dialog box is displayed.
- 4 In the **Offline Service Group(s)** dialog box, click **OK**.
- 5 In the **Offline Service Group(s)** dialog box, click **Close**.

To take multiple service groups offline using the organization tree

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select **Organization Tree** from the list. Select the appropriate OU Value node associated with the service groups that you want to take offline.
- 4 Right-click the selected OU Value object, and then click **Offline**. The **Offline OU** dialog box is displayed. If you are using the Firefox Web browser on a Linux computer, right-click the OU Value node, keep the right mouse button pressed, point to **Offline**, and then release the right mouse button.
- 5 In the **Offline OU** dialog box, click **OK**.
- 6 In the **Results** dialog box, click **Close**.

To take multiple service groups offline using sets

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select the set associated with the service groups that you want to take offline.

- 4 Right-click the set, and then click **Offline**. The **Offline Set** dialog box is displayed.
- 5 In the **Offline Set** dialog box, click **OK**.
- 6 In the **Results** dialog box, click **Close**.

To take multiple service groups offline using custom views

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select the set associated with the custom view. A set can contain one or more custom views. Expand the appropriate custom view, and then select the extended attribute value associated with the service groups that you want to take offline.
- 4 Right-click the selected extended attribute value, and then click **Offline**. The **Offline Service Group(s)** dialog box is displayed.
- 5 In the **Offline Service Group(s)** dialog box, click **OK**.
- 6 In the **Offline Service Group(s)** dialog box, click **Close**.

To take a service group offline on a specific system from the command line

- ◆ At the command prompt, type the following:

```
hagrp -offline [-propagate] group -sys system
[-user user@domain] [-domaintype domaintype]
```

To take a service group offline on all systems using the command line

- ◆ At the command prompt, type the following:

```
hagrp -offline -propagate group -everywhere
[-user user@domain] [-domaintype domaintype]
```

This command takes the specified service group and all its dependent service groups offline from all the systems on which they are currently online.

To take child and parent groups offline concurrently from the command line

- ◆ At the command prompt, type the following:

```
hagrp -offline -propagate group -sys system
[-user user@domain] [-domaintype domaintype]
```

To take child and parent service groups offline on all systems from command line

- ◆ At the command prompt, type the following:

```
hagrp -offline -propagate group -everywhere
[-user user@domain] [-domaintype domaintype]
```

This command takes the specified service group and all its dependent service groups offline from all the systems on which they are currently online.

Switching a service group

Use this procedure to switch a service group. When you switch a service group it is taken offline from its current system and brought online on another system.

To switch a service group

- 1 In the VCS One console, locate the service group that you want to switch. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, check the service group that you want to switch.
- 3 In the right pane, from the **Operations** menu, click **Switch**. The **Switch Service Group** dialog box is displayed.
- 4 In the **Switch Service Group** dialog box, select the system where you want the service group to be switched. To switch the service group to any system listed in the service group’s SystemList, select **Anywhere**. In case of parallel service groups, the **Anywhere** option is replaced by the **All Systems** option.
- 5 Select the **Evacuate lower priority service groups** check box, if you want to evacuate other low priority service groups on the specified system. Low priority service groups will be evacuated if the total load of all service groups exceeds the system’s capacity.
- 6 Consider the **Ignore the standby relationship** option. The switch operation will fail if the service group has a standby group running on a different system than the target system. Check this option to change this behavior and ignore the standby group relationship.
- 7 Consider the **Propagate** option. If you want this switch action to apply to all service groups in the same service group dependency tree. For example, to switch a parent service group and propagate the command to child service groups.
- 8 In the **Switch Service Group** dialog box, click **OK**.

To switch a service group from the group dependency view

- 1 In the VCS One console, locate the service group that you want to switch. See [“Locating a service group”](#) on page 321.

- 2 In the right pane, under **Service Groups**, check the service group that you want to switch.
- 3 In the left pane, under **Views**, click **Group Dependencies**. The **Service Group dependency view** is displayed.
- 4 In the **Service Group dependency view**, right-click the service group to be switched, and then click **Switch**. The **Switch Service Group** dialog box is displayed.
- 5 In the **Switch Service Group** dialog box, select the system where you want the service group to be switched. To switch the service group to any system listed in the service group's SystemList, select **Anywhere**. In case of parallel service groups, the **Anywhere** option is replaced by the **All Systems** option.
- 6 Select the **Evacuate lower priority service groups** check box, if you want to evacuate other low priority service groups on the specified system. Low priority service groups will be evacuated if the total load of all service groups exceeds the system's capacity.
- 7 In the **Switch Service Group** dialog box, click **OK**.

To switch a service group to a specific system from the command line

- ◆ At the command prompt, type the following:

```
hagrp -switch [-ejectlowpri | -propagate] group -to system  

[-user user@domain] [-domaintype domaintype]
```

When the *-propagate* option is specified and the service group has a local soft parent group online, the switch operation fails. However, if the service group has a global soft parent group online, the switch operation succeeds, but the global soft parent group is not switched and remains online on the same system.

To switch a service group to any system from the command line

- ◆ At the command prompt, type the following:

```
hagrp -switch [-ejectlowpri] group -any  

[-user user@domain] [-domaintype domaintype]
```

Flushing a pending action on a service group

You flush a pending action on a service group to cancel the online or offline operation that is currently being performed on the service group.

A flush is useful if the online or offline operation of the service group is not successful. In this case, you can flush the service group, resolve the error, and restart the online or offline operation.

You may also need to flush the GTQ to cancel the intent online entry for the service group.

See [“Flushing the plan of action on all service groups in the GTQ”](#) on page 338.

To flush a service group using the VCS One console

- 1 In the VCS One console, locate the service group that you want to flush. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group that you want to flush to go to the service group’s Details page.
- 3 In the right pane, from the **Operations** menu, click **Flush**. The **Flush Service Group** dialog box is displayed.
- 4 In the **Flush Service Group** dialog box, select the system on which you want to flush the service group.
- 5 Click **OK**.

To flush a service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -flush [-action] group -sys system  
[-user user@domain] [-domaintype domaintype]
```

Flushing the plan of action on all service groups in the GTQ

You can flush the plan of action on all service groups in the GTQ if you do not want the Policy Master to execute the planned GTQ actions.

See [“Mapping an application placement decision”](#) on page 282.

To flush the plan of action on a service group in the GTQ

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Workload** tab.
- 3 In the right pane, in the Waiting Groups panel, use the right-click mouse button to click **Flush all groups**.
- 4 In the Confirmation window, click **Yes**.

Stopping the current action for a service group in the GTQ

Every service group in the GTQ has an action plan. You may abort the action in progress without affecting the remainder of the plan.

To stop the current action for a service group in the GTQ

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Workload > Views > GTQ View**
- 3 In the Group Transition Queue panel, place the cursor over the service group on which you want to operate.
- 4 Right-click **Abort Action**.
- 5 In the Confirmation window, click **Yes**.

Freezing a service group

Freezing a service group enforces the following conditions:

- Online and offline operations are not allowed on the service group.
- The service group can not failover to another system.
- A manual switch of the service group is not allowed.

Freezing a service group is useful when you want to stop your operations, such as maintenance activities, from triggering a service group failover.

To freeze a service group

- 1 In the VCS One console, locate the service group that you want to freeze. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, check the service group that you want to freeze.
- 3 In the right pane, from the **Operations** menu, click **Freeze**. The **Freeze Service Group** dialog box is displayed.
- 4 In the **Freeze Service Group** dialog box, select the **Propagate to dependent groups** check box, if you want to propagate the freeze operation to the dependent service groups.
- 5 In the **Freeze Service Group** dialog box, click **OK**.

To freeze multiple service groups

- 1 In the VCS One console, locate the service groups that you want to freeze. See “[Locating a service group](#)” on page 321.
- 2 In the right pane, under **Service Groups**, select the check box corresponding to the service groups that you want to freeze.
- 3 In the right pane, from the **Operations** menu, click **Freeze**. The **Freeze Service Group(s)** dialog box is displayed.
- 4 In the **Freeze Service Group(s)** dialog box, select the **Propagate to dependent groups** check box, if you want to propagate the freeze operation to the dependent service groups.
- 5 In the **Freeze Service Group(s)** dialog box, review the list of service groups to be frozen.
- 6 Click **OK**.
- 7 In the **Freeze Service Group(s)** dialog box, click **Close**.

To freeze multiple service groups using custom views

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select the set associated with the custom view. A set can contain one or more custom views. Expand the appropriate custom view, and select the extended attribute value associated with the service groups that you want to freeze.
- 4 Right-click the selected extended attribute value, and then click **Freeze**. The **Freeze Service Group(s)** dialog box is displayed.
- 5 In the **Freeze Service Group(s)** dialog box, click **OK**.
- 6 In the **Freeze Service Group(s)** dialog box, click **Close**.

To freeze a service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -freeze [-propagate] group [-user user@domain]
[-domaintype domaintype]
```

Unfreezing a service group

You may only unfreeze a service group that is already in the FROZEN state.

Unfreezing a service group enforces the following conditions:

- All service group online and offline operations can once again occur.

- The service group can once again failover to another system, per policy configuration.
- A manual switch of the service group is allowed.

To unfreeze a service group

- 1 In the VCS One console, locate the service group that you want to unfreeze. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, check the service group that you want to unfreeze.
- 3 In the right pane, from the **Operations** menu, click **Unfreeze**. The **Unfreeze Service Group** dialog box is displayed.
- 4 In the **Unfreeze Service Group** dialog box, select the **Propagate to dependent groups** check box, if you want to propagate the unfreeze operation to the dependent service groups.
- 5 In the **Unfreeze Service Group** dialog box, click **OK**.

To unfreeze multiple service groups

- 1 In the VCS One console, locate the service groups that you want to unfreeze. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, select the check box corresponding to the service groups that you want to unfreeze.
- 3 In the right pane, from the **Operations** menu, click **Unfreeze**. The **Unfreeze Service Group(s)** dialog box is displayed.
- 4 In the **Unfreeze Service Group(s)** dialog box, select the **Propagate to dependent groups** check box, if you want to propagate the unfreeze operation to the dependent service groups.
- 5 In the **Unfreeze Service Group(s)** dialog box, click **OK**.
- 6 In the **Unfreeze Service Group(s)** dialog box, click **Close**.

To unfreeze multiple service groups using custom views

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 In the left pane, select the set associated with the custom view. A set can contain one or more custom views. Expand the appropriate custom view, and select the extended attribute value associated with the service groups that you want to unfreeze.

- 4 Right-click the selected extended attribute value, and then click **Unfreeze**. The **Unfreeze Service Group(s)** dialog box is displayed.
- 5 In the **Unfreeze Service Group(s)** dialog box, click **OK**.
- 6 In the **Unfreeze Service Group(s)** dialog box, click **Close**.

To unfreeze a service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -unfreeze [-propagate] group  
[-user user@domain] [-domaintype domaintype]
```

Enabling a service group

Use this procedure to enable a service group. You need to enable a service group before it can be brought online. During maintenance operations, if a service group is manually disabled, it must be enabled prior to being brought online after the maintenance operation is completed.

To enable a service group using the VCS One console

- 1 In the VCS One console, locate the service groups that you want to enable. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service groups that you want to enable.
- 3 In the right pane, from the **Operations** menu, click **Enable**. The **Enable Service Group** dialog box is displayed.
- 4 In the **Enable Service Group** dialog box, specify the system on which you want to enable the service group.
- 5 Click **OK**.

To enable a service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -enable group [-sys system]  
[-user user@domain] [-domaintype domaintype]
```

Disabling a service group

Use this procedure to disable a service group. When a service group is disabled, it cannot be brought online or taken offline. The disable operation temporarily stops VCS One from monitoring the service group.

To disable a service group using the VCS One console

- 1 In the VCS One console, locate the service groups that you want to disable. See “[Locating a service group](#)” on page 321.
- 2 In the right pane, under **Service Groups**, click the service groups that you want to disable.
- 3 In the right pane, from the **Operations** menu, click **Disable**. The **Disable Service Group** dialog box is displayed.
- 4 In the **Disable Service Group** dialog box, specify the system on which you want to disable the service group.
To disable the service group on all the systems, select **All Systems**.
- 5 Click **OK**.

To disable a service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -disable group [-sys system]
[-user user@domain] [-domaintype domaintype]
```

Faulting a service group in the Simulator

This task is only available using the Simulator, to simulate a service group fault.

To simulate a fault for one or more service groups

- 1 In the VCS One console, locate the service groups for which you want to simulate a fault. See “[Locating a service group](#)” on page 321.
- 2 In the right pane, under **Service Groups**, select the check box that corresponds to the appropriate service groups.
- 3 In the right pane, in the Simulation menu, click **Fault Service Groups**.
- 4 In the **Fault Service Groups** dialog box, select the system on which you want to fault the service groups.
- 5 Click **OK**.
- 6 Click **Close**.

To simulate a service group fault from the command line

- ◆ At the command prompt, type the following:

```
hasim -faultgrp group [-sys system]
[-user user@domain -domaintype domaintype]
```

Clearing a service group fault

Use this procedure to clear a service group fault. When a service group faults on a system, you need to clear the service group fault, before attempting to bring the service group online on the same system.

You can clear one fault, multiple faults or all the faults in a node of the organization tree.

To clear a service group fault

- 1 In the VCS One console, locate the faulted service group.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the faulted service group.
- 3 In the right pane, from the **Operations** menu, click **Clear Fault**. The **Clear fault for Service Group** dialog box is displayed.
- 4 In the **Clear fault for Service Group** dialog box, select the system on which you want to clear the service group fault. Select **All Systems**, to clear the service group fault on all the systems.
- 5 In the **Clear fault for Service Group** dialog box, click **OK**.

To clear multiple service group faults

- 1 In the VCS One console, locate the faulted service groups.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, select the check box corresponding to one or more faulted service groups.
- 3 In the right pane, from the **Operations** menu, click **Clear Fault**. The **Clear Service Groups Fault(s)** dialog box is displayed.
- 4 Click **OK > Close**.

To clear all the faults in a node of the organization tree

- 1 In the VCS One console, click **Manage > SGs and CSGs > Service Groups**.
- 2 In the left pane, click the organization tree node.
- 3 Click **Operations > Clear All Faults**.
- 4 Click **OK > Close**.

To clear a service group fault from the command line

- ◆ At the command prompt, type the following:

```
hagrp -clear {group | -setname setname | -ou expression | -ea  
expression | -ou expression -ea expression} [-sys system] [-user  
user@domain] [-domaintype domaintype]  
[-info]
```

Linking service groups

Use this procedure to link service groups. When service groups are linked, a dependency is created between them. As a result of this dependency, one service group becomes the parent service group and other becomes the child service group. The child service group must be brought online before the parent service group is brought online.

See [“About service groups and service group dependencies”](#) on page 38.

To link service groups using the VCS One console

- 1 In the VCS One console, locate the service groups that you want to link. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, from the **Configuration** menu, click **Create Group Dependency**.
- 3 In the **Create Service Group Dependency** dialog box, perform the following steps in the order presented:
 - In the **Select the parent group** box, select the parent service group.
 - In the **Select the child group** box, select the child service group.
 - Under **Relationship**, select one of the following:
 - Select **Local**, if the parent and child service groups must be brought online on the same system.
 - Select **Global**, if the parent and child service groups can be brought online on different systems.
 - Under **Dependency Type**, select one of the following:
 - Select **Firm**, if the parent and child service groups can be brought online or taken offline with moderate constraints.
 - Select **Soft**, if the parent and child service groups can be brought online or taken offline with minimum constraints.
 - Select **Hard**, if the parent and child service groups can be brought online or taken offline with maximum constraints.

More information is available about service group dependency types. See [“Soft, firm, and hard dependencies”](#) on page 250.
- 4 In the **Link Service Groups** dialog box, click **OK**.
- 5 In the **Results** dialog box, click **Close**.

To link service groups from the group dependency view

- 1 In the VCS One console, locate the service groups that you want to link. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group that you want to link.
- 3 In the left pane, under **Views**, click **Group Dependencies**.
- 4 In the **Group Dependency View**, right-click on the background. You may click one of the graph items for other action options.
- 5 Click **Create Group Dependency**.
- 6 Perform [step 3 - step 5](#) listed in the section [“To link service groups using the VCS One console”](#) on page 345.

To create locally linked service groups from the command line

- ◆ At the command prompt, type the following:

```
hagrp -link parentgroup childgroup local [soft|firm|hard] [-user user@domain] [-domaintype domaintype]
```

To create globally linked service groups from the command line

- ◆ At the command prompt, type the following:

```
hagrp -link parentgroup childgroup global [soft|firm|hard] [-user user@domain] [-domaintype domaintype]
```

Unlinking service groups

Use this procedure to unlink service groups.

To unlink a service group using the VCS One console

- 1 In the VCS One console, locate the service groups that you want to unlink. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, from the **Configuration** menu, click **Remove Group Dependency**. The **Remove Service Group Dependency** dialog box is displayed.
- 3 In the **Remove Service Group Dependency** dialog box, select the parent and child groups that you want to unlink.
- 4 Click **OK**.

To unlink a service group from the group dependency view

- 1 In the VCS One console, locate the service group that you want to unlink.

See [“Locating a service group”](#) on page 321.

- 2 In the right pane, under **Service Groups**, click the service group that you want to unlink.
- 3 In the left pane, under **Views**, click **Group Dependencies**.
- 4 In the **Group Dependency View**, right-click on the background. You may click one of the graph items for other action options.
- 5 Click **Remove Group Dependency**.
- 6 In the **Remove Service Group Dependency** dialog box, select the parent and child groups that you want to unlink.
- 7 Click **OK**.

To unlink a service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -unlink parentgroup childgroup  
[-user user@domain] [-domaintype domaintype]
```

Enabling service group resources

Use this procedure to enable one or more service group resources. Service group resources must be enabled before they can be brought online.

To enable one or more resources in a service group

- 1 In the VCS One console, locate the service group that contains the resources, which you want to enable.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group name.
- 3 Under **Resources**, check one or more resources.
- 4 Click **Operations > Enable Resources**.
- 5 Click **OK**.
- 6 Click **Close**.

To enable all the resources in a service group

- 1 In the VCS One console, locate the service group that contains the resources, which you want to enable.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group that contains the resources, which you want to enable.

- 3 Click **Operations > Enable All Resources**.
- 4 Click **OK**.
- 5 Click **Close**.

To enable all the resource in a service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -enableresources service_group [-user user@domain] [-domaintype domaintype]
```

Disabling service group resources

Use this procedure to disable one or more service group resources. Service group resources are disabled to prevent them from coming online. This is done when you want VCS One to temporarily stop monitoring the resources (rather than delete them) while the service group is still online. Make sure that the resources are offline before you disable them.

To disable one or more resources in the service group

- 1 In the VCS One console, locate the service group that contains the resources, which you want to disable.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group.
- 3 In the right pane, under **Resources**, select one or more resources.
- 4 Click **Operations > Disable Resources**.
- 5 Click **OK**.
- 6 Click **Close**.

To disable all the resources in the service group

- 1 In the VCS One console, locate the service group that contains the resources, which you want to disable.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group that contains the resources, which you want to disable.
- 3 In the right pane, from the **Operations** menu, click **Disable All Resources**. The **Disable All Resources** dialog box is displayed.
- 4 In the **Disable All Resources** dialog box, click **OK**.

To disable all the resource in a service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -disableresources service_group [-user user@domain] [-domaintype domaintype]
```

Probing service group resources

Use this procedure to probe service group resources. Resources are probed to determine if they are configured correctly and are ready to go online. You can also probe resources to determine their current status.

To probe one or more resources in a service group

- 1 In the VCS One console, locate the service group that contains the resources, which you want to probe.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group.
- 3 In the right pane, under **Resources**, select one or more resources, which you want to probe.
- 4 In the right pane, from the **Operations** menu, click **Probe Selected Resources**. The **Probe selected Resource(s) of Service Group** dialog box is displayed.
- 5 In the **Probe selected Resource(s) of Service Group** dialog box, click **OK**.
- 6 In the **Probe selected Resource(s) of Service Group** dialog box, click **Close**.

To probe all resources in a service group

- 1 In the VCS One console, locate the service group that contains the resources, which you want to probe.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group.
- 3 In the right pane, from the **Operations** menu, click **Probe All Resources**. The **Probe all resources of Service Group** dialog box is displayed.
- 4 In the **Probe all resources of Service Group** dialog box, select the system on which the service group resources will be probed.
- 5 Click **OK**.

Bringing service group resources online

Use this procedure to bring one or more service group resources online.

To bring one or more service group resources online

- 1 In the VCS One console, locate the service group that contains the resources, which you want to bring online.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group.
- 3 In the right pane, under **Resources**, select one or more resources.
- 4 In the right pane, from the **Operations** menu, click **Online Selected Resources**. The **Online selected Resource(s) of Service Group** dialog box is displayed.
- 5 In the **Online selected Resource(s) of Service Group** dialog box, select the system on which you want to bring the resources online.
- 6 Click **OK**.
- 7 Click **Close**.

Taking service group resources offline

Use this procedure to take one or more service group resources offline.

To take one or more service group resources offline

- 1 In the VCS One console, locate the service group that contains the resources, which you want to take offline.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group.
- 3 In the right pane, under **Resources**, select one or more resources.
- 4 In the right pane, from the **Operations** menu, click **Offline Selected Resources**. The **Offline selected Resource(s) of Service Group** dialog box is displayed.
- 5 In the **Offline selected Resource(s) of Service Group** dialog box, select the system on which you want to take the resources offline.
- 6 Click **OK**.
- 7 Click **Close**.

Cloning service groups

Use this procedure to clone a service group. Clone a service group to make several similar service groups without repeating all the steps each time.

Once you have created the service group clone, customize the service group. For example, add values for the resources.

To clone a service group

- 1 In the VCS One console, locate the service group that you want to clone. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, check the service group that you want to clone.
- 3 Click **Configuration > Clone Service Group**.
- 4 In the **Clone Service Group** dialog box, perform the following steps in the order presented:
 - In the **Select no. of clones** box, click the up arrow to increase the number of clones that you want to create. The default names of the clones will appear in the Group Name box.
 - If you want to change the default names of the clones, in the **Group Name** box, click the default clone name and enter a new name. The default clone name is the name of the service group that you are cloning suffixed with *_num*, where *_num* is increasing integers starting at 0.
- 5 Click **OK**.
- 6 Click **Close**.

Changing a service group's priority value

Use this procedure to change the service group's priority value. The service group's priority value determines its importance over other service groups in the VCS One cluster. Service groups with higher priority take precedence over service groups with lower priority while contending for VCS One cluster resources.

To change a service group's priority value using the VCS One console

- 1 In the VCS One console, locate the service group for which you want to set the priority value. See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group.
- 3 In the right pane, click **Priority**. The **Edit Attribute** dialog box is displayed.
- 4 In the **Edit Attribute** dialog box, perform the following steps in the order presented:

- In the **Value** box, enter a priority value between 1 to 5. 1 denotes highest priority while 5 denotes lowest priority.
 - Select the **Propagate** check box, if you want the new priority value to propagate to all service groups in the local dependency tree.
- 5 In the **Edit Attribute** dialog box, click **OK**.
 - 6 In the **Edit Attribute** dialog box, click **Close**.

To change a service group's priority value from the command line

- ◆ At the command prompt, type the following:
`hagrp -modify service_group Priority Priority_value`

The priority value must be between 1 and 5. 1 denotes highest priority while 5 denotes lowest priority.

Changing a service group's load value

Use this procedure to change the service group's load value. The service group's load value determines the extent of system resource that the service group utilizes.

To change a service group's load value using the VCS One console

- 1 In the VCS One console, locate the service group for which you want to set the load value.
See "[Locating a service group](#)" on page 321.
- 2 In the right pane, under **Service Groups**, click the service group.
- 3 In the right pane, click **Load**. The **Edit Attribute** dialog box is displayed.
- 4 In the **Edit Attribute** dialog box, enter a value for each load dimension.
- 5 Click **OK**.
- 6 In the **Edit Attribute** dialog box, click **Close**.

To change a service group's load value from the command line

- ◆ At the command prompt, type the following:
`hagrp -changeload [-ejectlowpri|-tryswitch] service_group {key value} ... [-user user@domain] [-domaintype domaintype]`

Configuring a service group's SystemList with a list of systems

Use this procedure to define a service group's SystemList attribute value with a list of systems. The service groups's SystemList determines the systems on which the service group can be brought online.

You may also define the SystemList attribute using an organization unit or extended attribute expression.

See [“Configuring a service group's SystemList with an expression”](#) on page 354.

To configure the SystemList for a service group using the VCS One console

- 1 In the VCS One console, locate the service group for which you want to configure the SystemList attribute.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group.
- 3 In the right pane, from the **Configuration** menu, click **Edit System List**.
- 4 Move the appropriate systems from the **Available Systems** list to the **System List** list using the arrows.
The Available Systems list are the systems that are valid SystemList candidates for the service group and for which you have appropriate privileges.
The SystemList list comprise the systems that comprise the service group's SystemList value.
- 5 Select the **Propagate** check box, to propagate the new system list to all service groups in the local dependency tree. You can also use the **Filter** option to filter systems.
See [step 9](#) in the section [“Adding a service group”](#) on page 315.
- 6 Click **OK > Close**.

To configure the SystemList for a service group using the command line

- ◆ At the command prompt, type the following:

```
hagrp -modify [-propagate] service_group SystemList [-add/-delete/-update/-refresh] system_name value
```

See the *Veritas Cluster Server One Command Reference Guide*.

Configuring a service group's SystemList with an expression

You may configure a service group's SystemList attribute using an OUValue or extended attribute expression. The expression that defines the SystemList attribute value is stored in the SystemListExpr attribute.

Using an expression allows the SystemList value to be dynamically updated to be any system that matches the expression.

Note: After you define the SystemList expression, you must refresh the SystemList attribute value.

You may also define the SystemList attribute using list of systems.

See [“Configuring a service group's SystemList with a list of systems”](#) on page 353.

To configure a service group's SystemList with an expression using the VCS One console

- 1 Locate the service group for which you want to configure the SystemList attribute.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, check one or more service groups.
- 3 Click **Configuration > Edit Attribute(s)**.
- 4 In the **Edit Attribute(s)** panel, in the list of attributes, click **SystemListExpr**.
- 5 Click **For all Group(s)** to configure the same value for all the selected groups, or click **For selected Group(s)** if you want to configure different values for each selected group.
- 6 Click the pencil icon to edit the value.
- 7 Type the OUValue or extended attribute expression. Click **OK**.
- 8 Check the **Propagate** check box, to propagate the new system list to all service groups in the local dependency tree.
- 9 Click **Next > Finish > Close**.
- 10 Click **Operations > Refresh System List**.

When you close the Edit Attribute(s) panel, the service groups that you selected in [step 2](#) remain checked. These are the same service groups on which you perform the Refresh System List operation.

Configuring a service group's compatibility list

Use this procedure to configure the compatibility list for a service group. The service group's compatibility list specifies the list of service groups that can remain online, on the same system and at the same time, along with the specified service group.

To configure the compatibility list for a service group using the VCS One console

- 1 In the VCS One console, locate the service group for which you want to configure the compatibility list.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group.
- 3 In the right pane, from the **Configuration** menu, click **Edit Compatibility**. The **Service Group Workload Configuration** dialog box is displayed.
- 4 In the **Service Group Workload Configuration** dialog box, select either the **Compatible** or **Incompatible** option depending on whether you want to specify a list of compatible or incompatible service groups.
 - If you select the **Compatible** option, do one of the following:
 - Select the **ALLGROUPS** check box, to make all the existing service groups and the new service groups that you add in future, compatible with the service group.
 - Click **Select Service Groups**, to add specific service groups that can co-exist or are compatible with the service group. Ensure that the **ALLGROUPS** check box is clear.
In the **Service Group Workload Configuration** screen, under **Available Groups**, select one or more service groups that you want to make compatible with the service group, and then click the right-arrow symbol. Ensure that the selected service groups are displayed under **Group List**.
 - Click **OK**.
If you do not click the **Select all groups** check box, all the other existing service groups as well as new service groups that you add in future, are incompatible with the service group.
 - If you select the **Incompatible** option, do one of the following:
 - Select the **Select all groups** check box, to make all the existing service groups and the new service groups that you add in future, incompatible with the service group.

- Click **Edit Selection**, to add specific systems that are incompatible with the service group. Ensure that the **Select all groups** check box is clear.
In the **Service Group Workload Configuration** screen, under **Available Groups**, select one or more service groups that you want to make incompatible with the service group, and then click the right-arrow symbol. Ensure that the selected service groups are displayed under **Group List**.
 - Click **OK**.
If you do not click the **Select all groups** check box, all the other existing service groups as well as new service groups that you add in future, are compatible with the service group.
 - Click the **Propagate** check box, to propagate the compatibility or incompatibility setting to other service groups that belong to the same local dependency tree.
 - In the **Service Group Workload Configuration** screen, click **OK**.
- 5 In the **Summary** screen, click **Close**.

To configure the compatibility list for a service group from the command line

- ◆ At the command prompt, type one of the following:

```
hagrp -[in]compatible [-propagate] group1 group2
[-user user@domain] [-domaintype domaintype]

hagrp -[in]compatible [-propagate] -setname set_name -with -
setname set_name [-user user@domain] [-domaintype domaintype] [-
info]

hagrp -[in]compatible [-propagate] {-ou expression | -ea
expression | -ou expression -ea expression} -with {-ou
expression | -ea expression | -ou expression -ea expression} [-
user user@domain] [-domaintype domaintype] [-info]
```

The *-propagate* option propagates the compatibility list values to local child and local parent service groups. This includes local service groups with soft, firm, and hard group dependencies.

Configuring a service group's fault policy

Use this procedure to configure the fault policy for a service group. The service groups's fault policy defines the service group behavior during a failover operation.

To configure the fault policy for a service group

- 1 In the VCS One console, locate the service group for which you want to configure the fault policy.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, check one or more service groups.
- 3 Click **Configuration > Edit Fault Policy**.
- 4 In the **Configure Fault Policy** screen, perform the following steps in the order presented:
 - In the **Group Fault Policy** box, select either **Failover** or **No Failover**. If you select **Failover**, the service group automatically fails over to the next available system in the event of a service group fault. If you select **No Failover**, the service group does not automatically fail over to any other system in the event of a service group fault. In this case, you need to manually failover the service group.
 - In the **Node Fault Policy** box, select either **Failover** or **No Failover**. If you select **Failover**, the service group automatically fails over to the next available system in the event of a system fault. If you select **No Failover**, the service group does not automatically fail over to any other system in the event of a system fault. In the latter case, you need to manually failover the service group.
 - Under **Resource Fault Policy**, for each resource, set the fault policy to **FaultNone**, **FaultHold**, **FaultPropagateAll**, or **FaultPropagateParent**.
See [“Resource level control”](#) on page 228.
 - In the **Configure Fault Policy** screen, click **Finish**.
- 5 In the **Summary** screen, click **Close**.

Creating an off-host resource in a service group

A resource is called an off-host resource if the resource and its respective service group reside on the local system, while the agent that monitors it is located on a remote system. In other words, an off-host resource is a resource that is defined and located on the local system but is monitored and operated from a remote system.

Only a resource of type **NetAppExport** can be configured as an off-host resource. More information is available about off-host resources.

See [“About off-host resources in service groups”](#) on page 260.

See [“ControlGroup”](#) on page 738.

See [“ControlMode”](#) on page 738.

More information is available about the NetAppExport resource type.
See *Veritas Cluster Server One Bundled Agents Reference Guide*.

Note: Not all platforms support the NetAppExport resource type.
See *Veritas Cluster Server One Release Notes*.

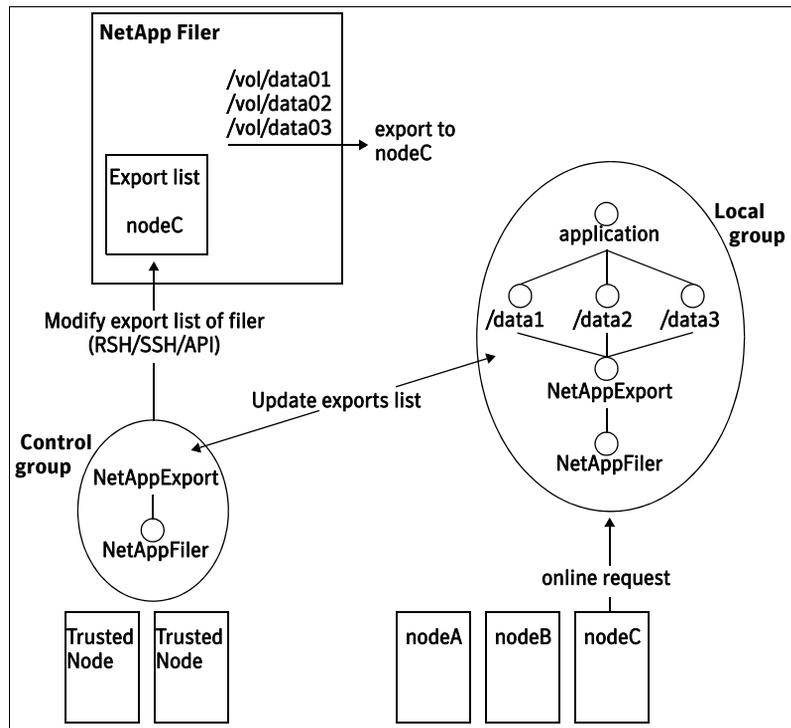
Creating an off-host resource with NetApp Filer

The following example describes the process to create and configure an off-host resource for use with a NetApp Filer. This example uses password free SSH to access and update the NetApp Filer.

Note: You can also set up off-host resources using API access. For API access, it is not necessary to setup password free SSH access to the Filer.

[Figure 16-1](#) depicts the off-host resource with NetApp Filer.

Figure 16-1 Off-host resource with NetApp Filer



Preparing the NetApp Filer

Perform the following tasks on the NetApp Filer:

- Create the shared volumes.
- Add SSH keys to the `/etc/sshd/root/.ssh/authorized_keys` file. Ensure that you add the SSH keys on all the nodes that are listed in the control group's SystemList attribute. This enables VCS One clients to SSH into the Filer and update the exports list.

Creating the control group

To create the control group, perform the following steps:

- 1 Add the base IP address of all the systems listed in the control group's SystemList attribute to the `/etc/hosts` file on the Network Appliance Filer. This ensures that VCS One clients can communicate with the NetApp Filer without depending on an external name service, such as DNS or NIS.

- 2 Create a control service group. The SystemList attribute for the control group includes VCS One clients with password free SSH access to the NetApp Filer.
- 3 Run the following command on each system listed in the control group's SystemList attribute. At the command prompt, type the following:

```
ssh netappfilername exportfs
```

Here *netappfilername* is the name of the Filer.

This command verifies password free SSH access for the systems listed in the control group's SystemList attribute. It also creates entries for the Filer in the list of known hosts in the SSH configuration on the systems that are part of the control group's system list.

- 4 Create the following resources in the control group:
 - NetAppFiler
This resource verifies that the node, which hosts the control group has connectivity to the NetAppFiler.
 - NetAppExport
This is a stub resource that notifies VCS One clients to start the NetAppExport agent on the host. Set the ControlMode attribute for the off-host definition resource to 1 and enable it. This ensures that the off-host resource is managed only from the system where the control group is currently online. Note that it is mandatory to first set the ControlMode attribute value to 1 and then enable the resource.

Creating the local group

To create the local group, perform the following steps:

- 1 Add the base IP address of all the systems listed in the local group's SystemList attribute to the `/etc/hosts` file on the Network Appliance Filer. This ensures that VCS One clients can communicate with the NetApp Filer without depending on an external name service, such as DNS or NIS. Clients that mount the exported file systems must have their base IP address listed in the `/etc/hosts` file on the Network Appliance Filer.
- 2 Create a local service group with nodeA, nodeB, and nodeC listed in the service group's SystemList attribute. Configure all the resource attributes. At a minimum, the local service group consists of the following resources:
 - NetAppFiler
This resource verifies that the application node has connectivity to the NetAppFiler. The application node requires connectivity to mount the NFS shares.
 - NetAppExport

This resource defines the parameters that update the exports list on the NetApp Filer.

- **Mount**

This resource mounts the NFS file systems. Each NFS file system that is exported on the NetApp Filer has its own corresponding Mount resource.

Linking the local and control service groups

Link the NetAppExport resource in the local service group such that it points to the NetApp resource in the control group.

To link the local and control service groups

- ◆ At the command prompt, type the following:

```
hares -modify NetAppExport ControlGroup ControlGroup
```

NetAppExport is the name of the NetAppExport type resource in the local service group. ControlGroup is the name of the control group.

Bringing the local group online

Before performing operations on the local group, you must bring the control group online. When the NetAppExport resource is brought online it relays the online command to the control node. The control node then reaches into the NetApp Filer to update the exports list with the appropriate client name. It then returns control back to the VCS One client where the rest of the local service group is brought online.

Viewing off-host resource sample configuration

The following sample configuration describes an off-host NetAppExport resource that is configured for a service group called sg. The SystemList has SysA and SysB. The resource specifies sg.filer for the FilerResName attribute. All communication with the Filer uses API-access for updating the export option for /vol/agentvol/p5 on the Filer.

If the ControlGroup attribute is omitted, the resource definition changes to a non-off-host or a local resource definition.

```
<resource name="hgexport" type="NetAppExport">
  <attribute name="ControlGroup"><scalar>"cg"</scalar>
</attribute>
<attribute name="FilerPathName"><scalar>"/vol/agentvol/p5"
</scalar></attribute>
<attribute name="FilerResName"><scalar>"sg.filer"</scalar>
</attribute>
<attribute name="ExportACL">
```

Creating an off-host resource in a service group

```
    <val key="SysA">"SysA"</val>
    <val key="SysB">"SysB"</val>
  </attribute>
</resource>
```

Managing composite service groups

This chapter includes the following topics:

- [About managing composite service groups](#)
- [Creating a composite service group](#)
- [Listing composite service groups and unassociated service groups](#)
- [Viewing details about a composite service group](#)
- [Modifying the group list of the CSG](#)
- [Editing a composite service group's attributes](#)
- [Deleting a composite service group](#)
- [Moving a local composite service group in the organization tree](#)
- [Bringing a composite service group online](#)
- [Taking a composite service group offline](#)
- [Flushing a pending action on a composite service group](#)

About managing composite service groups

A composite service group is a collection of objects. Use composite service groups to manage a group of objects as a single logical object.

See [“About composite service groups”](#) on page 40.

Creating a composite service group

Create a local composite service group when you want to manage multiple service groups as one logical unit within a single VCS One cluster.

A service group may only be part of one composite service group at a time.

To add a composite service group using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 From the Configuration menu, click **Add CSG**.
- 5 Click **Next**.
- 6 In the **Name** text box, enter a name for the composite service group.
- 7 In the **CSG belongs to:** field, click the ellipsis to select an organization unit to associate with the composite service group.
In the Select Organization Unit panel, select the organization tree OUValue node to which to attach the composite service group.
- 8 Click **OK**.
- 9 Click **Next**.
You may click **Finish > Close** and configure the rest of the composite service group later.
- 10 In the GroupList Configuration panel, add service groups to the composite service group.
The GroupList is the list of service groups that comprise the composite service group.

Use the following information to configure the GroupList:

Filter By	<p>Use different filters or expressions to narrow the list of groups that appear in the Available Groups field.</p> <p>If you filter by Name or OUValue, the service groups that appear are ones that the user has appropriate permissions to view and do not belong to another CSG.</p> <p>If you filter by a set or an expression, consider the user of the Force option.</p>
Available Group(s)	<p>Select groups from this area that you want to add to the GroupList.</p> <p>Click the arrow to move the groups to the Selected Groups column.</p>
Selected Group(s)	<p>Groups that comprise the composite service group's GroupList attribute.</p> <p>To remove groups from this list, select the group and click the arrow to move the groups to the Available Groups area.</p> <p>If none of the service groups selected can be added to the CSG, the CSG is not created.</p>

11 Check or uncheck Force.

Use the following information to determine the Force option:

Check Force	<p>Even if some of the selected service groups can not be added to the GroupList, the remaining service groups are added.</p> <p>This option can be useful if you use an expression or set name for adding groups.</p>
Uncheck Force	<p>If some of the selected service groups can not be added to the GroupList then the new CSG is not added.</p>

12 Click Next

You may click **Finish > Close** and configure the rest of the composite service group later.

13 In the Cluster List Configuration panel, configure one or more VCS One clusters on which the composite service group can run.

If no VCS One cluster, or only the local VCS One cluster, is listed in the ClusterList attribute, the composite service group is local. If there are more than one VCS One clusters in the ClusterList attribute the composite service group is global.

See [“About VCS One global clusters”](#) on page 66.

Use the following information to configure the Cluster List:

Available Cluster(s)	Select VCS One clusters from this column that you want to add to the ClusterList. Click the arrow to move the VCS One clusters to the Selected Cluster(s) column.
Selected Cluster(s)	VCS One clusters that comprise the composite service group's ClusterList attribute. To remove a VCS One cluster from this list, select the VCS One cluster and click the arrow to move the cluster to the Available Cluster(s) column.

14 Click **Next**.

15 Click **Finish** to execute the operations, or click **Back** to make changes to the commands to be executed.

16 Click **Close**.

To add a composite service group using the command line

◆ Type the following command

```
hacsg -add csg [node] -grp [-force] grouplist
```

Use the following information to replace the appropriate variables

csg	The name of the composite service group.
node	The full path of the OUValue node in the organization tree where the composite service group is attached.
grouplist	The following formats are valid for the grouplist variable: <ul style="list-style-type: none">■ <i>list of groups</i>■ <i>-ea extended attribute expression</i>■ <i>-ou organization unit expression</i>■ <i>-setname name of a set</i>
force	Add as many groups as possible. See step 11 on page 365

Listing composite service groups and unassociated service groups

The VCS One console lists all the composite service groups and service groups the user has permissions to view. An unassociated service group is a service group that is not part of a composite service group.

More information is available on navigation tools, filtering tools, and views in the VCS One console.

See [“Using the VCS One console”](#) on page 107.

To list composite service group using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.

Note: The folder **Unassociated SGs** appears if service groups that are not part of any composite service group exist.

To list composite service groups using the command line

- ◆ Type the following command
`hacsg -list`

To view the groups in a composite service group using the command line

- ◆ Type the following command
`hacsg -groups csg`
 Use the following information to replace the appropriate variables

`csg` The name of the composite service group.

To view the name of a composite service group that a service group belongs to using the command line

- ◆ Type the following command
`hagr -value group CSGName`
 Use the following information to replace the appropriate variables

`group` The name of the service group.

Viewing details about a composite service group

The detail page of a CSG provides the following details about the composite service group:

- Service groups
- VCS One clusters
- Automation information
- Attributes and their values configured

To view details about a composite service group using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Click the name of the composite service group to go to the detail page for that CSG.

Use the following information to view detailed information about composite service group:

Service Groups	<p>Lists the service groups that are associated with the CSG.</p> <p>Click the name of the service group to go to the details page of that service group. Service groups that are not hyperlinks indicate a group to which the user does not have appropriate privileges.</p> <p>Click the Groups link to scroll the view to this table.</p> <p>See “About composite service groups” on page 40.</p>
CSG’s Status Information on Remote Clusters	<p>If the CSG is local, you see CSG is not global.</p> <p>If the CSG is global, all VCS One clusters that may run this CSG are listed.</p> <p>Click the Remote Status link to scroll the view to this table.</p> <p>Click the name of the VCS One cluster to go to the details page of that VCS One cluster.</p> <p>See “About VCS One global clusters” on page 66.</p>

Automation Information	Lists the rules and jobs that are associated with this CSG. See “ About managing automated tasks ” on page 410.
Attributes	Lists the attributes that are associated with the CSG. Click the pencil icon to edit the value of an attribute.

To view a composite service group using the command line

- ◆ Type the following command

```
hacsg -display csg
```

Use the following information to replace the appropriate variable

csg The name of the composite service group.

Modifying the group list of the CSG

The GroupList attribute defines the list of service groups that comprise the composite service group.

To perform this operation the user must have the following privileges:

- Modify CSG privilege on the composite service group.
- Add Group to GroupList privilege or Delete Group from GroupList privilege on the service group, depending on the modification.

To modify the group list of the CSG using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Check a composite service group to modify.
- 5 From the Configuration menu, click **Edit GroupList**.
- 6 In the GroupList Configuration panel, modify the list of service groups that comprise the composite service group.

Use the following information to modify the GroupList:

Filter By	Select different filters to narrow the list of groups that appear in the Available Groups field. Only service groups that the user has appropriate permissions to view appear.
-----------	---

Available Group(s)	Select groups from this area that you want to add to the GroupList. Click the arrow to move the groups to the Selected Groups column.
Selected Group(s)	Groups that comprise the composite service group's GroupList attribute. To remove groups from this list, select the group and click the arrow to move the groups to the Available Groups area.

7 Check or uncheck Force.

Use the following information to determine the Force option:

Check Force	Even if some of the selected service groups can not be added to the GroupList, the remaining service groups are added. This option can be useful if you use an expression or set name for adding groups.
Uncheck Force	If some of the selected service groups can not be added to the GroupList then none of the service groups are added.

8 Click Finish > Close.

To modify the group list of the CSG using the command line

◆ Type the following command

```
hacsg -addgrp [-force] csg grouplist  
hacsg -deletegrp [-force] csg grouplist
```

Use the following information to replace the appropriate variables

csg	The name of the composite service group.
grouplist	The following formats are valid for the grouplist variable: <ul style="list-style-type: none">■ <i>list of groups</i>■ <i>-ea extended attribute expression</i>■ <i>-ou organization unit expression</i>■ <i>-setname name of a set</i>
force	Add as many groups as possible. See step 11 on page 365

Editing a composite service group's attributes

Attributes specify the characteristics of the composite service group, and define how VCS One controls it.

See “[Composite service group attributes](#)” on page 692.

To edit a composite service group's attributes

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Click the name of the composite service group to go to the details page.
- 5 In the right pane, click **All Attributes**.
- 6 In the Edit column, click the pencil icon next to the attribute name you want to edit, and modify the value of the attribute.
If there is no pencil icon, you may not edit the attribute.
- 7 Click **Next**.
- 8 On the **Summary** page, review the prepared edits.
- 9 Click **Finish** to execute the changes.
- 10 Click **Close**.

To edit a composite service group's attributes using the command line

- ◆ Type the following command

```
hacsg -modify csg attribute [action] value
```

Use the following information to replace the appropriate variables

<code>csg</code>	The name of the composite service group.
<code>attribute</code>	The name of the attribute you want to modify.
<code>action</code>	The action for the command, for example, -add or -delete
<code>value</code>	The new value for the attribute.

Deleting a composite service group

Deleting a composite service group deletes the logical container of the CSG. It does not delete the individual service groups that are contained in the composite service group.

To delete a composite service group

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Check one or more composite service groups to delete.
- 5 From the Configuration menu, click **Delete CSG(s)**.
- 6 Click **OK > Close**.

To delete a composite service group using the command line

- ◆ Type the following command

```
hacsg -delete csg
```

Use the following information to replace the appropriate variables

`csg` The name of one composite service group.

Moving a local composite service group in the organization tree

A composite service group is attached to the organization tree at an OUValue node. The node where the composite service group is attached determines the user privileges that are associated with it.

See [“About designing roles and privileges for users”](#) on page 218.

To move a composite service group in the organization tree using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Check one or more composite service groups to move.
- 5 From the Configuration menu, click **Move CSG(s)**.
- 6 In the Organization Unit Selection panel, select the organization tree OUValue node to which to attach the composite service group.
- 7 Consider the **Modify Privileges if move invalidates the assigned role of users** option.
Consider this option in the use case when the composite service group moves to an OUValue node that is not in the subtree of the original

organization tree node. In this case, you must check this option to remove privileges from users attached at the original node that are no longer valid due to the move of the composite service group. Otherwise, the move is rejected.

This option is equivalent to the `-updateroles` option in the command line.

8 Click **Finish** > **Finish** > **Close**.

To move one or more composite service groups using the command line

◆ Type the following command

```
hacsg -move csg [csg1] -ou node
```

Use the following information to replace the appropriate variables

`csg, csg1` The name of the composite service group or groups.

`node` The full path of the OUValue node in the organization tree to which the composite service group is moved.

Bringing a composite service group online

A composite service group is online when all the service groups that are contained in the composite service group are online. The online operation for a CSG performs an online action for each service group that is contained in the CSG.

The propagate option, when used with the online option, initiates the online of child service groups outside the composite service group on which service groups inside the CSG depend.

The following conditions result in the rejection of the online operation of the composite service group:

- The GroupList is empty.
- The composite service group is already online, either in the local cluster, or in another cluster in a global cluster environment.
See [“About VCS One global clusters”](#) on page 66.
- The composite service group has the PENDING flag set, which means the constituent service groups are in transition within the cluster.
- Any group in the CSG is frozen.
- Any group in the CSG has no configured resources.
- Any group in the CSG has all resources disabled.

To perform this operation the user must have the following privilege on the composite service group:

- Online CSG

To bring a composite service group online using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Select one or more composite service groups that you want to bring online.
- 5 From the Operations menu, click **Online CSG(s)**.
- 6 The **Force** option is only valid for global composite service groups. Use the force option to take over Authority as part of the online operation if the cluster on which the CSG had Authority set has gone down. See [“Taking over a global CSG”](#) on page 503.
- 7 Check **Propagate** if you want VCS One to also attempt to bring online all child service groups outside the CSG that have a dependency with service groups inside the CSG.
- 8 Click **OK > Close**.

To bring a composite service group online using the command line

- ◆ Type the following command

```
hacsg -online [-propagate] [-force] csg
```

Use the following information to replace the appropriate variables

csg	The name of the composite service group.
propagate	The propagate option initiates the online of service groups outside the composite service group on which service groups inside the CSG depend.
force	Transfer authority for the CSG to the local VCS One cluster. Only the VCS One cluster that has the authority for the CSG may bring it online. Applicable to global CSG only.

Taking a composite service group offline

A composite service group is offline when all the service groups that are contained in the composite service group are offline.

To perform this operation the user must have the following privileges on the composite service group:

- Offline CSG

To take a composite service group offline using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Select one or more composite service groups that you want to take offline.
- 5 From the Operations menu, click **Offline CSG(s)**.
- 6 Check Propagate if you want VCS One to also take offline all parent service groups outside the CSG that have a dependency with service groups inside the CSG.
- 7 Click **OK > Close**.

To bring a composite service group online using the command line

- ◆ Type the following command

```
hacsg -offline [-propagate] csg
```

Use the following information to replace the appropriate variables

`csg` The name of the composite service group.

Flushing a pending action on a composite service group

You flush a pending action on a composite service group to cancel the online or offline operation that is currently being performed on the CSG.

A flush is useful if the online or offline operation of the CSG is not successful. In this case, you can flush the CSG, resolve the error, and restart the online or offline operation.

In the following conditions, an IntentOnline entry is added for the service group in the Group Transition Queue (GTQ):

- A service group faults everywhere in the VCS One cluster
- A service group is unable to failover to a different system
- If a service group can not come online from an offline state

The flush operation removes the IntentOnline entry for all groups inside the CSG, which prevents VCS One from bringing the CSG online automatically.

See [“AttnInfo”](#) on page 692.

You may also need to flush the GTQ to cancel the intent online entry for the service groups contained in the CSG.

See [“Flushing the plan of action on all service groups in the GTQ”](#) on page 338.

To flush a composite service group using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Select one or more composite service groups that you want to flush.
- 5 From the Operations menu, click **Flush CSG(s)**.
- 6 Click **OK**.
- 7 Take care of the issue that prevented the CSG from coming online.
- 8 Clear the faults on any service groups inside the CSG
- 9 See [“Clearing a service group fault”](#) on page 344.
- 10 Online the CSG
See [“Bringing a composite service group online”](#) on page 373.

To flush a composite service group using the command line

- ◆ Type the following command
`hacsg -flush csg`
Use the following information to replace the appropriate variables

`csg` The name of the composite service group.

Managing resources

This chapter includes the following topics:

- [Using the Resource Dependency View](#)
- [Adding a resource to a service group](#)
- [Deleting a resource from a service group](#)
- [Editing resource attributes](#)
- [Modifying zone resource attributes](#)
- [Enabling resources in a service group](#)
- [Disabling resources in a service group](#)
- [Bringing a resource online](#)
- [Taking a resource offline](#)
- [Taking parent and child resources offline concurrently](#)
- [Probing a resource](#)
- [Faulting a resource using the Simulator](#)
- [Repairing a resource using the Simulator](#)
- [Clearing a resource fault](#)
- [Clearing resources in the ADMIN_WAIT state](#)
- [Linking resources](#)
- [Unlinking resources](#)
- [Viewing resources in the configuration by resource type](#)
- [Defining an attribute value with a resource variable](#)
- [Displaying values to be affected by a change in a resource variables definition](#)

- Updating the value of a resource variable

Using the Resource Dependency View

The VCS One console provides various views to effectively manage the VCS One cluster. This section discusses the different views related to resource administration.

Locating the Resource Dependency View

Use this procedure to locate the Resource Dependency View. You require at least Read privileges on the service group to view its resource dependencies.

To locate the resource dependency view

- 1 In the VCS One console, locate the service group that contains the resources, which you want to view.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, check the service group.
- 3 Click **Views > Resource Dependencies**.

Performing operations from Resource Dependency View

The resource dependency view displays the existing resource dependencies for a service group.

You can perform the following operations on resources in this view:

- Bring a resource online
See [“Bringing a resource online”](#) on page 384.
- Take a resource offline
See [“Taking a resource offline”](#) on page 385.
- Clear resource faults
See [“Clearing a resource fault”](#) on page 388.
- Link resources
See [“Linking resources”](#) on page 390.
- Unlink resources
See [“Unlinking resources”](#) on page 392.

Arranging the Resource Dependency View using the Navigator

In large VCS One cluster configurations, the dependency view has many service groups and resources on display. You can use the Navigator to pan or zoom into the view.

See [“Summary information on the dependency view”](#) on page 135.

Adding a resource to a service group

Use this procedure to add a resource to a service group.

To add a resource to a service group using the VCS One console

- 1 In the VCS One console, locate the service group to which you want to add the resource.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the right pane, from the **Configuration** menu, click **Add/Modify Resource**. The **Add Resource** dialog box is displayed.
- 4 In the **Add Resource** dialog box, perform the following steps for each resource that you want to add:
 - In the **Type** box, select the resource type.
 - In the **Name** box, enter the name of the resource. The name of the resource cannot exceed 128 characters.
 - Select the **Enable Resource** check box, to enable the resource.
 - Click **Add Resource**, to add the resource to the service group. After the resource is added to the service group it is displayed in the **Resource List**.
 - In the **Resource List**, click the **Edit** icon corresponding to the newly added resource.
 - In the **Edit Resource** dialog box, do one of following:
 - Under **Attribute List**, select the resource attribute. Under **Apply to**, select **All Systems in the system list**, if the attribute is a global attribute and its value is the same for all the systems listed in the service group’s SystemList. In the **Value** box, enter the common attribute value.
 - Under **Attribute List**, select the resource attribute. Under **Apply to**, select **Selected Systems**, if the attribute is a local attribute and its value is different for all the systems listed in the service group’s SystemList. In the **Value** box, enter the attribute value for each system.
 - In the **Edit Resource** dialog box, click **OK**. If any of the mandatory resource attributes are not specified, a warning icon is displayed next to the resource.
 - In the **Add Resource** dialog box, click **OK**.

- In the **Result** dialog box, click **Close**.

To add a resource to a service group from the command line

- ◆ At the command prompt, type the following:

```
hares -add resource type group  
[-user user@domain] [-domaintype domaintype]
```

Deleting a resource from a service group

Use this procedure to delete a resource from a service group. Prior to deleting a resource all the resource dependencies are removed.

By default, you may not delete an online resource, but you may configure this behavior.

See “[AllowedOnlineOps](#)” on page 723.

To delete a resource from a service group using the VCS One console

- 1 In the VCS One console, locate the service group that contains the resources that you want to delete.
See “[Locating a service group](#)” on page 321.
- 2 In the right pane, click the service group name.
- 3 Check the resource that you wish to delete.
- 4 Click **Configuration > Delete Resource**.
- 5 Click **OK**.
- 6 Click **Close**.

To delete a resource from a service group from the command line

- ◆ At the command prompt, type the following:

```
hares -delete resource [-user user@domain] [-domaintype  
domaintype]
```

Editing resource attributes

You may edit attributes of global scope from the All Attributes page of an attribute.

To edit resource attributes using the VCS One console

- 1 In the VCS One console, locate the service group that contains the resources, which you want to modify.
See “[Locating a service group](#)” on page 321.

- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the **Resource Name** table, click the resource that you want to modify.
- 4 Click **All Attributes**.
- 5 In the **All Attributes** table, locate the attribute that you want to modify.
- 6 Click the attributes pencil icon.
The resource attributes that can be modified have a pencil icon. If the pencil icon is absent, you may not edit that resource attribute from this page.
- 7 Use the following information to edit the attribute:

Resource	Name of the resource
Attribute	Name of the resource's attribute.
Description	A short description of the attribute. A more detailed description is available. See " Attributes reference "
All systems in the SystemList	Select this option to modify the resource attribute value for all the systems listed in the service group's SystemList attribute.
Selected system	Select this option to modify the resource attribute value individually for each system.
Value	Type the new resource attribute value for the selected system.

- 8 In the **Edit Attribute** dialog box, click **OK**.
- 9 In the **Edit Attribute** dialog box, click **Close**.

To edit resource attributes from the command line

- ◆ At the command prompt, type the following:

```
hares -modify resource attribute value [-sys system]
[-user user@domain] [-domaintype domaintype]
```

Modifying zone resource attributes

Use this procedure to modify zone resource attributes.

To modify zone resource attributes using the VCS One console

- 1 In the VCS One console, locate the service group that contains the zone resource, which you want to modify.
See "[Locating a service group](#)" on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.

- 3 Click **Configuration > Add/Modify Resource**.
- 4 In the **Add Resource - Group** panel, click **OK**.
- 5 In the **Results** dialog box, click **Advanced**. The **Edit Attribute** dialog box is displayed.
- 6 In the **Edit Attribute** dialog box, under **Value**, locate the zone resource attribute that you want to modify and change its value.
- 7 In the **Edit Attribute** dialog box, click **OK**.
- 8 In the **Edit Attribute** dialog box, click **Close**.

Enabling resources in a service group

Use this procedure to enable the resources in a service group. Before you bring a resource online, ensure that the resource is enabled and probed.

To enable resources in a service group using the VCS One console

- 1 In the VCS One console, locate the service group that contains the resources, which you want to enable.
 See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group name that contains the resources you want to enable.
 In the service group detail view, options under the menu bar are service group-specific operations; options accessed by a right-click are resource-specific operations.
- 3 Use the following information to choose the next step:

To enable one or more resources	1	Right-click the resource in the Resource Name table
	2	Click Operations > Enable Resources
To enable all resources	■	Click Operations > Enable All Resources
- 4 Click **OK**.
- 5 Click **Close**.

To enable a resource in a service group using the command line

- ◆ At the command prompt, type the following:
`hares -modify servicegroup.resource Enabled 1`

Disabling resources in a service group

Disable a resource in a service group to prevent it from starting up, or going online. You may also use this procedure when you want VCS One to stop monitoring the resource while the service group is still online.

You may only disable an online resource. To disable an offline resource, first bring the resource online.

To disable resources in a service group using the VCS One console

- 1 In the VCS One console, locate the service group that contains the resources, which you want to disable.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the service group name that contains the resource(s) you want to disable.
- 3 Use the following information to choose the next step:

- | | |
|----------------------------------|---|
| To disable one or more resources | 1 Right-click the resource in the Resource Name section |
| | 2 Click Operations > Disable Resources |
| To disable all resources | ■ Click Operations > Disable All Resources |

- 4 Click **OK**.
- 5 Click **Close**.

To resources in a service group from the command line

- ◆ At the command prompt, type the following:

```
hagrp -disableresources service_group [-user user@domain] [-domaintype domaintype]
```

Bringing a resource online

Use this procedure to bring a resource online.

To bring a resource online from the Service Groups section

- 1 In the VCS One console, locate the service group that contains the resource, which you want to bring online.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under Service Groups, click the name of the service group that contains the resource you want to bring online.

- 3 Under Resources, right-click the resource that you want to bring online.
- 4 Click **Operations > Online**.
- 5 In the Online Resource panel, select the system on which you want to bring the resource online.
- 6 Click **OK**.

To bring a resource online from the Resource Dependency View

- 1 In the VCS One console, locate the service group that contains the resource, which you want to bring online.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, check the appropriate service group.
- 3 Click **Views > Resource Dependencies**.
- 4 In the Resource Dependency View, right-click the resource to be brought online
- 5 Click **Online**.
- 6 In the **Online Resource** panel, select the system on which you want to bring the resource online.
- 7 Click **OK**.

To bring a resource online from the command line

- ◆ At the command prompt, type the following:

```
hares -online resource -sys system  
[-user user@domain] [-domaintype domaintype]
```

Taking a resource offline

When you take a resource offline, VCS One executes the stop procedure for the resource.

To take a resource offline using the VCS One console

- 1 In the VCS One console, click **Manage** tab.
- 2 Click the **Resources** tab.
- 3 In the right pane, click **Operations > Offline**
- 4 In the **Offline Resource** dialog box, select the system from which you want to take the resource offline.

- 5 Check the **Ignore state of parent resource** box, if appropriate. This option allows the parent resources to remain online.
- 6 Click **OK**.

To take a resource offline from the command line

- ◆ At the command prompt, type the following:

```
hares -offline [-ignoreparent] resource -sys system
[-user user@domain] [-domaintype domaintype]
```

The *ignoreparent* option lets the parent resources remain online.

Taking parent and child resources offline concurrently

Use this procedure to take a parent resource offline and propagate the command to child resources. You can use the Offline Propagate feature to propagate the offline state of a parent resource to the child resources. If a parent resource is taken offline, all the resources that are dependent on it must be taken offline as well.

To take parent and child resources offline concurrently

- 1 In the VCS One console, click **Manage** tab.
- 2 Click the **Resources** tab.
- 3 In the right pane, click **Operations > Offline Propagate**
- 4 In the **Offline Resource** dialog box, select the system from which you want to take the resource offline.
- 5 Click **OK**.

To take a resource offline from the command line

- ◆ At the command prompt, type the following:

```
hares -offline -propagate resource -sys system
[-user user@domain] [-domaintype domaintype]
```

Probing a resource

Use this procedure to probe a resource. Each resource is periodically monitored at specific time interval. The probe operation instantaneously initiates a monitor cycle and checks the resource configuration, current resource state, and determines if the resource is ready to be brought online.

To probe a resource using the VCS One console

- 1 In the VCS One console, locate the service group that contains the resource, which you want to probe.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the right pane, under **Resources**, click the resource that you want to probe.
- 4 In the right pane, from the **Operations** menu, click **Probe**. The **Probe Resource** dialog box is displayed.
- 5 In the **Probe Resource** dialog box, select either all the systems or a particular system on which you want the resource to be probed.
- 6 Click **OK**.

To probe a resource from the command line

- ◆ At the command prompt, type the following:

```
hares -probe resource -sys system  
[-user user@domain] [-domaintype domaintype]
```

More information is available about probing selected resources in a service group.

See [“Probing service group resources”](#) on page 349.

Faulting a resource using the Simulator

This task is only available using the Simulator, to simulate the fault of a resource.

To simulate a resource fault

- 1 In the VCS One console, locate the service group that contains the resource you want to fault.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the right pane, under **Resources**, click the resource for which you want to simulate a fault.
- 4 In the right pane, in the Simulation menu, click **Fault Resource**.
- 5 In the Fault Resource dialog box, select the system on which you want to fault the resource.
- 6 Click **OK**.

To simulate a resource fault from the command line

- ◆ At the command prompt, type the following:

```
hasim -faultres resource [-sys system] [-grp group]  
[-user user@domain -domaintype domaintype]
```

Repairing a resource using the Simulator

This task is only available using the Simulator, to simulate a resource repair operation.

To simulate a resource repair operation

- 1 In the VCS One console, locate the service group that contains the faulted resource.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the right pane, under **Resources**, click the faulted resource for which you want to simulate a repair operation.
- 4 In the right pane, in the **Simulation** menu, click **Clear Fault and Online**.
- 5 In the **Simulate Clear Resource** dialog box, select the system on which you want to clear the resource fault.
- 6 Click **OK**.

To simulate a resource repair operation from the command line

- ◆ At the command prompt, type the following:

```
hasim -clearresfault resource -sys system [-grp group]  
[-user user@domain -domaintype domaintype]
```

Clearing a resource fault

Use this procedure to clear a resource fault. A resource fault may occur due to various reasons, such as a power failure or a faulty configuration. In such a situation, you need to clear the resource fault in order to remove the fault and make the resource available to go online again.

To clear a resource fault from the Service Groups section

- 1 In the VCS One console, locate the service group that contains the faulted resource.
See [“Locating a service group”](#) on page 321.

- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the right pane, under **Resources**, click the faulted resource.
- 4 In the right pane, from the **Operations** menu, click **Clear Fault**. The **Clear Resource** dialog box is displayed.
- 5 In the **Clear Resource** dialog box, select the system on which you want to clear the resource fault.
- 6 Click **OK**.

To clear a resource fault from the Resource Dependency View

- 1 In the VCS One console, locate the service group that contains the faulted resource.
 See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the left pane, under **Views**, click **Resource Dependencies**.
- 4 In the **Resource Dependency View**, right-click the faulted resource, and then click **Clear Fault**.
- 5 In the **Clear Resource** dialog box, select the system on which you want to clear the resource fault.
- 6 Click **OK**.

To clear a resource fault from the command line

- ◆ At the command prompt, type the following:


```
hares -clear resource [-sys system]
[-user user@domain] [-domaintype domaintype]

hares -clearadminwait [-fault] resource -sys system
[-user user@domain] [-domaintype domaintype]
```

Clearing resources in the ADMIN_WAIT state

When VCS One sets a resource in the ADMIN_WAIT state, it invokes the resadminwait trigger according to the reason the resource entered the state. You can configure policy regarding a resource in the ADMIN_WAIT state. See [Table 11-1, “ResFaultPolicy values for resource level control of fault behavior,”](#) on page 229.

To clear a resource in the ADMIN_WAIT state using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.

- 2 Click the **Resources** tab.
- 3 In the right pane, under **Resources**, check the appropriate resource.
- 4 Click **Operations > Clear Admin Wait**.
- 5 Click **OK**.

To clear a resource in the ADMIN_WAIT state using the command line

- 1 Take the necessary actions outside VCS One to bring all resources into the required state.
- 2 Verify that resources are in the required state by issuing the command:

```
hagr -clearadminwait group -sys system
```

This command clears the ADMIN_WAIT state for all resources. If VCS One continues to detect resources that are not in the required state, it resets the resources to the ADMIN_WAIT state.
- 3 If resources continue in the ADMIN_WAIT state, repeat step 1 and step 2, or issue the following command to stop VCS One from setting the resource to the ADMIN_WAIT state:

```
hagr -clearadminwait -fault group -sys system
```

This command has the following results:

- If the resadminwait trigger was called for reasons 0 or 1, the resource state is set as ONLINE|UNABLE_TO_OFFLINE.
- If the resadminwait trigger was called for reasons 2, 3, or 4, the resource state is set as FAULTED. Please note that when resources are set as FAULTED for these reasons, the clean entry point is not called. Verify that resources in ADMIN-WAIT are in clean, OFFLINE state prior to invoking this command.

When a service group has a resource in the ADMIN_WAIT state, the following service group operations cannot be performed on the resource: online, offline, switch, and flush. Also, you cannot use the hastop command when resources are in the ADMIN_WAIT state. When this occurs, you must issue the hastop command with -force option only.

Linking resources

Use this procedure to link resources. You can link two or more resources in a service group. After you link resources, one resource becomes the parent resource and the other the child resource. A child resource must be brought online before the parent resource is brought online.

To link resources from the Service Groups section

- 1 In the VCS One console, locate the service group that contains the resources, which you want to link.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the right pane, from the **Configuration** menu, click **Link/Unlink Resource**.
- 4 In the **Link/Unlink Resource** dialog box, perform the following steps for each resource pair that you want to create:
 - In the **Parent Resource** box, select the parent resource.
 - In the **Child Resource** box, select the child resource. Only resources that are available as child resources are displayed.
 - Click **Add Link**. After the resource dependency between the parent and child resources are created they are displayed in the **Currently Linked** list.
- 5 Click **OK**.

To link resources from the Resource Dependency View

- 1 In the VCS One console, locate the service group that contains the resources, which you want to link.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the left pane, under **Views**, click **Resource Dependencies**.
- 4 In the **Resource Dependency View**, right-click the parent resource, and then click **Link**.
- 5 Move the mouse pointer to the child resource. A grey line extends as you move the mouse pointer. When the mouse pointer changes to a hand symbol, click the child resource.
- 6 In the **Question** dialog box, click **Yes**.

To link resources from the command line

- ◆ At the command prompt, type the following:

```
hares -link parentresource childresource  
[-user user@domain] [-domaintype domaintype]
```

Unlinking resources

Use this procedure to unlink resources. You can unlink resources only if they are previously linked.

To unlink resources from the Service Groups section

- 1 In the VCS One console, locate the service group that contains the resources, which you want to unlink.
See “[Locating a service group](#)” on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the right pane, from the **Configuration** menu, click **Link/Unlink Resource**.
- 4 In the **Link/Unlink Resource** dialog box, under **Currently Linked**, select the parent and child pair, and then click the corresponding **Remove** icon. Repeat this step for all the resources that you want to unlink.
- 5 Click **OK**.

To unlink resources from the Resource Dependency View

- 1 In the VCS One console, locate the service group that contains the resource, which you want to unlink.
See “[Locating a service group](#)” on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the left pane, under **Views**, click **Resource Dependencies**.
- 4 In the **Resource Dependency View**, right-click the link between the resources to be unlinked, and then select **Unlink**.
- 5 In the **Question** dialog box, click **Yes**.

To unlink resources from the command line

- ◆ At the command prompt, type the following:

```
hares -unlink parentresource childresource  
[-user user@domain] [-domaintype domaintype]
```

Viewing resources in the configuration by resource type

You can view the resources in use in the VCS One cluster by their resource type. You can also view the following information in this view:

- The state of the resources of that type

- The service groups that contain that resource type
- The platform on which the resource type runs
- The date and time the resource type's configuration was updated
- The date and time the resource type was created.

To view resources in the configuration by resource type

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Resources** tab.
- 3 Click **Views > Resource Types**
- 4 Use the following information to perform further actions:

To sort the view of the resource types Click the column heading of the table to sort by that category.

To view the resources of that type, their state, and the corresponding service groups Click the resource type in the name column.

Defining an attribute value with a resource variable

VCS One allows you use a variable in the definition of certain attribute values.

See [“Designing attribute values using variables”](#) on page 233.

When variables are used in resource attribute values, and you have to change what those variables represent, you must refresh the value of the attribute.

See [“About designing attribute values using variables”](#) on page 234.

To define an attribute value with a variable using the VCS One console

- 1 In the VCS One console, locate the service group or the system that contains the resources to which you want to define the variable.
 See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the right pane, under **Resources**, click the resource to which you want to add the variable.
- 4 In the right pane, click **All Attributes**.
- 5 In the **All Attributes** list, locate the resource attribute that you want to modify, and then click its corresponding pencil icon to change its value. The pencil icon is displayed next to attributes that are editable.

Displaying values to be affected by a change in a resource variables definition

- 6 In the **Edit Attribute** dialog box, under **Value**, specify the variable in one of the following syntax formats:
 - `@{attribute_name}`
 - `@{object.attribute_name}`
 - `@{object.attribute_name:association_key}`
 - `@{object.extended_attribute}`
 See “[Resource variable syntax](#)” on page 238.
- 7 Click **OK**.

To define an attribute value with a variable using the command line

- ◆ Type the following command

```
hares -modify rname aname @{variable}
```

Use the following information to replace the appropriate variables:

<i>rname</i>	The name of resource.
<i>aname</i>	The name of the attribute of the resource that will have a variable as a value.
<code>@{variable}</code>	The variable that determines the value of the attribute. This variable can be in one of the following formats: <ul style="list-style-type: none"> <code>@{attribute_name}</code> <code>@{object.attribute_name}</code> <code>@{object.attribute_name:association_key}</code> <code>@{object.extended_attribute}</code>

For example, to use the system attribute SysName as a variable in the resource attribute MountPath, enter the following:

```
hares -modify r1 pathname /tmp/{system.SysName}
```

Displaying values to be affected by a change in a resource variables definition

Before you change a built-in attribute value or an extended attribute value, use this procedure to ensure you know what resources are affected.

You can not perform this task using the VCS One console.

To display values to be affected using the command line

- ◆ Type the following command before you modify an attribute value that may contain a resource variable.

hacmd -infovars obj attribute

Use the following information to replace the appropriate variables:

<i>hacmd</i>	Type <i>hagrp</i> for a group-related attribute or <i>hasys</i> for a system-related attribute.
<i>obj</i>	The name of the group or the system.
<i>attribute</i>	The name of the attribute.

Updating the value of a resource variable

When variables are used to define the value of an attribute, you must refresh or update the value of the attribute under the following conditions:

- When you move a system or service group between nodes in the organization tree.

The object is not moved and an error message is logged if one of the following items is true:

- The object has extended attributes that are variables.
- The values of the variables are not valid in the new location.

To override this behavior and move the object, use the `–refreshvars` option of the command. Doing so will update value of the resource attributes.

- When you modify the value of a system or service group attribute that is a resource variable.

The value is not modified and an error message is logged if the object has built-in or extended attributes that are variables.

To override this behavior and modify an extended attribute value that is a variable, use the `–refreshvars` option. Doing so will modify the value of the resource attributes that use the variable.

To update the value of a resource variable because of a move a system in the organization tree

- ◆ Type the following command:

```
hacmd -move -refreshvars objects -ou oupath
```

Use the following information to replace the appropriate variables:

<i>hacmd</i>	Replace with <i>hasys</i> to move systems. Replace with <i>hagrp</i> to move service groups.
<i>objects</i>	A list of one or more objects. The objects may be systems or service groups.
<i>oupath</i>	The new OUValue path for the object.

To update the value of a resource variable because of modification of an attribute value using the command line

- ◆ Type the following command:

```
hacmd -modify -refreshvars object attribute value
```

Use the following information to replace the appropriate variables:

hacmd Replace with *hasys* to move systems. Replace with *hagrp* to move service groups.

object The object that the attribute describes. The object may be a system or a service group.

attribute The attribute whose value you are editing.

value The new value of the attribute.

More options are available for the *hasys* command and the *hagrp* command. See *The Veritas Cluster Server One Command Reference Guide*.

Managing application placement

This chapter includes the following topics:

- [About managing application placement](#)
- [Viewing the application placement](#)

About managing application placement

VCS One enables you to manually designate, or have VCS One automate, the decision of where an application will run based on the configuration of certain service group, system, and cluster attributes. The set of configuration settings that affect this behavior is referred to as the application placement policy.

This set contains the following attributes:

- Service group attributes
 - SystemList
 - Priority
 - CompatibleGroups
 - IncompatibleGroups
 - Load
- System attributes
 - Capacity
- Cluster attributes
 - PrecedenceOrder
 - FragmentationPolicy

More information is available on how application placement policy settings affect where a service group will run.

See [“Designing application placement policy”](#) on page 273.

Additionally, the failover behavior of a service group is decided by the following attributes:

- ResFaultPolicy
- GrpFaultPolicy
- NodeFaultPolicy

More information is available on the values of these attributes.

See [“Designing actions taken after a fault”](#) on page 227.

Defining the SystemList attribute for a service group

The SystemList attribute is an ordered list of the names of the systems that the service group may run on. The SystemList attribute is the only attribute related to application placement policy that must be configured for all service groups.

If you use a set name in the definition of the SystemList, and an OUValue path is not explicitly specified, the service group's home organization unit is the default.

See “[Service group attributes](#)” on page 712.

To define the SystemList attribute using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Service Groups** tab.
- 3 From the list of service groups, click the link that is the name of the service group you wish to edit.
- 4 In the right pane, from the **Configuration** menu, click **Edit SystemList**. The **SystemList Configuration** window appears.
- 5 Under **Available Systems**, select one or more systems, and then click the right-arrow icon to add the systems to the service group's SystemList.
 - Click the heading **Available Systems** to arrange the systems in ascending or descending alphabetical order.
 - Select the **Filter** button if you want to filter the systems that are shown in the **Available Systems** windows based on extended attributes, system attributes, organization units, sets or expressions.
 - Select the **No Filter** button, if you do not want to set a filter criteria.
- 6 Once you have all the required systems in the **SystemList** box, order the SystemList.

To move a system earlier or later in the SystemList, click the name of a system. Click the up arrow to the right of the SystemList box to move the system earlier in the SystemList, click the down arrow to move the system later in the SystemList.
- 7 If required, click the **Propagate** check box to make sure the change is propagated to all service groups in the same dependency tree.
- 8 Click **OK**.
- 9 Click **Close**.

To define the SystemList attribute from the command line

- ◆ Type the following on the command line:

```
hagrp -modify <group> SystemList [ -add | -delete ] <system value>
```

Defining service group priority

You define service group priority with the Priority attribute. Valid values are 1 to 5. 1 is the highest priority, 5 is the lowest priority.

To define service group priority using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 In the right pane, click the **Service Groups** tab.
- 3 From the list of service groups, select the check box corresponding to the service group you wish to edit.
- 4 In the right pane, from the **Configuration** menu, click **Edit Attribute**. The Edit Attribute dialog box appears.
- 5 From the **Attribute Name** drop-down list, select the **Priority** attribute.
- 6 In the **Values** box, click the current value, and type in the new value.
- 7 If required, click the **Propagate** check box to make sure the change is propagated to all service groups in the local dependency tree.
- 8 Click **OK**.
- 9 Click **Close**.

To define service group priority from the command line

- ◆ Type the following on the command line:
`hagrp -modify <group> Priority <priority_value>`

Defining service group compatibility or incompatibility

To specify the definition of CompatibleGroups and IncompatibleGroups using an expression, you must use the command line interface. If an OUValue path is not explicitly specified in the expression, the search for service group begins at the user's home organization unit path node.

To define service group compatibility using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 In the right pane, click the **Service Groups** tab.
- 3 From the list of service groups, select the link that is the name of the service group you wish to edit.

- 4 In the right pane, from the **Configuration** menu, click **Edit Compatibility**. The **Service Group Workload Configuration** window for compatible / incompatible groups appears.
- 5 Choose the Compatibility Type.
 Chose **Compatible** if you want to designate groups in the next step that can run on the same system at the same time as the group you are modifying. The remaining service groups, and all service groups added in the future, will be incompatible with the group being configured.
 Choose **Incompatible** if you want to designate groups in the next step that can not run on the same system at the same time as the group you are modifying. The remaining service groups, and all service groups added in the future, will be compatible with the group being configured.
- 6 Select the groups you want to apply your chosen Compatibility Type.
 - Click the **ALLGROUPS** check box to designate all the service groups in the VCS One cluster are compatible (if you chose the **Compatible** option) or incompatible (if you chose the **Incompatible** option) with the group being modified.
 - Click the **Select Service Groups** check box to chose specific service groups to apply your chosen Compatibility Type.
 Under **Available Groups**, select one or more systems, and then click the right-arrow icon to add the systems to the **GroupList**.
 - Click the heading **Available Groups** to arrange the groups in ascending or descending alphabetical order.
 - Select the **Filter** button if you want to filter the groups that are shown in the **Available Groups** windows based on extended attributes, the Organization Tree, sets or expressions.
 - Select the **No Filter** button, if you do not want to set a filter criteria.
- 7 Once you have all the required groups in the **GroupList** box, click **OK**.
- 8 Select the **Propagate** check box if the groups you selected in the previous step are part of a local dependency tree. This ensures that all the groups that are part of the local dependency have the same set of compatible or incompatible groups.
- 9 Click **OK**.
- 10 Click **Close**.

To define service group compatibility from the command line

- ◆ Type the following on the command line:


```
hagrp -compatible [-propagate] <group1> <group2>
hagrp -compatible [-propagate] <group> ALLGROUPS -force
```

```
hagrp -incompatible [-propagate] <group1> <group2>  
hagrp -incompatible [-propagate] <group> ALLGROUPS -force
```

See the *Veritas Cluster Server One Command Reference Guide*.

Defining a resource's fault policy

The failover behavior of a service group, in the event of a service group, a system, or a resource fault is decided by taking into consideration the service group fault policy, the system fault policy, and the resource fault policy.

See [“Defining a service group's fault policy”](#) on page 402.

See [“Defining a system's fault policy”](#) on page 403.

To define the resource fault policy

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 From the list of service groups, click the service group for which you wish to specify the resource fault policy.
- 4 From the **Resources** table, click the resource for which you wish to specify the resource fault policy.
- 5 In the resource page, in the top-right corner, click **All Attributes**.
- 6 In the list of attributes, click the pencil icon for the **ResFaultPolicy** attribute.
- 7 In the **Edit Attribute** window, in the **Value** box, select the new value
The attribute value will be one of the following:
FaultNone, FaultHold, FaultPropagateAll, FaultPropagateParent.
More information is available on these values.
See [“ResFaultPolicy”](#) on page 742.
- 8 Click **Next**.
- 9 Click **Finish > Close**.

Defining a service group's fault policy

The failover behavior of a service group, in the event of a service group, a system, or a resource fault is decided by taking into consideration the service group fault policy, the system fault policy, and the resource fault policy.

See [“Defining a resource's fault policy”](#) on page 402.

See [“Defining a system's fault policy”](#) on page 403.

To define the service group fault policy

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click **SGs and CSGs > Service Groups**.
- 3 From the list of service groups, click one or more service groups for which you wish to specify the service group fault policy.
- 4 In the right pane, click **Configuration > Edit Fault Policy**.
- 5 From the **Fault Policy** box, select **GrpFaultPolicy**.
- 6 Click **All Groups** or **Selected Groups**.
If you click Selected Groups, you may set different values for each group. If you click All Groups, you set the same value for each group.
- 7 In the **Select Value** box, choose **Failover** or **NoFailover**.
More information is available on these values.
See [“GrpFaultPolicy”](#) on page 714.
- 8 Click the **Propagate** check box if you want the change to be propagated to all service groups in the local dependency tree.
- 9 Click **Next**.
- 10 Click **Finish > Close**.

Defining a system's fault policy

The failover behavior of a service group, in the event of a service group, a system, or a resource fault is decided by taking into consideration the service group fault policy, the system fault policy, and the resource fault policy.

See [“Defining a resource's fault policy”](#) on page 402.

See [“Defining a service group's fault policy”](#) on page 402.

To define the system fault policy

- 1 Click **SGs and CSGs > Service Groups**.
- 2 From the list of service groups, click one or more service groups for which you wish to specify the service group's system fault policy.
- 3 In the right pane, click **Configuration > Edit Fault Policy**.
- 4 From the **Fault Policy** box, select **NodeFaultPolicy**.
- 5 Click **All Groups** or **Selected Groups**.
If you click Selected Groups, you may set different values for each group. If you click All Groups, you set the same value for each group.

- 6 In the **Select Value** box, choose **Failover** or **NoFailover**.
More information is available on these values.
See “[NodeFaultPolicy](#)” on page 716.
- 7 Click the **Propagate** check box if you want the change to be propagated to all service groups in the local dependency tree.
- 8 Click **Next**.
- 9 Click **Finish > Close**.

Defining the VCS One cluster's load and capacity keys

The server-farm-wide keys used to designate the values of service group load and system capacity are defined in the VCS One cluster's `PrecedenceOrder` attribute:

To define the VCS One cluster's load and capacity keys using the VCS One console

- 1 From the VCS One console, click **Administration > Settings**.
- 2 In the left pane, click the **Global Settings** link.
- 3 In the right pane, in the Name column, find the `PrecedenceOrder` attribute.
- 4 Click the pencil icon in the Edit column of the `PrecedenceOrder` row.
- 5 In the Edit Attribute panel, perform one of the following tasks:
 - Click the name of a key in the value column to edit or change the name of a key
 - Click the plus sign to add a key.
There can be a maximum of four keys defined.
 - Click a key name and then click the minus sign to delete a key. You may delete a `PrecedenceOrder` key only if all group loads and system capacities have zero values associated with the key.
- 6 Click **OK**.
- 7 Click **Close**.

To define the VCS One cluster's load and capacity keys from the command line

- ◆ Type the following on the command line:

```
haclus -modify PrecedenceOrder [-add | -delete] key value
```

Defining service group load

You define service group load with the Load attribute.

To define service group load using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 In the right pane, click the **Service Groups** tab.
- 3 From the list of service groups, select the check box corresponding to the service group you wish to edit.
- 4 In the right pane, from the **Configuration** menu, click **Edit Attribute**. The Edit Attribute dialog box appears.
- 5 From the **Attribute Name** drop-down list, select the Load attribute. The **Values** box will contain the keys set by the PrecedenceOrder attribute.
- 6 In the **Values** box, click in the **value** column to edit value of the key.
- 7 Click **OK**.

To update a service group load value from the command line

- ◆ Type the following on the command line:

```
hagrp -modify <group> Load -update key value
```

Defining system capacity

You define system capacity with the Capacity attribute.

To define system capacity using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 In the right pane, click the **Systems** tab.
- 3 From the list of systems, select the check box corresponding to the system you wish to edit.
- 4 In the right pane, from the **Configuration** menu, click **Edit Attribute**. The Edit Attribute dialog box appears.
- 5 From the **Attribute Name** drop-down list, select the **Capacity** attribute.
- 6 In the **Values** box, click in the **value** column to edit value of the key.
- 7 Click **OK**.

To update a system capacity value from the command line

- ◆ Type the following on the command line:

```
hasys -modify <sys> Capacity -update key value
```

Defining the VCS One cluster's FragmentationPolicy attribute

This attribute defines how VCS One automates the choice of a target host system for a service group when more than one system is equally qualified in all other aspects.

See [“Breaking the tie: the FragmentationPolicy attribute”](#) on page 281.

To define the VCS One cluster's FragmentationPolicy attribute using the VCS One console

- 1 From the VCS One console, click the **Administration** tab.
- 2 In the left pane, click the **Global Settings** link.
- 3 In the right pane, in the Attribute Name column, find the FragmentationPolicy attribute.
- 4 Click the pencil icon in the Edit column of the FragmentationPolicy row.
- 5 In the Edit Attribute panel, perform one of the following tasks:
 - Click **BiggestAvailable**, **Heuristic**, or **BestFit** to choose your desired behavior.
See [“Breaking the tie: the FragmentationPolicy attribute”](#) on page 281.
 - Click **<Blank Value>** to remove any value from FragmentationPolicy.
- 6 Click **OK**.
- 7 Click **Close**.

To define the VCS One cluster's FragmentationPolicy attribute from the command line

- ◆ Type the following on the command line:
`haclus -modify FragmentationPolicy value`

Viewing the application placement

The **Workload** tab shows service groups arrayed on systems in a variety of possible views. This allows the administrator to graphically view the many aspects of workload management, including the relative capacity and available capacity of systems, or the utilization of a particular system.

The groups listed in the **Waiting Groups** table on the **Workload** tab are groups that are in the Group Transition Queue (GTQ), waiting for an available resource to online as set by the application placement policy.

More information is available on the Workload tab.

See [“Workload tab menus”](#) on page 121.

More information is available on the GTQ

See [“About the Group Transition Queue”](#) on page 283.

Managing automated tasks

This document includes the following topics:

- [About managing automated tasks](#)
- [Creating a business rule](#)
- [Creating a job](#)
- [Associating a job with a rule](#)
- [Viewing rules and jobs that are associated with an object](#)
- [Cloning a job](#)
- [Modifying a job](#)
- [Running a job](#)
- [Deleting a job](#)
- [Changing the owner of a rule](#)
- [Enabling a rule](#)
- [Disabling a rule](#)
- [Modifying a rule](#)
- [Deleting a rule](#)
- [About configuring tasks](#)
- [Exporting a rule or a job to an XML file](#)
- [Importing a rule or a job from an XML file](#)

About managing automated tasks

Automated tasks are configured by setting up rules. Rules can be either business rules or notification rules. The components of rules are events, rules, jobs, tasks, and notifications.

A rule will not execute unless it is enabled and error-free.

Automated business rules

The following steps describe how an automated business rule flows:

- An event occurs
- Conditions are checked
- A rule is triggered
- A job is run
- Tasks in the job are executed

Events are not part of a workflow; the order of job execution in a business rule may not be the same as the order of the events that invoke the job. However, multiple tasks associated with a job are executed in sequence.

More information is available on the types of tasks you can automate.

See [“How you can configure automated tasks and group operations”](#) on page 62.

The following steps describe the configuration process at a high level:

- Create a rule
 - Define events that trigger the rule
 - Specify object filtering that can trigger the rule (event-based rules)
 - Define conditions for the rule
 - Create a jobs or associate an existing job with the rule
- Create a job
 - Define tasks of the job

Further details are available about each of these items.

See [“Automated tasks reference”](#) on page 643.

Automated notification rules

The following steps describe how an automatic notification rule flows:

- An event occurs
- Notification is sent

Creating a rule

A rule can be either a business rule or a notification rule.

Creating a business rule

Business rules are triggered by a Policy Master or a scheduled event, and result in the execution of a job. You can also create rules that result in a form of notification that the event occurred.

See [“Creating a notification rule”](#) on page 414.

To create a business rule using the VCS One console

- 1 In the VCS One console, click **Manage** tab.
- 2 Click the **Automation > Business Rules** tab.
- 3 Click **Configuration > Add Rule > Next**.

4 In the Configure Rule details panel, enter the following information:

Name	The name for the rule.
Trigger using	The type of the event that will trigger the rule. Choose one of the following types based on how the event is generated: <ul style="list-style-type: none">■ Click Event for a Policy Master generated event■ Click Schedule for a schedule generated event.
Description	The description for the rule.
Rule belongs to:	The path of the OU Node associated with the rule. Click the pencil icon to select a path from the organization tree view. The rule can only access objects in the scope of this organization unit path. The scope of this path includes the objects attached at or below this OU Node.
Run using privilege of:	The owner of the rule. Choose the owner from the drop-down menu. The owner of the rule determines the user whose privileges will be applied when the rule is run. See “About privileges” on page 218.
Quiet time	Controls how often a rule may be triggered for the same object and the same event. The number of seconds to wait after the rule has been triggered, and before the rule may be triggered again for the same object and the same event. Use this option to prevent overrun of logs or notifications.
Enable this Rule	Check to make the rule active. A rule will not execute unless it is enabled.

5 Click **Next**.

The type of event you chose in the **Trigger using** field determines the next window. Use the following information to determine

Type of event in Trigger using field	Action
Event	See “To define an event that triggers a rule using the VCS One console” on page 413.
Schedule	See “To define a schedule that triggers a rule using the VCS One console” on page 414.

To define an event that triggers a rule using the VCS One console

1 In the Event Selection window, enter the following information:

- | | |
|------------------------|---|
| Events involving | The type of object that will trigger the event. Options are Group , Composite Service Group (CSG), System , Resource , User , UserGroup , Organization Unit , and Farm . |
| Select all events | Check if you want to select all events of this object type. |
| Select specific events | Check the box next to each event that will trigger this rule. The rule will trigger when any one of these checked events occurs.

More information is available about each event.

See Table 34-1, “VCS One events and associated parameters,” on page 645. |
| Specify objects | Click the pencil icon to select the specific objects that will trigger this rule.

If you select specific objects, only those objects undergoing the selected event triggers the rule.

If you do not select specific objects, any object undergoing the selected event triggers the rule.

If you specify an OU expression, any object under that OU node that undergoes the selected event triggers the rule. |

2 Click **Next**.

3 In the Conditions panel, you have the option to define conditions for the rule.
 See [“Adding or modifying conditions and filters for the rule”](#) on page 417.

4 In the Job details panel, you specify the details of a job
 See [“Creating a job”](#) on page 421.

5 Click **Next**.

6 Click **Finish**.
 In the Summary panel, you can view the pending commands before they are executed. Reverse back through the wizard to modify the commands.

7 Click **Close**.

To define a schedule that triggers a rule using the VCS One console

- 1 In the Schedule Configuration window, enter the following information:

Start Date	A start date for the rule.
Start Time	The hour and minutes the rule goes into effect. Time is based on a 24-hour clock. Rule is run per the time on the web server host.
Create recurrence	Check this box to automated repeated execution of the rule.
Daily	Click one of the recurrence patterns, Daily , Weekly , or Monthly , and then select the options that you want relative to that pattern.
Weekly	
Monthly	
End recurrence by Date	A stop date for the rule.

- 2 Click **Next**.
- 3 In the Conditions panel, you have the option to define conditions for the rule.
See [“Adding or modifying conditions and filters for the rule”](#) on page 417.
- 4 In the Job details panel, you specify the details of a job
See [“Creating a job”](#) on page 421.
- 5 Click **Next**.
- 6 Click **Finish**.
In the Summary panel, you can view the pending commands before they are executed. Reverse back through the wizard to modify the commands.
- 7 Click **Close**.

Creating a notification rule

Notification rules are triggered by a Policy Master event, and result in a form of notification that the event occurred. You can also create rules that result in the execution of a job.

See [“Creating a business rule”](#) on page 411.

To create a notification rule using the VCS One console

- 1 In the VCS One console, click **Manage > Automation** tabs.
- 2 Click the **Notification Rules** tab.
- 3 Click **Configuration > Add Rule > Next**.

4 In the Configure Rule details panel, enter the following information:

Name	The name for the rule.
Description	The description for the rule.
Rule belongs to:	<p>The path of the OU Node associated with the rule. Click the pencil icon to select a path from the organization tree view.</p> <p>The rule can only access objects in the scope of this organization unit path. The scope of this path includes the objects attached at or below this OU Node.</p>
Run using privilege of:	<p>The owner of the rule. Choose the owner from the drop-down menu.</p> <p>The owner of the rule determines the user whose privileges will be applied when the rule is run.</p> <p>See “About privileges” on page 218.</p>
Quiet time	<p>Controls how often a rule may be triggered for the same object and the same event.</p> <p>The number of seconds to wait after the rule has been triggered, and before the rule may be triggered again for the same object and the same event. Use this option to prevent overrun of logs or notifications.</p>
Enable this Rule	Check to make the rule active. A rule will not execute unless it is enabled.

5 Click **Next**.

6 In the Event Selection panel, enter the following information:

Events involving	The type of object that will trigger the event. Options are Group, Composite Service Group (CSG), System, Resource, User, UserGroup, Organization Unit, and Farm.
Select all events	Check if you want to select all events of this object type.
Select specific events	Check the box next to each event that will trigger this rule. The rule will trigger when any one of these checked events occurs. More information is available about each event. See Table 34-1, “VCS One events and associated parameters,” on page 645.
Specify objects	Click the pencil icon to select the specific objects that will trigger this rule. If you select specific objects, only those objects undergoing the selected event will trigger the rule. If you do not select specific objects, any object undergoing the selected event will trigger the rule.

7 Click **Next**.

8 In the Notification Recipients panel, enter the following information:

Specify Email recipients	The email address of each person you want to receive an email notification if the event occurs. Check Use Owner’s Email if you want the owner of the rule to receive an email notification.
Specify SNMP consoles	The name or IP address of the SNMP consoles to which you wish to write a log message if the event occurs. Check Use Owner’s SNMP if you want to include the SNMP console of the owner of the rule.
Specify Syslog hosts	The name or IP address of the Syslog hosts to which you wish to write a log message if the event occurs.

9 Click **Next**.

10 Click **Finish > Close**.

To create a rule using the command line

- 1 Type the following command to create the rule

```
harule -add rule objType -oupath path
```

Use the following information to replace the appropriate variable:

<code>rule</code>	The name of the rule.
<code>objType</code>	The type of object that will trigger the notification.
<code>path</code>	The organization tree node where this rule is attached, denoted by the organization tree path

- 2 Use the `harule -modify` command to add filtering criteria and specify recipients to the newly created rule.

Adding or modifying conditions and filters for the rule

Within the rule definition, you can define conditions to evaluate before the job is executed. If you define conditions on a rule, the rule only gets executed if the conditions are met.

A condition is created in the form of a condition expression, and can be one of the following types:

- Attribute-based condition
See [“To add or modify an attribute-based condition to a rule using the VCS One console”](#) on page 417.
- Schedule-based condition
See [“To add an scheduled-based condition to a rule using the VCS One console”](#) on page 418.

You may define both attribute-based conditions and scheduled-based conditions for the same rule.

If you arrive at this procedure from the Rule Configuration Wizard, you start at [step 4](#).

To add or modify an attribute-based condition to a rule using the VCS One console

- 1 In the VCS One console, click **Manage > Automation** tabs.
- 2 Click the **Business Rules** tab.
- 3 Click **Configuration > Add/Modify Conditions**.
- 4 From the Conditions page, enter conditions for the rule. Use the following information to perform this task.

Select Condition Type	Click Attribute based
Specify Object	Click Group or System to select the type of object. Click the pencil icon to select the specific objects of that type that apply to this condition. If you select specific objects, only those objects undergoing the selected event will trigger the condition.
Specify Condition	The conditions you can configure depend on the type of object you select in the Specify Object field. Each object has multiple attributes that you can use to define a condition. Select the attribute in the first menu. Select = (equal to) or != (not equal to) in the second menu. Select the value of the attribute that should cause the condition to be true in the third menu.

- 5 Click **Add**.
- 6 Repeat [step 4](#) and [step 5](#) until you define all your conditions.
- 7 Click **Next** or **OK > Finish > Close**.
The text of this step depends on whether you enter this procedure from the Rule Configuration Wizard or from the Add/Modify Conditions menu item.

To add an scheduled-based condition to a rule using the VCS One console

- 1 In the VCS One console, click **Manage > Automation** tabs.
- 2 Click the **Business Rules** tab.
- 3 Click **Configuration > Add/Modify Conditions**.
- 4 From the Conditions page, enter conditions for the rule. Use the following information to perform this task.

Select Condition Type	Click Time based
Event occurs before	Use this option if you want the automation engine to only consider this condition true if the event occurs before the time you specify.
Event occurs after	Use this option if you want the automation engine to only consider this condition true if the event occurs after the time you specify.

Event occurs between Use this option if you want the automation engine to only consider this condition true if the event occurs between two designated points in time.

- 5 Click **Add**.
- 6 Repeat [step 4](#) and [step 5](#) until you define all your conditions.
- 7 Click **Next** or **OK > Finish > Close**.
The text of this step depends on whether you enter this procedure from the Rule Configuration Wizard or from the Add/Modify Conditions menu item.

Listing rules

By default, the VCS One console lists all rules. You may filter the view to limit the list of rules.

To list rules using the VCS One console

- 1 In the VCS One console, click **Manage > Automation** tabs.
- 2 Click the **Business Rules** tab to display the rules that specify what job is executed. The rule is triggered by an event or a schedule. The job is a collection of one or more actions.
- 3 Click the **Notification Rules** tab to display the rules that specify where notifications for an event will be sent or logged.

To list rules using the command line

- ◆ Type the following command to list notification rules
`harule -list`

Displaying the details of a rule

The details page of a rule displays the attributes associated with the rule.

To display the details of a rule using the VCS One console

- 1 In the VCS One console, click **Manage > Automation** tabs.
- 2 Click the **Business Rules** tab to display the rules that specify an action that is triggered by an event or a schedule.
- 3 Click the **Notification Rules** tab to display the rules that specify recipients that will receive notification for an event.

To display the details of a rule using the command line

- ◆ Type the following command to display a notification rule

```
harule -display rule
```

Use the following information to replace the appropriate variables:

`rule` The name of the notification rule to display. If you do not specify the rule name, all policy rules and all attributes display. Does not display business rules.

Viewing rules and jobs that are associated with an object

You can view the following automation-related information about objects:

- Rules defined on the object
- Rules that refer to the object
- Jobs that refer to the object

To view rules and jobs that are associated with an object

- 1 Go to the details page of the object.
- 2 In the right pane, click **Automation Info**.

Cloning a rule

Use this procedure to create a new rule that closely resembles a rule already in the configuration. Once you clone the rule, edit the new rule as appropriate.

See “[Modifying a rule](#)” on page 427.

You may only clone a rule if you are the owner of the rule. You must also have the privilege to add a rule.

To clone a rule using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click the **Business Rules** tab or the **Notification Rules** tab.
Business rules specify an action that is triggered by an event or a schedule. Notification rules specify recipients that will receive notification for an event.
- 3 Click the name of the rule you wish to clone to go to the rule details page.
- 4 Click **Configuration > Clone Rule**.

- 5 In the Clone Rule panel, enter the number of clones of the rule to create.
- 6 In the Rule Names box, you may select and edit the auto-generated names of the clone rules.
- 7 Click **OK**.
- 8 Click **Finish**.
- 9 Click **Close**.

Creating a job

A job is associated with one or more business rules. Jobs are not associated with notification rules.

If you arrive at this procedure from the Rule Configuration Wizard, you start at [step 5](#).

To create a job using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click **Jobs**.
- 3 In the right pane, from the **Configuration** menu, click **Add Job**.
- 4 In the Job Configuration Wizard screen, click **Next**.
- 5 In the Job details page, enter the following information:

Job Name	The name for the job. If the job you want to associate with the event already exists, click the down arrow and select the job.
Description	The description for the job.
Job belongs to:	The path of the OU Node associated with the job. Click the pencil icon to select a path from the organization tree view. The job can only access objects in the scope of this OU Path. The scope of this OU Path includes the objects attached at or below this OU Node. When you create a job from the Add Rule wizard, this field is automatically populated with the OU Node configured with the rule.
Add Task	Click to go to the Task Details Page, where you can add a new task as described in step 6 .

- Clone Task** Click to duplicate a task. This option is useful to shorten the procedure to create a new task that closely resembles a task that already exists.
You can click the pencil icon to edit the details of the task.
- Import Job Task** Click to import tasks that already exist as part of other jobs.

6 In the Task Details Page, use the following information to configure the details of the task:

- Select Action Type** The action types list the available tasks.
Once you choose an action type, the panel changes to show the configuration details specific to that task.
See [Table 34-2, “Predefined task actions and required task parameters,”](#) on page 663.
- Halt on Error** Click **Yes** if the job should end if the task fails or does not complete by the value in the Timeout field.
Click **No** if the job should continue even if this task fails.
- Timeout** Enter the number of seconds to wait for the task to complete. If this time period is exceeded, the **Halt on Error** field is evaluated.
- Wait after invoking** Enter the number of seconds to wait between invoking this task and invoking the next task.
This field can be useful when the task executes a process and you want to give the process time to complete.
- Task Details** The information that appears in the remainder of the panel is custom to the selection in the **Select Action Type** field.
Enter the configuration options specific to the Action Type selected.

Note: When using action type **Execute HA Command**, click the **Validate** button to ensure the command is valid and supported.

- 7** To add this task and return to the Job details page, click **OK**.
- 8** Repeat [step 6](#) and [step 7](#) until you define all your tasks for the job.
- 9** Click **Next**.
- 10** Click **Finish > Close**.

Associating a job with a rule

You may create jobs independently from creating rules. A rule can only have one job associated with it. A job can be associated to multiple rules.

A job should be attached to the organization tree at the same OU node where the rule is attached.

You associate jobs with a rule as part of the procedure to create a rule.

See “[Creating a business rule](#)” on page 411.

Cloning a job

Use this procedure to create a new job that closely resembles a job already in the configuration. Once you clone the job, edit the new job as appropriate.

See “[Modifying a job](#)” on page 423.

To clone a job using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click the **Jobs** tab.
- 3 In the right pane, click the link of the job you wish to clone.
- 4 In the right pane, from the **Configuration** menu, click **Clone Job**.
- 5 In the Clone Job panel, specify the number of clones of the job to create.
- 6 In the Job Names box, you may select and edit the auto-generated names of the clone jobs.
- 7 Click **OK**.
- 8 Click **Finish**.
- 9 Click **Close**.

Modifying a job

Modify a job using the job details panel. If the job is associated with a Rule, modifying the job may invalidate Rules associated to that Job.

More information about the job details page is available.

See “[Creating a job](#)” on page 421.

To modify a job using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.

- 2 Click **Jobs**.
- 3 In the right pane, click the link of the job you wish to clone.
- 4 In the **Configuration** menu, click **Modify Job**.
- 5 View the impact analysis of modifying this job. Understand the implications of modifying this job.
Rules can become invalid due to job modification. This panel displays the rules associated with the selected job.
- 6 Click **Next**.
- 7 In the Job details panel, edit the properties of the job.
- 8 Click **Next**.
- 9 Click **Finish**.
- 10 Click **Close**.

Running a job

Use this procedure to manually initiate the job to run immediately.

To run a job using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click the **Jobs** tab.
- 3 In the right pane, check the box of job you wish to run.
- 4 In the right pane, from the **Operation** menu, click **Run Job**.
- 5 In the Job panel, select the number of runs of the job to be executed.
- 6 If the job has variables defined, enter the values for the variables.
- 7 Click **Next**.
- 8 Click **Finish**.
- 9 Click **Close**.

Deleting a job

Use this procedure to delete a job. If rules are configured for a job you attempt to delete, the list of affected rules are shown.

To delete a job using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.

- 2 Click the **Jobs** tab.
- 3 In the right pane, check one or more jobs that you wish to delete.
- 4 In the right pane, from the **Configuration** menu, click **Delete Job(s)**.
- 5 Click **OK**.
- 6 Click **Close**.

Changing the owner of a rule

You can assign the owner of a rule to be any user that is explicitly added to the configuration, or any configured user groups.

To change the owner of a rule using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click the **Business Rules** tab or the **Notification Rules** tab.
Business rules specify an action that is triggered by an event or a schedule. Notification rules specify recipients that will receive notification for an event.
- 3 Check the rules that you want to change owner.
- 4 In the right pane, from the **Operations** menu, click **Change Owner**.
- 5 In the Change Rule Owner window, click the user that you want to make the rule owner from the menu.
- 6 Click **OK**.
- 7 Click **Close**.

Enabling a rule

Enabling a rule activates it. Perform the following procedure to enable a new rule or re-enable a rule that has been disabled. The Rules console window lists the total number of rules, the number of enabled rules, and the number of disabled rules.

To enable a rule using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click the **Business Rules** tab or the **Notification Rules** tab.
Business rules specify an action that is triggered by an event or a schedule. Notification rules specify recipients that will receive notification for an event.

- 3 Check the rules that you want to enable.
- 4 In the right pane, from the **Operations** menu, click **Enable Rule**.
- 5 In the Enable Rule / Rules window, click **OK** to confirm.
- 6 Click **Close**.

To enable a rule using the command line

- ◆ Type the following command

```
harule -enable rule
```

Use the following information to replace the appropriate variable:

`rule` The name of the rule to enable.

This command line is applicable only for notification rules.

Disabling a rule

Disabling a rule deactivates the rule without deleting it. Events cannot trigger a disabled rule.

The Rules console window lists the total number of rules, the number of enabled rules, and the number of disabled rules.

To disable a rule using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click the **Business Rules** tab or the **Notification Rules** tab.
Business rules specify an action that is triggered by an event or a schedule. Notification rules specify recipients that will receive notification for an event.
- 3 Check the rules that you want to disable.
- 4 In the right pane, from the **Operations** menu, click **Disable Rule**.
- 5 In the Disable Rule / Rules window, click **OK** to confirm.
- 6 Click **Close**.

To disable a rule using the command line

- ◆ Type the following command

```
harule -disable rule
```

Use the following information to replace the appropriate variable:

`rule` The name of the rule to disable.

This command line is applicable only for notification rules.

Modifying a rule

When you modify a rule using the VCS One console, you follow a similar procedure to when the rule was created. When you modify a rule using the command line, you modify attribute values.

To modify a rule using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click the **Business Rules** tab or the **Notification Rules** tab.
Business rules specify an action that is triggered by an event or a schedule. Notification rules specify recipients that will receive notification for an event.
- 3 Check the rule name that you want to modify.
- 4 Click **Configuration > Modify Rule**.
- 5 In the Rule Configuration wizard, click **Next**.
- 6 In the Configure Rule details panel, modify the desired characteristics. See [“To create a business rule using the VCS One console”](#) on page 411.
- 7 Click **Finish**.
- 8 Click **Close**.

To modify a rule using the command line

- ◆ Type the following command
`harule -modify rule attribute value`

Use the following information to replace the appropriate variable:

`rule` The name of the rule to modify.

`attribute` The name of the attribute that you want to modify.

`value` The new value of the attribute.

Deleting a rule

When you delete a rule, the rule is removed from the VCS One configuration. You cannot undo the rule delete command. You may disable a rule to deactivate it without deleting it.

See [“Disabling a rule”](#) on page 426.

To delete a rule using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click the **Business Rules** tab or the **Notification Rules** tab.
Business rules specify an action that is triggered by an event or a schedule. Notification rules specify recipients that will receive notification for an event.
- 3 Check one or more rules that you want to delete.
- 4 In the right pane, from the Configuration menu, click **Delete Rule**.
If the jobs associated with this rule are also associated with other rules they will not be deleted.
- 5 In the Delete Policy/Policies window, click **OK** to confirm.
- 6 Click **Close**.

To delete one or more rules using the command line

- ◆ Type the following command

```
harule -delete rule
```

Use the following information to replace the appropriate variables:

rule The name of the rule to delete.

About configuring tasks

A task does not exist by itself. It is always part of a job. Define tasks as part of the job definition.

See [“Creating a job”](#) on page 421.

Exporting a rule or a job to an XML file

You can export rules, jobs, tasks, and their properties to an XML file. This file can later be imported for use.

You may use the bpa.xml file to accomplish the following tasks:

- Edit the rules, jobs, and tasks using an XML editor, rather than the GUI interface.
- Transfer rule definitions and properties between the Simulator and the running VCS One installation.
- Upgrade purposes

To export rule or a job to XML using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click one of the following menu items to select which object type you wish to import.
 - Click **Jobs** to import jobs.
 - Click **Business Rules** to import rules that result in a task.
 - Click **Notification Rules** to import rules that result in a notification.
- 3 In the right pane, check one or more rules or jobs you wish to export.
- 4 Click **Operations**.
- 5 Click **Export Rules** or **Export Job(s)** as appropriate.
- 6 In the File Download popup, click **Save**.
- 7 Enter a location to save the file.
- 8 In the Download complete pane, click **Close**.

Importing a rule or a job from an XML file

You can import an XML file to the Simulator or an existing VCS One installation. You can only import rules or jobs for which the logged in user is the owner.

To import a rule or a job to an XML file using the VCS One console

- 1 In the VCS One console, click the **Manage > Automation** tabs.
- 2 Click one of the following menu items to select which object type you wish to import.
 - Click **Jobs** to import jobs.
 - Click **Business Rules** to import rules that result in a task.
 - Click **Notification Rules** to import rules that result in a notification.
- 3 Click **Operations**.
- 4 Click **Import Rules** or **Import Job** as appropriate.

Importing a rule or a job from an XML file

- 5 In the Select file to Import pane, enter or browse to the XML file name to import.
- 6 Click **OK**.
- 7 In the Import Rule and/or Jobs pane, select each rule or job you wish to import or check **Select All**.
- 8 Click **OK > Close**.

Tasks: Managing virtualization technologies

This section includes the following chapters:

- [“Managing objects in Solaris zones”](#) on page 433
- [“Managing objects in AIX Workload Partitions \(WPARs\)”](#) on page 453

Managing objects in Solaris zones

This chapter includes the following topics:

- [About managing objects in Solaris zones](#)
- [Zone configuration prerequisites](#)
- [Deciding on the zone root location](#)
- [Creating a Solaris zone](#)
- [About installing applications in a zone](#)
- [Configuring the application service group for the zone](#)
- [Configuring the local zone to run ha-commands](#)
- [Configuring Zone-Policy Master communication](#)
- [Viewing zone operations](#)
- [Modifying zone resource attributes](#)
- [Example of configuring an application to run inside a zone](#)

About managing objects in Solaris zones

Solaris zones allow you to create one or more isolated virtual environments on a single operating system instance. The application that runs inside a zone runs with exclusive access to resources configured for that zone. The application also has its own file system namespace, users, and network.

VCS One enables high availability for an application configured in a zone by making the zone itself highly available.

To manage non-global or local zones on VCS One Solaris systems, you need to perform the following tasks in the order given.

Table 21-1

Step	Action
1	Before you configure objects in Solaris zones in the VCS One cluster, be familiar with the design principles. See “Designing service groups that run in Solaris zones” on page 264.
2	Review the prerequisites for configuring zones. See “Zone configuration prerequisites” on page 435.
3	Decide on the location of the zone root. See “Deciding on the zone root location” on page 436.
4	Decide how to configure the file system on shared storage that stores the application’s data. The file system can be directly mounted relative the global zone’s root directory or it can be loop back mounted. For the loop back mount, the mount is configured within the non-global zone. More information is available about Veritas file systems. Refer to <i>Veritas File System (VxFS)</i> documentation.
5	Configure, install, and boot the zone. See “Creating a Solaris zone” on page 436.
6	Install the application in the zone. See “About installing applications in a zone” on page 438.
7	Create the service group for the application and configure its resources. See “Configuring the application service group for the zone” on page 439.
8	Configure the local zone to run ha-commands. See “Configuring the local zone to run ha-commands” on page 439.

Table 21-1

Step	Action
9	Configure zone-specific resources and set up communication between the zone and Policy Master. See “Configuring Zone-Policy Master communication” on page 440.

Zone configuration prerequisites

Zone configuration prerequisites are as follows:

- Each system on which applications will be configured in zone must run the same version of Solaris. The Solaris version must be a VCS One supported version.
 See *Veritas Cluster Server One Release Notes*
- VCS One supports UFS and VxFS file system mounts for the zone root. CFS mounts are not supported.
- The autoboot property for the zone must be set to False.
- Mounts must meet one of the following conditions:
 - Loop-back file system
 All mounts used by the application must be part of the zone configuration and must be configured in the service group. For example, you can create a zone called z-ora, and define the file system that contains the application’s data to have the mount point as /oradata. When you create the zone, you can define a path in the global zone, such as /export/home/oradata, that the mount directory in the non-global zone maps to. The MountPoint attribute of the Mount resource for the application should be set to /export/home/oradata.
 - Direct mount file system
 All file system mount points used by the application running in a zone must be set relative to the zone’s root. For example, if the Oracle application uses /oradata, and you create the zone with the zonename as /z_ora, the mount must be /z_ora/root/oradata. The MountPoint attribute of the Mount resource must be set to this path.
 More information is available about how to configure the application service group for the zone.
 See [“Configuring the application service group for the zone”](#) on page 439.

Custom agent requirements

If you use custom agents to monitor the applications that run in zones, make sure that the agents use script-based entry points. VCS One does not support running C++ entry points in non-global zones.

Deciding on the zone root location

The zone root is a top-level directory in a particular section of the file system hierarchy where the non-global zone is configured.

Each non-global zone has its own section in the file system hierarchy. Processes running in the zone can access files only within the zone root.

You can set the zone root in two ways:

- **Zone root on local storage**
In this configuration, create a zone on each system listed in the service group's SystemList attribute.
- **Zone root on shared storage**
If the zone root resides on shared storage, it can exist in the same disk group that contains the application's data.
In this configuration, create a zone in shared storage from one system and then create identical configurations on each system listed in the service group's SystemList attribute.
Setting the zone root on shared storage involves installing the non-global zone on shared storage from only one system. The non-global zone and the zone root can fail over to the other systems. The system software, including the patches, must be identical on each system during the existence of the zone.

Creating a Solaris zone

To create a zone with the zone root on local or shared storage, perform the following tasks:

- Configure the zone
- Install the zone
- Boot the zone

Ensure that the zone has been completely installed, including an initial boot of the zone, before you install the VCS One client.

To configure a Solaris zone

- 1 Create the zone using the `zonecfg` command. At the command prompt, type the following:

```
zonecfg -z newzone  
zonecfg:newzone> create
```

- 2 Set the `zonpath` parameter to the location of the zone root. At the command prompt, type the following:

```
zonecfg:newzone> set zonpath=/export/home/newzone
```

- 3 Set the zone `autoboot` parameter to false

```
zonecfg:newzone> set autoboot=false
```

- 4 Application data can reside on the loop back mounted file system or the direct mount file system. The loop back file system must reside inside the zone configuration. The direct mount file system must reside outside the zone configuration. Both the loop back file system and direct mount file system must be under VCS One control.

The `zonecfg` command displays information about the zone's properties and values. The zone information for a zone root created on local storage using the loop back file system (for application data) should be similar to the following:

```
zonecfg -z newzone info  
zonpath: /export/home/newzone  
autoboot: false  
pool:  
inherit-pkg-dir:  
  dir: /lib  
inherit-pkg-dir:  
  dir: /platform  
inherit-pkg-dir:  
  dir: /sbin  
inherit-pkg-dir:  
  dir: /usr  
fs:  
  dir: /oradata  
  special: /export/home/oradata
```

The zone information for a zone root created on shared storage using the direct mount file system (for application data) should be similar to the following:

```
zonecfg -z newzone info  
zonpath: /export/home/newzone  
autoboot: false  
pool:  
inherit-pkg-dir:  
  dir: /lib
```

```
inherit-pkg-dir:  
  dir: /platform  
inherit-pkg-dir:  
  dir: /sbin  
inherit-pkg-dir  
  dir: /usr
```

To install a Solaris zone

- ◆ Install the non-global zone using `zoneadm` command. At the command prompt, type the following:

```
zoneadm -z newzone install  
Preparing to install zone <newzone>.  
.....  
Zone <newzone> is initialized.  
...
```

If you want to configure the zone root on shared storage, you need to configure but not install the zone on all the systems listed in the service group's `SystemList` attribute. For all other cases, you must configure and install the zone on all the system listed in the service group's `SystemList` attribute.

To boot a Solaris zone

- ◆ At the command prompt, type the following:

```
zoneadm -z newzone boot
```

More information is available about how to configure, install, and boot zones. Refer to *Sun Microsystems* documentation.

About installing applications in a zone

Perform the following tasks in the order provided to install the application in a zone:

- If you have created zones locally on each system, install the application in the zone, identically on each system.
- Install the agent.
Agent packages are installed in the global zone and the currently existing non-global zones. The operating system installs the agents in future non-global zones when they are created.
More information is available about how to install the Oracle agent. Refer to the *Veritas Cluster Server One Agent for Oracle Installation and Configuration Guide*.

- Mounts that are used by the application and accessed from within the zone, must be defined in the service group's configuration.

Configuring the application service group for the zone

Configure the application service group and the required resource dependencies.

More information is available about how to add a service group.

See [“Adding a service group”](#) on page 315.

A example of configuration of an application service group for the zone is available.

See [“Example of configuring an application to run inside a zone”](#) on page 443.

Configuring the local zone to run ha-commands

To execute ha-commands, such as `hares`, from within the local zone, you need to configure certain environment variables.

[Figure 21-1](#) lists the variables to set to configure the local zone to run ha-commands.

To configure the local zone to run ha-commands

- ◆ Set the following environment variables:

Figure 21-1 Variables to set to configure the local zone to run ha-commands

Environment Variable	Description
VCSONE_SERVER_IP	The virtual IP address of the Policy Master cluster. The virtual IP address of the Policy Master remains static during a Policy Master switch or failover operation. For example: 192.168.1.2.
VCSONE_SERVER_PORT	The port configured for the Policy Master as defined in <code>vsone.ini</code> . This port is the port on which the Policy Master is listening for connections. For example: 14151.
VCSONE_DOMAINTYPE	The domain type of the domain in which the Zone user is created. For example: vx.

Figure 21-1 Variables to set to configure the local zone to run ha-commands

Environment Variable	Description
VCSONE_USERNAME	The user name assigned to the Zone user. For example: Z1zone1@VCSONE_CONTAINER_USERS@vcsone_cluster
VCSONE_LOCAL_NAME	The name of the global zone.
PATH	Add the path /opt/VRTSvcsone/bin to your PATH variable.

Configuring Zone-Policy Master communication

To execute commands within a local zone, such as monitor, start, and stop an application, the agent needs to communicate with the client daemon running in the global zone. To allow this communication, secure communication must be established between the zone and the Policy Master cluster, and a long-term service user credential is cached in the local zone.

The Zone agent renews the zone user credential after every 180 day period of time. The zone must be ONLINE or the renewal will not occur.

How to configure Zone-Policy Master communication varies slightly depending on whether your configuration is set up for a local site only or whether your configuration includes a disaster recovery site.

Configuring Zone-Policy Master communication within a local site

To configure Zone-Policy Master communication within a local site

- 1 Set up network identity and capability for the zone.
 The non-global zone requires a virtual IP address and a hostname to communicate on the network, independent of the global zone in which it exists. Modify the network specific files in the non-global zone's /etc directory. For example, the network hostname used by Z1 is Z1zone.
- 2 Type the following command to bring the zone resource to the ONLINE state.
`hares -online zoneress -sys globalzonesys`
- 3 Ensure the application resource is not ONLINE or enabled.
- 4 Provision a new user for the local zone and deploy a user credential for that user inside the local zone.
 Type the following command
`hares -action zoneress provision_zuser -actionargs password -sys globalzone`

Use the following information to replace the appropriate variables

zoneres	The name of the zone resource
password	The password of the zone user
globalzone	The name of the global zone
globalzonesys	The name of the system that runs the global zone.

Configuring Zone-Policy Master communication with a disaster recovery configuration

In a disaster recovery configuration, the zone root may or may not be replicated from a primary site to a secondary site.

To configure Zone-Policy Master communication with a disaster recovery configuration if the zone root is replicated

- ◆ Configure the Zone attribute DROpts at each site.
 When DROpts is configured correctly, the Zone agent manages the user credential provisioning at each site.
 The value of this attribute consists of the following keys that define the disaster recovery (DR) options for the Zone.

- DNSDomain
 The domain name to use within the Zone at this site.
- DNSSearchPath
 The domain search path used by this Zone at this site.
- DNSServers
 The list of DNS servers used by this Zone at this site.
- Gateway
 The default Gateway used by this Zone at this site.

In a DR configuration, if one or more of these keys are set, the resource is considered to be DR-enabled. If all the keys stay at their default value (""), then the resource is not DR-enabled even if it is in a disaster recovery configuration.

The agent modifies the networking files inside the Zone during a cross-site failover if the resource is considered to be DR-enabled.

See the *Veritas Cluster Server One Bundled Agent's Reference Guide*.

To configure Zone-Policy Master communication with a disaster recovery configuration if the zone root is not replicated

You must manually provision a new user for the local zone and deploy a user credential for that user inside the local zone at each disaster recovery site.

See [“To configure Zone-Policy Master communication within a local site”](#) on page 440.

Viewing zone operations

The operation privileges within the zone apply only to the service group configured for the zone.

The ZoneUserGroup role entails group and resource level administrative and operator privileges.

The ZoneUserFarm role includes only the Add Log privilege, which is required by the agents controlling the service group’s resources.

To view the ZoneUserGroup and ZoneUserFarm role privileges

- 1 In the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Roles** tab.
- 3 In the right pane, under **All Roles**, click **ZoneUserGroup**.
- 4 View the group and resource privileges associated with the Zone User Group role.
- 5 Click **VCS One Roles** in the upper-left corner of the screen.
- 6 In the right pane, under **All Roles**, click **ZoneUserFarm**.
- 7 View the group and resource privileges associated with the Zone User Farm role.

Modifying zone resource attributes

This topic describes how to modify zone resource attributes.

To modify zone resource attributes using the VCS One console

- 1 In the VCS One console, locate the service group that contains the zone resource, which you want to modify.
See [“Locating a service group”](#) on page 321.
- 2 In the right pane, under **Service Groups**, click the appropriate service group.
- 3 In the right pane, from the **Configuration** menu, click **Add/Modify Resource**. The **Add Resource - Group** dialog box is displayed.
- 4 In the **Add Resource - Group** dialog box, click **OK**. The **Results** dialog box is displayed.

- 5 In the **Results** dialog box, click **Advanced**. The **Edit Attribute** dialog box is displayed.
- 6 In the **Edit Attribute** dialog box, under **Value**, locate the zone resource attribute that you want to modify and change its value.
- 7 In the **Edit Attribute** dialog box, click **OK**.
- 8 In the **Edit Attribute** dialog box, click **Close**.

Example of configuring an application to run inside a zone

This topic provides a step-by-step example of configuring a managed application be associated with a Solaris zone.

Create the service group with the standard managed application resource types (Application, Storage, Networking) with the addition of a Zone resource. Configure the service group's ContainerInfo attribute, and each resource's ContainerOpts attribute.

See [“Designing service groups that run in Solaris zones”](#) on page 264.

To configure a service group to run inside a Solaris zone

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Service Groups** tab.
- 3 From the right pane, in the Configuration menu, click **Add service group**.
- 4 In the Service Group Configuration Wizard, click **Next**.
- 5 In the Name field, enter the name of the service group.
In this example, the name will be zone_sg1.
- 6 In the Load area, in the CPU field, enter the number that denotes the CPU load of this service group.
The values set for the CPU Load value is used to configure the number of CPU shares used by the Zone.
See [“About service group Load and system Capacity for physical systems”](#) on page 280.
- 7 In the Load area, in the MEM field, enter the number that denotes the memory load of this service group.
The values set for the MEM Load value is used to configure the number of MEM shares used by the Zone.
- 8 You may also choose to enter values in the STBW and NRBW fields.

Example of configuring an application to run inside a zone

- 9 Click **Next**.
- 10 In the System List Configuration window, select the systems from the Available Systems column on the left that you want to be configured in the SystemList of the service group.
You may use the Filter and Search option on this page to narrow the list of service groups that appear in the Available Systems column.
- 11 Click the forward arrow to move the selected systems to the right, into the SystemList column.
- 12 Click **Next**.
- 13 In the Container Information window, enter the following information:

Associate Service Group with a Container	Check this box. This specifies that the service group is associated with a container technology.
Type	Click Zone to indicate the service group is associated to a zone.
Name	Type the name of the zone. The zone must already be installed and configured.
Enabled	Click Yes to enable the service group.
Add Container resource to the Service Group	Check this box. to automatically add a Zone resource to the service group, allowing the zone agent to bring online, take offline, monitor, and clean the zone. A zone resource must be present in every zone-enabled service group.
Resource Name	Type a name for the zone resource.

- 14 Click **Next**.
- 15 In the Add Resource window, enter the following information to configure the Application resource that will run inside the local zone.

Type	Click Application .
Name	Type the name of the resource (of Type Application) that will run inside the local zone.
Enable Resource	Check this box to enable the resource.
Add Resource	Click Add Resource to add the resource to the Resource List table.

- 16 In the Resource List, click the Edit icon in the row that corresponds to the Application resource you added in [step 15](#) to configure the resource's attributes.
- 17 In the Edit attribute window, enter the following information. Click the name of the attribute in the Attribute List table, and type the value of the attribute in the Values table:

Start Program	The full path of the executable program that starts the application.
Stop Program	The full path of the executable program that stops the application.
ContainerOpts	RunInContainer = 1 to denote this application runs in the local zone.

You may also edit other attribute values as necessary to your environment. More information is available on what attributes are required for each resource type.

See *Veritas Cluster Server One Bundled Agents Reference Guide*.

- 18 Click **OK**.
- 19 In the Add Resource window, enter the following information to configure the Application resource that will run inside the global zone.

Type	Click Application .
Name	Type the name of the resource (of Type Application) that will run inside the global zone.
Enable Resource	Check this box to enable the resource.
Add Resource	Click Add Resource to add the resource to the Resource List table.

- 20 In the Resource List, click the Edit icon in the row that corresponds to the Application resource you added in [step 19](#) to configure the resource's attributes.
- 21 In the Edit attribute window, enter the following information. Click the name of the attribute in the Attribute List table, and type the value of the attribute in the Values table:

Start Program	The full path of the executable program that starts the application.
Stop Program	The full path of the executable program that stops the application.
ContainerOpts	RunInContainer = 0 to denote this application should not run in the local zone. Therefore it will run in the global zone.

Example of configuring an application to run inside a zone

You may also edit other attribute values as necessary to your environment. More information is available on what attributes are required for each resource type.

See *Veritas Cluster Server One Bundled Agents Reference Guide*.

22 Click OK.**23** In the Add Resource window, enter the following information to configure the IP resource for the service group.

Type	Click IP .
Name	Type the name of the IP resource.
Enable Resource	Check this box to enable the resource.
Add Resource	Click Add Resource to add the resource to the Resource List table.

24 In the Resource List, click the **Edit** icon in the row that corresponds to the IP resource to configure the resource's attributes.**25** In the Edit attribute window, enter the following information. Click the name of the attribute in the Attribute List table, and type the value of the attribute in the Values table:

Address	The virtual IP address associated with the interface specified in the Device attribute.
Device	The name of the NIC device associated with the IP address specified in the Address attribute.
ContainerOpts	RunInContainer = 0 to denote this IP address should run in the global zone. The IP address should run in the global zone unless you use Exclusive-IP Zones. PassContainerInfo = 1 to allow the association with the IP address configured in the global zone to the local zone.

You may also edit other attribute values as necessary to your environment.

26 Click OK.**27** In the Add Resource window, enter the following information to configure the NIC resource for the service group.

Type	Click NIC .
Name	Type the name of the NIC resource.

Enable Resource Check this box to enable the resource.

Add Resource Click **Add Resource** to add the resource to the Resource List table.

- 28 In the Resource List, click the **Edit** icon in the row that corresponds to the NIC resource to configure the resource's attributes.
- 29 In the Edit attribute window, enter the following information. Click the name of the attribute in the Attribute List table, and type the value of the attribute in the Values table:

Device	The name of the NIC device. For example, qfe0.
--------	---

You may also edit other attribute values as necessary to your environment.

- 30 Click **OK**.
- 31 In the Add Resource window, enter the following information to configure the DiskGroup resource for the Zone root.

Type	Click DiskGroup .
Name	Type the name of the DiskGroup resource for the Zone root.
Enable Resource	Check this box to enable the resource.
Add Resource	Click Add Resource to add the resource to the Resource List table.

- 32 In the Resource List, click the **Edit** icon in the row that corresponds to the DiskGroup resource to configure the resource's attributes.
- 33 In the Edit attribute window, enter the following information. Click the name of the attribute in the Attribute List table, and type the value of the attribute in the Values table:

DiskGroup	The name of the disk group configured with Veritas Volume Manager.
-----------	--

You may also edit other attribute values as necessary to your environment.

- 34 Click **OK**.
- 35 In the Add Resource window, enter the following information to configure the DiskGroup resource for the application in the global zone.

Type	Click DiskGroup .
------	--------------------------

Example of configuring an application to run inside a zone

Name	Type the name of the DiskGroup resource for the global zone.
Enable Resource	Check this box to enable the resource.
Add Resource	Click Add Resource to add the resource to the Resource List table.

36 In the Resource List, click the **Edit** icon in the row that corresponds to the DiskGroup resource to configure the resource's attributes.

37 In the Edit attribute window, enter the following information. Click the name of the attribute in the Attribute List table, and type the value of the attribute in the Values table:

DiskGroup	The name of the disk group configured with Veritas Volume Manager.
-----------	--

You may also edit other attribute values as necessary to your environment.

38 Click **OK**.

39 In the Add Resource window, enter the following information to configure the Mount resource for the disk group in the Zone root.

Type	Click Mount .
Name	Type the name of the Mount resource for the disk group in the Zone root.
Enable Resource	Check this box to enable the resource.
Add Resource	Click Add Resource to add the resource to the Resource List table.

40 In the Resource List, click the **Edit** icon in the row that corresponds to the Mount resource to configure the resource's attributes.

41 In the Edit attribute window, enter the following information. Click the name of the attribute in the Attribute List table, and type the value of the attribute in the Values table:

BlockDevice	The block device for the mount point.
FSType	The type of file system, such as vxfs or ufs.
MountPoint	The directory for the mount point.

You may also edit other attribute values as necessary to your environment.

42 Click **OK**.

- 43** In the Add Resource window, enter the following information to configure the Mount resource for the disk group in the global zone.

Type	Click Mount .
Name	Type the name of the Mount resource for the disk group in the local zone.
Enable Resource	Check this box to enable the resource.
Add Resource	Click Add Resource to add the resource to the Resource List table.

- 44** In the Resource List, click the **Edit** icon in the row that corresponds to the Mount resource to configure the resource's attributes.

- 45** In the Edit attribute window, enter the following information. Click the name of the attribute in the Attribute List table, and type the value of the attribute in the Values table:

BlockDevice	The block device for this mount point.
FSType	The type of file system, such as vxfs or ufs.
MountPoint	The directory for this mount point.

In [step 52](#), you edit the ContainerOpts attribute of this resource to denote this mount point is in the local zone.

You may also edit other attribute values as necessary to your environment.

- 46** Click **OK**.

[Figure 21-2](#) shows an example of the resource table at this point in the procedure.

Figure 21-2 Example resource list for a service group inside a Solaris zone.

Resource List: To edit a resource select and edit resource

Name	Type	Enable	Edit	Del
myzone	Zone	<input checked="" type="checkbox"/>	...	X
app1	Application	<input checked="" type="checkbox"/>	...	X
app2	Application	<input checked="" type="checkbox"/>	...	X
ip	IP	<input checked="" type="checkbox"/>	...	X
nic	NIC	<input checked="" type="checkbox"/>	...	X
zone_dg	DiskGroup	<input checked="" type="checkbox"/>	...	X
app_dg	DiskGroup	<input checked="" type="checkbox"/>	...	X
zone_mnt	Mount	<input checked="" type="checkbox"/>	...	X
app_mnt	Mount	<input checked="" type="checkbox"/>	...	X

- 47 Click **Next** to configure resource dependencies.
- 48 In the Link/Unlink Resource window, enter the following information to make the appropriate resource dependencies:

Parent field	Child field	Click
Application resource in the local zone	IP resource	Add Link
Application resource in the local zone	Mount resource for the disk group in the local zone	Add Link
Application resource in the global zone	IP resource	Add Link
Mount resource for the disk group in the local zone	Zone resource	Add Link
IP resource	Zone resource	Add Link
IP resource	NIC resource	Add Link
Zone resource	DiskGroup resource for the Zone root	Add Link
Zone resource	Mount resource for the disk group in the Zone root	Add Link
Zone resource	DiskGroup resource for the application in the global zone	Add Link

- 49 Click **Finish**.

- 50 Click **Advanced** to configure the compatibility and fault policy of the service group.
- 51 Click **Close**.
- 52 Edit the ContainerOpts attribute of the mount resource for the disk group in the local zone.
Use the **All Attributes** link on the details page of the resource to edit this attribute.

```
ContainerOpts  RunInContainer = 1  
                PassContainerInfo = 0
```

You may now online the service group.

See [“Bringing a service group online”](#) on page 329.

[“Adding a service group”](#) on page 315

Example of configuring an application to run inside a zone

Managing objects in AIX Workload Partitions (WPARs)

This chapter includes the following topics:

- [About managing service groups in AIX Workload Partitions](#)
- [Prerequisites for configuring VCS One in WPARs](#)
- [Setting the WPAR root path](#)
- [Installing the application](#)
- [Creating the WPAR-enabled service group](#)
- [Configuring WPAR-Policy Master communication](#)
- [Adding the WPAR hostname as a principal](#)
- [Maintenance tasks](#)

About managing service groups in AIX Workload Partitions

An AIX workload partition (WPAR) is a virtualized operating system environment within an instance of the AIX operating system. AIX WPARs provide an isolated and secure environment for running applications.

The WPAR must be installed and configured before it can be brought under VCS One control.

Before you configure VCS One with WPARs, be familiar with proper VCS One WPAR service group design.

See [“Designing service groups that run in AIX WPARs”](#) on page 269.

Note: VCS One provides support for system WPARs. VCS One does not provide support for application WPARs.

Configuring VCS One in WPARs involves the following tasks:

Step 1	Review the prerequisites. See “Prerequisites for configuring VCS One in WPARs” on page 454.
Step 2	Decide on the location of the WPAR root. A WPAR root is the topmost directory in a section of the file system hierarchy in which the WPAR is configured. See “Setting the WPAR root path” on page 455.
Step 3	Install the application in the WPAR. See “Installing the application” on page 458.
Step 4	Create the application service group and configure its resources. See “Creating the WPAR-enabled service group” on page 459.

Prerequisites for configuring VCS One in WPARs

Check the following prerequisites before configuring WPARs:

- All systems hosting applications configured in WPARs must be running the same version and a supported version of the operating system.
See *Veritas Cluster Server One Release Notes*.
- The WPAR root must be installed on JFS, JFS2, or NFS.

- Configure the WPAR to not auto start on boot of the global environment.
- Mounts must meet one of the following two conditions:
 - Use a namefs file system
In this condition, the file system mount point used by the application running in a WPAR is mounted from a directory that exists inside the Global environment.
For example, in the global environment you have the directory `/export/home/oradata` which is to be used by the WPAR to store application data. When you create the WPAR, provide the directory path from the global environment (e.g `/export/home/oradata`) along with the mount location inside the WPAR (i.g. `/oradata`), specifying the vfs type of 'namefs'.
 - Use a direct mount file system.
In this condition, the file system mount point used by the application running in a WPAR is mounted inside the global environment relative to the WPAR's root.
For example, if the Oracle application uses `/oradata`, and you create the WPAR with the WPARpath as `/wpars/w_ora`, then inside the global environment the file system must be mounted to `/wpars/w_ora/oradata`. The MountPoint attribute of the Mount resource must be set to this path.

Using custom agents in WPARs

- If you use custom agents to monitor applications running in WPARs, make sure the agents use script-based entry points. VCS One does not support running C++ entry points inside a WPAR.
- If you want the custom agent to monitor an application in the WPAR, for the custom agent type, set the following values for the ContainerOpts attribute: RunInContainer = 1 and the PassCInfo = 0.
- If you don't want the custom agent to monitor an application in the WPAR, for the custom agent type, set the following values for the ContainerOpts attribute: RunInContainer = 0 and the PassCInfo= 0.

Setting the WPAR root path

Each WPAR has its own section of the file system hierarchy in the *WPAR root* directory. Processes running in the WPAR can access files only within the WPAR root.

You can set the WPAR root in two ways:

- WPAR root on local storage—In this configuration, you must create a WPAR on each client system in the VCS One cluster.
- WPAR root on NFS—In this configuration, create a WPAR on the NFS storage. In this case, you need to duplicate the configuration across all the client systems.

When you set the WPAR root on NFS, install the WPAR from one client system only. The WPAR root can fail over to the other client systems. The system software, including the patches, must be identical on each client system during the existence of the WPAR.

Creating a WPAR root on local disk

Use the following steps to create a WPAR root on the local disk of each client system.

To create a WPAR root on local disks of each client system

- 1 Create the actual WPAR root directory.
- 2 Use the `mkwpar` command to create the WPAR.

```
mkwpar -n wpar -h host -N ip_info -d wroot -o /tmp/wpar.log
```

Use the following information to replace the appropriate variables:

`wpar` The name of the WPAR.

`hostname` The name of the system on which the WPAR is created.

`ip_info` Replace this variable with the information to set the virtual IP address of the system to be the IP address of the WPAR. This value also defines the device name for the NIC associated with the IP address.

If you don't specify the value of the interface or netmask, the global partition's values are used.

Use the following format to replace `ip_info`:

```
interface=interface netmask=netmask address=IPaddress
```

For example:

```
interface='en0' address='172.16.0.0'
netmask='255.255.255.0'
```

`wroot` Replace this variable with the location of the WPAR root directory, for example, `/wpars`.

- 3 Repeat the command in [step 2](#) to create the WPAR on each system in the service group's SystemList.

- 4 On one of the systems in the SystemList, mount the shared file system containing the application data.
- 5 Start the WPAR.

Creating WPAR root on shared storage using NFS

Use the following steps to create a WPAR root on shared storage using NFS.

To create WPAR root on shared storage using NFS

- 1 Create a file system on NFS storage for the WPAR root. The file system that is to contain the WPAR root may be in the same file system as the file system containing the shared data.

- 2 Type the following `mkwpar` command to create the WPAR:

```
mkwpar -n wpar -h host -N ip_info -r -M r_fs -M v_fs
-M h_fs -M t_fs -d wroot
```

Use the following information to replace the appropriate variables:

`wpar` The name of the WPAR.

`host` The name of the system on which the WPAR is created.

`ip_info` Replace this variable with the information to set the virtual IP address of the system to be the IP address of the WPAR. This value also defines the device name for the NIC associated with the IP address.

If you don't specify the value of the interface or netmask, the global partition's values are used.

Use the following format to replace `ip_info`:

```
interface=interface netmask=netmask address=IPaddress
```

For example:

```
interface='en0' address='172.16.0.0'
netmask='255.255.255.0'
```

`r_fs` Replace this variable with the information to specify the NFS volume to use for the root private file system for the WPAR. For example:

```
directory=/ vfs=nfs host=host123 dev=/root01
```

`v_fs` Replace this variable with the information to specify the NFS volume to use for the /var private file system for the WPAR. For example:

```
directory=/ var vfs=nfs host=host123 dev=/var01
```

h_fs Replace this variable with the information to specify the NFS volume to use for the /home private file system for the WPAR. Examples of values:

```
directory=/home vfs=nfs host=host123 dev=/home01
```

t_fs Replace this variable with the information to specify the NFS volume to use for the root private file system for the WPAR. Examples of values:

```
directory=/tmp vfs=nfs host=host123 dev=/tmp01
```

wroot Replace this variable with the location of the WPAR root directory, for example, /wpar.

- 3 Use the `lswpar` command to display information about the WPAR's properties and their values.
- 4 On the system where you created the WPAR, run the command:
`mkwpar -w -o config_file_name -e wparname_just_created`
- 5 On all the other systems copy the configuration file, run the command:
`mkwpar -p -f config_file_name -n wparname_just_created`
- 6 List the WPAR.
- 7 Start the WPAR.
- 8 On one system, mount the shared file system containing the application data.
- 9 Make sure the WPAR created from the first system is in the D state on all other systems in the service group's System List.

Installing the application

Install the application in the WPAR.

- If you have created WPARs on each client system, install the application identically on each client system. If you are installing an application supported by a VCS One enterprise agent, see the installation and configuration guide for the agent.
- Install the agent.
Agent packages are installed in the global environment as well as the currently existing WPARs. The operating system installs the agents in future WPARs when they are created.
- In the WPAR, configure all mount points used by the application.
 - If you use namefs mounts, verify the global directories are properly mounted inside the WPAR.

- If you use a direct mount, verify the mount points used by the application have been mounted relative to the WPAR's root. For example, if a WPAR *w_ora* needs to use /oracle, mount the drive at /wpars/w_ora/oracle.

Creating the WPAR-enabled service group

Create a service group with the standard managed application resource types (Application, Storage, Networking) with the addition of a WPAR resource.

See [“Adding a service group”](#) on page 315.

Use the following information to customize the service group to be WPAR-enabled:

- Configure the service group's ContainerInfo attribute.
- Configure each resource's ContainerOpts attribute.
- If the application requires an IP address, set the ContainerInfo:Name attribute for the IP resource to the name of the WPAR.
- Set the ContainerInfo:Type attribute = WPAR for the Application resource.
- Set the ContainerInfo:Name attribute for the Application resource to the name of the WPAR in which the application runs.
- Set the MountPoint attribute of the Mount resource to the mount path.
- Modify the resource dependencies to reflect your WPAR configuration. See [“Designing resource dependencies for WPAR-enabled service groups”](#) on page 271.
- Where the WPAR root file system is on shared storage, you can configure separate mounts for the WPAR and the application but you may configure the same disk group for both.

Save the service group configuration and bring the service group online.

Configuring WPAR-Policy Master communication

To execute commands within a WPAR, secure communication must be established between the WPAR and the Policy Master cluster.

The following procedures describe how to do this task:

- Setting up network identity and capability for the WPAR. See [“Setting up network identity and capability for the WPAR”](#) on page 460.
- Creating a cluster private domain with the repository type as Authentication Broker for WPARs.

See “[Creating a cluster private domain for WPARs](#)” on page 460.

- Adding the WPAR hostname as a principal in the private domain repository for WPARs.
See “[Adding the WPAR hostname as a principal](#)” on page 461.
- Creating a WPAR user and assigning the appropriate roles for executing commands that are used by the agents within the WPAR. The available roles for the WPAR user are:
 - ContainerUserGroup
Provides the privileges to execute service group level operations within the WPAR on the group for which the WPAR is configured.
 - ContainerUserFarm
Provides Add Log privilege, which the agents that control the service group’s resources require.See “[Adding a WPAR user and assigning privileges](#)” on page 462.
- Obtaining a credential for the WPAR user using the `halogin` command.
See “[Obtaining credentials and creating a user profile](#)” on page 464.

Setting up network identity and capability for the WPAR

Set up networking capability inside the WPAR. The WPAR requires a virtual IP address and a hostname to communicate on the network, independent of the global environment in which it exists. Modify the network-specific files in the WPAR’s `/etc` directory. For example, the network hostname that is used by WPAR W1 is W1wpar.

Creating a cluster private domain for WPARs

If you use LDAP, you do not need to create a private domain for WPARs as Symantec Product Authentication Service points to the LDAP domain, which hosts the required user accounts. For all other domains, you must create a private domain for WPARs. Create the private domain repository (PDR) on shared storage so that it is accessible by all the Policy Master cluster nodes in the event of a Policy Master cluster failover. Perform the following steps to create a cluster private domain for WPARs.

To create a cluster private domain for WPARs

- 1 Log on to the Policy Master system with root user credentials.
- 2 Create a cluster private domain for WPAR users. Use the `haat` command. Note this domain is created automatically by the installer. If you need to create the domain, name the cluster private domain `VCSONE_CONTAINER_USERS`.

Note: WPAR users must be a part of `VCSONE_CONTAINER_USERS` domain otherwise the service group that manages the local-WPAR might not successfully go online and offline

For example, if the private domain repository type is `cluster`, type the following command:

```
# /opt/VRTSvcsone/bin/haat createpd -t cluster -d \  
VCSONE_CONTAINER_USERS
```

Adding the WPAR hostname as a principal

Perform the following steps to add the WPAR hostname as a principal in the private domain repository for WPARs.

To add a WPAR hostname as a principal

To add the WPAR hostname as a principal, you add the WPAR that you created in the private domain repository.

- 1 Type the following command:

```
# /opt/VRTSvcsone/bin/haat addprpl -t PDRtype -d domain_name \  
-p principal_name -s password -q principal_type
```

Use the following information to replace the appropriate variables:

<code>PDRtype</code>	The type of private domain repository. Specify <code>root</code> , <code>ab</code> (for authentication broker), <code>cluster</code> , or <code>local</code> .
<code>domain_name</code>	The name of the private domain repository in the following format: <code>pdrname@domain</code> For example: <code>VCSONE_CONTAINER_USERS@vcsone_cluster</code>
<code>principal_name</code>	The name of the principal you want to create, for example, <code>W1wpar</code> .
<code>password</code>	The password for the principal. The minimum password length is five characters.
<code>principal_type</code>	The type of principal to be created. Specify <code>default</code> , <code>user</code> , or <code>service</code> . To add the WPAR hostname as a principal, specify <code>service</code> . <code>user</code> indicates that the principal type is an individual user. <code>service</code> indicates that the principal type is a process. The default principal type is <code>user</code> .

- 2 View the confirmation output:

```
...  
Created Principal Wlwpwr
```

Adding a WPAR user and assigning privileges

You can add a WPAR user and assign privileges using the VCS One console or command-line commands.

More information is available on adding a user using the console.

See [“Adding or deleting a user or usergroup”](#) on page 530.

To assign privileges to the WPAR user using the VCS One console

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Users** tab.
- 3 Check the box next to the WPAR user.
- 4 Click **Configuration > Assign / Unassign Roles**.
- 5 In the **Step1 - Select a user / user group and a role** screen, perform the following steps in the order presented:
 - Select the **User** option.
 - In the **Select the user name** box, select the name of the WPAR user that you created.
 - In the **Select the role name** box, select **ContainerUserGroup**. Review the list of privileges that are associated with the role, and then click **Next**.
- 6 In the **Step2 - Specify or delete objects for the selected role** screen, click **Add Objects**.
- 7 Select the **All Objects** option, and then click the select the service group for which the WPAR is configured. Click **OK**.
- 8 In the **Step2 - Specify or delete objects for the selected role** screen, click **OK**.
- 9 In the **Results** screen, click **Close**.
- 10 Repeat steps 1-3, and then perform step 10.
- 11 In the **Step1 - Select a user / user group and a role** screen, perform the following steps in the order presented:
 - Select the **User** option.
 - In the **Select the user name** box, select the name of the WPAR user that you created.

- In the **Select the role name** box, select **ContainerUserFarm**, and then click **Next**.

12 Repeat steps 5-8.

To create a WPAR user and assign privileges using the command line

Note: Do not perform this procedure if you have created a user and assigned a role to the user using the VCS One console.

- 1 Log on with root user credentials on a Policy Master cluster system.
- 2 Add the WPAR user. Use the fully qualified domain name of the network hostname. At the command prompt, type the following command:


```
hauser -add W1wpar@VCSONE_CONTAINER_USERS@vcsone_cluster
```
- 3 Modify the user's attributes to include an email address and an SNMP address. At the command prompt, type the following command:


```
hauser -modify W1wpar@VCSONE_CONTAINER_USERS@vcsone_cluster
Email
"W1wpar@VCSONE_CONTAINER_USERS@vcsone_cluster"
hauser -modify W1wpar@VCSONE_CONTAINER_USERS@vcsone_cluster
SnmpAddress
"192.168.1.2"
```
- 4 Add the role ContainerUserGroup to the new user. At the command prompt, type the following command:


```
hauser -addrole W1wpar@VCSONE_CONTAINER_USERS@vcsone_cluster
ContainerUserGroup
gr_zn1
```

This role enables the WPAR user to execute service group-related commands on the service group gr_zn1.
- 5 Add the role ContainerUserFarm to the new user. At the command prompt, type the following command:


```
hauser -addrole W1wpar@VCSONE_CONTAINER_USERS@vcsone_cluster
ContainerUserFarm
```

This role enables the user to perform Add Log operations in the WPARs.
- 6 Display the user information. At the command prompt, type the following command:


```
hauser -display W1wpar@VCSONE_CONTAINER_USERS@vcsone_cluster
```

Obtaining credentials and creating a user profile

Execute the following commands to obtain the user credential and create a user profile.

To obtain the user credential and create a user profile using the `halogin` command

- 1 Log on as root in the WPAR. At the command prompt, type the following command:

```
clogin w1
```

- 2 Set the following environment variables:

Variable	Definition
<code>VCSONE_SERVER_IP</code>	The virtual IP address of the Policy Master cluster. For example: 192.168.1.2.
<code>VCSONE_BROKER_HOST</code>	The IP address of the authentication broker on the Policy Master system. For example: 192.168.1.2.
<code>VCSONE_SERVER_PORT</code>	The port configured for the Policy Master as defined in <code>vcson.ini</code> . For example: 14151.
<code>VCSONE_DOMAINTYPE</code>	The domain type of the domain in which the WPAR user is created. For example: vx.
<code>VCSONE_USERNAME</code>	The user name assigned to the WPAR user. For example: W1wpar@VCSONE_CONTAINER_USERS@vcson_cluster

- 3 Execute the `halogin` command to obtain the user credential and create user profile. At the command prompt, type the following command:

```
halogin -passwd password
```

Maintenance tasks

- Make sure that the WPAR configuration files are consistent on all the client systems at all times.
Run the `mkwpar -e wparname -w -o config_filename` command to view the file.
- When you add a patch or upgrade the operating system on one client system, make sure to upgrade the software on all client systems. Use the `syncwpar` command to upgrade the software in the WPAR.
- In configurations where the WPAR moves between systems, sure that the application configuration is identical on all system. If you update the

application configuration on one system, apply the same updates to all systems.

Tasks: Setting up and managing global clusters

This section includes the following chapters:

- [“Setting up VCS One global clusters”](#) on page 469
- [“Managing remote clusters”](#) on page 477
- [“Managing global composite service groups”](#) on page 497

Setting up VCS One global clusters

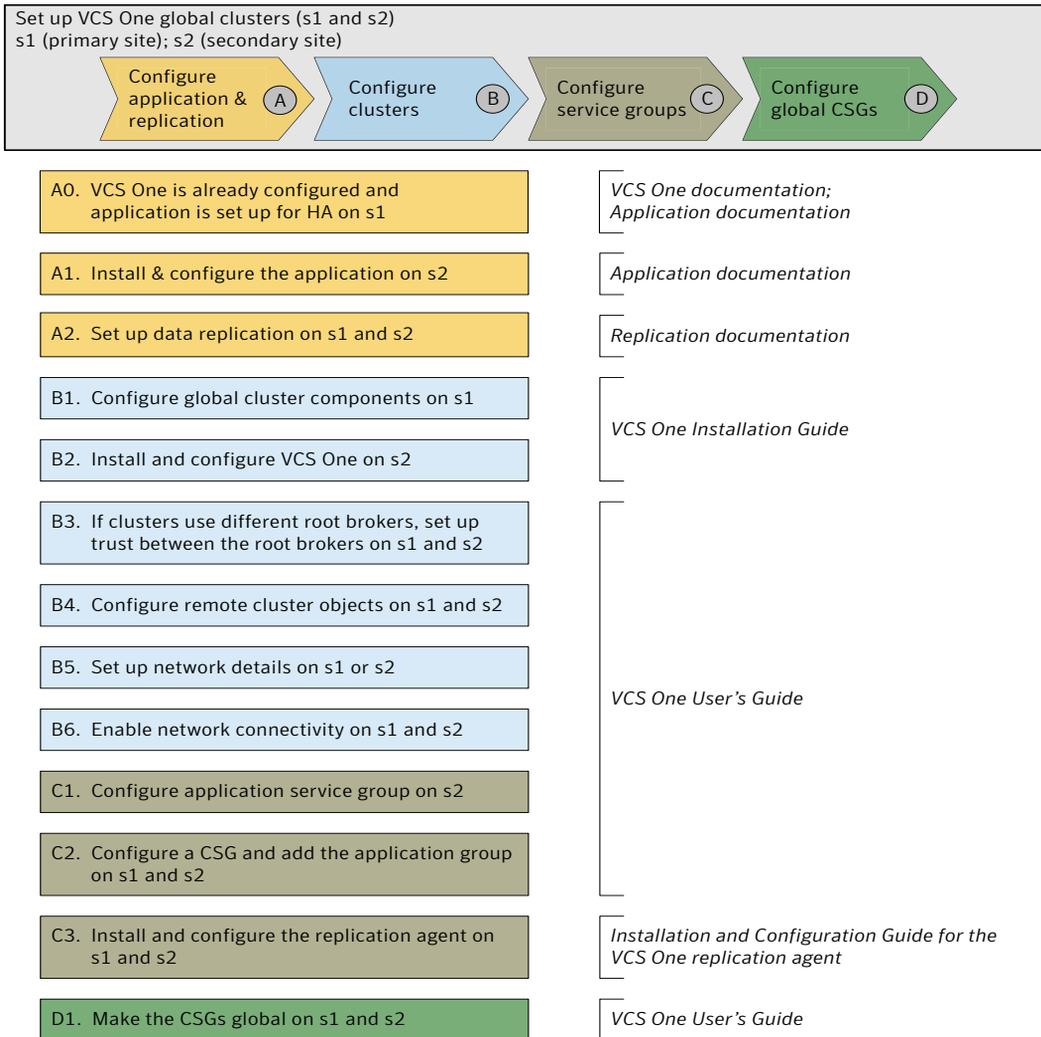
This chapter includes the following topics:

- [About setting up VCS One global clusters](#)
- [Setting up a global cluster configuration](#)
- [Testing VCS One disaster recovery support](#)

About setting up VCS One global clusters

Figure 23-1 depicts the high-level workflow to set up a global cluster where VCS One cluster is already configured at the primary site s1, and has application set up for high availability.

Figure 23-1 High-level workflow to set up VCS One global clusters



Before you set up the global cluster, make sure you completed the following:

- Review the concepts.
See [“About VCS One global clusters”](#) on page 66.
- Plan the configuration and verify that you have the required physical infrastructure.
See [“Typical VCS One global cluster setup”](#) on page 68.
See [“About global cluster building blocks”](#) on page 67.
- Verify that you have the required software to install VCS One and the appropriate replication agent.

Setting up a global cluster configuration

This procedure assumes that you have configured a VCS One cluster at the primary site and have set up application for high availability.

[Table 23-1](#) lists the high-level tasks to set up VCS One global clusters.

Table 23-1 Task map to set up VCS One global clusters

Task	Reference
Task A	See “Configuring application and replication” on page 471.
Task B	See “Configuring clusters” on page 472.
Task C	See “Configuring service groups” on page 473.
Task D	See “Configuring global CSGs” on page 473.

Configuring application and replication

Perform the following steps to configure application at the secondary site. This procedure assumes that you have already set up application for high availability at the primary site.

To configure application and replication

- 1 At the secondary site, install and configure the application that you want to make highly available.
See the corresponding application documentation for instructions.
- 2 At each site, set up data replication using a replication technology that VCS One supports.
See the corresponding replication documentation for instructions.

Configuring clusters

Perform the following steps to configure the clusters for disaster recovery.

To configure clusters

- 1 If you want to use the Policy Master virtual IPs for inter-cluster communication, then skip to [step 2](#).

At the primary site, configure the virtual IP addresses for inter-cluster communication.

If you have not already completed these steps during the VCS One cluster configuration, run the following command on one of systems in the Policy Master and follow the prompts:

```
# /opt/VRTS/install/installvcsonepm -configuredr
```

The `-configuredr` option of the `installvcsonepm` program creates a DRSG service group.

See the *Veritas Cluster Server One Installation Guide* for instructions.
- 2 At the secondary site, install and configure VCS One cluster.

Note the following points for Policy Master installation and configuration:

 - Enter a unique cluster name.
 - If you want to use the Policy Master virtual IPs for inter-cluster communication, then skip this step. Otherwise, configure unique virtual IP addresses for inter-cluster communication.

See the *Veritas Cluster Server One Installation Guide* for instructions.
- 3 At each site, verify the cluster configuration. Perform the following steps:

 - Make sure that the PMSG service group is up and running.

```
# /opt/VRTSvcsone/bin/haadmin -state
```

The output must show the PMSG state as `ONLINE`.

If you had configured unique virtual IPs for inter-cluster communication, then the output must also show the DRSG state as `ONLINE`.
 - Make sure that the Policy Master is running.

```
# /opt/VRTSvcsone/bin/haclus -display -attribute ClusterState
```

The output must show the cluster state as `RUNNING`.
- 4 At each site, set up trust with the root broker of the remote cluster.

```
# /opt/VRTSvcsone/bin/haat setuptrust \  
-b remote_broker_ip:remote_broker_port -s securitylevel
```

For *securitylevel*, use one of the following values: `low`, `medium`, or `high`.

You must set up trust for each IP address that is used for inter-cluster communication.

See the *Veritas Cluster Server One Installation Guide* for instructions.

- 5 At each site, configure the remote cluster object.
Add a remote cluster and set up communication between the clusters. VCS One requires you to specify the remote cluster connection details only on the cluster that VCS One designates to initiate the connection request between the clusters.
See [“Adding remote clusters”](#) on page 478.
See [“How VCS One global clusters communicate with each other”](#) on page 69.
- 6 At each site, enable the connectivity to the remote cluster.
See [“Enabling connections between clusters”](#) on page 485.

Configuring service groups

Perform the following steps to configure the service groups for disaster recovery.

To configure service groups

- 1 At the secondary site, set up the application for high availability.
Configure VCS One service groups for the application.
See [“Adding a service group”](#) on page 315.
- 2 At each site, configure a composite service group.
Perform the following steps:
 - Create a CSG.
You must create the CSG at the same OU node (or at a higher OU node) as that of the service groups that it will contain.
The CSG name must be the same as the one that you configured at the primary site. However, the service group names need not be the same at both the sites.
 - Add the application service group to the CSG.
 - Verify the state of the CSG.
 - Configure users and privileges for the CSG.
See [“Creating a composite service group”](#) on page 364.
- 3 At each site, install and configure the VCS One agent for replication.
See the Installation and Configuration Guide for the corresponding VCS One replication agent for instructions.

Configuring global CSGs

Perform the following steps to configure global composite service groups (CSGs) for disaster recovery.

To configure global CSGs

- 1 On each site, configure the CSGs for disaster recovery.
Perform the following steps:
 - Make the CSG a global CSG.
 - Verify the state of the global CSG.
The global CSG must be online at the primary site.
See [“Configuring a global CSG”](#) on page 498.
- 2 If your setup uses BIND DNS, add a resource of type DNS to the application service group at each site.
Refer to the *Veritas Cluster Server One Bundled Agent’s Reference Guide* for more details.

Testing VCS One disaster recovery support

After you have set up VCS One global clusters, test the HA/DR support. This test is to perform a planned switchover and a switchback of the global CSG and the test requires some planned downtime.

See [“Switching a global CSG”](#) on page 502.

Note: Depending on the replication technology, you may have to update the data on the primary site before you switch back the global CSG.

To test VCS One disaster recovery support

- 1 Perform a planned switchover.
Switch over the global CSG from the primary site to the secondary site.

```
# hacsg -switch csg_name -clus secondary_clus
```
- 2 Perform a planned switchback.
Depending on whether the replication technology requires you to manually update the data at the primary site, perform the following steps:

Data requires manual update on the primary
 - Take the global CSG offline at the primary site.
 - Perform the replication agent’s update action at the primary site.
 - Bring the global CSG online on the primary site.Refer to the Installation and Configuration Guide for the corresponding VCS One replication agent for details.

Data is automatically updated on the primary

Run the following command to switch back the global CSG from the secondary site to the primary site:

```
# hacsg -switch csg_name -clus primary_clus
```


Managing remote clusters

This chapter includes the following topics:

- [About managing remote clusters](#)
- [Adding remote clusters](#)
- [Determining the connection role of clusters](#)
- [Viewing remote clusters](#)
- [Viewing remote cluster details](#)
- [Editing remote cluster attributes](#)
- [Deleting remote clusters](#)
- [Enabling connections between clusters](#)
- [Disabling connections between clusters](#)
- [Viewing the status of individual network links](#)
- [Viewing the consolidated status of network links](#)
- [Viewing the state of the clusters](#)
- [Modifying remote cluster configuration](#)
- [Changing the local cluster's DR port value](#)
- [Changing the local cluster's DR address value](#)
- [Faulting a remote cluster using the Simulator](#)
- [Clearing a simulated cluster fault using the Simulator](#)
- [Simulating a link fault](#)
- [Clearing a simulated link fault](#)

About managing remote clusters

In a global cluster setup, a remote cluster object defines the other clusters to which the local cluster connects and communicates over an IP network.

See [“About VCS One global clusters”](#) on page 66.

Adding remote clusters

You must have Add Cluster privilege in the farm category to add a remote cluster to the VCS One cluster.

See [“Catalog of farm privileges”](#) on page 630.

You must provide the following details for the remote cluster that you want to add.

ClusterName	Name of the cluster at the remote site The name of the remote cluster must not exceed 128 characters. The name cannot start with a number or contain any special characters.
DRPort (On initiator cluster)	Port address on which the remote cluster listens for connections If you do not specify the port address, the default value 14151 is used.
NetworkConnections (On initiator cluster)	Network connection details for the remote cluster Note: Symantec recommends that you configure at least two network connections in a VCS One global cluster setup. You must specify a value for the destination IP address. If you do not specify a source IP address, VCS One uses any of the available IP addresses on the local cluster to connect to the remote cluster.

See [“Remote cluster attributes”](#) on page 697.

See [“How VCS One global clusters communicate with each other”](#) on page 69.

Use the following procedure to add a remote cluster.

To add a remote cluster using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed.
- 3 Click **Configuration > Add Remote Cluster**.

The Remote Cluster Configuration wizard is displayed.

- 4 In the **Specify Remote Cluster Details** screen, enter the name of the remote cluster in the **Remote Cluster Name** box.
Based on the cluster name, VCS One designates either the local or the remote cluster to initiate connection between the clusters.
 - If the local cluster's connection role is not to initiate connection, click **Finish** and skip to step [step 9](#).
 - If the local cluster's connection role is to initiate connection, then the wizard displays the **Specify Remote Cluster Connection Details** screen.
- 5 In the **Remote Cluster's DR Listening Port** box, retain the default port address or enter a value for the remote cluster listening port.
- 6 In the **Network Connections** area, provide the network connection details for the local cluster to establish connection with the remote cluster:
 - Click **Add**.
 - In the **Add Connection** dialog box, enter the following details:
 - In the **Remote Cluster IP** box, enter the IP address of the remote cluster.
 - In the **Source IP** box, enter the IP address of the local cluster if you do not want VCS One to use any of the available IP addresses.
 Repeat this step if you want to add more network links that the local cluster can use to connect to the remote cluster.
- 7 Click **Next**.
- 8 In the **Summary** screen, click **Finish**.
- 9 In the **Results** screen, click **Close**.

To add a remote cluster from the command line

- 1 Type the following command to add a remote cluster:

```
haclus -add remoteclasser_name
[-user user@domain] [-domain domaintype]
```

where *remoteclasser_name* is the name of the remote cluster.

- 2 Determine whether you must define the network connection details on this cluster.

```
# haclus -display remoteclasser_name -attribute ConnectionRole \
[-user user@domain] [-domain domaintype]
```

See [“Determining the connection role of clusters”](#) on page 480.

- If the command displays the output as Initiator, you need not specify any other details. You have successfully added a remote cluster.

- If the command displays the output as Acceptor, then the local cluster is the initiator. Proceed to [step 3](#).

- 3 Type the following command to specify the network connection details of the remote cluster:

```
haclus -modify NetworkConnections -add destinationIP:sourceIP
-clus remoteclassifier_name
[-user user@domain] [-domain domaintype]
```

where:

<i>destinationIP</i>	The IP address of the remote cluster. You must specify a value for the destination IP address.
<i>sourceIP</i>	The IP address of the local cluster. If you do not specify a source IP address, VCS One uses any of the available IP addresses on the local cluster to connect to the remote cluster.
<i>remoteclassifier_name</i>	Name of the remote cluster.

- 4 To specify a different remote cluster port other than the default port 14151, type the following command:

```
haclus -modify DRPort remoteclassifier_port
-clus remoteclassifier_name
[-user user@domain] [-domain domaintype]
```

where:

<i>remoteclassifier_port</i>	The remote cluster port on which the local cluster listens for incoming connections from the remote clusters.
<i>remoteclassifier_name</i>	Name of the remote cluster.

See the *Veritas Cluster Server One Command Reference Guide*.

Determining the connection role of clusters

VCS One stores the connection role information of the remote cluster in the ConnectionRole attribute of the remote cluster object at each site.

See [“How VCS One global clusters communicate with each other”](#) on page 69.

You must have Read Only privilege in the object category to determine the connection role of clusters.

See [“Catalog of object privileges”](#) on page 631.

Use the following procedure to determine the connection role of a cluster.

To determine the connection role of a cluster from the command line

- ◆ Type the following command to display the value of the ConnectionRole attribute of a remote cluster:

```
haclus -display remotecluster_name -attribute ConnectionRole  
[-user user@domain] [-domain domaintype]
```

where:

remotecluster_name Name of the remote cluster.

See the *Veritas Cluster Server One Command Reference Guide*.

- If the command displays the output as Initiator, then the cluster at the local site accepts network connections from the cluster at the remote site.
- If the command displays the output as Acceptor, then the cluster at the local site initiates network connections to the cluster at the remote site.

Viewing remote clusters

You must have Read Only privilege in the object category to view the remote clusters.

See [“Catalog of object privileges”](#) on page 631.

Use the following procedure to view remote clusters in your disaster recovery setup.

To view remote clusters using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed with the list of remote cluster objects.

To view remote clusters from the command line

- ◆ Type the following command:

```
haclus -list  
[-user user@domain] [-domain domaintype]
```

The command lists the local cluster and the remote clusters that form the VCS One global cluster. The local cluster is indicated with an asterisk.

See the *Veritas Cluster Server One Command Reference Guide*.

Viewing remote cluster details

You must have Read Only privilege in the object category to view the remote cluster attributes and its details.

See “[Catalog of object privileges](#)” on page 631.

Use the following procedure to view remote cluster attributes.

To view remote cluster attributes using the VCS One console

- 1 In the VCS One console, navigate to the **Disaster Recovery** page to view the remote clusters.
See “[Viewing remote clusters](#)” on page 481.
- 2 In the **Remote Clusters** pane, click the appropriate remote cluster.
The details page for the remote cluster is displayed with the following information:
 - Details of the remote cluster such as name, state, and consolidated network link status
 - Details of the global CSGs that are configured to run on this remote cluster
 - Details on the network links between the clusters

To view remote cluster attributes from the command line

- ◆ Type the following command:
 - To display the values of all the attributes of a remote cluster:

```
haclus -display remotecluster_name  
[-user user@domain] [-domain domaintype]
```
 - To display the value of a specific attribute of a remote cluster:

```
haclus -display remotecluster_name -attribute attribute  
[-user user@domain] [-domain domaintype]
```

where:

remotecluster_name Name of the remote cluster.

If you do not specify the remote cluster name, the command displays the values for the local cluster.

attribute Name of the specific remote cluster attribute.

See “[Remote cluster attributes](#)” on page 697.

See the *Veritas Cluster Server One Command Reference Guide*.

Editing remote cluster attributes

You must have Modify Cluster privilege in the farm category to edit the remote cluster attributes. Review the remote cluster attributes description to find whether the attribute is editable.

See “[Catalog of farm privileges](#)” on page 630.

See “[Remote cluster attributes](#)” on page 697.

Use the following procedure to edit remote cluster attributes.

To edit remote cluster attributes using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed.
- 3 In the **Remote Clusters** area, click the appropriate remote cluster.
The details page for the remote cluster is displayed.
- 4 In the right pane, click **All Attributes**.
- 5 In the **All Attributes** page, click the **Edit** icon for the attribute that you want to edit.
- 6 In the **Edit Attribute** dialog box, perform the following steps:
 - In the **Value** box, select or enter a value for the attribute.
 - If the attribute stores a list of values, you can change or delete the existing values and add new values in the **Values** table.
 - To change a value, select the appropriate row in the **Values** table and enter the value.
 - To delete a value, select the appropriate row in the **Values** table and click the - icon in the right corner of the table.
 - To add a value, click the + icon in the right corner of the **Values** table and enter the value in the new row.
 - Click **OK**.
 - Click **Close**.

To edit remote cluster attributes from the command line

- ◆ Type the following command to modify the attribute value of type SCALAR for a remote cluster:

```
haclus -modify attribute value -clus remotecluster_name  
[-user user@domain] [-domain domaintype]
```

where:

<i>attribute</i>	Name of the specific attribute for a remote cluster.
<i>value</i>	Value for the specified attribute.
<i>remotecluster_name</i>	Name of the remote cluster. If you do not specify the <code>-clus</code> option, the command modifies the values for the local cluster.

See the *Veritas Cluster Server One Command Reference Guide* for details on how to modify the attribute of type VECTOR, KEYLIST, and ASSOCIATION.

Deleting remote clusters

You must have Delete Cluster privilege in the farm category to delete a remote cluster from the VCS One cluster.

See [“Catalog of farm privileges”](#) on page 630.

Use the following procedure to delete a remote cluster.

Before you delete a remote cluster, ensure that the local cluster is not connected to the remote cluster.

See [“Disabling connections between clusters”](#) on page 485.

To delete a remote cluster using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed.
- 3 In the **Remote Clusters** area, select a remote cluster that you want to delete.
- 4 Click **Configuration > Delete Remote Cluster(s)**.
The Delete Remote Cluster wizard is displayed.
- 5 In the **Delete Remote Cluster(s)** screen, click **OK**.
- 6 Click **Close**.

To delete a remote cluster from the command line

- ◆ Type the following command:

```
haclus -delete remotecluster_name  
[-user user@domain] [-domain domaintype]
```

where *remotecluster_name* is the name of the remote cluster.

See the *Veritas Cluster Server One Command Reference Guide*.

Enabling connections between clusters

After you have specified the network connection details of the remote cluster, you can enable network connectivity between the clusters. You must perform this procedure from both the local and the remote clusters between which you want to initiate connection.

You must have Modify Cluster privilege in the farm category.

See “[Catalog of farm privileges](#)” on page 630.

Use the following procedure to enable connections between clusters.

To enable connections between clusters using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed.
- 3 In the **Remote Clusters** area, select a remote cluster to which you want the local cluster to establish connection.
- 4 Click **Operations > Enable Connection(s)**.
- 5 In the **Enable connections with Remote Cluster(s)** screen, click **OK**.
- 6 Click **Close**.

To enable connections between clusters from the command line

- ◆ Type the following command:

```
haclus -modify EnableConnections 1 -clus remotecluster_name
```

where *remotecluster_name* is the name of the remote cluster.

See the *Veritas Cluster Server One Command Reference Guide*.

Disabling connections between clusters

After you have specified the network connection details of the remote cluster, you can disable network connectivity between the clusters.

You must have Modify Cluster privilege in the farm category.

See “[Catalog of farm privileges](#)” on page 630.

Use the following procedure to disable connections between clusters.

To disable connections between clusters using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed.

- 3 In the **Remote Clusters** area, select a remote cluster from which you want the local cluster to remove connection.
- 4 Click **Operations > Disable Connection(s)**.
- 5 In the **Disable connection with Remote Cluster(s)** screen, click **OK**.
- 6 Click **Close**.

To disable connections between clusters from the command line

- ◆ Type the following command:

```
haclus -modify EnableConnections 0 -clus remotecluster_name
```

where *remotecluster_name* is the name of the remote cluster.

See the *Veritas Cluster Server One Command Reference Guide*.

Viewing the status of individual network links

You must have Read Only privilege in the object category to view the status of network links.

See “[Catalog of object privileges](#)” on page 631.

The status of the network links between the clusters can be UP, DOWN, or DISABLED. The status of the links are not displayed if the initiator cluster has not yet established connection with the remote cluster.

See “[Network link states in VCS One global clusters](#)” on page 763.

Use the following procedure to view the status of individual network links between the clusters.

To view the status of individual network links using the VCS One console

- 1 In the VCS One console, navigate to the **Disaster Recovery** page to view the remote clusters.
See “[Viewing remote clusters](#)” on page 481.
- 2 In the **Remote Clusters** pane, click the appropriate remote cluster.
The details page for the remote cluster is displayed.
- 3 View the status of each network link that you configured between the local and the remote clusters in the Link Status area of the details page.

To view the status of network links from the command line

- ◆ Type the following command to display the status of the individual network links between the local and the remote clusters:

```
haclus -display remotecluster_name -attribute LinkStatus  
[-user user@domain] [-domain domaintype]
```

where:

remotecluster_name Name of the remote cluster.

If you do not specify the remote cluster name, the command displays the values for the local cluster.

See the *Veritas Cluster Server One Command Reference Guide*.

Viewing the consolidated status of network links

You must have Read Only privilege in the object category to view the status of network links.

See [“Catalog of object privileges”](#) on page 631.

The consolidated status of the network links between the clusters can be UP, DOWN, PARTIAL UP, DISABLED, or DISABLED DOWN. The status of the links are not displayed if the initiator cluster has not yet established connection with the remote cluster.

See [“Network link states in VCS One global clusters”](#) on page 763.

Use the following procedure to view the consolidated status of network links between the clusters.

To view the consolidated status of network links using the VCS One console

- 1 In the VCS One console, navigate to the **Disaster Recovery** page to view the remote clusters.
See [“Viewing remote clusters”](#) on page 481.
- 2 View the Link Status column for the remote cluster in the **Remote Clusters** pane.

To view the consolidated status of network links from the command line

- ◆ Type the following command to display the consolidated status of the network links between the local and the remote clusters:

```
haclus -display remotecluster_name
-attribute ConsolidatedLinkStatus
[-user user@domain] [-domain domaintype]
```

where:

remotecluster_name Name of the remote cluster.

If you do not specify the remote cluster name, the command displays the values for the local cluster.

See the *Veritas Cluster Server One Command Reference Guide*.

Viewing the state of the clusters

You must have Read Only privilege in the object category to view the state of clusters.

See “[Catalog of object privileges](#)” on page 631.

See “[Cluster states in VCS One global clusters](#)” on page 762.

Use the following procedure to view the state of the clusters.

To view the state of the cluster from the command line

- ◆ Type the following command to display the state of the clusters:

```
haclus -state  
[-user user@domain] [-domain domaintype]
```

See the *Veritas Cluster Server One Command Reference Guide*.

Modifying remote cluster configuration

You can modify the remote cluster configuration only on the cluster that VCS One has designated to initiate connection request.

You must have Modify Cluster privilege in the farm category to modify the remote cluster configuration.

See “[Catalog of farm privileges](#)” on page 630.

Before you use the following procedure to modify remote cluster configuration, you must disable the network connections to the remote cluster for which you want to modify the network connection settings.

See “[Disabling connections between clusters](#)” on page 485.

Use the following procedure to modify the remote cluster configuration.

To modify remote cluster configuration using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed.
- 3 In the **Remote Clusters** area, select a remote cluster that you want to modify.
- 4 Click **Configuration > Modify Remote Cluster**.
The Remote Cluster Configuration wizard is displayed.

- 5 In the **Remote Cluster Port** box of the **Specify Remote Cluster Details** screen, retain the default port address or enter a value for the remote cluster port.
- 6 In the **Network Connections** area, modify the network connection details that the local cluster uses to connect to the remote cluster:
 - To add more network connections, do the following:
 - Click **Add**.
The Add Connection dialog box appears.
 - In the **Remote Cluster IP** box, enter the IP address of the remote cluster.
 - In the **Source IP** box, enter the IP address of the local cluster if you want VCS One to use a specific IP address.
 - To edit an existing network connections, do the following:
 - In the **Remote Cluster IP** column, enter the IP address of the remote cluster.
 - In the **Source IP** column, enter the IP address of the local cluster if you want VCS One to use a specific IP address.
- 7 Click **Next**.
- 8 In the **Summary** screen, click **Finish**.
- 9 In the **Results** screen, click **Close**.

To modify remote cluster configuration from the command line

- 1 Disable network connections to the remote cluster for which you want to modify the network connection settings.

```
haclus -modify EnableConnections 0 -clus remotecluster_name
```

- 2 Type the following command to change the remote cluster port:

```
haclus -modify DRPort remotecluster_port  
-clus remotecluster_name
```

- 3 Modify the network connection details for the remote cluster:

- To specify network connection values for the first time after you added the cluster:

```
haclus -modify NetworkConnections key  
-clus remotecluster_name
```

- To add additional network connections:

```
haclus -modify NetworkConnections -add key \  
-clus remotecluster_name
```

- To delete a particular network connection:

```
haclus -modify NetworkConnections -delete key \  
-clus remotecluster_name
```

Modifying remote cluster configuration

- To delete all the network connections:

```
haclus -modify NetworkConnections -delete -keys \  
-clus remotecluster_name
```

where:

remotecluster_port The remote cluster port on which the local cluster listens for incoming connections from the remote clusters.

remotecluster_name Name of the remote cluster.

key Value for the NetworkConnections attribute.

See the *Veritas Cluster Server One Command Reference Guide*.

Changing the local cluster's DR port value

Use the following procedure to modify the local cluster's `DRListingPort` attribute.

Warning: If you change the `DRListingPort` value for the cluster that accepts the connection requests, make sure you make the equivalent changes to the `DRPort` attribute for the remote cluster object that represents this cluster. See [“Modifying remote cluster configuration”](#) on page 488.

To change the local cluster's DR port values

- 1 Stop the Policy Master daemon; take the Policy Master resource offline.

```
hastop -pm
```

- 2 Export the information in the cluster configuration database to XML-formatted files.

```
haconf -dbtoxml location_of_the_xml_directory
```

- 3 Edit the `main.xml` file.

Add `DRListingPort` attribute to the local cluster's cluster object.

For example, the bold text in the following sample cluster object indicates the line you must add to define the `DRListingPort` attribute with the value 60000:

```
<cluster name="seattle">
  <attributes>
    <attribute name="DefaultPlatform"><scalar>"linux/x86"</scalar></attribute>
    <attribute name="DRListingPort"><scalar>60000</scalar></attribute>
    <attribute name="FarmUUID"><scalar>"15e15b64-1dd2-11b2-b76a-b60f6c745dd1"
      </scalar></attribute>
    <attribute name="LogDbg"></attribute>
  </attributes>
</cluster>
```

- 4 Validate the configuration information in the XML files.

```
haconf -verify location_of_.xml_config_files
```

- 5 Clean the configuration database.

```
haconf -cleandb
```

- 6 Load the XML configuration into the database.

```
haconf -loaddb location_of_the_xml_directory
```

where *location_of_the_xml_directory* is the location you specified in [step 2](#).

- 7 Start the Policy Master daemon; bring the Policy Master resource online.

```
hastart -pm
```

Changing the local cluster's DR address value

Use the following procedure to modify the local cluster's DRAddress attribute.

To change the local cluster's DR address value

- 1 Make sure that the Policy Master daemon `vcsoned` is running in the Policy Master cluster.

```
haclus -display -attribute ClusterState
```

The output must show the cluster state as `RUNNING`.

- 2 Run the following command to add an IP address for the Policy Master to start listening on this IP address for inter-cluster connection.

```
haadmin -addrip ipaddress nic netmask
```

The command updates the cluster-level attribute `DRAddress` and also updates the IP resource in the `DRSG` service group. The variable `nic` represents the NIC device that is used for the disaster recovery IP address.

Faulting a remote cluster using the Simulator

This task is only available using the Simulator to simulate a remote cluster fault.

This procedure assumes that two simultaneous instances of the Simulator are running on the same system and that you already have a remote cluster set up and running. Faulting the remote cluster stops the Policy Master of the remote cluster.

See [“How global clusters work”](#) on page 69.

To simulate a remote cluster fault

- 1 In the VCS One Simulator console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed.
- 3 In the **Remote Clusters** area, select a remote cluster which you want to fault.
- 4 Click **Simulation > Fault Remote Cluster(s)**.
- 5 In the **Fault Remote Cluster(s)** screen, click **OK**.
- 6 Click **Close**.

To fault a remote cluster from the command line

- ◆ Type the following command:

```
hasim -faultcluster remoteclasser_name
```

where `remoteclasser_name` is the name of the remote cluster.

See the *Veritas Cluster Server One Command Reference Guide*.

Clearing a simulated cluster fault using the Simulator

This task is only available using the Simulator to clear a simulated remote cluster fault.

To clear the fault, you must start the Policy Master of the remote cluster. Because the user interface is unavailable for the Simulator instance of a faulted remote cluster, you must use the command line to clear the fault.

To clear a faulted remote cluster from the command line

- ◆ Type the following command:

```
hasim -start -pm
```

This command must be invoked from the command line of the faulted remote cluster.

See the *Veritas Cluster Server One Command Reference Guide*.

Simulating a link fault

This task is only available using the Simulator to simulate a link fault.

A remote cluster can have multiple link connections and you can fault one or more links at the same time. The link fault can be induced only on the cluster that VCS One has designated to initiate connection request. The link status for a faulted link is displayed as **DOWN**. If you fault all links of a remote cluster then the remote cluster appears faulted from the local cluster; however, the Policy Master of the remote cluster will still be in a running state.

To simulate a link fault

- 1 In the VCS One Simulator console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed.
- 3 In the **Remote Clusters** area, select a remote cluster whose links you want to fault. Alternatively, you can click the remote cluster name to navigate to the Link Status page and then select the links.
- 4 Click **Simulation > Fault Link(s)**.
- 5 In the **Fault Link for Cluster** screen, select one of the following options:
 - **Fault any Link**
Select this option to fault the main link.
 - **Fault specific Link(s)**

Select this option to fault specific links. In the Available Links area, select the check box next to each of the links which you want to fault.

- 6 Click **OK**.

To simulate a link fault from the command line

- ◆ Type the following command:

```
hasim -faultrlink remotecluster_name [rlink]
```

where *remotecluster_name* is the name of the remote cluster and *rlink* is the name of the remote link. If *rlink* is not specified, then the first available link which is in the UP state is faulted.

See the *Veritas Cluster Server One Command Reference Guide*.

Clearing a simulated link fault

This task is only available using the Simulator to clear a simulated link fault.

If all links are in a Down state then the remote cluster appears faulted from the local cluster. Clearing a fault on any one of the faulted links brings the link up and the state of the remote cluster again changes to **RUNNING**. The link fault can be cleared only from the cluster that VCS One has designated to initiate connection request.

To clear a simulated link fault

- 1 In the VCS One Simulator console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed.
- 3 In the **Remote Clusters** area, select a remote cluster whose link fault you want to clear. Alternatively, you can click the remote cluster name to navigate to the Link Status page and then select the links.
- 4 Click **Simulation > Clear Link Fault(s)**.
- 5 In the **Clear Link Fault for Cluster** screen, select one of the following options:
 - **Clear Fault on any Link**
Select this option to clear the fault on the first available link as listed in the `NetworkConnections` attribute.
 - **Clear Fault on specific Link(s)**
Select this option to clear the fault on specific links. In the Available Links area, select the check box next to each of the links whose fault you want to clear.
- 6 Click **OK**.

To clear a link fault from the command line

- ◆ Type the following command:

```
hasim -clearlinkfault remotecluster_name [rlink]
```

where *remotecluster_name* is the name of the remote cluster and *rlink* is the name of the remote link. If *rlink* is not specified, then the first available link which is in the DOWN state is cleared.

See the *Veritas Cluster Server One Command Reference Guide*.

Managing global composite service groups

This chapter includes the following topics:

- [About managing global composite service groups](#)
- [Configuring a global CSG](#)
- [Requesting authority for a global CSG](#)
- [Bringing a global CSG online](#)
- [Switching a global CSG](#)
- [Taking over a global CSG](#)

About managing global composite service groups

A composite service group (CSG) is a container that combines one or more objects into a single logical object. A global CSG is a CSG with wide-area failover capability in a global cluster environment.

See [“About composite service groups”](#) on page 40.

See [“About managing composite service groups”](#) on page 364.

Configuring a global CSG

Use this procedure to make a composite service group (CSG) local or global.

When you create a CSG, the CSG is local by default. The CSG is confined to the cluster on which you created the CSG. In a global cluster environment, you must configure this CSG as a global CSG to enable wide-area failover across the clusters.

See [“Creating a composite service group”](#) on page 364.

The ClusterList attribute value determines whether the CSG is local or global. A global CSG must meet the following characteristics:

- The ClusterList attribute must include the cluster names on which the CSG can run.
- The ClusterList attribute must include at least one remote cluster.
- The ClusterList attribute value must match across the local and the remote clusters.

When you configure a composite service group as global, VCS One adds the local cluster name to the ClusterList attribute by default. You cannot remove the local cluster from a global composite service group.

Note: When you delete a remote cluster, VCS One removes the cluster name from the ClusterList attribute of the corresponding CSG.

To configure a global CSG using the VCS One console

- 1 In the VCS One console, locate the CSG for which you want to configure the ClusterList attribute.
See [“Listing composite service groups and unassociated service groups”](#) on page 367.
- 2 In the right pane, under **Composite Service Groups**, click the CSG.
- 3 From the Configuration menu, click **Configure Global CSG**.

The **Composite Service Group Configuration Wizard (Configure Global CSG)** dialog box is displayed.

- 4 In the **Cluster List Configuration** screen, add or remove the appropriate clusters from the Available Clusters or the Selected Clusters list.
- 5 Click **Finish**.
- 6 In the **Results** screen, click **Close**.

To configure a global CSG from the command line

- ◆ At the command prompt, type the following command:
 - To add a remote cluster to the ClusterList attribute:

```
hacsg -modify globalcsg_name ClusterList \  
-add remotecluster_name
```
 - To remove a remote cluster from the ClusterList attribute:

```
hacsg -modify globalcsg_name ClusterList \  
-delete remotecluster_name
```
 - To remove all remote cluster from the ClusterList attribute:

```
hacsg -modify globalcsg_name ClusterList \  
-delete -keys
```

where:

remotecluster_name Name of the remote cluster.

globalcsg_name Name of the global CSG.

See the *Veritas Cluster Server One Command Reference Guide*.

Requesting authority for a global CSG

The value of the Authority attribute must be set to 1 for VCS One to be able to bring a global composite service group (CSG) online on a local cluster.

You must perform the request authority operation in the following cases:

- The remote cluster where the global CSG was online has faulted and you must bring the global CSG online on the local cluster.
- You want to bring online the service groups within the global CSG on the local cluster.

You must have Request Authority privilege in the CSG category to request authority.

See [“Catalog of composite service group privileges”](#) on page 635.

To request authority for a global CSG using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Select one or more global CSGs for which you want to request authority. You can also click the name of the CSG to go to the detail page to request authority for the selected CSG.
- 5 From the Operations menu, click **Request Authority**.
- 6 Select the **Force** option to acquire authority for the global CSG on the local cluster when the remote cluster is not running or is disconnected from the local cluster.
- 7 Click **OK**.
- 8 Click **Close**.

To request authority for a global CSG from the command line

- ◆ At the command prompt, type the following command:

```
hacsg -requestauth globalcsg_name
```

If the remote cluster on which the global CSG that has authority is not running or is disconnected from the local cluster, you can use the `-force` option to acquire authority for the global CSG on the local cluster. Run the following command:

```
hacsg -requestauth -force globalcsg_name
```

where:

globalcsg_name The name of the global CSG.

Bringing a global CSG online

When you bring a composite service group (CSG) online, the operation brings all the service groups that are contained in the CSG online and then brings the CSG online. This operation has the following additional options:

Propagate option Initiates the online operation on the service groups outside the CSG on which service groups inside the CSG depend.

Force option Takes over the global CSG from the remote cluster that is in INIT or in FAULTED state.

In a global cluster setup, the local cluster acquires authority for the global CSG from the remote cluster and then brings the global CSG online on the local cluster.

See [“Taking over a global CSG”](#) on page 503.

The following conditions result in the rejection of the online operation of the CSG:

- The GroupList is empty.
- The CSG is already online in one of the clusters.
- The CSG has the PENDING flag set, which means the constituent service groups are in transition within the cluster.
- Any group in the CSG is frozen.
- Any group in the CSG has no configured resources
- Any group in the CSG has all resources disabled.

You must have the Online CSG privilege on the CSG to perform this operation.

To bring a CSG online using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Select one or more CSGs that you want to bring online.
 If you select multiple CSGs with service groups that have inter-dependencies, then you must first perform the request authority operation for each CSG before you bring the CSGs online.
 See [“Requesting authority for a global CSG”](#) on page 499.
- 5 From the Operations menu, click **Online CSG(s)**.
- 6 If you want to take over a global CSG from a remote cluster that is in INIT or in FAULTED state, then select the **Force** option.
- 7 Select the **Propagate** option if you want VCS One to also attempt to bring online all child service groups outside the CSG that have a dependency with service groups inside the CSG.
- 8 Click **OK > Close**.

To bring a CSG online from the command line

- ◆ Type the following command

```
hacsg -online [-propagate] [-force] csg_name
```

where

csg_name Name of the global CSG.

See the *Veritas Cluster Server One Command Reference Guide*.

Switching a global CSG

A switch operation is a planned failover which takes the global CSG offline and brings the global CSG online on the cluster that you specify. You must perform the switch operation on a CSG that is online or partially online. You must switch the global CSG to a cluster that is running.

Note: The switch operation on a global CSG fails for CSGs with service groups that have parent service groups outside the CSG which are online.

To switch a global CSG using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **SGs and CSGs** tab.
- 3 Click the **Composite Service Groups** tab.
- 4 Select a global CSG that you want to switch.
You can also click the name of the CSG to go to the detail page to switch the selected CSG.
- 5 From the Operations menu, click **Switch CSG**.
- 6 In the **Switch Composite Service Group** screen, select the cluster on which you want to bring the CSG online.
- 7 Click **OK**.
- 8 In the **Results** screen, click **Close**.

To switch a global CSG from the command line

- ◆ At the command prompt, type the following command:

```
hacsg -switch csg_name -clus cluster_name
```

where:

<i>csg_name</i>	Name of the global CSG.
<i>cluster_name</i>	Name of the cluster where you want to switch the global CSG.

See the *Veritas Cluster Server One Command Reference Guide*.

Taking over a global CSG

A takeover operation brings the global CSG online on the local cluster. You can perform a takeover operation if the remote cluster where the global CSG was online has faulted. You can take over multiple global CSGs using the VCS One console.

You must have Online CSG privilege to perform this operation.

Perform the following procedure on the cluster where you want to bring the global CSG online.

To take over global CSGs using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Disaster Recovery** tab.
The Disaster Recovery page is displayed.
- 3 In the **Remote Clusters** area, select the remote cluster from which you want to take over the global CSG.
- 4 Click **Operations > Take Over CSG(s)**.
- 5 In the **Select the Composite Service Groups for the local cluster to take over** screen, perform the following:
 - To select specific CSGs, select the CSGs from the list that is displayed.
 - To select all CSGs, select the option **Select All Composite Service Groups**.
- 6 Click **OK > Close**.

To take over global CSGs from the command line

- ◆ At the command prompt, type the following command:
`hacsg -online [-propagate] -force globalcsg_name`
where:

<i>globalcsg_name</i>	Name of the global CSG.
-----------------------	-------------------------

If the CSG has service groups with other dependant service groups that are outside the CSG, then use the `-propagate` option to bring those child service groups online.

The takeover operation fails or partially succeeds if the child service groups that are outside of the CSG are not brought online.

See the *Veritas Cluster Server One Command Reference Guide*.

Tasks: Administering your Enterprise environment

This section includes the following chapters:

- [“Administering the organization tree”](#) on page 507.
- [“Administering attributes and settings”](#) on page 515.
- [“Administering users and roles”](#) on page 529.
- [“Administering sets of objects”](#) on page 549.

Administering the organization tree

This chapter includes the following topics:

- [About administrating the organization tree](#)
- [Administering the organization tree](#)

About administrating the organization tree

Before building an organization tree, analyze your environment and user requirements.

See [“About users and the Organization tree”](#) on page 221.

An organization tree is a logical hierarchical structure of the VCS One cluster that is used to delineate user views and privileges.

Administering the organization tree features that correspond to virtualization may be visible to the user. This capability is not supported in the current release, but will be available in the future.

About building an organization tree

The organization tree is built in the order of a tree hierarchy. To build an organization tree, perform the following steps in the order presented:

- The first node you add to the organization tree is an OUName node that is attached to the top-level ServerFarm node.
- Next add one or more OUValue nodes to the initial OUName node.
- Continue adding OUName and OUValue nodes until your organization tree is complete.

Indicate where in the organization tree to attach the next node by specifying the organization tree path. The organization tree path is denoted by a list of OUName=OUValue pairs, separated by a forward slash (/).

You may add extended attribute definitions to your OUValue nodes at any time.

See [“Moving systems, service groups, or users between organization tree nodes”](#) on page 511.

How to build an organization tree

Use alphanumeric characters, along with the underscore character when defining organization unit nodes.

To add an OUName node to the organization tree using the VCS One console

- 1 In the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Organization Units** tab.
In the left pane, the organization tree displays in a hierarchical view.
In the right pane, the full path of the current organization unit displays.
When building the first node in the organization tree, the value will be /.
- 3 In the left pane, click the OUValue node in the organization tree where you want to attach the OUName node.

When building the first node in the organization tree, click the top-level OUValue node **ServerFarm(/)**.

- 4 In the right pane, from the **Configuration** menu, click **Add OUName**.
 Alternatively, from the left pane, you can right-click the OUValue node in the organization tree and click **Add OUName**.
 The **Add OUName** dialog box appears. The Parent OUValue displays.
- 5 In the **OUName** text box, type the name of the OUName node to add to the organization tree.
- 6 Click **OK**.
 In the left pane view of the organization tree, the new node appears.
 In the right pane, the name appears in the **OUNames applicable for this OUValue** table.

To add an OUName node to the organization tree from the command line

- ◆ The following command adds a OUName node to the organization tree:

```
haou -add OUName OUValuePath
```

 where
OUName is the name of the OUName node to be added.
OUValuePath is the location in the tree to add the node, as denoted by an organization tree path. The organization tree path is denoted by a list of OUName=OUValue pairs, separated by a forward slash (/).

To add an OUValue node to the organization tree using the VCS One console

- 1 In the left pane, click the OUName node where you want to attach the OUValue node.
 In the right pane, the full path of the current organization unit displays.
- 2 In the right pane, from the **Configuration** menu, click **Add OUValue**.
 Alternatively, from the left pane, you can right-click the OUName node in the organization tree and click **Add OUValue**.
 The **Add OUValue** dialog box appears. The Parent OUName displays.
- 3 In the **OUValue(s)** box, click the **+** to add an OUValue node to the organization tree.
- 4 Type the name of the OUValue node.
 You may add multiple OUValue nodes at this point. To add multiple nodes, click the **+** after adding each node and before moving to the next step.
- 5 Click **OK**.
 In the left pane view of the organization tree, the new node appears. In the right pane, the name appears in the **OUValues applicable for this OUName** table.

To add an OUValue node to the organization tree from the command line

- ◆ The following command adds *OUValue* to the list of valid values for the *OUName* node specified by *OUNamePath* in the organization tree

```
haou -addvalue OUValue OUNamePath
```

where
OUValue is one or more value(s) of the *OUName* node above it in the organization tree.
OUNamePath is the location in the tree to add the value, as denoted by an organization tree path that ends in an *OUName*. The organization tree path is denoted by a list of *OUName=OUValue* pairs, separated by a forward slash (/).

Administering the organization tree

You can do the following tasks on an organization tree:

- View the organization tree hierarchy
- List the current defined set of *OUNames*
- List the defined set of objects associated with an *OrgUnit*
- Delete an *OUName* from the organization tree
- Delete an *OUValue* from the organization tree

Viewing the organization tree hierarchy

To view the organization tree hierarchy using the VCS One console

- ◆ In the VCS One console, click the **Administration** tab.
The organization tree displays in the left pane.

To view the organization tree hierarchy from the command line

- ◆ Type the following command to list the entire organization tree hierarchy:

```
haou -list [-tree]
```

The *-tree* option displays that hierarchy in tree format.
- ◆ Type the following command to list the organization tree hierarchy from the node (*OuName* or *OUValue*) specified by *OUNamePath* or *OUValuePath*:

```
haou -list OUNamePath  
haou -list OUValuePath
```

Appropriate privileges are required to view a part or the whole of the organization tree.

Moving systems, service groups, or users between organization tree nodes

To move systems between nodes in the organization tree

See [“Moving a system to another organization tree node”](#) on page 306.

To move service groups between nodes in the organization tree

See [“Moving a service group to another organization tree node”](#) on page 327.

To move composite service groups between nodes in the organization tree

See [“Moving a local composite service group in the organization tree”](#) on page 372.

To move users between nodes in the organization tree

See [“Moving a user to another Organization Tree node:”](#) on page 539.

List the OUName for an OUValue

There can not be more than one OUName for each OUValue.

There is no CLI equivalent for this console command.

To list the OUName for an OUValue using the VCS One console

- 1 In the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Organization Units** tab.
- 3 In the left pane, click the applicable OUValue node.
View the list in the **OUNames applicable for this OUValue** table.

List the set of OUValues for an OUName

To list the set of OUValues for an OUName node using the VCS One console

- 1 In the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Organization Units** tab.
- 3 In the left pane, click the applicable OUName node.
View the list in the **OUValues applicable for this OUName** table.

To list the current defined set of OUValues for an OUName from the command line

- ◆ The following command lists the OUValues in the OUNamePath:

```
haou -displayval OUNamePath
```

List the defined set of objects associated with an organizational unit

To list the set of objects associated with an organizational unit using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 In the left pane, click the OrgUnit node in the organization tree where you want to list the set of objects.
- 3 Click one of the following tabs:

Service Groups	Lists service groups associated with this organization unit and its subtree.
Systems	Lists systems associated with this organization unit and its subtree.
Virtualization	Lists frames associated with this organization unit and its subtree.

To list the current defined set of objects associated with an OrgUnit from the command line

- ◆ The following command lists all the objects that are associated with an individual OrgUnit in the OrgUnitPath.

```
haou -displayobj -exclusive [-grp] [-sys] [-frame] [-userobject] [-usergroup] OUValuePath
```

- ◆ The following command lists all the objects that are associated with an OrgUnit in the OrgValuePath, including the objects in the subtrees.

```
haou -displayobj [-grp] [-sys] [-frame] [-userobject] [-usergroup] OUValuePath
```

Deleting an OUName node from the organization tree

You can not delete an OUName node that has child OUValue nodes unless you use the `-force` option.

You may not delete a node from the organization tree if an extended attribute is used as a resource variable at or below the node.

To delete an OUName node from the organization tree using the VCS One console

- 1 In the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Organization Units** tab.
- 3 In the left pane, click the OUName node you want to delete.

- 4 In the right pane, from the **Configuration** menu, click **Delete OUName**. Alternatively, from the left pane, you can right-click the OUName node in the organization tree and click **Delete**. The **Delete OUName** dialog box appears, asking for confirmation.
- 5 Select or deselect the **Delete the complete subtree** check box.
- 6 Click **OK**.

To delete an OUName from the organization tree using the command line

- ◆ The following command deletes an OUName node from the organization tree:

```
haou -delete OUNamePath
```

where *OUNamePath* is the location in the tree to delete the node.
- ◆ The following command deletes the OUName node and the complete subtree from the organization tree:

```
haou -delete -force OUNamePath
```

Deleting OUValue nodes from the organization tree

You can not delete an OUValue node that has child OUName nodes, or that has objects attached unless you use the `-force` option. If an OUValue node is deleted, the objects that are attached to that OUValue node are automatically reattached to the parent OUValue node.

You can not delete a node from the organization tree if an extended attribute is used as a resource variable at or below the node.

To delete OUValue nodes from the organization tree using the VCS One console

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Organization Units** tab.
- 3 Perform one of the following actions to select the node(s) to delete:

To delete one OUValue node	In the left pane, click the OUValue node that you want to delete.
----------------------------	---

To delete multiple OUValue nodes	In the left pane, click the OUName node above the OUValue nodes you want to delete. In the right pane, check the boxes next to the OUValue nodes you want to delete.
----------------------------------	---

- 4 In the right pane, from the **Configuration** menu, click **Delete OUValue(s)**.

- 5 Check or uncheck the **Delete the complete subtree** check box.
Check this box if you want to also delete all the nodes below this node in the organization tree.
- 6 Click **OK**.
- 7 Click **Close**.

To delete OUValue nodes from the organization tree using the command line

- ◆ Type the following command to delete an OUValue node from the organization tree:
`haou -deletevalue path`
- ◆ Type the following command to delete an OUValue node and all the nodes below it from the organization tree. You must also use the `-force` option if objects are attached at this node:
`haou -deletevalue -force path`

Use the following information to replace the appropriate variables:

`path` The location of the node in the organization tree; denoted by the OUValue path for the object.

Administering attributes and settings

This chapter includes the following topics:

- [About administering attributes and settings](#)
- [Editing VCS One cluster attributes](#)
- [About extended attributes](#)
- [Defining an extended attribute](#)
- [Assigning an extended attribute a value](#)
- [Combining extended attributes in an expression](#)
- [Deleting an extended attribute](#)
- [Modifying the value of an inherited extended attribute](#)
- [Modifying the value of a locally defined extended attribute](#)
- [Modifying notification settings](#)
- [Enabling notification settings](#)
- [Disabling notification settings](#)
- [Enabling syslog notifications](#)
- [Disabling syslog notifications](#)
- [Enabling script execution](#)
- [Disabling script execution](#)
- [Testing notification settings](#)

About administering attributes and settings

Attributes consist of a name and value. The following types of attributes exist in VCS One:

- Attributes that are pre-defined in the product. They define the properties of the objects in the configuration.
- Extended attributes that the user defines. They allow you to attach metadata to the objects in the configuration for more sophisticated administration capabilities.
Analyze your environment and design a plan for the use of extended attributes.

Settings consist of values that you can set for notifications, including SMTP, SNMP, Syslog, and test.

Administering attributes features that correspond to virtualization may be visible to the user. This capability is not supported in the current release, but will be available in the future.

Each object has a procedure on how to edit attributes of that object type.

See [“Editing VCS One cluster attributes”](#) on page 516.

See [“Editing a composite service group’s attributes”](#) on page 371.

See [“Editing resource attributes”](#) on page 381.

See [“Editing system attributes”](#) on page 297.

See [“Editing user or user group attributes”](#) on page 538.

Editing VCS One cluster attributes

Attributes at the cluster level define properties across the entire VCS One cluster.

To view VCS One cluster attributes

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Settings** tab.
- 3 In the left pane, click **Global Settings**.
- 4 In the right pane, in the All Attributes table, click the pencil icon of an attribute to edit it.

If there is not a pencil icon next to the attribute name, the attribute is not editable. You may only edit attributes of global scope from this page.

About extended attributes

The extended attribute is given a value for a specific object. Extended attributes are defined at an OUValue node. An extended attribute definition applies to objects that are attached to the OUValue node where they are defined, and objects below that node in the organization tree.

Extended attributes that correspond to virtualization may be visible to the user. This capability is not supported in the current release, but will be available in the future.

Extended attributes can be one of the following types:

- System extended attribute– defines a characteristic for a system object that is attached to that OUValue node.
- Service group extended attribute – defines a characteristic for a service group object that is attached to that OUValue node.
- Common extended attribute – defines a characteristic for all system and service group objects attached to that OUValue node.

Note: Extended attributes can not be associated with user objects.

About values of extended attributes

The value of an extended attribute can be one of the following:

- Enumerated
An enumerated extended attribute has a set of valid values called a validation set. The value of the extended attribute at an object must be one of the values in the validation set.
A default value can be specified for an enumerated extended attribute at an OUValue path.
- Freeform
A freeform extended attribute does not have a predefined set of valid values or a default value. You can specify any value for the extended attribute at an object.

About names of extended attributes

The name of an extended attribute can use alphanumeric characters and the underscore character, and can be up to 32 characters.

See [“Planning the names of your VCS One cluster objects and attributes”](#) on page 209.

Defining an extended attribute

An extended attribute is defined at a particular OUValue node in the Organization Tree. All subnodes of that OUValue node also inherit the extended attribute definition.

To define an extended attribute using the VCS One console

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Extended Attributes** tab.
- 3 In the left pane, click the OUValue node where you want to define the extended attribute.
In the right pane, the full path of the current organization unit displays.
- 4 In the right pane, from the **Configuration** menu, click **Add Extended Attribute**.
Alternatively, from the left pane, you can right-click the OUValue node in the Organization Tree and click **Add Extended Attribute**.
The **Add Extended Attribute** window appears.
- 5 Fill in the **Add Extended Attribute** window text box with the following values:

Name	Name of the extended attribute
Description	Description of the extended attribute
Category	Select one of the following values: Common: The extended attribute is associated with service groups and systems. Group: The extended attribute is associated with service groups. System: The extended attribute is associated with systems.
Type	Click one of the following radio buttons: Freeform: When the extended attribute is given a value, freeform text is used. The value of the extended attribute does not have a preset list of possible options. Enumerated: The extended attribute has a preset list of possible values that is enforced.

Value	<p>If the Value Type for the extended attribute is Enumerated, this box defines the preset list of values.</p> <p>To add a value: Click + and type the value in the box.</p> <p>To delete a value: Click the value, then click -.</p> <p>Caution: Do not use commas in an extended attribute value. If a single extended attribute (EA) value contains a comma, the value is interpreted as multiple values.</p>
Default Value	<p>If Enumerated is the Value Type, one of the preset values can be designated as a default value for the extended attribute.</p> <p>Choose the attribute value from the drop down list.</p>

6 Click **OK**.

7 Click **Close**.

In the right pane view of the Organization Unit window, the new extended attribute appears in the **Locally-defined Extended Attributes** table.

To define an extended attribute from the command line

Use the haea -add command to add an extended attribute from the command line. More information is available on the haea command.

See *Veritas Cluster Server One Command Reference Guide*.

Assigning an extended attribute a value

You can change an extended attribute value in the details page of the attribute.

To assign an extended attribute a value using the VCS One console

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click one of the following tabs:

Service Groups	For a service group type extended attribute
Systems	For a system type extended attribute

- 3 In the right pane, click the name of the object that you want to define an extended attribute value.
- 4 In the right pane, find the row in the Extended Attributes table that has the extended attribute whose value you wish to define or edit.
- 5 Click the **Edit** button of that attribute row.

- 6 In the **Edit Extended Attribute** window, in the Value box, enter the value of the extended attribute.
Either type in a freeform value, or click predefined enumerated value from the drop-down list.
- 7 Click **OK**.
- 8 Click **Close**.

To assign an extended attribute a value using the command line

- ◆ Type the following command

```
ha_command -modify object ea value
```

Use the following information to replace the appropriate variables:

ha_command	The command used depends on the object that the extended attribute describes. Use the following guideline: <ul style="list-style-type: none">■ Use hasys for system extended attributes■ Use hagrps for group extended attributes
object	The name of the group or system object.
ea	The name of the extended attribute.
value	The value to assign the extended attribute.

Combining extended attributes in an expression

Extended attributes can be combined into an expression using either an AND or an OR logical operator.

The following examples are valid extended attribute expressions:

- osname=solaris
- osname=solaris AND location=london AND building=bldg_a
- osname=solaris OR osname=linux AND building=bldg_a

An expression can have a maximum of 65536 name=value pairs.

If you combine extended attributes using the console, the AND operator will be populated in the expression. To use the OR operator, manually edit the expression.

Deleting an extended attribute

To delete an extended attribute using the VCS One console

- 1 In the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Extended Attributes** tab.
- 3 In the organization tree in the left pane, click the OUValue node that contains the extended attribute you wish to delete.
- 4 In the **Locally-defined Extended Attributes** table, find the rows that contains the extended attribute in the **Name** column.
- 5 Check each extended attribute that you want to delete.
- 6 Click **Configuration > Delete Extended Attribute(s)**.

To delete an extended attribute from the command line

- ◆ Type the following command:

```
haea -delete [-sys | -grp ] attribute
```

where *attribute* is the name of the attribute to be deleted.

Modifying the value of an inherited extended attribute

You can modify the value of an extended attribute in the following ways:

- Reset the default value of an extended attribute:
- Reset the valid values of the extended attribute

You may only override the valid values of inherited extended attributes if the new list of valid values of the inherited extended attribute is a subset of the list of valid values of its parent.

Modifying the default value of an extended attribute at an OUValue node does not change the value of the extended attributes of objects that are already attached at that node. The new value will be applied to the new objects that get attached.

To reset the values of a inherited extended attribute using the VCS One console

- 1 In the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Extended Attributes** tab.

Modifying the value of an inherited extended attribute

- 3 In the organization tree in the left pane, click the OUValue node that contains the extended attribute you wish to reset.
- 4 In the **Inherited Extended Attributes** table, find the rows that contains the extended attribute in the **Name** column.
- 5 Click the pencil icon to edit.
- 6 In the **Modify Extended Attribute** window, in the **Value** table, modify the list of inherited attribute values.
- 7 Click the **Reset valid values** button to redefine the valid values of the extended attribute
- 8 Click the **Reset default value** button to change the value of the extended attribute to the default value.
- 9 Choose a propagate option, if appropriate

Propagate (add the value to EAs in the OU sub-tree) Use this option to propagate your modification to this extended attribute to all the nodes below this node in the organization tree.

Deleting an extended attribute value will always propagate.

Propagate (change the default value for EAs in the sub-tree) Use this option to propagate your modification to this extended attribute to all the nodes below this node in the organization tree that use the default value.

- 10 Click **OK > Close**.

To reset the values of an extended attribute from the command line

- ◆ Type the following command:

```
haea -reset [-sys | -grp ][-validvalues] OUValuePath attribute
[-user user@domain] [-domaintype domaintype]
```

where

OUValuePath is the location in the tree the attribute is attached.

attribute is the attribute name to be reset.

If **-validvalues** option is specified, the list of valid values for the extended attribute is synced up with the list of valid values of the attribute in the parent node of OUValuePath.

Modifying the value of a locally defined extended attribute

To modify the value of a locally defined extended attribute

- 1 In the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Extended Attributes** tab.
- 3 In the organization tree in the left pane, click the OUValue node that contains the extended attribute you wish to modify.
- 4 In the **Locally-defined Extended Attributes** table, find the rows that contains the extended attribute in the **Name** column.
- 5 Click the pencil icon to edit.
- 6 In the **Modify Extended Attribute** window, in the **Value** table, modify the list of extended attribute values.
- 7 Choose a propagate option, if appropriate

Propagate (add the value to EAs in the OU sub-tree) Use this option to propagate your modification to this extended attribute in all the node below this node in the organization tree.

Propagate (change the default value for EAs in the sub-tree) Use this option to propagate your modification to this extended attribute in all the nodes below this node in the organization tree that use the default value.

- 8 Click **OK > Close**.

Modifying notification settings

The Simple Mail Transfer Protocol (SMTP) is an application layer protocol, that is used to send emails over the Internet.

Simple Network Management Protocol (SNMP) is a component of the TCP/IP protocol. It enables network devices to exchange management information with each other and facilitates the node management over an IP network.

VCS One enables you to send SMTP email notifications for specific events in the VCS One cluster to the recipients configured in the rules. VCS One also enables you to send SNMP notifications for specific events in the VCS One cluster to an SNMP management station.

Use this procedure to configure or edit the SMTP and SNMP settings.

A user with Modify Notifier privileges can configure SMTP notification settings.

A user with Notify SNMP privileges can configure SNMP settings. A user with either Modify Notifier privileges or Notify SNMP privileges can configure SNMP notification settings.

A user with ModifyAutomationSettings privileges can modify these settings.

To modify notification settings

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Settings** tab.
- 3 In the left pane, click **Automation Settings**.
- 4 Click **Configuration > Edit Settings**.
- 5 Use the following information to enter information in the Edit Settings panel.

SMTP Server	Enter the name or IP address of the SMTP server. All email notifications are disabled until you specify an SMTP server.
Secondary SMTP Server	Enter the name or IP address of the secondary SMTP server
Server timeout	After sending SMTP commands to the mail server, the notifier waits for this number of seconds for a response from the mail server. If this timeout happens, the rule will report an error.
SMTP From Path	Enter the SMTP from path. The default value is VCSOne-Notifier.
SMTP Return Path	Enter a valid email address for the SMTP return path. If delivery of an email fails, the bounced email is delivered to this email address.
Web Console Address	Enter the IP address of the Web console. If the Policy Master has multiple IP addresses, enter the IP address that is accessible to all the email recipients. If you do not specify an IP address, the base IP address that is used in the Web console URL appears in the notifications.

Maximum Emails Limit	<p>The maximum number of emails that will be sent in a given hour per email address.</p> <p>When this limit is reached, a message is sent out with the subject line “Notifications are halted”</p>
SNMP Trap Port	<p>Enter the number of the port on which the SNMP traps are sent.</p> <p>An SNMP trap is an alert message, which is sent to the management station.</p>
SNMP Community	<p>Enter the name of the SNMP community, which includes the SNMP management station.</p> <p>An SNMP community is a group of SNMP enabled network devices and management stations. An SNMP device can belong to one or more SNMP communities, and responds only to requests from the management stations that belong to one of its communities. The default SNMP communities are private and public.</p> <p>Default value = public</p>
Default SNMP Console	<p>Enter the name or IP address of the default SNMP management station to which you want to send SNMP notifications.</p> <p>Used as the default value for SNMP Consoles field when adding a Notification Rule. User may erase this default value or specify a new value.</p>

6 Click **OK**.

7 Use the following information to enable notifications.

Enable SMTP notifications Click **Operations > Enable SMTP Notifications**.

Enable SNMP notifications Click **Operations > Enable SNMP Notifications**.

8 Test the new configuration.

See “[Testing notification settings](#)” on page 528.

Enabling notification settings

Use this procedure to enable SMTP or SNMP. In an actual installation these values are enabled by default. In simulated environments, these values are disabled by default.

To enable notification settings

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Settings** tab.
- 3 In the left pane, click **Automation Settings**.
- 4 Use the following information to enable SMTP and SNMP.

Enable SMTP notifications Click **Operations > Enable SMTP Notifications**.

Enable SNMP notifications Click **Operations > Enable SNMP Notifications**.

- 5 Click **Yes**.

Disabling notification settings

Use this procedure to disable SMTP or SNMP. If disabled, rules and jobs that have email or SNMP tasks will be marked as error and not execute.

To disable notification settings

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Settings** tab.
- 3 In the left pane, click **Automation Settings**.
- 4 Use the following information to disable SMTP and SNMP.

Disable SMTP notifications Click **Operations > Disable SMTP Notifications**.

Disable SNMP notifications Click **Operations > Disable SNMP Notifications**.

- 5 Click **Yes**.

Enabling syslog notifications

A user with the Syslog privileges in the Notifier privilege category can configure syslog notifications.

To enable syslog notifications

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Settings** tab.
- 3 In the left pane, click **Automation Settings**.

- 4 Click **Operations > Enable Syslog Notifications**.
- 5 Click **Yes**.

Disabling syslog notifications

A user with the Syslog privileges in the Notifier privilege category can configure syslog notifications.

To disable syslog notifications

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Settings** tab.
- 3 In the left pane, click **Automation Settings**.
- 4 Click **Operations > Disable Syslog Notifications**.
- 5 Click **Yes**.

Enabling script execution

Use this procedure to enable automation policy to execute a script.

To enable script execution

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Settings** tab.
- 3 In the left pane, click **Automation Settings**.
- 4 Click **Operations > Enable Script Execution**.
- 5 Click **Yes**.

Disabling script execution

Use this procedure to disable automation policy's ability to execute a script. If disabled, all rules and job that have script tasks will be marked as error and will not execute.

To disable script execution

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Settings** tab.
- 3 In the left pane, click **Automation Settings**.

- 4 Click **Operations > Disable Script Execution**.
- 5 Click **Yes**.

Testing notification settings

Use this procedure to test SMTP, SNMP, or Syslog notification settings. After you configure notification settings, test the settings to ensure that they work correctly.

If the SMTP server is not configured correctly, email notifications are disabled.

To test notification settings

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Settings** tab.
- 3 In the left pane, click **Automation Settings**.
- 4 Click **Configuration > Test Settings**.
- 5 Enter the following information in the Test Setting window:

Notification Type Click **Email**, **SNMP**, or **Syslog** to identify the type of test.

Recipient Enter the following information depending on what Notification Type option you selected:

- The email address of the recipient
- The hostname to send the SNMP traps
- The hostname to send the log messages

- 6 Click **OK**.
- 7 Click **Close**.

Administering users and roles

This chapter includes the following topics:

- [About administering users and roles](#)
- [Adding or deleting a user or usergroup](#)
- [Assigning or unassigning a role and objects to a user or usergroup](#)
- [Adding custom roles](#)
- [Cloning a role](#)
- [Editing a role](#)
- [Deleting a role](#)
- [Modifying user or usergroup settings](#)
- [Editing user or user group attributes](#)
- [Moving a user to another Organization Tree node:](#)
- [Enabling a user or usergroup](#)
- [Disabling a user or usergroup](#)
- [Viewing a user's or user group's settings, roles and associated objects](#)
- [Authenticating VCS One users](#)

About administering users and roles

When a user performs an operation, VCS One authorizes the action and the objects the user can act upon using the user's configured privileges. If the user does not have appropriate privileges, the operation will not execute.

VCS One has both predefined roles and the ability to create custom roles.

See [“About users, user groups, and their roles”](#) on page 43.

Administering users and roles features that correspond to virtualization may be visible to the user. This capability is not supported in the current release, but will be available in the future.

Checking your VCS One cluster privileges

Privileges define what actions the user can perform, such as adding a system to the VCS One cluster or modifying a service group.

When a user tries to perform an operation, VCS One authorizes the user's action against the privileges associated with the user's role(s).

To check your VCS One cluster privileges

- 1 From the VCS One console, click the **Administration** tab.
- 2 Click the **Users** tab.
- 3 In the right pane, click your login name in the **User Name** column.
- 4 In the User privilege details table, view the objects and roles associated with your login.
- 5 In the Roles Associated column, click the role to view the specific privileges granted.

A granted privilege has a check mark next to it.

See [“Reference of privileges”](#) on page 627.

Adding or deleting a user or usergroup

Defining a VCS One usergroup allows you to assign privileges and roles to a user group that is external to VCS One, for example an LDAP defined user group.

Usergroup functionality is not supported in the VCS One simulator when it is running in non-secure mode.

You may clone a usergroup if there is a usergroup already in the configuration that closely resembles the usergroup you wish to create.

Adding a user or usergroup

Add a user or usergroup via the console or the command line. You may assign one or more roles to a user or usergroup after adding it.

To add a user using the VCS One Console

- 1 From the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Users** tab.
- 3 From the **Configuration** menu, click **Add User / User Group**.
- 4 From the **Add User / Usergroup Wizard** window, click **Next** to continue.
- 5 Enter the name of the user or usergroup in the form: name@domain.
- 6 Enter the first name of the user or usergroup in the **First Name** text box. Enter the last name of the user or usergroup in the **Last Name** text box.
- 7 If using notification, enter the email address of the user or usergroup.
- 8 If using notification, enter the SNMP address of the user or usergroup.
- 9 If adding a usergroup, click the **Create a User Group** box.
- 10 In the Add User / Usergroup window, do one of the following tasks:
 - Click **Finish**
This will add the user or usergroup to the configuration.
 - Click **Next** to select the organization unit to associate with the user.
From the organization tree, select the OUValue node where you want to attach the user.
When choosing the OUValue node, keep in mind the privileges assigned to a user are valid for the node the user is attached to and all the nodes below that node in the Organization Tree.
- 11 Click **Finish**.
- 12 From the Summary window, do one of the following tasks:
 - Click **Assign Roles** to assign roles to the newly added user or usergroup. This will launch the Assign-Roles wizard.
See [“Assigning or unassigning a role and objects to a user or usergroup”](#) on page 533
 - Click **Close** to close the window

To add a user using the command line

- ◆ Use the `hauser` command with `-add` option to add user as `user@domain`
`hauser -add username@domain`

To add a usergroup using the command line

- ◆ Use the `hauser` command with the `-add` and `-usergroup` option to add usergroup as `usergroup@domain`

```
hauser -add -usergroup usergroupname@domain
```

Cloning a user or user group

Use this procedure to create a new user or user group that closely resembles a user or user group already in the configuration. Once you clone the user or user group, edit it as appropriate.

See [“Assigning or unassigning a role and objects to a user or usergroup”](#) on page 533.

To clone a user or usergroup using the VCS One console

- 1 From the VCS One console, click the **Administration** tab.
- 2 Click the **Users** tab.
- 3 In the right pane, select a user or user group to clone.
- 4 From Configuration menu, click **Clone User/UserGroup**.
- 5 In the New User or User Group Name box, enter a name for the new user or user group.
- 6 Click **OK**.

Deleting a user or usergroup

A user can not delete his or her self.

To delete a user or usergroup using the VCS One console

- 1 From the VCS One console, click the **Administration** tab.
- 2 From the right pane, click the **Users** tab.
- 3 Click the box to the left of the user or usergroup.
Locate the user or usergroup under the **User Name** heading. Use the **Table filter** to restrict the view if needed.
- 4 From the Configuration menu, click **Delete Users / User Groups**.
- 5 From the **Delete User / User groups** confirmation window, click **OK**.

To delete a user using the command line

- ◆ Use the `hauser` command with the `-delete` option.

```
hauser -delete user@domain
```

To delete a usergroup using the command line

- ◆ Use the `hauser` command with the `-delete` and `-usergroup` options.
`hauser -delete -usergroup usergroupname@domain`

Assigning or unassigning a role and objects to a user or usergroup

You can view existing roles, assign predefined roles to users or create and assign custom roles to users. Predefined roles have specific names and prescribe a specific set of operations for each role type. Custom roles allow for flexibility in defining roles specific to your environment.

When assigning roles to a user or user group, the role must be a subset of the union of all privileges of the current user and the user's associated user groups.

If you have just added a user and launched the Assign-Roles wizard, continue with assigning the role at [step 6](#) of “[To assign or unassign a role and objects to a user or usergroup using the VCS One console](#)”.

See “[Displaying roles](#)” on page 542.

See “[Adding custom roles](#)” on page 534.

To assign or unassign a role and objects to a user or usergroup using the VCS One console

- 1 From the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Users** tab.
- 3 Select the name of an existing user, or select the box to the left a user.
- 4 Click **Configuration > Assign / Unassign Roles**.
- 5 Click **Next**
- 6 In the Select Roles panel, use the following information to select roles for the user.

Add	From the Available Roles table, click the role to add to the user, and click Add . The new role appears in the Selected Roles table.
Remove	From the Selected Roles table, click the role to remove from the user and click Remove . The role is removed from the Selected Roles table.

Objects To configure the object(s) for which the user has the privileges, click the edit button in the Objects column.

In the Selected Role Details page, select the Objects or Organization Units, as appropriate. Click **OK**.

7 Click **Next > Finish > Close**.

To assign a role to a user using the command line

- ◆ Use the `hauser` command with the `-addrole` option.

The following example adds the SystemAdministrator role for three systems to `username@example.com`.

```
hauser -addrole username@example.com SystemAdministrator  
sysA sysC sysE
```

The following example adds the SystemAdministrator role to `username@example.com` for the organization unit `/Division=retail/Dept=internet`

```
hauser -addrole username@example.com SystemAdministrator  
-ou Division=retail/Dept=internet
```

To assign a role to a usergroup using the command line

- ◆ Use the `hauser` command with the `-addrole` and `-usergroup` options.

```
hauser -addrole -usergroup usergroupname rolename object
```

To delete a role for a usergroup using the command line

- ◆ Use the `hauser` command with the `-deleterole` and `-usergroup` options.

```
hauser -deleterole -usergroup usergroupname rolename object
```

Adding custom roles

VCS One provides predefined roles, but also enables you to define new roles. For example, you may want to identify roles by the name of an application, limit a role to a subset of systems, or tailor the set of operations you assign to a user.

You may clone a role if there is a role that closely resembles the role you wish to create.

See [“Cloning a role”](#) on page 536.

To add a new role with the VCS One console

- 1 From the VCS One console, click the **Administration** tab.
- 2 From the right pane, click the **Roles** tab.

- 3 From **Configuration** menu, click **Add Role**.
- 4 Specify a name for the new role. For example, *FinanceGroupOperators*.
- 5 Specify a description for the new role. For example, “*Role for finance group operators only.*”
- 6 Select a role type. For example *Group*.
- 7 The role type you select will filter the types of privilege categories available to that role.
- 8 Select the privileges for the role type. Select all privileges, specific privileges, or none.
- 9 Click **Add New Role**.
- 10 The **All Roles** view displays and shows the new role under **Role Name**.
- 11 To assign the new role to users, click **Assign / Unassign Roles** from the **Configuration** menu.
See “[Assigning or unassigning a role and objects to a user or usergroup](#)” on page 533.

To create a new role with custom privilege set with the command line

The following example shows adding a custom System type role called MySysAdmin that has a subset of system operation privileges.

- 1 Add the role using the following command:

```
harole -add MySysAdmin -type System -desc "Custom System Admin role"
```

To display the role types available, use the `harole -listtypes` command.
- 2 Define custom privileges for the new role using the following command:

```
harole -addpriv MySysAdmin S_AddSystemtoSystemList  
S_DeleteSystemfromSystemList S_FreezeSystem S_EvacuateSystem  
S_UnFreezeSystem
```

You can display all privileged operations for a role type.
See “[Displaying the permitted operations for a role type:](#)” on page 542.

To create a role with inherited privileges from the command line

In this example, the new role inherits *GroupAdministrator* role privileges but has a new role name for purposes of assigning it to specific users to perform operations on specific system objects.

- 1 Use the `harole` command with the `-add` option and the `-inherit` option.

```
harole -add MyGroupAdmin -inherit GroupAdministrator
```
- 2 Display information about the new role:

```
harole -display MyGroupAdmin
```

The display shows operations the new role permits a user to perform. The list of operations is identical to that for the *GroupAdministrator* role. Operations can be added or deleted using the `-addpriv` or `-deletepriv` option of the `harole` command.

See the *Veritas Cluster Server One Command Reference Guide*.

Cloning a role

Use this procedure to create a new role that closely resembles a role already in the configuration. Once you clone the role, edit the new role as appropriate.

See [“Editing a role”](#) on page 536.

To clone a role using the VCS One console

- 1 From the VCS One console, click the **Administration** tab.
- 2 Click the **Roles** tab.
- 3 From the All Roles table, select a role that you want to clone.
- 4 From Configuration menu, click **Clone Role**.
- 5 In the Clone role panel, in the New Role Name box, enter a name for the new role.
- 6 Click **OK**.

You may have to refresh the screen to see the new role in the All Roles list.

To clone a role using the command line

- ◆ Type the following command

```
harole -add role1 -inherit role2
```

Use the following information to replace the appropriate variables:

`role1` The name of the new role.

`role2` The name of the role that you want to clone from the configuration.

Editing a role

You may modify the list of privileges for either a custom role that you create or certain predefined roles.

See [“About roles”](#) on page 219.

To edit a role using the VCS One console

- 1 From the VCS One console, click the **Administration** tab.
- 2 Click the **Roles** tab.
All roles display in a list. Use the Table filter box to filter the results shown on the page.
- 3 Click the name of role under the **Role Name** column.
- 4 Click the **Description** link to edit the description of the role.
- 5 Click each link in the **Privilege Category** list to view the privileges available in that category for that role.
The privileges identified with checked boxes indicate the permitted operations for the role.
- 6 Check or uncheck privileges for the role.
Greyed out check boxes indicate you may not modify the list of privileges for that role. Click All to select all privileges in that privilege category.
- 7 At the far right of the window, click **Update Role**.

Deleting a role

A role may not be deleted if it is assigned to a user.

To delete a role using the VCS One console

- 1 From the VCS One console, click the **Administration** tab.
- 2 From the right pane, click the **Roles** tab.
- 3 From the All Roles table, select one or more roles that you want to delete.
- 4 From Configuration menu, click **Delete Role(s)**.
- 5 Click **OK**.
- 6 Click **Close**.

To delete a role using the command line

- ◆ Type the following command

```
harole -delete role
```

Use the following information to replace the appropriate variables:

role	The name of the role that you want to delete from the VCS One configuration.
------	--

Modifying user or usergroup settings

You may modify a user's or usergroups's name, email, and SNMP address information. To modify other user attributes, go to "[Editing user or user group attributes](#)" on page 538.

To modify user or usergroup settings using the VCS One console

- 1 From the VCS One console, click the **Administration** tab.
- 2 From the right pane, click **Users**.
- 3 Locate the user or usergroup under the **User Name** heading.
- 4 For the specified user, click the corresponding **pencil** symbol at the beginning of the row.
- 5 Modify the **First name**, **Last name**, **E-mail** or **SNMP Address**.
- 6 Click **OK**.

To modify user settings using the command line

- ◆ Use the `hauser` command with `-modify` option.
For example, if the user will receive notifications, you can modify the user's Email attribute and SnmpAddress attribute to assign values.

```
hauser -modify username@example.com Email "username@example.com"  
hauser -modify username@example.com SnmpAddress "127.0.0.1"
```

Enclose the attribute values in quotes if the values have delimiters such as "." or "@".

To modify usergroup settings using the command line

- ◆ Use the `hauser` command with `-modify` and `-usergroup` option.

```
hauser -modify -usergroup usergroupname@domain Email  
"usergroupname@domain"
```

Editing user or user group attributes

You can modify some attributes of a user. More information is available on user level attributes.

See "[User attributes](#)" on page 747.

To modify a user's attributes using the VCS One console

- 1 From the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Users** tab.

- 3 In the **All Users** table, click the user name link under the **User Name** heading.
- 4 Click the **All Attribute** link to the far right of window.
- 5 In the **All Attributes** table, click the **Edit** button for any editable attributes. You may only edit attributes of global scope from this page.
- 6 In the Edit Attribute box, type a new value in the **Value** box.
- 7 Click **OK**.

Moving a user to another Organization Tree node:

The privileges a user is given correspond to the objects, systems or service groups, at the nodes the user is attached, and all the nodes below that node in the Organization Tree.

To move a user to another organization unit node

- 1 From the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Users** tab.
- 3 Select an existing user by clicking the check box to the left of the user.
- 4 From the **Configuration** menu, click **Move Users / User Groups**.
- 5 From the **Organization Unit Selection** window, click the new OUValue node.
- 6 Consider the **Modify Privileges if move violates the assigned roles** check box.
- 7 Click **Finish**.

To move a user to another organization unit node using the command line

- ◆ Type the following command at the prompt:

```
hauser -move user@domainname -ou ounode_path
```

Enabling a user or usergroup

You can enable users or usergroups using the console or the command line. A newly added user or usergroup is enabled by default. Enabling a user or usergroup enables all the associated privileges.

To enable a user or usergroup using the console

- 1 From the VCS One console, click the **Administration** tab.
- 2 From the right pane, click **Users**.

- 3 Click the link of an existing user or usergroup from the **User Name** column.
- 4 From the **Configuration** menu, click **Enable User / User Group**.
- 5 From the **Enable User** or **Enable User Group** confirmation box, click **OK**.

To enable multiple users or usergroups using the console

- 1 From the VCS One console, click the **Administration** tab.
- 2 From the right pane, click **Users**.
- 3 In the **Users and UserGroups** window, click the box to the left of each existing user you wish to enable, or click the box in the blue heading row of the table to select all users.
You may use the **Table filter** to filter the list of users viewed.
- 4 From the **Configuration** menu, click **Enable Users / User Groups**.
- 5 From the **Enable Users / User groups** confirmation box, click **OK**.

To enable a user using the command line

- ◆ Type the following command at the prompt:
`hauser -enable user@domainname`

To enable a usergroup using the command line

- ◆ Type the following command at the prompt:
`hauser -enable -usergroup usergroup@domainname`

Disabling a user or usergroup

You can disable users in VCS One using the console or the command line. Disabling a user revokes all privileges of the user, including read privileges, without deleting the user. A disabled user will not be able to log in.

To disable a user or usergroup using the console

- 1 From the VCS One console, click the **Administration** tab.
- 2 From the right pane, click **Users**.
- 3 Click the link of the user you wish to disable from the **User Name** column.
- 4 From the **Configuration** menu, click **Disable User / User Group**.
- 5 From the **Disable User** confirmation box, click **OK**.

To disable multiple users or usergroups using the console

- 1 From the VCS One console, click the **Administration** tab.

- 2 From the right pane, click **Users**.
- 3 In the **Users and UserGroups** window, click the box to the left of each existing user you wish to disable, or click the box in the blue heading row of the table to select all users.
You may use the **Table filter** to filter the list of users viewed.
- 4 From the **Configuration** menu, click **Disable Users / User Groups**.
- 5 From the **Disable Users / User groups** confirmation box, click **OK**.

To disable users using the command line

- ◆ Type the following command at the prompt:
`hauser -disable user@domainname`

To disable a usergroup using the command line

- ◆ Type the following command at the prompt:
`hauser -disable -usergroup usergroup@domainname`

Viewing a user's or user group's settings, roles and associated objects

Perform the following steps to view a user's or user group's settings.

To view a user's or user group's settings using the console

- 1 From the VCS One console, click the **Administration** tab.
- 2 In the right pane, click the **Users** tab.
The users and usergroups are listed that are relative to the node selected in the Organization Tree in the left pane.
To filter the view, use the **Table filter** box.
- 3 Click the user name link to display the user's settings, including assigned roles and associated objects.

To view a user's or user group's settings using the command line

- ◆ Type the following command to display a user.
`hauser -display user@domainname`
- ◆ Type the following command to display a user group.
`hauser -display -usergroup user@domainname`

Displaying roles

You can view both predefined and custom-created roles.

To display roles using the console

- 1 From the VCS One console, click the **Administration** tab.
- 2 From the right pane, click the **Roles** tab.
All roles display in a list. To filter the view to find a specific role, use the **Table filter** box.
- 3 Click the name of role under the **Role Name** column.
View the role name, role type, and description. The privileges identified with checked boxes indicate the permitted operations for the role.
- 4 Click each link in the **Privilege Category** list to view the privileges available in that category for that role.

To display roles using the command line

- ◆ Type the following command to display the list of custom-created roles and pre-defined roles:

```
harole -list -all
```

To display information about a role using the command line

- ◆ Type the following command to display information about a role:

```
harole -display MySysAdmin
```

Included in the output are the operations the role permits a user to perform.

Displaying role types

To display role types

- ◆ User the harole command to display the role types, or privilege categories.

```
harole -listtypes
```

Displaying the permitted operations for a role type:

- ◆ User the harole command to list the permitted operation for a role type.

```
harole -listoperations -type system
```

The display lists all privileged operations for the system role type in VCS One, with output lines similar to the following example.
S_AddSystemtoSystemList
S_DeletSystemfromSystemList
S_FreezeSystem

Note that privileges are denoted as operations prefixed with a letter that indicates the role type.

[Table 28-1](#) denotes the prefix and the corresponding role type.

Table 28-1 Role prefix and corresponding role type

Prefix of role	Role type
F	Cluster
S	System
V	Frame (future functionality)
O	Object
G	Group
R	Resource
U	User
O	Organization tree
N	Notifier
A	Automation
C	Composite Service Group

Authenticating VCS One users

In VCS One, you can issue commands to perform tasks associated with your assigned roles. To ensure security in a VCS One environment, a user executing a command requires a credential acceptable to the Policy Master. A VCS One user is one who has been added by the administrator or is part of a usergroup that has been added to the VCS One configuration.

Authentication in a VCS One environment is controlled by the Symantec Product Authentication Service (AT). The Policy Master, the VCS One clients, and the services obtain credentials from the authentication broker running on the Policy Master system. These credentials enable secure communication between users and services in the VCS One cluster.

For information about supported authentication service types and setting up authentication plug-ins in a VCS One environment, see the *Veritas Cluster Server One Installation Guide*.

Issuing commands from the command line

In VCS One, you may issue commands from different contexts, depending on your identity and domain type. The context of a logged-in user is the default user context on an VCS One cluster system. Some logged-in users may already have credentials to issue commands, others may not.

Logged-in users may authenticate with the authentication broker and obtain a credential, enabling them to successfully issue VCS One commands from client systems using the following methods:

- Use the `-user` and `-domaintype` options with each command to specify the user profile. For example:

```
hasys -display SysC -user user@domain -domaintype unixpwd
```

Accepted values for `-domaintype` *domaintype* are `unixpwd`, `nis`, `nisplus`, `ldap`, `pam`, and `vx`. These values are case sensitive.

You will be prompted for a password for the first time you issue the command. You will not be prompted for a password for the next 24 hours, after which you will be required to re-enter the password.

See “[Issuing commands with an explicit user profile](#)” on page 544.

- Set `VCSONE_USERNAME` and `VCSONE_DOMAINTYPE` environment variables on the client system to specify the user’s profile. The first VCS One command issued after setting these variables requires a user password. Subsequently, a user may execute commands without the `-user` and `-domaintype` options until the credential expires.

See “[Issuing commands with environment variables set](#)” on page 545.

- Use the `halogin` command to specify an explicit user profile to store, along with a credential, in the user’s home area, and use as a default context. After running `halogin`, you may issue commands from the system without having to use the `-user` and `-domaintype` options or having to enter passwords for a duration, typically 24 hours. The default context set by `halogin` may be overridden using the `-user` and `-domaintype` options or by resetting the environment variables. The order of preference for determining the user context is:

`-user/-domaintype` option *over* environment variables *over* `halogin`

See “[Issuing commands using halogin](#)” on page 545.

Issuing commands with an explicit user profile

Perform the following steps to issue commands with an explicit user profile.

To issue commands with an explicit user profile

A VCS One user can enter a command by providing a fully qualified domain user name, a valid domain type, and a password when prompted. In the following

example, a VCS One user, *username@example.com* of a valid domain type *unixpwd*, with SystemAdministrator privileges can enter a command to freeze a system:

- 1 Enter the command, providing the user and domain type information:

```
hasys -freeze [-evacuate] sys [-user username@domainname]  
[-domaintype domaintype]
```

For example:

```
hasys -freeze SysA -user username@example.com -domaintype  
unixpwd
```

- 2 When prompted, enter the password for the user.

Issuing commands with environment variables set

Perform these steps on all systems from where you wish to run VCS One commands.

To issue commands with environment variables set

- 1 Set the `VCSONE_USERNAME` and `VCSONE_DOMAINTYPE` environment variables. For example:

```
export VCSONE_USERNAME=username@example.com  
export VCSONE_DOMAINTYPE=unixpwd
```

- 2 Issue the VCS One command. For example:

```
hasys -freeze SysA
```

- 3 If prompted, enter the password for the user.

Issuing commands using halogin

Use the `halogin` command on all systems from where you wish to run VCS One commands. You should obtain the user credentials, issue the VCS One commands, and delete the user credentials. The obtained credentials are typically valid for 24 hours.

The user with login *username* should have an account on all systems that will host the Policy Master. You do not have to be logged in with the same username as you are using with `halogin`.

To obtain a credential by using halogin

- 1 Enter the `halogin` command, providing a fully qualified user name and domain type. For example:

```
halogin -user username@name_of_PolicyMaster.example.com  
-domaintype unixpwd
```

- 2 You are prompted to enter the password. Use the password for the username account on the Policy Master.

You may also include the password using the `-passwd` option in the original command, for example:

```
halogin -passwd password -user username@example.com  
-domaintype unixpwd
```

You obtain the credentials after the command is successful. These credentials are stored in the `.vcsoneprofile` file, in the user's home directory, on the system where the command was run. This user profile is used for communicating with the Policy Master.

To end the halogin session

- ◆ Type the following command at the prompt:

```
halogin -endsession IP_address_of_Policy_Master
```

For example:

```
halogin -endsession 192.168.10.15
```

Usually the Policy Master IP address is a virtual IP address.

Issuing commands through a script from client systems

A user with the appropriate privileges can create users with credentials to issue commands from within scripts on client systems. Typically, logged-in users have a credential that expires in 24-hours, whereas users who can run commands from within scripts may require long-term credentials.

To obtain long-term credentials, the user must be added to the cluster private domain repository (PDR).

For instructions about how to add a user to the cluster private domain for any of the authentication service types supported by VCS One, see “Setting up authentication plug-ins in VCS One” in the *Veritas Cluster Server One Installation Guide*.

Thereafter, the user with the credential can authenticate by using one of the following methods:

- Running halogin to set up the user profile
- Including the `-user` and `-domaintype` options with the commands from within the scripts
- Setting the environment variables within the scripts

To run commands from within a script with authentication

The following methods are available to run commands from within a script with authentication:

- Method 1 – Include `-user` and `-domaintype` options with each command in the script.

See [“Issuing commands with an explicit user profile”](#) on page 544.

- Method 2 – Before running the scripts, create a user profile on the system for the user in whose context the scripts will be run. With profile set, the user can run the scripts and the commands are authenticated. See [“Issuing commands using halogin”](#) on page 545.
- Method 3 – Use environment variables.

Administering sets of objects

This chapter includes the following topics:

- [About administrating sets of objects](#)
- [Building a set](#)
- [Viewing objects in a set](#)
- [Viewing the details of a set definition](#)
- [Deleting a set](#)
- [Modifying a set](#)
- [Configuring a custom view of the organization tree and extended attributes](#)
- [Deleting a custom view](#)
- [Modifying a custom view](#)

About administrating sets of objects

A set specifies a collection of VCS One objects. Valid objects to include in a set are systems or service groups.

You should have at least one of the following structures in use before you define a set:

- An Organizational Tree structure defined.
See [“About users and the Organization tree”](#) on page 221.
- Extended attributes defined and assigned value for system or service group objects.
See [“About extended attributes”](#) on page 517.

Administering sets features that correspond to virtualization may be visible to the user. This capability is not supported in the current release, but will be available in the future.

Building a set

A set is a named collection of systems and service groups.

A set is created using a combination of OUValue nodes in the organization tree and extended attributes. You may create a set using the procedure in this topic or by applying table filters and using the Save as Set button.

See [“Filtering results in a table”](#) on page 115.

This named set expression is stored in the Policy Master database, specific to the user that defines it. The user that creates the set name must have the proper permissions configured to see all of the OrgTree specified by the OUValuePath.

- OUvalue node
An OUValue nodes is represented by an organization tree path. The set is defined as all systems or groups that are at this node unless extended attribute are used to further filter the selection criteria.
An organization tree path is denoted by a list of OUName=OUValue pairs, separated by a forward slash (/).
For example, a sample organization tree path could be:
LOB=Enterprise/Division=WebHosting/Department=Engineering
- Extended attributes
Extended attributes can be combined with the AND or the OR logical operator.

When using a set expression as part of a predefined attribute definition, explicitly specify an OUValuePath.

To build a set using the VCS One console

- 1 In the VCS One console, click the **Administration > Sets**.
- 2 Click **Configuration > Add Set**.
- 3 Click **Next**.
- 4 In the Add Set panel, use the following information to fill in the fields:

Name	The name of the set.
Description	A description for the set.
OU Expression	To add an OUValue node to the set, enter an OUValue node path in this text box. You may also click the edit ellipse to select an OUValue node from the organization tree view. Click OK to return to the Add Set panel.
EA Expression	To add an extended attribute expression to the set, enter an expression in the text box. You may also click the edit ellipse to build an extended attribute expression. Click OK to return to the Add Set panel.

- 5 Click **OK** to create the set.
- 6 Click **Add Custom View** to create a custom view for the newly created set or click **Close** to finish the wizard.
See [“Configuring a custom view of the organization tree and extended attributes”](#) on page 553.

To build a set using the command line

- ◆ You can specify a set with a name by typing any of the following commands at the command prompt:

```
haset -add set_name -ea expression
haset -add set_name -ou expression
haset -add set_name -ea expression -ou expression
```

where

set_name is the name of the set

expression is a expression using extended attributes or using an OrgTree path, as appropriate to the flag.

for example:

```
haset -add UKRetailSolaris -ou "LineofBusiness=Retail" -ea
"OSname=Solaris AND Location=London"
```

Would allow you to replace the command:

```
hasys -display -ou "LineofBusiness=Retail"
-ea "OSname=Solaris AND Location=London"
```

with the command:

```
hasys -display -setname UKRetailSolaris
```

Viewing objects in a set

Use this procedure to view the objects in a set.

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Service Groups** tab to display the service groups in the set
- 3 Click the **Systems** tab to display the systems in the set.
- 4 In the left pane, click the name of the set from the drop down menu.

Viewing the details of a set definition

The following information displays when you view a set:

- Name
- Description
- Associated OU expression
- Associated extended attributes expressions
- Custom view defined for the set

To view the details of a set with the console

- 1 In the VCS One console, click **Administration > Sets**.
- 2 In the right pane, click the link that is the name of the set you wish to view.

To view the details of a set with the command line

- ◆ Type the following at the command prompt:

```
haset -display SetName
```

To view the details of all sets that you have the permissions to display

- ◆ Type the following at the command prompt:

```
haset -display
```

Deleting a set

Deleting a set removes it from the Policy Master database.

To delete a set using the VCS One console

- 1 In the VCS One console, click the **Administration > Sets**.
- 2 Check one or more sets that you wish to delete.
- 3 Click **Configuration > Delete Set(s)**.
- 4 Click **OK**.
- 5 Click **Close**.

To delete a set using the command line

- ◆ Type the following at the command prompt:

```
haset -delete SetName
```

Modifying a set

To modify a named set with the console

- 1 In the VCS One console, click the **Administration > Sets**.
- 2 In the right pane, click the link that is the name of the set you wish to modify.
- 3 In the **Configuration** menu, click **Modify Set**.
You may also right click the name of the set in the left pane, and click Edit.
- 4 In the **Modify Set** window, you may modify the **Description**, **OU Expression** or **EA Expression** related to the set.
- 5 Click **OK**.

To modify a named set with the command line

- ◆ Type the following at the command prompt:

```
haset -modify setname attribute value
```

Configuring a custom view of the organization tree and extended attributes

A custom view allows you to create a specialized view for a given set. Custom views can be used to organize objects under a set by filtering the view using organization units and extended attributes.

View the custom view in the tree under the set name in the left pane of the console. The custom view displays the selected expressions in the order that they are listed in the custom view definition.

To configure a custom views using the VCS One console

- 1 In the VCS One console, click the **Administration > Sets**.
- 2 In the right pane, click the name of the set for which you wish to add a custom view.
- 3 From the Configuration menu, click **Add Custom View**.
- 4 Click **Next**.
- 5 Fill in the **Add Custom View** window text box with the following values:

Name	Name of the custom view
Description	Description of the custom view
Type	Click one of the following choices: Group: The custom view is associated with service groups. System: The custom view is associated with systems. OU: The custom view is associated with organization units
Extended Attributes or Organization Tree	The left table lists different text depended in the Type selected: Group: The group extended attributes are listed System: The system extended attributes are listed OU: The Organization Tree is displayed Click the objects in the left table that you wish to have in your custom view. Click the right arrow to move the selections to the Selected Expression table.
Selected Expression	Lists the selected expressions or organization units for the custom view. To remove a selection, click the expression and click the left arrow. The custom view displays the selected expressions in the order that they are listed in this table. To move a selection higher in the table: Click the up arrow. To move a selection lower in the table: Click the down arrow.

- 6 Click **OK**.
- 7 Click **Close**.
The custom view is presented in the form of a tree under the set name in the left pane of the console.

Deleting a custom view

When you delete a custom view, it is removed from the VCS One configuration.

To delete a custom view

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Sets** tab.
- 3 Click the name of the set for which you wish to delete a custom view.
- 4 From the **Custom Views defined** table, check the custom view you wish to delete.
- 5 Click **Configuration > Delete Custom View**.
- 6 Click **OK**.
- 7 Click **Close**.

Modifying a custom view

Use this procedure to make changes to an existing custom view.

To modify a custom view

- 1 In the VCS One console, click the **Administration > Sets**.
- 2 Click the link that is the name of the set for which you wish to modify a custom view.
- 3 From the **Custom Views defined** window, find the name of the custom view you wish to modify under the **Name** column.
- 4 Click the pencil icon to edit.
- 5 Fill in the **Modify Custom View** window text box with the following values:

Name	Name of the custom view. You may not modify this field.
Description	Description of the custom view
Type	Click one of the following choices: Group: The custom view is associated with service groups. System: The custom view is associated with systems. OU: The custom view is associated with organization units

Extended Attributes or Organization Tree	<p>The left table lists different text depended in the Type selected:</p> <p>Group: The group extended attributes are listed</p> <p>System: The system extended attributes are listed</p> <p>OU: The Organization Tree is displayed</p> <p>Click the objects in the left table that you wish to have in your custom view. Click the right arrow to move the selections to the Selected Expression table.</p>
Selected Expression	<p>Lists the selected expressions or organization units for the custom view.</p> <p>To remove a selection, click the expression and click the left arrow.</p> <p>The custom view displays the selected expressions in the order that they are listed in this table.</p> <p>To move a selection higher in the table, click the up arrow.</p> <p>To move a selection lower in the table, click the down arrow.</p>

6 Click **OK**.

7 Click Close.

The custom view displays in the form of a tree under the set name in the left pane of the console.

Tasks: Administering the Veritas Cluster Server One product

This section includes the following chapters:

- [“Administering the Policy Master service group”](#) on page 559
- [“Administering the VCS One cluster configuration database”](#) on page 565.
- [“Troubleshooting VCS One issues”](#) on page 581.

Administering the Policy Master service group

This chapter include the following topics:

- [About administering the Policy Master service group](#)
- [About the Policy Master service group](#)
- [Monitoring the state of the Policy Master service group](#)
- [Tuning attributes of the Policy Master service group](#)
- [Bringing the PMSG online](#)
- [Taking the PMSG offline](#)

About administering the Policy Master service group

Some administration tasks require the Policy Master service group to be offline. See [“Taking the PMSG offline”](#) on page 563.

You can configure notification to be sent if certain events happen to the Policy Master service group.

See [“Policy Master events reference”](#) on page 645.

Information regarding installation and uninstallation of the Policy Master service group is available.

See *Veritas Cluster Server One Installation Guide*.

About the Policy Master service group

The resources in the policy master service group vary depending on whether you use Storage Foundation-based or NFS-based storage for the configuration database.

[Table 30-1](#) describes the resources in Policy Master service group when the Policy Master uses Storage Foundation for storing configuration information.

Note: If you are using local-dir, the `pmdg`, `pmvol`, or `pmmount` resources may not exist. If you are using Network Appliance filer, the `pmdg` resource may not exist.

Table 30-1 PMSG resources when the Policy Master uses Storage Foundation

Resource	Description
<code>pmip</code>	Policy Master virtual IP address
<code>pmnic</code>	Policy Master virtual IP NIC device
<code>vcsonedb</code>	VCS One database
<code>pm</code>	Policy Master daemon
<code>vxss</code>	Symantec Product Authentication Service daemon
<code>VCSOneWeb</code>	VCS One web console
<code>pmdg</code>	The database and repository disk group
<code>pmvol</code>	The volume for the file system containing the database
<code>pmmount</code>	The file system mount point

Table 30-2 describes the resources in the Policy Master service group when the Policy Master uses NFS for storing configuration information.

Table 30-2 PMSG resources when the Policy Master uses NFS

Resource	Description
pmip	Policy Master virtual IP address
pmnic	Policy Master virtual IP NIC device
vcsonedb	VCS One database
pm	Policy Master daemon
atd	Symantec Product Authentication Service daemon
pmmount	Mount point for the volume/qtree exported from NetApp filer when NFS is selected for shared storage
pmexport	Exports and deports the volume/qtree on NetApp filer to active and passive Policy Master nodes, respectively
pmfiler	Monitors ICMP connectivity between the Policy Master and the NetApp filer
VCSOneWeb	VCS One web console

Monitoring the state of the Policy Master service group

The Policy Master service group has the following states:

- **ONLINE**
The Policy Master service group is running as expected.
- **OFFLINE**
The Policy Master service group is not running
- **UNKNOWN**
The agent is not able to determine if the Policy Master process is running or not. For example, if insufficient memory is available, the Policy Master agent fails to function and declares an UNKNOWN state.

To monitor the state of the Policy Master agent using the command line

- ◆ Type the following command to display the status of the groups configured in the VCS Policy Master cluster

```
/opt/VRTSvcs/bin/hagrp -state
```

- ◆ Type the following command to display the status of the resources configured in the VCS Policy Master cluster

```
/opt/VRTSvcs/bin/hares -state
```

Tuning attributes of the Policy Master service group

Depending on your configuration, you may decide to change the default values of the attributes of the Policy Master service group (PMSG).

Use the following information to determine whether you need to tune the attributes of resources in the Policy Master service group

Tuning the DetailMonitoring attribute of the Policy Master resource

The DetailMonitoring attribute determines the monitor type and frequency for the Policy Master resource in the PMSG. Detail monitoring is also called second-level monitoring.

In some cases, the Policy Master monitor action may not return in the allocated time configured in the MonitorTimeout interval. This may result in the agent declaring the Policy Master resource OFFLINE when it is not.

Tune this attribute to a higher number if you have monitor time out issues on the Policy Master resource. This may be caused by a VCS One cluster with thousands of resources, where the Policy Master system is heavily loaded. Or any reason that the Policy Master system has less capacity for processing.

See [“DetailMonitoring”](#) on page 563.

Table 30-3

VCS One cluster Attribute	Description
DetailMonitoring	<p>Determines the monitor type and frequency for the Policy Master resource in the PMSG. Set the value with consideration to the system load.</p> <p>See “Tuning the DetailMonitoring attribute of the Policy Master resource” on page 562.</p> <p>The following values are valid for this attribute:</p> <p>0 – the agent checks if the Policy Master resource is running every monitor cycle.</p> <p>N – where N is an integer, the agent checks if the Policy Master resource is running every monitor cycle. In addition, checks if the resource is responding every Nth monitor cycle using the haddebug -pingnw command.</p> <p>Default value = 1</p> <p>You may edit the value of this attribute using the haattr -modify command.</p>

Bringing the PMSG online

The PMSG must be online in order for VCS One to manage your applications.

To bring the PMSG online using the command line

- ◆ Type the following command
`/opt/VRTSvcs/bin/hagrp -online -sys vcs_PM_cluster_system`

Taking the PMSG offline

To take the PMSG offline using the command line

- ◆ Type the following command
`/opt/VRTSvcs/bin/hagrp -offline -sys vcs_PM_cluster_system`

Administering the VCS One cluster configuration database

This chapter includes the following topics:

- [About the VCS One configuration](#)
- [About the configuration files](#)
- [Starting the Policy Master in Cold mode](#)
- [Managing the configuration database](#)
- [Backing up and restoring VCS One data](#)

About the VCS One configuration

VCS One maintains the VCS One cluster configuration information in a highly-available configuration database. When VCS One is first installed, the database is created and initialized. At this point, the database is empty; it contains no VCS One cluster configuration.

The database is populated with a VCS One cluster configuration using one of the following methods:

- Create VCS One cluster objects with the VCS One console (GUI)
- Create VCS One cluster objects using commands with the command line interface (CLI)
- Load a pre-existing configuration from XML files or a previous backup of a VCS One database.

During each VCS One cluster startup, the Policy Master obtains configuration information from the configuration database. When changes are made to the VCS One cluster configuration, they are stored in the database. You can back up the configuration database or export the database information to XML-formatted files.

Exporting the configuration database to XML-formatted files can be a powerful tool when used along with the VCS One simulator. The simulator can be used to create and test a VCS One cluster configuration. Once the testing is complete with the simulator, the configuration database can be exported to XML files. Those XML files can be loaded into an actual VCS One database. Similarly, you can export a live VCS One configuration database to XML-formatted files and import those XML files to the simulator to test VCS One cluster operations.

About the configuration files

The VCS One configuration is stored in a configuration database. The configuration database can not be edited directly, but you can import it from or export it to the following files:

ext/bpa.xml	Define the instances of business and notification rules, jobs, and automation settings.
main.xml	Defines the instances of specific objects in the VCS One cluster, including the system, service group, and resource objects. The definable attributes for these instances come from the types.platform.xml and vcsone.xml files.
vcsone.xml	Defines the attributes for specific object types in the VCS One cluster, including the cluster, group, system, user, user group, and user role objects. Do not edit this file.
ext/prefs.xml	Defines the user preferences and custom views.
AgentTypes.xml	Defines Types specific to the agent <i>Agent</i> , such as OracleTypes.xml for the Oracle agent.
otherTypes.xml	Used only with the simulator.
orgtree.xml	Defines the Organization tree structure and extended attribute definitions in the configuration.
simuser.xml	Used only with the simulator.
types.platform.xml	Defines bundled Resource Types. Resource Types are a template that define a set of attributes and default values for controlling a resource object, such as Mount or NIC. See “ About the types file ” on page 568. The following files are examples of these files: <ul style="list-style-type: none">■ types.win.xml■ types.hpux.xml■ types.aix.xml■ types.sun.xml■ types.sunx86.xml■ types.linux.xml

Location of the configuration files

In an actual VCS One installation, these files reside in the following directory:

`$VCSONE_CONF/conf/confxml`

The default path is:

```
/etc/VRTSvcSone/conf/conf.xml
```

For the VCS One Simulator, the configuration files are located in the following directory:

```
installed_location\VCSOne\Simulator\conf
```

where *installed_location* is the location where the Simulator is installed.

If the Simulator is installed in the default location, the configuration files are located here:

```
C:\Documents and Settings\UserName\Desktop\VCSOne\  
Simulator\conf
```

More information is available on how the configuration is used in the VCS One cluster.

See [“How the Policy Master and the VCS One clients start up”](#) on page 54.

More information is available on administration of the configuration.

See [“Managing the configuration database”](#) on page 571.

About the types file

The types *platform.xml* file contains the types definition, which are used for the following functions:

- To define the set of attributes that control that type of object.
- To define the default values of each attribute.
- To define the type of values that may be set for each attribute.
In the DiskGroup example, the NumThreads and OnlineRetryLimit attributes are both classified as integer. The DiskGroup, StartVolumes, and StopVolumes attributes are defined as strings. In the IP example, the Address attribute is classified as string.
- To define the parameters passed through the ArgList attribute.
The line `static str ArgList[] = { xxx, yyy, zzz }` defines the order in which parameters are passed to the agents for starting, stopping, and monitoring resources. The sequence of arguments indicates the online command, the name of the resource, then the contents of the ArgList. Since MonitorOnly is not set, it is passed as a null. This is always the order: command, resource name, ArgList.

The following text shows the correlation between the names of the Type file and the name of the platform(s) represented.

Table 31-1 Platform-related type files and corresponding platform support

Type file	Platform support
types.aix.xml	AIX, AIX/RS6000
types.hpux.xml	HPUX/IA64, HPUX/PA
types.linux.xml	Linux, Linux/x86 RHEL and SLES x86 and x86_64
types.sun.xml	Solaris/sparc
types.sunx86.xml	Solaris/x86 or Solaris/x64

Starting the Policy Master in COLD mode

In cold start mode, the Policy Master enforces the configuration in the configuration database, but does not enforce state information. The Policy Master probes all resources on all systems, determines their current state, and accepts that state as the correct state. Any existing GTQ entries are eliminated. This mode is used when you do not want to treat new state information as a fault.

See “[Cold start up mode](#)” on page 55.

The procedure to start the Policy Master in COLD mode differs depending on the state of the Policy Master cluster.

To start the Policy Master in cold mode when the Policy Master cluster is down

- 1 Start the machine running the Policy Master service group (PMSG) in single-user mode.
This is to avoid running VCS and to have the PMSG remain offline.
- 2 Edit the PM resource in the main.cf file in the Policy Master VCS cluster.
- 3 Use your favorite editor to set the Mode attribute to cold in the PM resource. The change appears similar to the following example:

```
PM PM_resource_name(
    StartProgram = "/opt/VRTSvcsone/bin/vcsoned"
    StopProgram = "/opt/VRTSvcsone/bin/hastop.bin -pm -block"
    MonitorProcess = "/opt/VRTSvcsone/bin/vcsoned.bin"
    Mode = "-cold"
```

- 4 Boot the machine running the PMSG to multi-user mode so that VCS and PMSG start up
- 5 Optionally, type the following command to modify the Mode attribute back to normal using the VCS command line

```
haconf -makerw
hares -modify pm Mode ""
haconf -dump
```

To start the Policy Master in COLD mode when the Policy Master cluster is running but the Policy Master service group is in the OFFLINE state.

- 1 Type the following command to modify the Mode attribute of the PM resource to the value COLD.

```
hastart -pm -cold
```

- 2 Bring the PMSG online.

See “[Bringing the PMSG online](#)” on page 563.

- 3 Optionally, type the following command to modify the Mode attribute back to normal using the VCS command line.

```
haconf -makerw
hares -modify pm Mode ""
haconf -dump
```

Managing the configuration database

To manage the configuration database, you perform administrative tasks on the database, such as start, clean, seed, and stop.

Note: Under most circumstances you will not need to manage the configuration database.

Starting the database

Starting the database starts the database processes.

To start the database

- ◆ At the command prompt, type the following:

```
hadb -up [-quiet|-verbose]
```

If you execute this command after the database has started, an information message is displayed, which states that the database is already started.

Cleaning the database

Cleaning the database entails flushing the database. The best practice is to clean the database before loading the VCS One cluster configuration. Stop the Policy Master before cleaning the database.

To clean the database

- ◆ At the command prompt, type the following:

```
hadb -cleandb [-quiet|-verbose]
```

You can also clean the database using the `haconf` utility before loading the VCS One cluster configuration into the database.

More information is available about the `hadb` command.

See the *Veritas Cluster Server One Command Reference Guide*.

Caution: Use this command with care. Cleaning the database flushes the existing data and creates a blank database.

Verifying the configuration

Verifying the database configuration involves validating the configuration information present in the XML files before loading it into the database, or validating the database itself.

To verify the configuration

- ◆ At the command prompt, type the following:

```
haconf -verify location of .xml config files
```

To verify the configuration after loading it into the database

- ◆ At the command prompt, type the following:

```
haconf -verify -db
```

Seeding the database using XML files

Seeding the database using XML files entails reading the configuration information stored in the XML files and writing it to the database.

Use this command if you have an XML backup of the database configuration which you want to load. Information about backing up the configuration database is available.

See [“Backing up the VCS One configuration database”](#) on page 575.

To seed the database using XML files

- ◆ At the command prompt, type the following:

```
hadb -loaddb [-quiet|-verbose]
```

The `hadb` utility reads the configuration information from the XML files located at `$VCSONE_CONF/conf/conf.xml`. You can also seed the database using the `haconf` utility.

Seeding the database using existing database files

Seeding the database using existing database files entails reading and using the configuration information stored in existing database files. These database files comprise the database file itself and the database transaction log files.

Use this command if you have a backup of the database configuration which you want to load. Information about backing up the configuration database is available.

See “[Backing up the VCS One configuration database](#)” on page 575.

To seed the database using existing database files

- ◆ At the command prompt, type the following:

```
hadb -reloaddb db_file_dir [-quiet|-verbose]
```

Here, *db_file_dir* is the location of the existing database and transaction log files.

Stopping the database

Stopping the database stops the configuration database along with its processes. Ensure that you stop the Policy Master before stopping the database.

To stop the database

- ◆ At the command prompt, type the following:

```
hadb -down [-quiet|-verbose]
```

If you execute this command after the database has stopped, an information message is displayed, which states that the database is already stopped.

Restarting the database

Restarting the database stops and starts the configuration database. Ensure that you stop the Policy Master before restarting the database.

To restart the database

- ◆ At the command prompt, type the following:

```
hadb -restart [-quiet|-verbose]
```

Viewing the database status

Viewing the database status enables you to determine if the database is currently running or not running and if it is loaded or clean.

The database status command returns one of the following messages:

- The database engine is not running. Start the database engine.

- Database engine is RUNNING and configuration is not loaded.
- Database engine is RUNNING and loaded with configuration /xxx/yyy/zzz

To view the database status

- ◆ At the command prompt, type the following:

```
hadb -status
```

Changing the database password

Change the database password using the `hadb -dbpasswd` command.

Then copy the `odbc.ini` file (located at `/etc/VRTSvcsone/odbc.ini`) to all the other Policy Master cluster nodes.

Caution: Initializing the database creates a blank database.

To change the database password

- ◆ At the command prompt, type the following:

```
hadb -dbpasswd [-quiet | -verbose]
```

Initializing the database

Caution: Use the database initialization command with extreme care. Under normal circumstances you will not need to initialize the database. One possible case when you might have to use this command is when the database is corrupt and you do not have a backup database.

When the database is initialized, VCS One creates a blank database (`vcsone.db` and `vcsone.log`) and resets the database password to its default value. After the database is initialized, if you want to change the database password, start the database.

To start the database, use the `hadb -up` command. Change the database password using the `hadb -dbpasswd` command, and then copy the `odbc.ini` file (located at `/etc/VRTSvcsone/odbc.ini`) to all the other Policy Master cluster nodes.

For the VCS One Simulator instance using the default configuration, the database location is:

```
installed_location\VCSOne\Simulator\multisim\default\  
conf\db\vcstone.db
```

where *installed_location* is the location where the Simulator is installed.

If the VCS One Simulator instance is installed in the default location, the database location is:

```
C:\Documents and Settings\UserName\Desktop\VCSOne\  
Simulator\multisim\default\conf\db\vcstone.db
```

The database location for other Simulator instances that are not using the default configuration is:

```
installed_location\VCSOne\Simulator\multisim\  
instance_name\conf\db\vcstone.db
```

To initialize the database

- ◆ At the command prompt, type the following:

```
hadb -initdb [-quiet|-verbose]
```

Warning: Use this command with care. Initializing the database creates a blank database.

Backing up and restoring VCS One data

Backing up and restoring VCS One data includes the following activities:

- See [“Backing up the VCS One configuration database”](#) on page 575.
- See [“Restoring the VCS One configuration database”](#) on page 577.
- See [“Backing up Symantec Product Authentication Service configuration information”](#) on page 578.
- See [“Restoring Symantec Product Authentication Service configuration information”](#) on page 578.

Backing up the VCS One configuration database

Backing up the database entails creating an additional, secondary copy of the entire database. Symantec highly recommends to periodically back up the configuration database.

You can back up the database in the following ways:

- Offline backup

Copy the database files, `vcstone.db` and `vcstone.log` when the database server is not running.

- Online backup
Copy the database files when the database server is running. Online backup can be a “full” or an “incremental” backup.
See “[Full and incremental backups](#)” on page 576.
- XML backup
Back up the database configuration to XML files.
See “[XML backup](#)” on page 576.

XML backup

An XML backup involves backing up the database configuration to XML files. Refer to the documentation for the `hadb` and `haconf` utilities in the *Veritas Cluster Server One Command Reference Guide*.

To back up the database to XML files

- ◆ At the command prompt, type the following:

```
haconf -dbtoxml backup_dir [-quiet|-verbose]
haconf -loadddb [-force] backup_dir
```

Here, `backup_dir` is the location where the backed-up XML files are created.

Full and incremental backups

A full backup is an online backup that backs up the entire database, that is, all database files and transaction log files. Restoring from such backups is easier and quicker as it involves restoring all the backed up files. However, backing up the entire database can take a lot of storage.

Incremental backup is also an online backup that backs up only the transaction log files. As a result, an incremental backup must be preceded by a full backup. The time taken to restore from an incremental backup depends on the time since the last full backup.

Both full and incremental backups have their advantages. Hence, Symantec recommends using both the options to intelligently backup your configuration database. For example, you could do a full backup once a week and backup the transaction log files during the week.

Restoring the database involves restoring or retrieving data from a previously backed up database.

See “[Restoring the VCS One configuration database](#)” on page 577.

To perform a full database backup

- ◆ At the command prompt, type the following:

```
haadmin -backup -db fullpathname_backup_dir
```

Here, *fullpathname_backup_dir* is the location where the backed up database and transaction log files are created.

To perform an incremental database backup

- ◆ At the command prompt, type the following:

```
haadmin -backup -db -incremental fullpathname_backup_dir
```

Here, *fullpathname_backup_dir* is the location where the backed up database and transaction log files are created.

You can perform an incremental database backup only after performing a full database backup.

Restoring the VCS One configuration database

Restoring the database involves restoring or retrieving data from a previously backed-up database.

Ensure the Policy Master service group is offline.

Before you load a configuration from XML, the cluster must have the ClusterName attribute defined. To define the ClusterName attribute, add a <cluster> tag definition in the main.xml file.

The following text is an example ClusterName definition from the main.xml file.

```
<cluster name="Test_Farm">
<attributes>
  <attribute name="DefaultPlatform"><scalar>linux/x86</scalar>
  </attribute>
</attributes>
</cluster>
```

To restore the database

- ◆ At the command prompt, type the following:

```
haadmin -restore -db fullpathname_backup_dir
```

Here, *fullpathname_backup_dir* is the location of the backed up database and transaction log files from which data is restored.

Symantec recommends that you perform a full database backup to a different directory, after successfully restoring it.

Backing up Symantec Product Authentication Service configuration information

You can back up the Symantec Product Authentication Service (AT) configuration information and data using the `haadmin` command. Backing up the AT configuration information entails creating a second copy of the configuration information.

Back up the authentication configuration information from the active Policy Master system. The active Policy Master system is the one that has the Policy Master service group online.

In the event of a Policy Master cluster failure, you can use the backup to restore the security information to the last known good state.

To back up authentication configuration information

- 1 Ensure that the `vcsonesatd` process is up and running.
- 2 Back up the authentication configuration information. At the command prompt, enter the following command:

```
# /opt/VRTSvcsone/bin/haadmin -backup -vss backup_directory_name
```

This command creates a compressed backup file called `vcsones_vxssbackup.tar` that contains the authentication service configuration information and data. If a file named `vcsones_vxssbackup.tar` already exists, it is renamed with the suffix `.old`.

Restoring Symantec Product Authentication Service configuration information

You can restore Symantec Product Authentication Service (AT) configuration information using the `haadmin` command. The restore operation enables you to retrieve and reconstruct the VCS One authentication configuration information from the backup.

The back up and restore directory structure of the mount point should be the same.

Restore the authentication configuration to the active Policy Master cluster system. The active Policy Master system is the one that has the Policy Master service group online.

To restore the authentication configuration information

- 1 Enter the following command on the active Policy Master node to stop the authentication daemon, `vcsonesatd`.

```
# /opt/VRTSvcsone/bin/hares -offline atd
```

- 2 Ensure that the shared storage is mounted. Use the mount point that you specified during the Policy Master installation.
- 3 Restore the authentication configuration information that was backed up earlier. At the command prompt, enter the following command:

```
# /opt/VRTSvcsone/bin/haadmin -restore -vss \  
backup_directory_name
```

- 4 Start the `vcsoneatd` process. At the command prompt, enter the following command:

```
# /opt/VRTSvcsone/bin/vcsoneatd
```


Troubleshooting VCS One issues

This chapter includes the following topics:

- [About VCS One log messages](#)
- [Troubleshooting VCS One issues](#)
- [Troubleshooting Simulator issues](#)
- [Troubleshooting VCS One global cluster issues](#)
- [Troubleshooting authentication issues](#)
- [About the hagetcf utility](#)
- [About Symantec Technical Support](#)

About VCS One log messages

The Policy Master and client system logs provide messages that can help with the following tasks:

- Monitor the health of the VCS One cluster
- Track the events and operations of the VCS One cluster
- Troubleshoot issues

Adding custom log messages to the log file

In addition to the logs that VCS One generates, a user with `ServerFarmAdministrator` privileges may add messages to the log file with the `halog` command.

Adding a manual entry allows the log file to be used as an administrative notebook to add more context to the log files as well as a reminder of actions performed.

To add a custom log message to the log file using the command line

- ◆ Type the following command

```
halog -add "log message" -sev C | E | W | N | I [-sys system]
```

Use the following information to replace the appropriate variables and option:

<code>log message</code>	The text of the message you want to appear in the logs. Note the message must begin and end with a double quotation mark.
<code>sev</code>	Adds a message of a specified severity to the log file. The severity values C, E, W, N, and I have the following significance: C = Critical E = Error W = Warning N = Notice, I = Information
<code>system</code>	Specifies the system. The user must have Modify System privileges or system administrator privileges to use this option.

For example, the following command could log a maintenance action:

```
halog -add "replace NIC card on system systemname." -sev N
```

Policy Master logs

Log messages are generated on the Policy Master by the Policy Master daemon, VCS One console, and VCS One commands.

Log messages generated on the Policy Master daemon are saved in the engine_A.log file. This log file is located in the `/var/VRTSvcsone/log/` directory. (Also the `$VCSOne_Log` directory.) You can view the policy master logs in the VCS One console from the **Logs** tab.

See [“Logs tab options”](#) on page 156.

The size of the engine_A.log file can be specified using the cluster’s LogSize attribute and cannot exceed 33 MB (33554432 bytes). If the log file exceeds the specified maximum value, the existing engine_A.log file is renamed to engine_B.log, and a new engine_A.log file is created. The most recent log messages are recorded in the new engine_A.log file. VCS One maintains three engine log files, engine_A.log, engine_B.log, and engine_C.log. The engine_A.log file contains the most recent log messages while the engine_C.log file contains the oldest log messages. Unauthorized access attempts are not logged in the engine logs.

Log messages generated by the VCS One management console are saved in the log files that start with the name `vcsonems-`. These log files are located in the `/var/VRTSvcsone/log/directory`.

Error messages generated by VCS One commands are saved in the `stderr` file. These messages are also recorded in the engine_A.log file and are displayed in the Logs tab of the VCS One console.

VCS One log messages are structured in such a way so as to enable easy troubleshooting. Additional information about how to interpret the log messages is available.

See [“Interpreting VCS One log messages”](#) on page 587.

VCS One client logs

Log messages are generated on the VCS One client systems by the VCS One client daemon (`vcsonclientd`) and resource agents. You cannot view client log entries from the VCS One console.

Log messages that are generated by the VCS One client daemon are saved in the `vcsonclientd` file. This file is located in:

```
/var/VRTSvcsone/log/vcsonclientd_A.log
```

Log messages generated by the agents are saved in the `agent_name_A.log` file. This file is located in:

```
/var/VRTSvcsone/log/agent_A.log
```

Simulator logs

Log messages generated by the VCS One Simulator are saved in the following files:

- On Windows computers, if the Simulator is installed in the default location, the Simulator log messages are saved in the `vcsonesim_A.txt` file.

This file is located in the following location:

```
C:\Documents and Settings\UserName\Desktop\VCSOne\
Simulator\multisim\instance_name\log\vcsonesim_A.txt
```

where `instance_name` is the name of the Simulator instance whose log files you are searching. In case of the default instance, replace `instance_name` with “default”.

If the Simulator is installed in a different location, the log messages are saved in the following location:

```
installed_path\VCSOne\Simulator\multisim\instance_name\
log\vcsonesim_A.txt
```

where `installed_path` is the location where the Simulator is installed.

Symantec Web server logs

The Symantec Web server must be installed on the same system as the Policy Master.

You can not view web server log entries from the VCS One console. Log files generated by the Symantec Web server are located in the following directory:

```
/var/VRTSweb/log/
```

To set the log level for the Web Server to maximum logging (verbose mode)

- ◆ Type the following command in the URL bar of the browser.

```
https://ipaddress:14171/LoggerAdmin.do?logLevel=TRACE5
```

Use the following information to replace the appropriate variable

`ipaddress` The IP address of the host where the Web server is running. This is also the host where the Policy Master service group is online.

Turning on Symantec Product Authentication Service logs

The Symantec Product Authentication Service (AT) logs report information about the authentication service. AT manages secure communications between the Policy Master and the client nodes.

To turn on the authentication logs

- ◆ Type the following command

```
# /opt/VRTSvcsone/bin/haat setloglevel -l 0|1|2|3|4 \  
[-f log_file_name]
```

Use the following information to choose the log level and indicate the name of the file for client-side log messages

0|1|2|3|4

To indicate the level of detail of the authentication logs, specify a number from 0 to 4. The higher the number, the greater the level of detail.

Client-side logging has 5 log levels. By default, the client-side log level is 0 (no logging).

Server-side logging has 4 log levels. By default, the server-side log level is 1.

The following log levels exist:

- Log level 0 does not log anything in the log files.
- Log level 1 logs only critical error messages that require administrator attention.
- Log level 2 logs all errors.
- Log level 3 logs all errors and warnings.
- Log level 4 logs everything, including trace messages.

-f log_file_name

Specify the -f option for client-side logging and indicate the name of the file to store the client-side log messages. When the log file size reaches the maximum, the file is moved to filename.1, filename.2, filename.3, filename.4, and filename.5.

Viewing logs from commands generated by the VCS One console

Log files generated by modules such as BPA are located as follows:

- /var/VRTSvcsone/logs/

About logs generated from events

Event logs are associated with Business Policy Automation (BPA). The list of events that generate logs is available.

See [Table 34-1, “VCS One events and associated parameters,”](#) on page 645.

When an event is missed because the BPA scheduler is down, they will be logged as ‘Missed events.’

Viewing an event’s details

View the details page of an event to view more information about the event, including event parameters and recent rule executions.

To view an event's details

- 1 In the VCS One console, click the **Logs** tab.
- 2 Click the **Event Logs** tab.
- 3 In the right pane, from the Event Name column, click the name of the event.

About logs generated from rules

Rule execution logs are associated with Business Policy Automation (BPA). Logs generated from rules can be either from a business rule or from a notification rule.

By default, business log rules display in the console. To view notification rule logs, click the drop-down arrow and select from the list.

Deleting event and rule log entries

You delete log entries based on a date and time boundary. You can not filter the view to delete only subset of entries within the boundary you provide.

To delete log entries

- 1 In the VCS One console, click the **Logs** tab.
- 2 Click one of the following tabs:

Event Logs To delete log entries generated from Policy Master events

Rule Execution Logs To delete log entries generated by business policy automation rules.

- 3 In the right pane, from the Configuration menu, click **Purge Logs**.
- 4 Specify the date and time to delineate the boundary of the purge.
All the event logs, job logs, and rule logs that are older than the specified date will be deleted.
- 5 Click **OK**.

Deleting job log entries

Use this procedure to purge the logs of a specific job. You may also delete logs of events and rules.

See [“Deleting event and rule log entries”](#) on page 586.

To delete log entries

- 1 In the VCS One console, click the **Manage** tab.
- 2 Click the **Jobs** tab.
- 3 In the right pane, click the link of the job for which you wish to delete the logs to go to the job details page.
- 4 In the right pane, from the Operations menu, click **Purge Job Logs**.
- 5 Specify the date and time to delineate the boundary of the purge.
All the job logs that are older than the specified date will be deleted.
- 6 Click **OK**.

About the first failure data capture (FFDC) log

The first failure data capture (FFDC) log is enabled by default, and contains the most recent 1024 debug logs. This log supplements the system log files with debug data that may be useful in debugging a Policy Master daemon, vcsoned, and the client system daemon, vcsoneclientd, daemon crash.

The FFDC log can be enabled at the system level or the VCS One cluster level.

See [“EnableFFDC”](#) on page 705.

To enable the first failure data capture log from the VCS One console

- 1 In the VCS One console, click the **Administration** tab.
- 2 Click the **Settings** tab.
- 3 In the right pane, click the pencil icon next to the EnableFFDC attribute.
- 4 Edit the value of the attribute.
- 5 Click **OK > Close**.

Interpreting VCS One log messages

A typical VCS One log message resembles the following:

```
2007-02-12 13:38:40 VCS One NOTICE V-97-1-10323 Policy Master
changed state from LOCAL_BUILD to RUNNING
```

Each log message consists of the following information:

Item	Description	Example
Time-stamp	Displays the year, month, date, and time the log message was generated.	2007-02-12 13:38:40

Item	Description	Example
Mnemonic string	Displays the name of the product for which the log message was generated.	VCSone
Message severity	Displays the severity level associated with the log message. Severity levels can be classified as Critical, Error, Warning, Notice, and Information.	NOTICE
Unique message identifier (UMI)	Displays the unique message identifier code, which comprises four parts. The last part of this code is the message number.	V-97-1-10323
Message text	Displays the actual message text. The message text for agents is preceded by a header, which consists of <i>name_of_agent:name_of_resource:entry point</i> .	Policy Master changed state from LOCAL_BUILD to RUNNING Message text for agents: FileOnOff:MyFile:online :Resource could not be brought up because the attempt to create the file (/tmp/MyFile) failed with error (Is a Directory)

Troubleshooting VCS One issues

This section describes common VCS One issues and their resolution.

Using the Simulator to reproduce issues

In the Simulator configuration you can induce faults and view the resulting behavior to create and fine-tune the VCS One cluster configuration without using a production environment. The simulated configuration can then be imported into your production environment.

You may also import your production environment into the Simulator to reproduce an environment for testing or educational purposes. This is done by using the database configuration information imported from an actual running VCS One cluster.

See [“How to use the Simulator to duplicate your live installation”](#) on page 589.

You may use the Simulator to regenerate an environment using the database configuration information imported from an actual running VCS One cluster. Multiple Simulator start up modes are available to tune the preciseness of the simulation.

See [“About the Simulator”](#) on page 174.

How to use the Simulator to duplicate your live installation

Use these steps to save the configuration database and reload it into a system. You can use this procedure for diagnostic purposes, or to load a configuration from an actual VCS One cluster into a Simulator.

- 1 Backup the configuration with the following command
`haadmin -backup -db <backup-dir-location>`
- 2 Copy the database from the backup-dir-location to the test system at new-backup-dir-location.
- 3 Copy the database to the new directory
`haadmin -restore -db <new-backup-dir-location>`
- 4 Choose the appropriate start up mode for the Simulator.
 See [“About the Simulator’s start-up modes”](#) on page 177.
- 5 Do one of the following tasks:

To start the Simulator in Basic mode using the command line

◆ `hasim -start`

To start the Simulator in Extended mode using the command line

◆ `hasim -start - extended`

To start the Simulator in Extended and No Operation mode using the command line

◆ `hasim -start -extended -no_operation`

About disabled menu items

A menu item is disabled, in which it is greyed out and not selectable, if you do not have the correct privileges to perform the action.

See “[About administering users and roles](#)” on page 530.

A menu item may be enabled but may not complete if the operation is not valid for the current state of the object. Check the error generated or the log file for more information on why an operation did not complete.

CLI commands appear to hang

CLI commands can sometimes hang if the socket connection uses a virtual IP configured on the client node as its source IP. The socket connection created by CLI commands can use a virtual IP configured on the client node as its source IP. Doing so creates an issue if the virtual IP is brought down when there is an ongoing connection.

Since the virtual IP is no longer available in this situation, the CLI does not receive any further communication with the Policy Master and hangs indefinitely. This issue can also arise if the virtual IP is already plumbed before starting `vcsonclientd`. Because `vcsonclientd` uses the virtual IP as the source IP, it will not receive any Policy Master responses when the virtual IP is brought down.

Workaround

Specify a local IP address on the client node as the source IP to bind to while connecting to the Policy Master on an IP address specified in `vcson.conf`. Doing so prevents the socket connection from using the virtual IP as the source IP.

- 1 Specify the optional source IP for a given Policy Master IP in `vcson.conf` as follows:

```
PM_IPS=[pm_ip]:port:[src_ip]
```

or

```
PM_IPS=[pm_ip]:port:src_ip
```

Each `PM_IPS` record can have an additional source IP separated by a colon (:).

- 2 Even if the port is not specified (but a source IP is specified), indicate the port with an empty port (port) field:

```
PM_IPS=[pm_ip]::[src_ip]
```

Do not use blank spaces in any of the three fields.

Specify the source IP (src_ip) the same way you would specify the Policy Master IP. That is, enclose the IP in square brackets [] to indicate an IPv6 IP.

The Search tab does not display

The Search tab does not display if the Webserversubsystems attribute is edited to remove the SEARCH subsystem. You can check the value of the Webserversubsystems attribute from the Global Settings page.

See [“Settings tab operations”](#) on page 169.

More information is available about the Webserversubsystems attribute.

See [“Webserversubsystems”](#) on page 691.

Tuning the Policy Master to use a higher number of file descriptors

Each operating system that supports the Policy Master has a default maximum limit for the number of file descriptors that can be used per process.

[Table 32-1](#) shows these default limits.

Table 32-1 Default limit for the number of file descriptors

Operating system	Default limit for the number of file descriptors
Solaris	256
Linux	1024

If you would like to connect a large number of client systems to the Policy Master, you may need to increase the default limit for the number of file descriptors to allow the Policy Master to accept more connections.

If a large number of clients are connected to the Policy Master and you have not increased the limit for the number of file descriptors, commands may not be able to connect to the Policy Master to provide status and configuration functionality.

On Solaris, increase the maximum limit for the number of file descriptors if you would like to connect more than 128 client systems to the Policy Master.

On Linux, the default limit for the number of file descriptors should be sufficient. If a large number of clients are connected and commands are not responding, however, increase the value.

To tune the Policy Master to use a higher number of file descriptors

- 1 Open the `/opt/VRTSvcsone/bin/vcsoneenv` file in a text editor.
- 2 Add the following line at the beginning of the `vcsoneenv` file:
`path_to_ulimit/ulimit -n 8192`
- 3 Restart the Policy Master:
`hastop -pm`
`hastart -pm`

ha- commands run slowly when NIS or LDAP is unavailable

VCS One commands that begin with “ha” may run slowly when `nis` or `ldap` is specified as the database source in `/etc/nsswitch.conf`, and an NIS or a LDAP server is unavailable.

State of service group is UNKNOWN

Delete the Project or Zone resource in a service group before setting the `ContainerInfo:Enabled =0`, otherwise, the state of the service group will be reported as UNKNOWN.

Workaround: To remove the resource using the command line:

- 1 Delete the resource:
`# hares -delete resource_name`
- 2 Change the Service Group's `ContainerInfo:Enabled` attribute to 0:
`# hagrps -modify sg_name ContainerInfo -update Enabled 0`

To remove the resource using the VCS One console:

- 1 Delete the resource.
- 2 Change the Service Group's **ContainerInfo:Enabled** attribute to 0.

State of service group is incorrect

If a resource goes into UNKNOWN state because the agent is not able to probe the resource then the service group state will not change to reflect the UNKNOWN state of resource.

The service group will maintain its previous state.

Faulted resource state not reflected in service group state

If ResFaultPolicy of a resource is set to FaultHold, then the faulted state of the resource is not reflected in the state of service group.

In this case, the service group has one of the following states:

- PARTIAL if there are other OnOff type resources that are online
- OFFLINE in all other cases

Duplicate TCP line messages

Description

On Red Hat Linux computers, when a TCP connection is rapidly shutting down and attempting to re-connect using the same address and port pair, the following messages are displayed:

```
tcp 0 0 X.X.X.X:80 X.X.X.X:1035 TIME_WAIT
tcp 0 0 X.X.X.X:80 X.X.X.X:2028 TIME_WAIT
warning, got duplicate tcp line
warning, got duplicate tcp line
```

These messages do not impact or have an adverse effect on VCS One performance.

More information is available about this issue.

Refer to the *Red Hat Linux* documentation or the Knowledge Base article located at http://kbase.redhat.com/faq/FAQ_80_6180.shtm.

Resolution

To suppress duplicate messages

- 1 In the `sysctl.conf` file, located at `/etc/sysctl.conf`, change the following kernel parameter values:

- `tcp_tw_recycle = 0`
- `tcp_tw_resuse = 0`

- 2 Apply the changes. At the command prompt, type the following:

```
sysctl -p
```

VCS One client does not connect to Policy Master

Description

The Symantec Product Authentication Service may reject connections between the Policy Master system and the VCS One client system, if the time differential between them is more than 30 minutes. The following error message is displayed:

```
VCSone ERROR V-97-19-12358 Failed to obtain the credential from  
Local cache, please ensure that the System credential is  
deployed on the node and the System does not lag behind the PM  
node.
```

Resolution

Use the `NTP` utility to correct or modify the time settings on the VCS One client system and Policy Master system, such that the time differential between the systems does not exceed 30 minutes.

Policy Master service group stuck in PARTIAL state

Description

The Policy Master service group can get stuck in the `PARTIAL` state and cannot be brought online.

Resolution

Use the `hastart` command to bring the Policy Master service group online.

- ◆ At the command prompt, type the following:

```
hastart -cluster -sys system
```

Here, *system* is the name of the active Policy Master cluster node.

Increasing LogFileSize generates error

Description

Agents create a log file when they write the first log message to the log file. If you start VCS One and increase the value of `LogFileSize` attribute (resource type), before the agent creates the log file, the following message appears in the place of each log message entry.

```
Log File Pointer is NULL
```

In other words, whenever the agent attempts to write a log message entry to the log file, the log message entry is replaced by this message. This problem does not occur if you decrease the LogFileSize attribute value.

Resolution

To resolve this issue

To resolve this issue, perform the following steps:

- 1 Decrease the LogFileSize attribute value to a value, which is lower than the default value.
- 2 On the Policy Master cluster system, modify the LogDbg attribute to enable debug logging. This causes the agent to generate a log message and create a log file. When the agent writes the first log message it creates a log file.
- 3 After the agent writes the first log message, change the LogDbg attribute value to the default value. The default value is no debug logging.

Negative values not displayed in the Workload section

Description

VCS One brings resources in a service group online by using the `hagr` command. If the resources are brought online manually using the `hars` command, the statistics and graphical representations displayed in the Advanced Workload Management (AWM) or Workload view, may not be accurate.

For example, if you bring a service group online manually on a system where another service group is already online and uses all or most of the system's capacity, the AWM view does not display the system's available capacity as a negative value.

Resolution

Before you manually bring the resources in a service group online, ensure that the system's existing available capacity can accommodate the service group online operation.

User gets unexpectedly logged out from the VCS One console

Description

A user that is currently logged in to the VCS One console will get logged off when that user is deleted from the VCS One configuration. In the following conditions, the user may log back in again and continue to use VCS One:

- The user has the same name as a user with root-level permissions of any system in the Policy Master cluster.
- The user is part of a user group that remains in the VCS One configuration.

Resolution

Log in again to the VCS One console, if you continue to have appropriate permissions.

Small fonts displayed in Flash components

Description

The VCS One Flash components appear in small fonts due to a Web browser plug-in issue. This occurs when the Mozilla Firefox Web browser is used on Linux computers. Firefox uses GTK fonts. If these fonts are not available, Firefox uses KDE or any other available fonts, which might result in small or uninitialized fonts.

Resolution

Download and install the `gtk2-engines-gtk-qt` package. After you install this package, GTK styles and fonts are available for use in KDE's Control Center. You need to install the required plug-in files (`.so` files) in the `~/ .mozilla/ plugins` folder, so that Firefox can use these fonts.

Organization Tree and Extended Attributes views not click-able

Description

After you expand and collapse the Organization Tree or the Extended Attributes tree views, you cannot use the mouse pointer to select a tree node. This problem occurs only when the VCS One console is launched using the Firefox Web browser on Linux computers. A Firefox and Macromedia Flash plug-in issue causes this behavior.

The add and move wizards for service groups, systems, and users along with the add custom view wizard display this behavior.

Resolution

You may navigate to the nodes in the organization tree using one of the following methods:

- Use the `LEFT ARROW` and `RIGHT ARROW` keys to expand and collapse the tree views. Use the `UP ARROW` and `DOWN ARROW` keys to transverse the nodes of the tree.

- Click **Next** to move to the next panel, and immediately click **Back** to return to the panel. You may now click on the organization tree nodes.

Organization Tree right-click menu not functional on Linux Firefox

Description

When you use the Firefox Web browser on a Linux computer, you cannot select the right-click menu commands from the Organization Tree. If you right-click the Organization Tree, you can view right-click menu, however upon releasing the right mouse button the menu is no longer visible. This behavior is applicable to all the sections of the VCS One console that display the Organization Tree.

Resolution

Right-click the Organization Tree node, keep the right mouse button pressed, point to the desired menu command, and then release the right mouse button.

Summary and Workload sections not automatically refreshed

Description

Sometimes, console pages might not display up-to-date VCS One cluster information. Console pages display VCS One cluster details graphically using Macromedia Flash components which continuously poll the Symantec Web server for updates.

Resolution

Use the refresh option provided in the Web browser to manually refresh these pages.

Web browser crashes while performing AWM tasks

Description

Sometimes, the Web browser might crash while performing operations in the Advanced Workload Management (AWM) or Workload view. This happens if you are using Macromedia Flash version 8 or later as the Web browser plug-in.

Resolution

None.

Views containing Flash content take a long time to load

Description

Sometimes, the Web browser might take a long time to load views containing Flash content, such as the AWM view. An Adobe Flash Player pop-up window appears, which contains a confirmation message about whether you want to abort the script.

Some of the views that contain Flash content include the Advanced Workload Management (AWM) or Workload view, the Resource dependency view, the Group dependency view, and the Map view.

Resolution

In the Adobe Flash Player pop-up window, clicking **Yes** multiple times might solve the issue.

I/O fencing on client system appears to fail

Description

In certain cases, I/O fenced Linux client systems may appear to successfully block writes, which are buffered before they are written to the shared disk.

Resolution

Choose to write to the corresponding raw device. Writes that are properly I/O fenced are reported immediately.

More information is available about the `raw` command.

Refer to Linux documentation.

Console displays an unexpected error message

Description

If you are using the Mozilla Firefox Web browser, the following error message may be displayed in the VCS One console.

```
System_name has received an incorrect or unexpected message.  
Error Code: 12227.
```

This message is generated by the Web browser when the Secure Sockets Layer (SSL) handshake fails between the Web browser and the Symantec Web server. The SSL handshake fails when the client-side SSL certificates are not present in the Web browser, or if client-side SSL certificates are present but contain incorrect information. Note that this is not an VCS One error message.

Resolution

Ensure that the required client-side SSL certificates are present in the Web browser and the certificates contain valid information.

Loading XML configuration into the database fails

Description

If you try to load XML configuration into the database using the `haconf -loaddb` command, while the Policy Master daemon is up-and-running, the operation fails. The following error message is displayed:

```
VCS One ERROR V-97-1-17433 Cannot initiate this action because
the Policy Master or another instance of haconf may be running.
```

Resolution

To resolve this issue, perform the following steps in the order presented:

- 1 Stop the Policy Master daemon; take the Policy Master resource offline. At the command prompt, type the following:
hastop -pm
- 2 Clean the configuration database. At the command prompt, type the following:
haconf -cleandb
- 3 Load the XML configuration into the database. At the command prompt, type the following:
haconf -loaddb
- 4 Start the Policy Master daemon; bring the Policy Master resource online. At the command prompt, type the following:
hastart -pm

Service group will not go offline

Description

If a parent resource will not go offline until a child resource is forcefully brought offline, VCS One will not be able to offline the service group.

Resolution

To resolve this issue, perform the following steps in the order presented:

- 1 Type the following comment to flush any actions for the service group.
hagrp -flush -action group -sys system
- 2 Type the following command to take the child resource offline.

```
hagrp -offline -ignoreparent child_resource -sys system
```

Resource stuck in the unable to offline state

Description

A resource can get stuck in the UNABLE TO OFFLINE state. The resource cannot be brought online or taken offline when it is in the UNABLE TO OFFLINE state. In such a situation, if you execute the `hagrp -flush` command, the state of the resource changes from UNABLE TO OFFLINE to WAITING TO GO OFFLINE. The Policy Master does not attempt to take the resource offline and the resource is stuck in the WAITING TO GO OFFLINE state.

Resolution

To resolve this issue, do one of the following:

- For an off-host resource that is currently in the UNABLE TO OFFLINE state, you need to take its control group offline, and then bring the control group online again. After the control group is brought online, the Policy Master attempts to take the off-host resource offline. If the Policy Master still cannot take the off-host resource offline, you need to take the resource offline, outside VCS One control.
- For resources that are not off-host resources, you need to take the resource offline, outside VCS One control.

A rule does not execute

When a rule becomes invalid, it no longer executes.

Resolution

Check that one of the following criteria is in effect. Any one of these criteria may make a rule invalid:

- An object referenced by the rule has been deleted.
- An object reference by the rule has moved in the organization tree such that it is no longer in the user's policy node.
- An object referenced by the rule has moved out side of the job's organization unit.
- A user privilege on a referenced object got revoked.
- The owner of the rule has been disabled or deleted.

VCS One ha- commands do not work in a WPAR

Resolution

Verify your VCS One credentials. Make sure the password is not changed.
 Verify the AT certificate is not expired.

Resource does not come online in the WPAR

Resolution

- Verify VCS One and the agent packages are installed correctly.
- Verify the application is installed in the WPAR.
- Verify the configuration definition of the group. Make sure the ContainerInfo's properties (Type and Name) are defined.
- Verify the configuration definition of the resource agent. Make sure the ContainerOpts' property RunInContainer is defined.

Error messages occur when using the command script generated from the haconf command

Description

You may use the `haconf -dbtocmd` or the `haconf -xmltocmd` command to get the configuration of your VCS One cluster in the form of a command script.

See [“How the Policy Master loads the VCS One cluster configuration”](#) on page 56.

When the resulting command script is executed, you may see some error messages as a result of redundant commands.

Resolution

The following examples display error codes that may be ignored.

- VCS One ERROR V-97-1-10407

```
Example: hatype -add DNS -platform linux/x86
VCS One ERROR V-97-1-10407 Unable to add type 'DNS'. Type
already exists
```

- VCS One ERROR V-97-1-11354

```
Example: hatype -modify NetAppExport ArgList -delete -keys -
platform linux/x86
VCS One ERROR V-97-1-11354 [NetAppExport::ArgList] One or more
resources depend on the attribute dependency
'FilerResName:FilerName' defined in the ArgList. Remove these
before clearing ArgList
```

- VCS One ERROR V-97-1-17062
- VCS One ERROR V-97-1-17063
- VCS One ERROR V-97-1-17310
- VCS One ERROR V-97-1-17322
- VCS One ERROR V-97-1-17361
- VCS One ERROR V-97-1-17362
- VCS One ERROR V-97-1-17366
- VCS One ERROR V-97-1-17367
- VCS One ERROR V-97-1-17399

Troubleshooting Simulator issues

This section describes common Simulator issues and their resolution.

Console connection issue when using multiple Simulator instances through Firefox

When using Firefox, it is not possible to simultaneously log in to the consoles of multiple Simulator instances using the local host IP address (127.0.0.1). If a user tries to connect to a second instance (`https://127.0.0.1:port2`) when already connected to the first instance (`https://127.0.0.1:port1`), then the user will be logged off from the first instance. This happens because Firefox stores cookies only with the IP address and not with the port numbers. Since the IP address is the same in both the instances, they share the cookies which results in the user getting logged off from the first instance after logging in to the second instance.

Workaround

While adding the instance using the `hamultisim` command, use the `-hosts` option, then connect to both the instances from Firefox using the instance name and not the IP address. For example, connect to the first instance using `https://vcsone_<instance_name>:<port1>` and to the second instance using `https://vcsone_<instance_name>:<port2>`.

See [“Adding a Simulator instance”](#) on page 181.

Non-administrator users cannot start the Simulator on Windows Vista

On Windows Vista non-administrator users who have administrator group privileges cannot start the VCS One Simulator. The Policy Master log contains the following error: `VCS One ERROR V-97-1-10042 Command failed. The user must be Administrator.`

This issue occurs because of Windows Vista's privilege model where non-administrator users who have administrator group privileges are treated differently than the administrator user.

Workaround

Log in as the administrator and not as a non-administrator user.

Simulator does not start

If the Simulator does not start, check that the configuration is valid.

To check that a Simulator configuration is valid

- 1 Using the Windows command line, go to the appropriate configuration directory.
If the Simulator is installed in the default location, the directory for VCS One Simulator configuration files is located here:
`installation_directory\VCSOne\Simulator\conf`
If the Simulator is installed in a different location, the directory for VCS One Simulator configuration files is located here:
`installation_directory\VCSOne\Simulator\conf`
where *installation_directory* is the location where the Simulator is installed.
- 2 From the configuration directory, type the following command:
haconf -verify .
You should see the following message:
Server farm configuration is valid
If you do not see this message, fix the configuration.
See [“Duplicate TCP line messages”](#) on page 593.

Simulator fails to start in remote sessions

Description

The Simulator fails to start in remote sessions. This is because processes that run in remote sessions are executed in separate name spaces. Remote Desktop and Citrix Windows logon sessions, are examples of remote sessions, which run in separate name spaces. These name spaces differ from the name spaces used by the local server processes.

Local server processes cannot communicate with process that run in remote sessions. As a result, commands issued from a remote session that interact with a local session fail. Furthermore, commands issued from a local session that interact with a remote session also fail.

When you attempt to start the VCS One Simulator from a Remote Desktop session (from one name space), and the VCS One Simulator database is already started locally (in another name space), the command fails.

Resolution

None

Network connection error during Simulator startup

Description

When you start the VCS One Simulator from the command line or the Web browser, the following error message may be displayed:

```
V-97-1-10057 ClentHandle::net_recvb failed Error (-4)
```

This error message is displayed when the Policy Master attempts to initiate a control connection to the Simulator, and the Simulator is currently in the process of registering itself with the Policy Master.

Resolution

Wait till the Simulator successfully registers itself with the Policy Master. After the registration process completes, the Simulator automatically responds to subsequent attempts made by the Policy Master to initiate a control connection. You do not need to take any corrective action.

Enterprise users cannot execute non-Simulator commands

Description

Enterprise users can successfully execute Simulator (`hasim`) commands using the Simulator. However, all other VCS One commands issued by Enterprise users fail when executed from the Simulator. The following error message is displayed:

```
VCSone ERROR V-97-1-18079 Command failed.  

User 'username@domain_name' does not have privilege on server  

farm 'serverfarm_name'.
```

Before executing commands VCS One queries the domain controller and retrieves a list of all the global groups. VCS One determines user privileges based on the global group privileges assigned to the user. Since the Simulator works in a simulated environment, VCS One does not query the domain controller, and as a result non-simulator commands issued by Enterprise users fail.

Resolution

Add the Enterprise user to the list of VCS One users and assign `ServerFarmObjectAdministrator` privileges to the user. The user can now successfully execute non-simulator commands as the user is now a part of the VCS One configuration, and has explicit privileges defined.

Simuser log on failure with real-time VCS One cluster configuration

Description

The VCS One Simulator can load and use real-time VCS One cluster configuration. This information is obtained when you execute the `haconf -dbtoxml` command, which creates XML configuration files. However, after you load the real-time VCS One cluster configuration, you cannot log on to the Simulator as the default Simulator user (`simuser`) in the non-secure mode. The following error message is displayed:

```
VCSone ERROR V-97-1-18079 Command failed. User 'simuser@domain' does not have privilege on server farm 'VCSoneFarm'. Login Failed. Please try again.
```

The default configuration available with the Simulator has an in-built user (`simuser`) with `ServerFarmAdministrator` and `ServerFarmObjectAdministrator` privileges. Since `simuser` is not a real-time user the log on process fails.

Resolution 1

To resolve this issue, perform the following steps:

- 1 Copy the `simuser.xml` file to the directory that contains the XML configuration files for the real-time VCS One cluster. The `simuser.xml` file is located at:

```
installation_directory\VCSOne\Simulator\conf\confxml
```

- 2 Open the `main.xml` file, located in the directory that contains the XML configuration files for the real-time VCS One cluster.
- 3 Add the following text to the `main.xml` file under `<!DOCTYPE config SYSTEM "main.dtd">`:

```
<include>simuser.xml</include>
```

The `simuser.xml` file must exist in the same directory and must contain the definition for `simuser@domain`.

- 4 Save the `main.xml` file.
- 5 Restart the Simulator with the real-time VCS One cluster configuration, and log on using the following credentials:
 - User name: `simuser`
 - Password: `none`
 - Domain: `domain`

Resolution 2

You may also log in to the Simulator using one of the following methods:

- Use a login account of a VCS One user that is already present in the configuration of the real VCS One cluster.
- Use the login account of an operating system user that has administrator privileges on the local system.

Resolution 3

To resolve this issue, perform the following steps:

- 1 Load the real-time server configuration into the Simulator. At the command prompt, type the following:

```
hamultisim -startsim instance_name -d real_time_config
```

- 2 Open a CLI prompt for that instance. At the command prompt, type the following:

```
haomultisim -cliprompt instance_name
```

- 3) Add the simuser into the configuration. At the command prompt, type the following:

```
hauser -add simuser@domain -user user@domain -domaintype nt
```

where, ***user*** is the currently logged in user having administrator privileges, ***domain*** is the administrator domain (the local machine's domain), and ***domaintype*** is **nt**

- 4 Add privileges to the simuser@domain. At the command prompt, type the following:

```
hauser -addrole simuser@domain ServerFarmAdministrator
hauser -addrole simuser@domain ServerFarmObjectAdministrator
```

Troubleshooting VCS One global cluster issues

This section describes common VCS One global cluster issues and recommended resolutions.

Unable to establish connection between VCS One clusters

Table 32-2 lists the possible causes due to which VCS One is unable to establish connection between the VCS One clusters. In such situations, the state of the remote cluster is INIT and the state of individual network links is DOWN.

Table 32-2 Possible causes and recommended resolutions

Cause	Description and resolution
Security handshake failed	<p>You may see the following messages in the VCS One engine logs:</p> <pre>VCS One INFO V-97-1-11359 Initiating connection with remote cluster at [192.62.41.2]:14151 VCS One ERROR V-97-1-11370 Security Handshake failed with [192.62.41.2] VCS One ERROR V-97-1-11386 Could not open connection.</pre> <p>Resolution</p> <p>Set up trust between the remote clusters.</p> <p>For example, for two VCS One clusters seattle (primary) and tucson (secondary) with two different root brokers, you must establish trust between the root brokers of the two clusters.</p> <ul style="list-style-type: none"> ■ On seattle, run the following command: <pre># /opt/VRTSvcsone/bin/haat setuptrust \ -b IP_address_of_tucson:broker_port -s low</pre> ■ On tucson, run the following command: <pre># /opt/VRTSvcsone/bin/haat setuptrust -b \ IP_address_of_seattle:broker_port -s low</pre> <p>The <code>-s low</code> option indicates that the security level is low. Accepted values for the security level are <code>low</code>, <code>medium</code>, and <code>high</code>.</p>
Connections are not enabled	<p>If the <code>EnableConnections</code> attribute is set to 1 on the VCS One cluster that initiates connection (initiator) and if the attribute value is set to 0 on the VCS One cluster that accepts the connection (acceptor), VCS One logs the following error message:</p> <pre>VCS One ERROR V-97-1-12513 Rejecting connection from remote cluster 'C1' since attribute 'EnableConnections' is 0 for the remote cluster in the local configuration</pre> <p>Resolution</p> <p>Set the remote cluster object's <code>EnableConnections</code> attribute to 1 for both the clusters.</p> <p>See “Enabling connections between clusters” on page 485.</p>

Table 32-2 Possible causes and recommended resolutions

Cause	Description and resolution
DR port values do not match	<p>VCS One rejects the connection request from the remote cluster if the following values do not match:</p> <ul style="list-style-type: none"> ■ DRPort attribute for the remote cluster object on the VCS One cluster that initiates the connection request ■ DRListeningPort attribute for the cluster object on the VCS One cluster that accepts the connection request <p>See “How VCS One global clusters communicate with each other” on page 69.</p> <p>For example, if cluster seattle (initiator) has the value of DRPort attribute as 12345, and if the cluster tucson (acceptor) has the value of the DRListeningPort attribute as 23456, then the following message is seen in the VCS One log file on tucson:</p> <pre>Rejecting message of type 0x%x from remote cluster 'seattle' on port 12345. The message was received on a port other than the configured DR port = 23456. Ensure the DRPort on remote cluster 'seattle' is the same as the DRListeningPort on the local cluster.</pre> <p>Resolution</p> <p>On the VCS One cluster that initiates the connection request, modify the value of the DRPort attribute to match the value of the DRListeningPort attribute at the remote site.</p> <p>For example, on seattle change the value of the DRPort attribute (of the remote cluster object that represents tucson) from 12345 to match the value of the DRListeningPort (of the cluster-level attribute on tucson) which is 23456.</p> <p>See “Modifying remote cluster configuration” on page 488.</p>
Configuration is incorrect	<p>VCS One fails to establish a connection with the remote cluster if the NetworkConnections attribute is incorrectly specified.</p> <p>Resolution</p> <ul style="list-style-type: none"> ■ Make sure that you have defined the network connections. ■ Make sure that you have specified the value of the remote cluster’s IP address followed by the local cluster’s IP address in the NetworkConnections attribute. The local cluster’s IP address is optional. ■ Make sure that the name of the remote cluster you added is the same as the VCS One cluster name at the remote site. <p>See “About managing remote clusters” on page 478.</p>

VCS One cannot online DRSG service group

Description

In a DR configuration, if you stop the web resource and then stop the Policy Master using the `hastop -pm` command, then when you restart the Policy

Master using the `hastart -pm` command, the following error message is displayed:

```
VCS WARNING V-16-1-10805 Connection timed out
VCS One ERROR V-97-33-1120 Could not online parent group DRSG on
<system_name>.
Verify your DR configuration.
```

VCS One waits for five minutes for the PMSG to come online before it attempts to bring the DRSG online. The PMSG service group cannot go online because the web resource is offline and hence displays the error messages.

Resolution

When you are ready to bring all the resources online in the PMSG, run the `hastart -cluster` command. This command brings the PMSG and the DRSG service groups online.

Unable to view or modify remote cluster attributes

Description

When you run commands to view or modify the remote cluster attributes on the acceptor, you may encounter an error message similar to the following:

```
VCS One ERROR V-97-1-17103 Attribute 'NetworkConnections' does not
exist
```

Based on the VCS One cluster names, VCS One designates one of the clusters as the initiator. Some attributes are applicable only on the initiator.

See [“How VCS One global clusters communicate with each other”](#) on page 69.

Resolution

Modify the attributes on the initiator.

Unable to view CSG attributes for a remote cluster

Description

When you run the `hacsg -display csgname -clus clusname` command to display the remote cluster attributes for a CSG, only a subset of the CSG attributes are displayed.

Only some of the CSG attributes such as ClusterList, Authority, CSGState, and InTransition are exchanged among the VCS One clusters. So, the command displays only these attributes for the CSG for the remote cluster you have specified.

See [“How VCS One enables wide-area failover of a multi-tier application”](#) on page 71.

Inter-cluster operations fail for the CSG

Description

- Display of CSG attributes for the remote cluster fails

When you run the `hacsg -display csgname -clus clusname` command, the following error message is displayed.

For example:

```
# hacsg -display csg1 -clus tucson
VCS One ERROR V-97-1-16132 The Policy Master cannot display
attributes for the composite service group. The composite
service group 'csg1' is not configured on cluster 'tucson'.
Please specify names of composite service group objects that are
configured on the named cluster.
```

- CSG switch operation fails

When you perform a CSG switch operation, the following error message is displayed:

For example:

```
# hacsg -switch csg1 -clus seattle
VCS One ERROR V-97-1-16201 The composite service group 'csg1'
cannot be switched. Either the composite service group 'csg1'
does not exist on remote cluster 'seattle' or is not configured
as global on 'seattle'.
```

Resolution

CSG must be defined and must be global at each site where it can be brought online.

See [“Managing global composite service groups”](#) on page 497.

No concurrency violation triggered when CSG is online at both sites

Description

CSG is online or partially online at more than one site, however VCS One does not trigger a concurrency violation.

Resolution

Make sure that the CSG is global on all the clusters where it is defined, and that the value of the ClusterList attribute matches.

Service groups that belong to a CSG fail to come online

Description

When you run the following commands to bring the service groups online, the groups that belong to a global CSG for which there is no authority cannot come online:

- `hagrp -online -all`
- `hagrp -online -ou -ea`

Resolution

Perform the following steps to resolve this issue:

- 1 Identify the CSGs that the groups belong to.
- 2 Acquire authority for the CSGs.
- 3 Bring the service groups online.

See [“Managing global composite service groups”](#) on page 497.

Resources or groups that belong to a CSG fail to come online

Description

When there is a concurrency violation for a global CSG, the following operations fail:

- Online or switch operation for the CSG
- Online operation for the resources or service groups that belong to the global CSG
- Switch operation for the service groups that belong to the global CSG

You can only perform an offline operation in this case.

Resolution

When a concurrency violation has occurred for the CSG, you must first resolve the concurrency violation before you try to bring the resources, groups, or CSG online.

See [“CSG concurrency violation when the state of the CSG is up-to-date”](#) on page 613.

CSG concurrency violation when the state of the CSG is up-to-date

Description

When a global CSG is online or partially online at more than one site and when the value of the CSG attribute StateState is 0, VCS One reports a concurrency violation at each site.

A message similar to the following is logged:

```
Concurrency violation occurred for composite service group '%s'. The
composite service group '%s' is online or partially online on
cluster objects (%s). Take the composite service group offline on
all cluster objects but one.
```

Resolution

Identify the VCS One cluster where you want to have the global CSG online and take the global CSG offline on other VCS One clusters.

See [“Taking a composite service group offline”](#) on page 374.

CSG concurrency violation when the state of the CSG is stale

Description

When the value of the CSG attribute StateState is 1 and when the Policy Master is down on the local cluster, then VCS One reports a concurrency violation if a takeover of the CSG was performed on the remote cluster.

A message similar to the following is logged:

```
Concurrency violation occurred for composite service group '%s'. The
composite service group '%s' is online or partially online on
cluster objects (%s). This may be due to a takeover of the composite
service group from a remote cluster when the Policy Master in the
local cluster '%s' was down and the state of the composite service
group on the local cluster is not yet up-to-date. To resolve the
concurrency violation, take the composite service group offline on
all cluster objects but one.
```

Resolution

Verify that the CSG takeover operation was performed at the remote cluster. Perform the following steps on the local cluster to resolve concurrency violation for the CSG:

- 1 Flush out any pending actions for each group that belong to the CSG.
See [“Flushing a pending action on a service group”](#) on page 337.
- 2 Take the CSG offline on the local cluster.
See [“Taking a composite service group offline”](#) on page 374.

ATTN flag is set for the CSG

Description

The `ATTN` flag for a CSG is set if a group that belongs to the CSG is faulted, or if the group that belongs to the CSG is unable to come online on any system in the VCS One cluster.

Resolution

Run the `hacsg -infoattn` command.

The command displays the reason why the `ATTN` flag is set in the `CSGState` attribute of a CSG. Perform the following based on the reason that has caused the `ATTN` flag to be set:

- **Unable to Online**
The command lists the groups in the CSG that have caused the `ATTN` flag to be set. Fix the issues for the service groups.
- **Group Fault**
The command lists the groups in the CSG that have caused the `ATTN` flag to be set. Fix the issues for the service groups.
- **Concurrency Violation**
The command lists the CSG name. Resolve the concurrency violation issue. See [“CSG concurrency violation when the state of the CSG is up-to-date”](#) on page 613.
- **State is stale**
See [“How VCS One resolves authority for application that spans clusters”](#) on page 72.

VCS One does not clear the PENDING flag in the CSGState attribute

Description

If the CSG is in a steady `ONLINE` or `OFFLINE` state (no group or resource in that CSG is in transition), the `PENDING` flag is set in the `CSGState` attribute if some resource in the CSG goes to an `UNKNOWN` state.

Resolution

Perform the following steps to clear the `PENDING` flag:

- 1 Fix the issue that caused the resource to go to an `UNKNOWN` state.
See the log file of the agent that manages this resource to find the reason.
- 2 Probe the resource.

See [“Probing a resource”](#) on page 386.

Value of the LinkStatus attribute toggles between UP and DISABLED

Description

If the value of the EnableConnections attribute is set to 1 on the initiator cluster and is set to 0 on the acceptor cluster, then the initiator cluster continuously attempts to connect with the acceptor cluster at periodic intervals. This causes the LinkStatus attribute value toggle between UP and DISABLED.

Resolution

Set the EnableConnections attribute to 1 on the acceptor cluster.

See [“Enabling connections between clusters”](#) on page 485.

Troubleshooting authentication issues

This section describes common Symantec Product Authentication Service issues.

Changing FQDN causes authentication failure

Description

When the fully qualified domain name (FQDN) changes, the authentication process might fail.

The fully qualified domain name may change due to one of the following events:

- Change in the name of the Policy Master cluster systems.
- Ethernet connection is closed and the system re-connects via a wireless connection.

If the authentication service is not re-started, the following error message is displayed:

```
2006-01-17 11:22:38 VCSone ERROR V-97-1-10014 failed to
initialize security facade, Exiting
```

Resolution

To resolve this issue, do one or both of the following tasks:

- Change the broker name to a name that can be resolved or to the IP address of the Policy Master system.
- Re-start the Symantec Product Authentication Service on the system before attempting to log on.

To restart the authentication service on UNIX systems

On the system where authentication is being attempted, at the command prompt, type the following:

```
# /opt/VRTSvcsone/bin/vcsoneatd
```

Authentication broker and Policy Master trust not established

Description

Each Policy Master cluster system must have an explicit trust relationship with an authentication broker.

If you attempt to log on to the VCS One console and you specify an authentication broker system for which trust is not set up, the following error message is displayed:

```
VCSone ERROR V-97-11-24583 Peer certificate verification failed.  
Login Failed. Please try again.
```

Resolution

You must set up a trust relationship between the authentication broker system and each Policy Master cluster system. Use the following command:

```
# /opt/VRTSvcsone/bin/haat setuptrust -b broker_name:port \  
-s low|medium|high
```

where `-b` specifies the name and port of the authentication broker to be trusted and `-s` specifies the security level as either `low`, `medium`, or `high`.

For example, if you want to use an authentication broker system named `sys01`, you need to execute the following command on each Policy Master system. At the command prompt, type the following:

```
# /opt/VRTSvcsone/bin/haat setuptrust -b sys01:14159 -s medium
```

If, at a later stage, you add another system to the Policy Master cluster, you must set up an explicit trust relationship between the new Policy Master cluster system and the authentication broker.

Symantec Web Server log on failure

Description

At times, the Symantec Web Server may not be able to connect to the Policy Master. Attempts to logon to the Symantec Web Server may result in the following error message:

```
VCS One ERROR V-97-11-2 Correct Credentials were not received.
```

Resolution

To resolve this issue, restart the Symantec Web Server, and try to log on. If you still cannot log on, you need to delete the Symantec Web Server authentication credential that resides on the authentication broker system.

To delete current credential of the Symantec Web Server

- 1 The Symantec Web Server's principal name is `WebServer`. At the command prompt, type the following if you want to display it:

```
# /opt/VRTSvcsone/bin/haat showcred -d vx:VCSONE_WEB_USERS -p \  
WebServer
```

- 2 Delete the current Web Server authentication credential. At the command prompt, type the following:

```
# /opt/VRTSvcsone/bin/haat deletecred -d vx:VCSONE_WEB_USERS \  
-p WebServer -j broker
```

VCS One client certificate verification failure

Description

The VCS One client may fail to start due to a credential failure. This issue can be caused by a mismatched user name, mismatched credentials, or if no cached credentials are on the local disk. It can also be caused if the broker is reconfigured after the client is deployed. The following error message is displayed in the client log:

```
ERROR V-97-19-17505 Exiting: Security Initialization failed.
```

Resolution

In the event of client authentication failure, you need to do one of the following:

- Run the installer again to re-deploy the client.
- Manually set up an explicit trust relationship between the authentication broker and the VCS One client system.

The steps for performing these procedures follow.

To re-deploy the client

- 1 Verify whether the credential exists for the user name in `/etc/VRTSvcsone/vcsone.conf` by entering the following command:

```
# grep -i user_name /etc/VRTSvcsone/vcsone.conf
```

where `user_name` is the user name in this format:
`client.abc.com@VCSONE_USERS@vcsone_cluster`. The user name is typically either the host name or the fully qualified host name.
- 2 Display the credential by entering the following command:

```
# /opt/VRTSvcsone/bin/haat showcred -p user_name
```
- 3 Proceed to the next step if one of the following situations applies:
 - The credential does not exist.
 - The credential exists, but the client connection displays the error message. In this case, the credential is either invalid or the authentication broker was re-configured after the credential was issued.
- 4 To resolve either of these issues, redeploy the client in one of the following ways:
 - ◆ Use the installer to create the deployment credential and redploy the client. For instructions on installing the client using a deployment credential, see the *Veritas Cluster Server One Installation Guide*.

- ◆ Redeploy the client manually by performing the following steps:
 - a Make sure that the broker is running on the active Policy Master node by entering the following command:


```
# /opt/VRTSvcsone/bin/hares -state atd
```
 - b On the active Policy Master system, reset the password for the client user by entering the following command:


```
# /opt/VRTSvcsone/bin/haat resetpasswd -t ab -d \  
VCSONE_USERS -p user_name [-n new_passwd] \  
[-r repnewpasswd]
```
 - c On the client system, set up trust with the authentication broker by entering the following command:


```
# /opt/VRTSvcsone/bin/haat setuptrust -b \  
broker_host_or_IP:port -s medium -j client
```

 where *broker_host_or_IP* is the name or IP address of the authentication broker host and *port* is the port number for the authentication broker. In VCS One, this port number is 14159. The *-s* option indicates the security level. Accepted values for the security level are *low*, *medium*, and *high*.
 - d On the client system, reauthenticate the client by running the following command:


```
# /opt/VRTSvcsone/bin/haat authenticate -d \  
vx:VCSONE_USERS -p client_name -s password -b \  
broker_host_or_IP:port
```

 where *client_name* is the name of the client, *password* is the password, *broker_host_or_IP* is the name or IP address of the authentication broker host, and *port* is the port number for the authentication broker. In VCS One, this port number is 14159.

To manually set up trust

- 1 On the active Policy Master system, enter the following command:


```
# /opt/VRTSvcsone/bin/haat deleteprpl -t ab -p VCSONE_USERS \  
-p client_name
```

 where *client_name* is the name of the client.
- 2 On the active Policy Master system, enter the following command:


```
# /opt/VRTSvcsone/bin/haat addprpl -t -p VCSONE_USERS \  
-p client_name -s password -b broker_host_or_IP:port -q service
```

 where *client_name* is the name of the client, *password* is the password, *broker_host_or_IP* is the name or IP address of the authentication broker host, and *port* is the port number for the authentication broker.
- 3 On the client system, set up trust with the authentication broker by entering the following command:

```
# /opt/VRTSvcsone/bin/haat setuptrust -b \  
broker_host_or_IP:port -s medium -j client
```

where *broker_host_or_IP* is the name or IP address of the authentication broker host and *port* is the port number for the authentication broker. In VCS One, this port number is 14159. The *-s* option indicates the security level. Accepted values for the security level are low, medium, and high.

- 4 On the client system, reauthenticate the client by running the following command:

```
# /opt/VRTSvcsone/bin/haat authenticate -d vx:VCSONE_USERS \  
-p client_name -s password -b broker_host_or_IP:port
```

where *client_name* is the name of the client, *password* is the password, *broker_host_or_IP* is the name or IP address of the authentication broker host, and *port* is the port number for the authentication broker. In VCS One, this port number is 14159.

VCS One console fails to start

Description

If the authentication broker fails or stops responding, you cannot start a new VCS One console connection. All the existing console connections continue to function in a normal manner and are not affected. All attempts to start a new VCS One console connection with the Policy Master fail.

All command line interface commands that require authentication also fail when the authentication broker fails. However, the root user on the active Policy Master cluster node can successfully execute VCS One CLI commands and perform administration tasks.

Resolution

To resolve this issue, perform the following steps:

- 1 Check the authentication broker for errors. In the event of an authentication broker failure, resolve the problem, and ensure that the authentication broker is up and running.
- 2 Start a new VCS One console connection.

VCS One CLI commands fail to execute

Description

A VCS One command line interface failure with a security hand-shake error can occur for various reasons, including:

- The credential for the user name that is defined in `/etc/VRTSvcsone/vcsone.conf` does not exist. To check to see if the credential exists, enter the following command:

```
# /opt/VRTSvcsone/bin/haat showcred -p user_name
```
- The credential for the user name exists but does not match the broker credentials. This issue can be caused if the broker is reset after the client is deployed.

Resolution

If the credential for the user name exists, but does not match the broker credentials, run the installer again to re-deploy the client. See the *Veritas Cluster Server Installation Guide* for instructions.

Business policy automation not working

If Business Policy automation is not working, check the following items:

- The Webserver, BPA engine, and Policy Master daemon were all running when the event occurred.
 The BPA engine runs within the Webserver process, and both the Webserver and the BPA engine must be running when an event occurs in order for the event to be processed. There is no deferred or offline processing.
 Additionally, the Policy Master daemon, `vcsoned`, must be running to process an event.
- The Webserver, BPA engine, and Policy Master daemon did not fail while processing the event.
 If `vcsoned` or the BPA engine fails while processing an event, the event will not be finished. If there are five tasks in a job and during the third task the Webserver fails, when the Webserver is restarted the remaining tasks will not run. The execution log will show that the rule was triggered and that task three was scheduled to run.
- The job failed before it completed.
 If a job fails before it has completed, it does not restart
- Could not contact mail server and send notification
 Check correct spelling of email address. Note that VCS One does not queue the message. After two attempts the attempt logs as a delivery failure. Check the email server. If the email server is down, you will miss notifications.

About the `hagetcf` utility

The `hagetcf` command generates output about your VCS One cluster configuration. Symantec Technical Support might request you to run the `hagetcf` utility and send them the generated output in order to completely understand and analyze the VCS One cluster configuration.

See [“About Symantec Technical Support”](#) on page 623.

The `hagetcf` utility must be executed on one system at a time.

This utility gathers the following information:

- Installed software information
- System information
- Configuration information
 - If the system is part of the Policy Master cluster, configuration information comprises of VCS information, VCS One information, and VCS One database information.
 - If the system is a VCS One client, configuration information comprises of information about the agent directories and agent framework.
- Log information
 - If the system is part of the Policy Master cluster, log information includes installation logs, VCS One logs, lock files, and VCS logs.
 - If the system is a VCS One client, log information includes installation logs, log messages, and lock files.
- Important VCS One file information
- Symantec Product Authentication Service configuration backup file information
- Web console information

After gathering this information, the `hagetcf` utility creates a gzip file. This file may be located in the default or user-specified directory. You need to send the entire gzip file to Symantec Technical Support.

Caution: The `hagetcf` utility gathers sensitive information about the VCS One cluster environment. Ensure that you secure this information while sending it to Symantec Technical Support.

You can run the `hagetcf` utility in the interactive or silent mode. In addition, you can specify if you want to save the gzip file in the default or user specified directory.

To run `hagetcf` in the interactive mode

- ◆ At the command prompt, type the following:

```
hagetcf
```

When prompted, choose a directory for the gzip file.

To run `hagetcf` in the silent mode and use the default directory

- ◆ At the command prompt, type the following:

```
hagetcf -silent
```

The output gzip file is saved in the `/var/tmp` directory.

To run `hagetcf` in the silent mode and specify a user-defined directory

- ◆ At the command prompt, type the following:

```
hagetcf -silent -d directory_for_gzip
```

The output gzip file is saved in the directory that you specify.

hagetcf command usage

The `hagetcf` command has the following formats:

```
hagetcf [-h | -help]  

hagetcf [-s | -silent] [-d output_directory]  

hagetcf [-version]
```

More information is available about the `hagetcf` utility.

See the *Veritas Cluster Server One Command Reference Guide*.

About Symantec Technical Support

Visit http://www.symantec.com/enterprise/support/assistance_care.jsp for technical assistance. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and the customer email notification service.

If you encounter an error while using the product, include the error number preceding the message when contacting Technical Services. You can also use the error number to search for information in TechNotes or documents on the Web site.

Reference

This section includes the following chapters:

- [“Reference of privileges”](#) on page 627.
- [“Automated tasks reference”](#) on page 643.
- [“Configuration file reference”](#) on page 667.
- [“Attributes reference”](#) on page 677.
- [“State reference”](#) on page 761

Reference of privileges

This chapter includes the following topics:

- [Pre-defined roles in VCS One](#)
- [About role categories](#)
- [About privileges categories](#)

Pre-defined roles in VCS One

[Table 33-1](#) lists the roles that are predefined in VCS One. The roles are listed in alphabetical order.

Roles that correspond to virtualization may be visible to the user. This capability is not supported in the current release, but is planned for a future release.

Table 33-1 VCS One built-in user roles

Role Name	Role Type	Description
CSGAdministrator	CSG	Composite service group administrator role
CSGOperator	CSG	Composite service group operator role
GroupAdministrator	Group	Group administrator role
GroupOperator	Group	Group operator role
PFrameAdministrator	Pframe	Pframe administrator role
PFrameOperator	Pframe	Pframe operator role
ResourceAdministrator	Resource	Resource administrator role
ResourceOperator	Resource	Resource operator role
ServerFarmAdministrator	Farm	VCS One cluster administrator role
ServerFarmObjectAdministrator	Object	VCS One cluster object administrator role
ServerFarmObjectGuest	Object	VCS One cluster object guest role
ServerFarmObjectOperator	Object	VCS One cluster object operator role
SystemAdministrator	System	System administrator role
SystemOperator	System	System operator role
UserAdministrator	Object	User administrator role
UserOperator	User	User operator role
VCSOneClientFarm	Farm	System user role for farm object
VCSOneClientGroup	Group	System user role for group objects
VCSOneClientPFrame	Pframe	System user role for Pframe object
VCSOneClientSystem	System	System user role for system object

Table 33-1 VCS One built-in user roles

Role Name	Role Type	Description
VCSOneClientVFrame	Vframe	System user role for Vframe objects
VFrameAdministrator	Vframe	Vframe administrator role
VFrameOperator	Vframe	Vframe operator role
VObjectAdministrator	VObject	VObject administrator role
VObjectOperator	VObject	VObject operator role
ZoneUserFarm	Farm	Zone administrator role
ZoneUserGroup	Group	Group administrator role for zones

About role categories

Roles fall into a combination of categories, depending on whether and how users may display or modify them. [Table 33-2](#) describes VCS One role categories.

Table 33-2 Role categories in VCS One

Category	Description
System	Roles that are pre-defined by VCS One. Examples include <code>ServerFarmAdministrator</code> and <code>SystemOperator</code> . Users may not create system roles. Note that the term “system” does not refer to the system object.
Hidden	Roles that are used internally by VCS One and never displayed.
Removable	Roles that may be deleted. User-defined roles are in the removable category. Predefined roles are not removable.
Modifiable	Roles for which privileges may be added and deleted. User-defined roles are in the modifiable category, and so are some system roles. See “About roles” on page 219.

Most roles have two categories associated with them. For example, to display the `Category` attribute and its value for the `SystemAdministrator` role. Enter the command:

```
harole -value SystemAdministrator Category
```

Notice in the output that the `SystemAdministrator` role is in both the system category (that is, it is VCS One predefined) and in the removable category.

5 [system|removable]

About privileges categories

The following tables catalog the VCS One role types, and the operations available in each one.

Privileges that correspond to virtualization may be visible to the user. This capability is not supported in the current release, but is planned for a future release.

Catalog of farm privileges

[Table 33-3](#) displays the privileges in the Farm category:

Table 33-3 Privileges in the Farm category

Operation Privilege	Description
Add Cluster	Add a remote cluster definition to the VCS One cluster. (Applicable in VCS One global cluster setup)
Delete Cluster	Delete a remote cluster definition from the VCS One cluster. (Applicable in VCS One global cluster setup)
Modify Cluster	Modify the values of VCS One cluster attributes, including adding values, updating existing values, deleting values, and deleting attribute keys.
Add Type	Add a resource type definition.
Delete Type	Delete a resource type definition.
Modify Type	Change a resource type definition.
Add / Delete Attributes	Add or delete an attribute to an existing type. For example, the following command would add the attribute MyAttribute to the FileOnOff type: <pre>haattr -add FileOnOff MyAttribute</pre>
Modify Attributes	Modify an attribute of a particular type.
Add Role	Create a role definition.
Delete Role	Remove a role definition.
Modify Role	Change a role definition.
Log Add	This privilege is used by agents to log messages.

Table 33-3 Privileges in the Farm category

Operation Privilege	Description
Modify GTQ	Perform GTQ operations, which are actions to abort or flush service groups in the GTQ.
Modify Automation Settings	Change the settings for automated tasks.
Modify VType	Change a VObject type definition.
Purge Events	Delete notification log message events

Catalog of object privileges

[Table 33-4](#) displays the privileges in the Object category:

Table 33-4 Privileges in the object category

Operation Privilege	Description
Add System	Add a system to the VCS One cluster.
Delete System	Delete a system from the VCS One cluster.
Add Group	Add a service group to the VCS One cluster.
Delete Group	Delete a service group from the VCS One cluster.
Link Group	Create a service group dependency.
Unlink Group	Remove a service group dependency.
Modify Group Compatibility	Modify the compatibility specified for groups.
Add User	Add a user to the VCS One cluster.
Delete User	Delete a user from the VCS One cluster.
Read Only	View information about the object.
Add Frame	Not currently supported.
Delete Frame	Not currently supported.
Add Rule	Add a rule to automation policy.
Delete Rule	Delete a rule from automation policy.
Add Job	Add a job to automation policy.

Table 33-4 Privileges in the object category

Operation Privilege	Description
Delete Job	Delete a job from automation policy.
Execute Script	Execute a script as part of automation policy.
Add CSG	Add a composite service group to the VCS One cluster.
Delete CSG	Delete a composite service group from the VCS One cluster.
Add PFrame	Not currently supported.
Delete PFrame	Not currently supported.
Add VFrame	Not currently supported.
Delete VFrame	Not currently supported.
Link VFrame	Not currently supported.
Unlink VFrame	Not currently supported.
Modify VFrame Compatibility	Not currently supported.

Catalog of system privileges

[Table 33-5](#) displays the privileges in the System category:

Table 33-5 Privileges in the System category

Operation Privilege	Description
Add System to SystemList	Add system to service group's SystemList attribute. To add a system to a service group's SystemList, you must have this privilege on the system in addition to the Modify Group privilege on the group.
Delete Systems from SystemList	Remove system from a service group's SystemList attribute. To delete a system from a service group's SystemList, the user must have this privilege on the system and the Modify Group privilege on the group.
Freeze System	Freeze a system
Evacuate System	Evacuate a system
Unfreeze System	Unfreeze a system

Table 33-5 Privileges in the System category

Operation Privilege	Description
Modify System	Modify a system's attributes
Start Agent	Start an agent on a system
Stop Agent	Stop an agent on a system
Stop System	Stop a system
Modify Capacity	Modify a system's capacity attribute. User with this privilege requires Modify System privilege also.
Read Only	View information about systems
Modify OU	Move a system to a different location in the Organization Tree. You also need OU Move to Object and OU Move from Object privileges. See " Catalog of organization tree privileges " on page 637.
Link VFrame	Link a VFrame to a system. Not currently supported.
Unlink VFrame	Unlink a VFrame from a system. Not currently supported.
System Agent Dump FFDC	Allows the first failure data capture logs to dump on the system.

Catalog of group privileges

[Table 33-6](#) displays the privileges in the group category:

Table 33-6 Privileges in the group category

Operation Privilege	Description
Online Group	Bring a group online.
Offline Group	Take a group offline.
Switch Group	Switch a service group from one system to another.
Freeze Group	Freeze a service group, such that it cannot be brought online, taken offline, or failed over.
Unfreeze Group	Unfreeze a service group.
Enable Group	Enable a group, so that it may be brought online or switched, for example.

Table 33-6 Privileges in the group category

Operation Privilege	Description
Disable Group	Disable a group, such that it may not be brought online or taken offline.
Clear Group	Change resources from faulted to offline.
Flush Group	Cancel the online or offline operation that is currently being performed on the service group.
Modify Group	Modify the attributes of a service group. Users must have also this privilege to modify group priority, load, and fault policy.
Clear Admin Wait	Clear the ADMIN_WAIT state of resources in a group.
Add Resource	Add a resource to a group.
Delete Resource	Delete a resource from a group.
Enable Resource	Enable all resource in a group; agents start monitoring.
Disable Resource	Disable all resource in a group; agents stop monitoring.
Link Resource	Create a dependency link between resources.
Unlink Resource	Remove the dependency link between resources.
Modify Priority	Modify a service group's Priority attribute. User also requires Modify Group privilege
Modify Load	Modify a service group's Load attribute. User also requires Modify Group privilege.
Modify Fault Policy	Modify a service group's GrpFaultPolicy, NodeFaultPolicy, or ResFaultPolicy attribute. User also requires Modify Group privilege. To modify ResFaultPolicy attribute, user requires Modify Group and Group Fault Policy privileges for the parent resource group.
Read Only	View information about groups. This privilege also allows read privileges on the group's resources.
Modify OU	Move a group to a different location in the Organization Tree. You also need OU Move to Object and OU Move from Object privileges. See “Catalog of organization tree privileges” on page 637.

Table 33-6 Privileges in the group category

Operation Privilege	Description
Add to GroupList	<p>Add this group to a composite service group's GroupList attribute.</p> <p>To add a group to a composite service group, the user must have this privilege on the group as well as the Modify CSG privilege on the composite service group.</p>
Delete from GroupList	<p>Remove this group from a composite service group's GroupList attribute.</p> <p>To delete a group from a composite service group, the user must have this privilege on the group as well as the Modify CSG privilege on the composite service group.</p>

Catalog of composite service group privileges

[Table 33-7](#) displays the privileges in the composite service group category:

Table 33-7 Privileges in the composite service group category

Operation Privilege	Description
Modify CSG	Modify the attributes of a composite service group.
Read Only	View information about composite service groups.
Online CSG	<p>Bring a composite service group online.</p> <p>The user does not also require service group online privileges for the constituent service groups to bring a composite service group online.</p> <p>However, this privilege does not allow the user to bring the constituent groups online individually. To bring an service group online separate from the CSG, the user must have the Online Group privilege on the group.</p>
Offline CSG	<p>Take a composite service group offline.</p> <p>The user does not also require service group offline privileges for the constituent service groups to bring a composite service group offline.</p> <p>However, this privilege does not allow the user to bring the constituent groups offline individually. To bring an service group offline separate from the CSG, the user must have the Offline Group privilege on the group.</p>

Table 33-7 Privileges in the composite service group category

Operation Privilege	Description
Switch CSG	Switch a composite service group from one VCS One cluster to another.
Request Authority	Take Authority of a composite service group. See “Authority” on page 692.
Modify OU	Move a composite service group to a different node in the organization tree. You also need OU Move to Object and OU Move from Object privileges. See “Catalog of organization tree privileges” on page 637.
Flush CSG	Clear any IntentOnline entry for any constituent service group of the CSG. A user with this privilege does not require the Modify GTQ privilege to flush the IntentOnline entries.

Catalog of resource privileges

[Table 33-8](#) displays the privileges in the resource category:

Table 33-8 Privileges in the resource category

Operation	Description
Online Resource	Bring a resource online.
Offline Resource	Take a resource offline.
Offline Propagate	Offline a resource and specify its children be taken offline.
Clear Resource	Change a resource’s state from faulted to offline.
Clear Admin Wait	Remove resource from the ADMIN_WAIT state.
Probe Resource	Monitor a resource and send state to VCS One client daemon.
Modify Resource	Change the value of a resource attribute.
Action	Direct the agent take the specified action (in a token) on the resource.
Event	Able to invoke triggers for the resource

Table 33-8 Privileges in the resource category

Operation	Description
Refresh Info	Direct the Info entry point to update value of ResourceInfo entry point.
Flush Info	Clears the current value of ResourceInfo entry point.
Read Only	View information about resources.

Catalog of user privileges

[Table 33-9](#) displays the privileges in the user category:

Table 33-9 Privileges in the user category

Operation	Description
Modify User	Change the value of a user attribute.
Add Privilege	Add to the user's permitted operations.
Delete Privilege	Delete a user's privilege to perform an operation.
Enable User	Restore a disabled user's privileges.
Disable User	Disable a user. A disabled user has no privileges in the farm. Disabled users do not have read privileges.
Read Only	View information about users
Modify OU	Move a user to a different location in the Organization Tree. You also need OU Move to Object and OU Move from Object privileges. See “Catalog of organization tree privileges” on page 637.

Catalog of organization tree privileges

[Table 33-10](#) displays the privileges in the OT category:

Table 33-10 Privileges in the OT category

Operation	Description
Read Only	View the organization tree.
Add OUName	Add an OUName node to the organization tree.
Delete OUName	Delete an OUName node from the organization tree.

Table 33-10 Privileges in the OT category

Operation	Description
Modify OUName	Modify an OUName node in the organization tree.
Add OUValue	Add an OUValue node to the organization tree.
Delete OUValue	Delete an OUValue node from the organization tree.
Modify OUValue	Modify an OUValue node in the organization tree.
Move to Object	<p>Move a service group, system, user, user group, or frame object to a node in the organization tree.</p> <p>To move an object the user must also have Modify OU privilege on the object that is moved.</p>
Move from Object	<p>Move a service group, system, user, user group, or frame object away from a node in the organization tree.</p> <p>To move an object the user must also have Modify OU privilege on the object that is moved.</p>
Add EA	Add an extended attribute to an OUValue node.
Delete EA	Delete an existing extended attribute.
Modify EA	Modify an existing extended attribute.

Catalog of notifier privileges

[Table 33-11](#) displays the privileges in the notifier category:

Table 33-11 Privileges in the notifier category

Operation	Description
Email	Specify an email recipient to be notified as part of a notification or business rule.
SNMP	Specify SNMP console to be notified as part of a notification or business rule.
Syslog	Specify Syslog to be notified as part of a notification or business rule.

Catalog of VObject privileges

VObject privileges correspond to virtualization. This capability is not supported in the current release, but is planned for a future release.

[Table 33-12](#) displays the privileges in the VObject category:

Table 33-12 Privileges in the VObject category

VObject Privilege	Description
Modify Frame	Modify a VObject.
Modify OU	Modify the organization unit to which the VObject is attached. User may also need OU privileges Move to Object and Move from Object.
Read Only	View information about the VObject.
Associate	Associate the VObject with another object.
Dissociate	Dissociate the VObject from another object.
Action	Perform actions on a VObject. Some examples are start and stop. Also included are custom scripted actions.

Catalog of Pframe privileges

Pframe privileges correspond to virtualization. This capability is not supported in the current release, but is planned for a future release.

[Table 33-13](#) displays the privileges in the Pframe category:

Table 33-13 Privileges in the Pframe category

PFrame Privilege	Description
Add Pframe to SystemList	Add this Pframe to a service group's SystemList attribute value.
Delete Pframe from SystemList	Delete a Pframe to a service group's SystemList attribute value.
Freeze Pframe	Freeze a Pframe.
Evacuate Pframe	Evacuate a Pframe.
Unfreeze Pframe	Unfreeze a Pframe.
Modify Pframe	Modify the attributes of a Pframe.
Start Agent	Start an agent on the Pframe.
Stop Agent	Stop an agent from running on the Pframe.
Stop Pframe	Stop the vcsoneclientd daemon from running on the Pframe.

Table 33-13 Privileges in the Pframe category

PFrame Privilege	Description
Modify Capacity	Modify the Capacity attribute of the Pframe.
Read Only	View information about the Pframe.
Modify OU	Modify the organization unit to which the Frame is attached. User may also need OU privileges Move to Object and Move from Object.
Pframe Agent Dump FFDC	Allows the first failure data capture logs to dump on the Pframe.
Associate objects	Associate a Pframe with a VObject
Dissociate objects	Dissociate a Pframe with a VObject.

Catalog of Vframe privileges

Vframe privileges correspond to virtualization. This capability is not supported in the current release, but is planned for a future release.

[Table 33-14](#) displays the privileges in the Vframe category:

Table 33-14 Privileges in the Vframe category

Vframe Privilege	Description
Online Vframe	Bring a Vframe online on a Pframe.
Offline Vframe	Take a Vframe offline on a Pframe.
Switch Vframe	Switch a Vframe between two Pframes.
Freeze Vframe	Freeze a Vframe.
Unfreeze Vframe	Unfreeze a Vframe.
Enable Vframe	Enable a Vframe. A Vframe must be enabled before it can be used.
Disable Vframe	Disable a Vframe.
Clear Vframe	Clear a fault on a frame.
Flush Vframe	Flush a Vframe.
Modify Vframe	Modify attributes of a Vframe.
Clear Admin Wait	Clear the admin wait condition from a Vframe.

Table 33-14 Privileges in the Vframe category

Vframe Privilege	Description
Add Resource	Add a resource to a Vframe.
Delete Resource	Delete a resource from a Vframe.
Enable Resource	Enable a resource for use on a Vframe.
Disable Resource	Disable a resource for use on a Vframe.
Link Resource	Link a resource to a Vframe.
Unlink Resource	Unlink a resource from a Vframe.
Change Priority	Change the Priority attribute value on a Vframe.
Change Load	Change the Load value on a Vframe.
Change Fault Policy	Change the fault policy of a Vframe.
Read Only	View information about the frame.
Modify OU	Modify the organization unit to which the Frame is attached. User may also need OU privileges Move to Object and Move from Object.
Link System	Link a system object to a vframe object.
Unlink System	Unlink a system object from a vframe object.
Associate Objects	Associate a Vframe with a VObject
Dissociate Objects	Dissociate a Vframe with a VObject.
Perform Action	Perform actions on a frame. Some examples are start and stop. Also included are custom scripted actions.

Catalog of automation privileges

[Table 33-15](#) displays the privileges in the Automation category. The ServerFarmObjectAdministrator role has all these privileges by default

Table 33-15 Privileges in the Automation category

Operation	Description
Modify Rule	Modify a business policy automation rule. This privilege does not include the ability to create a rule.
Execute Rule	Execute a business policy automation rule.

Table 33-15 Privileges in the Automation category

Operation	Description
Modify Job	Modify a business policy automation job.
Execute Job	Execute a business policy automation job.
Read Only	View information about business policy automation rules and jobs in the OUPath over which the privilege has been assigned.
Take OwnerShip	Assume the ownership of a rule.

Automated tasks reference

This chapter included the following topics:

- [About events](#)
- [About rules](#)
- [About jobs](#)
- [About tasks](#)

About events

A single event triggers one or more rules.

The event that triggers a rule can be one of the following types:

- Policy Master (generated) event

These events are initiated by the Policy Master. Events can involve the following objects:

Farm	System	Service Group
Resource	User	User group
Composite Service Group		Organization unit

The actions taken can be proactive, such as directing a resource to go offline, or reactive, such as when a resource has faulted.

A complete list of events is available

See [Table 34-1, “VCS One events and associated parameters,”](#) on page 645.

- Scheduled events

These events are initiated by the Business Policy Automation scheduler. These events are defined by a day, date, time of day, or range of time. The scheduler triggers these events.

Policy Master events reference

Table 34-1 lists the events generated by the Policy Master, and the parameters that will be passed as arguments. These parameters are used to check pre-defined conditions before the job is run. They are also used as arguments to the tasks.

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
Farm (VCS One cluster) events			
CLUSTER_SECURITY_PRINCIPAL_DELETE	ERROR	The security principal from AT has been deleted.	<ol style="list-style-type: none"> 1 CLUSTER_SECURITY_PRINCIPAL_DELETE 2 PRPL_NAME The name of the principal that is deleted. 3 DOMAIN_NAME 4 DOMAIN_TYPE
PM_STARTED	INFORMATION	The Policy Master started up	<ol style="list-style-type: none"> 1 PM_STARTED 2 SYS Name of system where Policy Master has started
RCLUSTER_ADD	INFORMATION	Remote cluster added	<ol style="list-style-type: none"> 1 RCLUSTER_ADD 2 RCLUSTER
RCLUSTER_DELETE	INFORMATION	Remote VCS One cluster deleted	<ol style="list-style-type: none"> 1 RCLUSTER_DELETE 2 RCLUSTER
RCLUSTER_LINK_FAILOVER	WARNING	Remote VCS One cluster state changed to LINK_FAILOVER. See “Cluster states in VCS One global clusters” on page 762.	<ol style="list-style-type: none"> 1 RCLUSTER_LINK_FAILOVER 2 RCLUSTER

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
RCLUSTER_RUNNING	INFORMATION	Remote VCS One cluster state changed to RUNNING. See “Cluster states in VCS One global clusters” on page 762.	1 RCLUSTER_RUNNING 2 RCLUSTER
RCLUSTER_EXITED	INFORMATION	Remote VCS One cluster state changed to EXITED. See “Cluster states in VCS One global clusters” on page 762.	1 RCLUSTER_EXITED 2 RCLUSTER
RCLUSTER_FAULTED	ERROR	Remote VCS One cluster state changed to FAULTED. See “Cluster states in VCS One global clusters” on page 762.	1 RCLUSTER_FAULTED 2 RCLUSTER
RCLUSTER_TRANSITIONING	WARNING	Remote VCS One cluster state is TRANSITIONING	1 RCLUSTER_TRANSITIONING 2 RCLUSTER
System events			
SYS_ADD	INFORMATION	System added to VCS One cluster	1 SYS_ADD 2 SYS 3 PLAT 4 OUVPATH
SYS_DELETE	INFORMATION	System deleted from VCS One cluster	1 SYS_DELETE 2 SYS 3 PLAT 4 OUVPATH
SYS_FREEZE	INFORMATION	System frozen	1 SYS_FREEZE 2 SYS 3 PLAT 4 OUVPATH

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
SYS_UNFREEZE	INFORMATION	System unfrozen	1 SYS_UNFREEZE 2 SYS 3 PLAT 4 OUVPATH
SYS_MOVE	INFORMATION	System moved to different Organization Tree node	1 SYS_MOVE 2 SYS 3 PLAT 4 OUVPATH 5 MOVE_FROM 6 MOVE_TO
SYS_EXITED	INFORMATION	The vcsoneclient daemon is offline on this system.	1 SYS_EXITED 2 SYS 3 PLAT 4 OUVPATH
SYS_ATTR_CHANGE	INFORMATION	An attribute has changed on a system object.	1 SYS_ATTR_CHANGE 2 SYS 3 PLAT 4 OUVPATH 5 ATTRNAME 6 SCOPE 7 DIMENSION 8 DATATYPE 9 VALUE
SYS_RESTARTED_HASHADOW	ERROR	The vcsoneclient daemon has been restarted by the shadow	1 SYS_RESTARTED_HASHADOW 2 SYS 3 PLAT 4 OUVPATH
SYS_JOINED	INFORMATION	System joined the VCS One cluster.	1 SYS_JOINED 2 SYS 3 PLAT 4 OUVPATH

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
SYS_DDNA	ERROR	System is alive but the proxy is not running on the system. The state of the system is Daemon Dead Node Alive (DDNA)	<ol style="list-style-type: none"> 1 SYS_DDNA 2 SYS 3 PLAT 4 OUVPATH
SYS_FAULTED	ERROR	System has faulted	<ol style="list-style-type: none"> 1 SYS_FAULTED 2 SYS 3 PLAT 4 OUVPATH
SYS_AGENT_FAULTED	ERROR	Agent is faulted on the system	<ol style="list-style-type: none"> 1 SYS_AGENT_FAULTED 2 SYS 3 PLAT 4 OUVPATH 5 AGENT
SYS_AGENT_RESTART	WARNING	Agent has restarted on the system	<ol style="list-style-type: none"> 1 SYS_AGENT_RESTART 2 SYS 3 PLAT 4 OUVPATH 5 AGENT
SYS_SYSINFO_CHANGED	INFORMATION	System Sysinfo changed	<ol style="list-style-type: none"> 1 SYS_SYSINFO_CHANGED 2 SYS 3 PLAT 4 OUVPATH Path of the Organization unit value node. 5 KEY 6 OVAL Old value 7 NVAL New value

Service group events

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
GRP_ADD	INFORMATION	Group added to VCS One cluster	1 GRP_ADD 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 CSG
GRP_DELETE	INFORMATION	Group deleted from VCS One cluster	1 GRP_DELETE 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 CSG
GRP_FREEZE	INFORMATION	Group frozen	1 GRP_FREEZE 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 CSG
GRP_UNFREEZE	INFORMATION	Group unfrozen	1 GRP_UNFREEZE 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 CSG
GRP_MOVE	INFORMATION	Group moved to different Organization Tree node	1 GRP_MOVE 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 MOVE_FROM 7 MOVE_TO 8 CSG

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
GRP_FAULT	ERROR	Service group has faulted	<ol style="list-style-type: none"> 1 GRP_FAULT 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 CSG
GRP_ATTR_CHANGE	INFORMATION	Service group attribute changed.	<ol style="list-style-type: none"> 1 GRP_ATTR_CHANGE 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 ATTRNAME 8 SCOPE 9 DIMENSION 10 DATATYPE 11 VALUE 12 CSG
GRP_INIT_ONLINE	INFORMATION	Service group online initiated	<ol style="list-style-type: none"> 1 GRP_INIT_ONLINE 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 WHY Use either POLICY (Policy Master) or MANUAL (User initiated) to denote the source of the online. 8 CSG

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
GRP_ONLINE	INFORMATION	Service group is online	<ol style="list-style-type: none"> 1 GRP_ONLINE 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 CSG
GRP_INIT_OFFLINE	INFORMATION	Service group offline initiated	<ol style="list-style-type: none"> 1 GRP_INIT_OFFLINE 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 WHY Use either POLICY (Policy Master) or MANUAL (User initiated) to denote the source of the offline. 8 CSG
GRP_OFFLINE	INFORMATION	Service group is offline	<ol style="list-style-type: none"> 1 GRP_OFFLINE 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 CSG

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
GRP_SWITCH	INFORMATION	Service group switching initiated	<ol style="list-style-type: none"> 1 GRP_SWITCH 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 TOSYS 8 CSG
GRP_KICKOUT	WARNING	Service group is getting kicked out from a system to allow high priority groups to come online	<ol style="list-style-type: none"> 1 GRP_KICKOUT 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 HIPRIGRP 8 CSG
GRP_SWITCHING_LOAD_INCREMENTED	ERROR	Service group switching initiated due to increased load	<ol style="list-style-type: none"> 1 GRP_SWITCHING_LOAD_INCREMENTED 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 TOSYS 8 CSG
GRP_CONCURRENCY VIOLATION	CRITICAL	Service group is online on more than one system	<ol style="list-style-type: none"> 1 GRP_CONCURRENCY VIOLATION 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 CSG

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
GRP_ONLINE_CANCELLED_POSSIBLE_CONCURRENCY	CRITICAL	Failed to bring a service group online due to possible concurrency violation	<ol style="list-style-type: none"> 1 GRP_ONLINE_CANCELLED_POSSIBLE_CONCURRENCY 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 CSG
GRP_NOFAILOVER	CRITICAL	Service group could not failover to any other system in the VCS One cluster	<ol style="list-style-type: none"> 1 GRP_NOFAILOVER 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 CSG
GRP_COMPATIBILITY_VIOLATION	CRITICAL	Service group compatibility violation detected	<ol style="list-style-type: none"> 1 GRP_COMPATIBILITY_VIOLATION 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 CSG
GRP_LOAD_VIOLATION	CRITICAL	Service group compatibility load detected	<ol style="list-style-type: none"> 1 GRP_LOAD_VIOLATION 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 CSG

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
GRP_DEPENDENCY_VIOLATION	CRITICAL	Service group dependency violation detected	<ol style="list-style-type: none"> 1 GRP_DEPENDENCY_VIOLATION 2 GRP 3 PLAT 4 OUVPATH 5 PRIORITY 6 SYS 7 CSG
Composite service group events			
CSG_ADD	INFORMATION	Composite service group is added	<ol style="list-style-type: none"> 1 CSG_ADD 2 CSG 3 OUVPATH
CSG_ATTN	ERROR	Composite service group flagged to denote it requires user attention.	<ol style="list-style-type: none"> 1 CSG_ATTN 2 CSG 3 OUVPATH
CSG_ATTN_REMOTE	ERROR	Composite service group flagged to denote it requires user attention in the remote VCS One cluster.	<ol style="list-style-type: none"> 1 CSG_ATTN_REMOTE 2 CSG 3 RCLUSTER
CSG_DELETE	INFORMATION	Composite service group is deleted	<ol style="list-style-type: none"> 1 CSG_DELETE 2 CSG 3 OUVPATH
CSG_ONLINE	INFORMATION	Composite service group is online	<ol style="list-style-type: none"> 1 CSG_ONLINE 2 CSG 3 OUVPATH
CSG_ONLINE_REMOTE	INFORMATION	Composite service group is online on the remote VCS One cluster	<ol style="list-style-type: none"> 1 CSG_ONLINE_REMOTE 2 CSG 3 RCLUSTER

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
CSG_OFFLINE	INFORMATION	Composite service group is offline	1 CSG_OFFLINE 2 CSG 3 OUVPATH
CSG_OFFLINE_REMOTE	INFORMATION	Remote composite service group is offline	1 CSG_OFFLINE_REMOTE 2 CSG 3 RCLUSTER
CSG_MOVE	INFORMATION	Composite service group moves in the organization tree	1 CSG_MOVE 2 CSG 3 MOVE_FROM 4 MOVE_TO 5 OUVPATH
CSG_ATTR_CHANGE	INFORMATION	Modification of a composite service group attribute	1 CSG_ATTR_CHANGE 2 CSG 3 OUVPATH 4 ATTRNAME 5 SCOPE 6 DIMENSION 7 DATATYPE 8 VALUE
CSG_CONCURRENCY_VIOLATION	CRITICAL	Composite service group has a concurrency violation	1 CSG_CONCURRENCY_VIOLATION 2 CSG
CSG_PARTIAL	INFORMATION	Composite service group in partial state	1 CSG_PARTIAL 2 CSG 3 OUVPATH
CSG_PARTIAL_REMOTE	INFORMATION	Remote composite service group in partial state	1 CSG_PARTIAL_REMOTE 2 CSG 3 RCLUSTER

Resource events

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
RES_STATE_UNKNOWN	ERROR	Resource state is unknown	<ol style="list-style-type: none"> 1 RES_STATE_UNKNOWN 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS
RESOURCE_MONITOR_TIMEOUT	ERROR	Resource monitor timed out	<ol style="list-style-type: none"> 1 RESOURCE_MONITOR_TIMEOUT 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS
RES_OFFLINE_INEFFECTIVE	ERROR	Offline ineffective for the resource	<ol style="list-style-type: none"> 1 RES_OFFLINE_INEFFECTIVE 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS
RES_RESTARTING	ERROR	Resource is restarting	<ol style="list-style-type: none"> 1 RES_RESTARTING 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
RES_AUTO_ONLINE	WARNING	Resource went online outside VCS One control	1 RES_AUTO_ONLINE 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS
RES_FAULT	ERROR	Resource has faulted	1 RES_FAULT 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS
RES_ADMIN_WAIT	ERROR	Resource is in ADMIN_WAIT state	1 RES_ADMIN_WAIT 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS
AGENT_GEN_SNMP	CRITICAL	Agent for the resource has generated notification	1 AGENT_GEN_SNMP 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS 8 AGENTMSG

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
RESOURCE_MONITOR_TIME_CHANGED	WARNING	The time taken for execution of monitor entry point for resource has changed	<ol style="list-style-type: none"> 1 RESOURCE_MONITOR_TIME_CHANGED 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS 8 INFO
RES_STATE_CHANGE	INFORMATION	<p>Resource underwent a state transition on the system.</p> <p>Note: To generate the RES_STATE_CHANGE event, make sure the group level attribute, TriggerResStateChange, is set to 1.</p>	<ol style="list-style-type: none"> 1 RES_STATE_CHANGE 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS 8 ARG
RES_ATTR_CHANGE	INFORMATION	Resource attribute changed	<ol style="list-style-type: none"> 1 RES_ATTR_CHANGE 2 RES 3 GRP 4 TYPE 5 PLAT 6 OUVPATH 7 SYS 8 ATTRNAME 9 SCOPE 10 DIMENSION 11 DATATYPE 12 VALUE

User, User group, Organization Tree, Extended Attribute events

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
USER_MOVE	INFORMATION	User moved to new Organization Tree node	1 USER_MOVE 2 USER 3 OUVPATH 4 MOVE_FROM 5 MOVE_TO
USERGROUP_MOVE	INFORMATION	User group moved to new Organization Tree node	1 USERGROUP_MOVE 2 USER 3 OUVPATH 4 MOVE_FROM 5 MOVE_TO
OUNAME_ADD	INFORMATION	Organization unit name node added to Organization tree	1 OUNAME_ADD 2 OUNPATH
OUNAME_DELETE	INFORMATION	Organization unit name node deleted from Organization tree	1 OUNAME_DELETE 2 OUNPATH
OUVALUE_ADD	INFORMATION	Organization unit value node added to Organization tree	1 OUVALUE_ADD 2 OUVPATH
OUVALUE_DELETE	INFORMATION	Organization unit value node deleted from Organization tree	1 OUVALUE_DELETE 2 OUVPATH
EA_ADD	INFORMATION	Extended attribute added to VCS One cluster	1 EA_ADD 2 OUVPATH 3 EA 4 EATYPE

Table 34-1 VCS One events and associated parameters

Event	Severity	Description	Parameters Passed
EA_DELETE	INFORMATION	Extended attribute deleted from VCS One cluster	<ol style="list-style-type: none"> 1 EA_DELETE 2 OUVPATH 3 EA 4 EATYPE

About rules

A rule can be a business rule or a notification rule.

A rule is triggered by an event and executes a job. Events are not part of a workflow; the order of job execution may not be the same as the order of the events that invoke the job. However, multiple tasks associated with a job are executed in sequence.

Using notification rules you can specify email, SNMP and syslog notifications.

Rules are not user-private. All users that have read privileges of rules can view all rules configured in the VCS One cluster.

A rule has the following components:

Rule name	User-selected name of the rule. A valid name starts with an alpha character and has no special characters or white space.
Trigger using	The type of event that triggers the rule to run. Policy Master event or schedule event.
Rule description	Description of the rule.
Rule organization unit node path	The node in the Organization Tree that defines the objects in the Organization Tree affected by the rule.
Creator	User that created the rule.
Owner	Rule owner can be the rule creator or any of the user groups to which the creator belongs. The rule is run using the privileges associated with the owner.
Quiet time	<p>Controls how often a rule may be triggered for the same object and the same event.</p> <p>The number of seconds to wait after the rule has been triggered, and before the rule may be triggered again for the same object and the same event.</p>

Enabled	If true the rule will run, if not true the rule will not run.
Event criteria	The event criteria changes depending on the type of event: Policy Master event: Defines the list of objects and organization unit nodes on which the event will occur. Schedule event: Defines the date and time the event will occur.
Condition set	This field allows you to define a set of conditions to evaluate before the job executes. The rule can be attribute based or time based. See “Rule conditions reference” on page 661.
Job to execute	Job name to execute

More information is available about privileges for rules.
See [“Catalog of automation privileges”](#) on page 641.

Rule conditions reference

Within the rule definition, you can define conditions to evaluate before the job is executed. A condition is created in the form of a condition expression, and can be one of the following types:

Schedule based condition	Use schedule-based conditions to define a time for a Policy Master event. The condition is defined by being before or after a hour, minute and date. The time refers to the time on the Policy Master system.
Attribute-based condition	The attribute name can only be a scalar global attribute or extended attribute. Use attribute-based conditions to check of one of the following attribute values: <ul style="list-style-type: none">■ Object type: Checks if the object is of type System or Group■ Object name: Can be a specific system or group object name, or it could be a variable (explicit object or event object.)■ Condition - Operator (equal to or not equal to) - Value condition.

Multiple conditions are implicitly joined with the AND operator.

About jobs

A Job is associated with one or more rules. Jobs are executed automatically through pre-configured rules or manually through the console. You can not execute a job through the command line.

A job has an associated OUPath. Execution of a job can not access any objects outside of the scope of the OU path. The scope of the OUPath includes the OUNode and all nodes below that node in the Organization Tree. It does not include nodes above or adjacent to the node.

A user must have the Execute Job privilege to execute a job. A user must also have appropriate privileges to execute both the tasks in the job and the job itself.

Jobs are not user-private. A job is visible to all users on its OU node and above that have read privileges of business policy automation.

See [“Catalog of automation privileges”](#) on page 641.

Components of a job

A Job consists of one or more tasks, and has the following components:

Job name	User-selected name of the job.
Job description	Description of the job. Can be 1024 characters.
Job organization unit node path	The node in the Organization Tree that defines the objects associated with the job. This OUPath defines the objects in the Organization Tree affected by the job.
List of tasks	The list of tasks that the job executes

More information is available about privileges for jobs.

See [“Catalog of automation privileges”](#) on page 641.

Privileges of a job

The tasks associated with a job are executed with the privileges of the user who owns the job.

Manual job execution

VCS One checks if the user has the EXECUTE_JOB privilege for the job, as well as sufficient privileges for each task in the job.

Automated job execution

The job will be executed by the user in the context of the rule's owner.

Only the rule's owner explicit privileges will be used to execute the job. The owner's user group privileges will not be considered.

About tasks

Tasks are the actions taken in the VCS One cluster as the result of an event. Tasks do not exist alone; they are always part of a job. The list of available tasks are pre-defined and not user-editable.

One of the following actions is the result of a task:

- A VCS One command runs
- An email is sent
- A script runs
- A syslog notification

Each task has input parameters that provide information about the object(s) associated with the task.

The input parameters are configured during definition of the job.

[Table 34-2](#) lists the predefined tasks actions, description, and input parameters for each available action.

Table 34-2 Predefined task actions and required task parameters

Task action	Task description	Parameters
SCRIPT	Execute script	1 SCRIPTNAME 2 ARGS 3 USEEVENT

Table 34-2 Predefined task actions and required task parameters

Task action	Task description	Parameters
SSHSCRIPT	Execute script using SSH	<ol style="list-style-type: none"> 1 SCRIPTNAME 2 ARGS 3 USEEVENT 4 USER 5 HOST 6 GRPHOST 7 AUTH 8 PASSWORD 9 PASSPHRASE 10 PRIVATEKEY
SEND_MAIL	Send Mail	<ol style="list-style-type: none"> 1 ADDRESS 2 SUB 3 BODY 4 USE_OWNER_SNMP
SNMP_TRAP	Send an SNMP trap	<ol style="list-style-type: none"> 1 CONSOLES 2 USE_OWNER_SNMP
SYSLOG	Send Syslog	<ol style="list-style-type: none"> 1 HOSTS 2 MESSAGES 3 PREFIX_EVENT_MESSAGE
HACOMMAND	<p>Execute ha-command</p> <p>Note: Not all ha-commands are supported. Use the validate option in the Task Details page when you configure the details of the task to confirm whether a command is valid and supported.</p> <p>See “Creating a job” on page 421.</p>	<ol style="list-style-type: none"> 1 COMMAND
CSG_ONLINE	Bring composite service group online	<ol style="list-style-type: none"> 1 CSG Composite service group name
CSG_OFFLINE	Take composite service group offline	<ol style="list-style-type: none"> 1 CSG Composite service group name

Table 34-2 Predefined task actions and required task parameters

Task action	Task description	Parameters
GRP_ONLINE	Bring service group online	<ol style="list-style-type: none"> GRP Group name SYS Target system to online the group EVACLOWPRI PROPAGATE
GRP_OFFLINE	Take service group offline	<ol style="list-style-type: none"> GRP Group name SYS System to offline the group from PROPAGATE
GRP_ADDSYS_TO_SYSLIST	Add system to SystemList attribute	<ol style="list-style-type: none"> GRP Group name SYS PROPAGATE
GRP_FREEZE	Freeze service group	<ol style="list-style-type: none"> GRP Group name PROPAGATE
GRP_SETPRI	Set Service Group Priority	<ol style="list-style-type: none"> GRP Group name PRI Value to set the group's Priority attribute PROPAGATE
SYS_FREEZE	Freeze system	<ol style="list-style-type: none"> SYS EVACUATE
REFRESH_SYSTEMLIST	Refresh SystemList attribute	<ol style="list-style-type: none"> GRP
GRP_STATE_WAIT	Group state wait	<ol style="list-style-type: none"> GRP SYS STATE
SYS_STATE_WAIT	System state wait	<ol style="list-style-type: none"> SYS STATE

Table 34-2 Predefined task actions and required task parameters

Task action	Task description	Parameters
RES_STATE_WAIT	Resource state wait	1 RES 2 SYS 3 STATE

Privileges of a task

When using the Script task, the user running the task must have VCS One cluster level EXECUTE_SCRIPT privileges. The script is executed as the root user on the Policy Master node.

Configuration file reference

This chapter includes the following topics:

- [About the VCS One configuration in XML](#)
- [Building blocks of an XML configuration file](#)
- [The main.xml file format](#)
- [Sample main.xml configuration file](#)
- [The bpa.xml file format](#)
- [Sample bpa.xml configuration file](#)
- [The prefs.xml file](#)

About the VCS One configuration in XML

The VCS One configuration in XML format is provided in the following files. The XML configuration files are by default below the `$VCSONE_CONF/conf/directory`.

- `main.xml` – contains the VCS One object instances like service group, systems, etc. and their attributes.
- `types.xml` – contains the bundled agent definitions
- `bpa.xml` – contains definitions of business rules, notification rules, and jobs.
- `prefs.xml` – contains the user interface preferences and custom view definitions.

- `main.dtd` – reveals the schema and syntax of the `main.xml`. Make sure you include this in the beginning of the `main.xml` file:

```
<!DOCTYPE config SYSTEM main.dtd>
```

- `types.dtd` – reveals the schema and syntax of the `types.xml`. Make sure you include this in the beginning of `types.xml` file:

```
<!DOCTYPE config SYSTEM types.dtd>
```

- `orgtree.dtd` – reveals the schema and syntax of the `orgtree.xml` file. Make sure you include the following line in the beginning of the `orgtree.xml` file.

```
<!DOCTYPE config SYSTEM orgtree.dtd>
```

Building blocks of an XML configuration file

Following are some of the major building blocks of an VCS One XML configuration file:

Attribute definition

An attribute definition in an XML file looks like the following:

```
<attributes name="PathName" type="str" dimension="scalar">  
  <must_configure>1</must_configure>  
  <editable>1</editable>  
  <default><scalar>/tmp/foo</scalar></default>  
</attributes>
```

Attribute instance

An attribute instance in an XML file looks like the following:

```
<attribute name="PathName">  
  <scalar>"/tmp/test_res"</scalar>  
</attribute>
```

Object instance

An object instance in an XML file looks like the following:

```
<group name="Test_Group">
  <attributes>
    <attribute name="SystemList">
      <val name="prod_sys1">0</val>
      <val name="prod_sys2">1</val>
    </attribute>
  </attributes>
  <resources>
    <resource name="Test_Res" type="FileOnOff">
      <attribute name="Pathname">
        <scalar>"/tmp/test_res</scalar>
      </attribute>
    </resource>
    .....more resources.....
    <link parent="Test_Res1" child="TestRes2"/>
  </resources>
</group>
```

The above example depicts a service group definition. Other object definitions like clusters, systems, etc. will be similar.

Group dependency

A group dependency in a XML file looks like the following:

```
<group name="Test_Group1">
  .....
</group>
<group name="Test_Group2">
  .....
  <requires>
    <child>"Test_grp1"</child>
    <kind>"hard"</kind>
    <location>"local"</location>
  </requires>
</group>
```

The main.xml file format

The main.xml file has include clauses along with definitions for the cluster, systems, service groups, and resources. It also includes service group and resource dependency clauses. The following outlines the format of the main.xml file.

Include clauses

Include clauses provide a modular approach to allow additional configuration files to be incorporated into the main.xml file. The types.<platform>.xml file, which contains resource type definitions, is always an include clause in the main.xml file. Additional include clauses are typically required for the configuration files of custom agents. For example:

```
<include>"types.linux.xml"</include>
<include>"OracleTypes.xml"</include>
```

Cluster definition

Defines the attributes of the VCS One cluster, including the cluster name and the names of the users. For example:

```
<cluster name="Test_clus">
    ..... // Attributes
</cluster>
```

System definition

Specifies the name of each system in the VCS One cluster. The system names must match the one returned by the `hostname` command.

Service group definition

This section of the file defines the following name, attributes, resources and dependencies of the service group:

- Service group name and attributes

The VCS One cluster wide unique name of the service group and service group level attributes are defined first. The following is an example of the definition of the service group attribute `SystemList`, which designates all systems on which a service group can come online.

```
<group name="Test_Group1">
    .....// Attributes / Resources / Dependencies.
</group>
```

The following example configures the `SystemList` attribute for the service group to be able to come online on `SystemA`, `SystemB` and `SystemC`.

```
<SystemList>
    <val key="SystemA"></val>
    <val key="SystemB"></val>
    <val key="SystemC"></val>
</SystemList>
```

- Resources defined

Defines each resource used in the group. Resources can be added in any order.

- Service Group Dependency Clause

Defines dependencies between this service group and another. The keyword “requires” indicates a service group dependency. The following is an XML example of the section of the service group definition where the type of the service group dependency is defined. This example is of an local hard service group dependency.

```
<requires>
  <group>foo</group>
  <kind>hard</kind>
  <location>local</location>
```

- Resource Dependency Clause

A dependency between resources is indicated by the keyword “link” followed by the parent resource name and then the child resource name. For example:

```
<link parent="vol1" child="dg1" />
```

Resource dependencies indicate the child resource must be online before the parent resource can be brought online, and conversely, the parent must be offline before the child can be taken offline. To override this behavior, use the

`-ignoreparent` option of the `hares -offline` command.

Sample main.xml configuration file

```
<!DOCTYPE config SYSTEM "main.dtd">
<config>

<include>types.linux.xml</include>
<include>types.sun.xml</include>

<!-- Cluster Definition.-->
<cluster name="Test_Cluster1">
  <attributes>
    <!-- Scalar attribute. -->
    <attribute name="ClusterAddress">
      <scalar>192.168.0.2</scalar>
    </attribute>
    <!-- Recommended attribute. Should specify this.-->
    <attribute name="DefaultPlatform">
      <scalar>linux/x86</scalar>
    </attribute>
  </attributes>
</cluster>

<!-- System Definitions.-->
<system name="photon">
  <attributes>
```

```
        </attributes>
</system>
<system name="meson">
    <attributes>
    </attributes>
</system>

<!-- Group definitions. -->
<group name="GroupOne">
    <attributes>
        <!-- Association attribute. -->
        <attribute name="SystemList">
            <val key = "photon">0</val>
            <val key = "meson">0</val>
        </attribute>
    </attributes>

    <!-- Group's resources. -->
    <resources>
        <!-- Resource attribute. -->
        <resource name = "Test_fileonoff1" type = "FileOnOff">
            <!-- Localised attribute. -->
            <attribute name = "PathName" context = "photon">
                <scalar>"/tmp/foo"</scalar>
            </attribute>
        </resource>
    </resources>
</group>
<group name="VCS">
    <attributes>
        <!-- Association attribute. -->
        <attribute name="SystemList">
            <val key = "photon">0</val>
            <val key = "meson">0</val>
        </attribute>
    </attributes>

    <!-- Group's resources. -->
    <resources>
        <!-- Resource attribute. -->
        <resource name = "Test_fileonoff2" type = "FileOnOff">
            <!-- Localised attribute. -->
            <attribute name = "PathName" context = "photon">
                <scalar>"/tmp/fool"</scalar>
            </attribute>
        </resource>
    </resources>
    <requires>
        <child>"Veritas Cluster Server One"</child>
        <kind>"hard"</kind>
        <location>"local"</location>
    </requires>
</group>
```

```

        </requires>
    </group>
</config>

```

The bpa.xml file format

This file includes definitions of business rules, notification rules, and jobs. It resides in the ext directory. The ext directory is a subdirectory of the directory where main.xml is present.

Business rule definition

Defines properties of a business rule such as event selection criteria, object type, and associate-job.

```

<rule enabled="true" event_type="1" isusergrp="false"
name="sysrule" object_type="SYSTEM" ou="/VCSOneCO=Marketing"
owner="simuser@domain" quiet_time="0">
    <description></description>
    <object_selection type="LIST">mktg_linsys6</object_selection>
    <event_selection type="ALL"></event_selection>
    <associated-job name="sysjob" />
</rule>

```

Job Definition

Defines properties of the business rule such as organization unit and tasks.

```

<job name="sysjob" ou="/VCSOneCO=Marketing">
    <description></description>
    <task halt_on_error="true" timeout="5" type="GRP_SETPRI"
wait="0">
        <param name="%GRP">websvr6</param>
        <param name="%PRI">5</param>
        <param name="%PROPAGATE">>false</param>
    </task>
    <task halt_on_error="true" timeout="5" type="SCRIPT" wait="0">
        <param name="%ARGS">{Event parameters}</param>
        <param name="%SCRIPTNAME">backup.sh</param>
        <param name="%USEEVENT">>true</param>
    </task>
</job>

```

Notification rule definition

Defines various properties of notification rule such as event selection criteria, object type, and notification tasks.

```

<notification_rule enabled="true" event_type="1" isusergrp="false"
name="NR1" object_type="GROUP" ou="/" owner="simuser@domain"
quiet_time="0">

```

```
<description></description>
<object_selection type="ALL">Customers="CellStop"</
object_selection>
<event_selection type="ALL"></event_selection>
<task halt_on_error="false" timeout="1000" type="SEND_MAIL"
wait="0">
  <param name="%ADDRESS">admin@wirelessdept.com</param>
  <param name="%USE_OWNER_EMAIL">false</param>
</task>
<task halt_on_error="false" timeout="1000" type="SNMP_TRAP"
wait="0">
  <param name="%CONSOLES">sol_openview</param>
  <param name="%USE_OWNER_SNMP">false</param>
</task>
<task halt_on_error="false" timeout="1000" type="SYSLOG"
wait="0">
  <param name="%HOSTS">sol_syscollector</param>
</task>
</notification_rule>
```

Automation Settings

Defines various notification settings.

```
<settings SmtptFromPath="VCSOne-Notifier" SmtptReturnPath=""
SmtptServer="" SecondarySmtptServer="" SmtptServerTimeout="10"
SmtptWebconsole="" SmtptCommunity="public" MaxEmail="100"
SmtptTrapPort="162" DefaultSmtptConsole="" EnableScript="0"
EnableSmtpt="0" EnableSmtpt="0" EnableSyslog="0"
BusinessEvalMaxThreads="10" BusinessEvalMinThreads="5"
BusinessEvalQueueSize="100" DefaultTaskMaxThreads="10"
DefaultTaskMinThreads="5" DefaultTaskQueueSize="100"
EmailTaskMaxThreads="1" EmailTaskMinThreads="1"
EmailTaskQueueSize="500" ExecutorMaxThreads="10"
ExecutorMinThreads="5" ExecutorQueueSize="100"
NotificationEvalMaxThreads="1" NotificationEvalMinThreads="1"
NotificationEvalQueueSize="500" SNMPTaskMaxThreads="1"
SNMPTaskMinThreads="1" SNMPTaskQueueSize="500"
ScriptTaskMaxThreads="20" ScriptTaskMinThreads="10"
ScriptTaskQueueSize="500" SleepThreads="2" SyslogTaskMaxThreads="1"
SyslogTaskMinThreads="1" SyslogTaskQueueSize="500"
TimeoutThreads="2" />
```

Sample bpa.xml configuration file

```
<bpa>
  <!-- Job Definition -->
  <job name="provisionJob" ou="/">
    <description></description>
    <task halt_on_error="true" timeout="5" type="SCRIPT"
wait="10">
```

```
<param name="%ARGS">{Event parameters}</param>
<param name="%SCRIPTNAME">provision.sh</param>
<param name="%USEEVENT">>true</param>
</task>
<task halt_on_error="true" timeout="5" type="SEND_MAIL"
wait="10">
  <param name="%ADDRESS">admin@corp.com</param>
  <param name="%SUB">Provision Completed</param>
  <param name="%BODY">For application @{x}</param>
</task>
</job>

<!-- Business Rule Definition -->
<rule enabled="true" event_type="1" isusergrp="false"
name="ProvisionRule" object_type="GROUP" ou="/"
owner="simuser@domain" quiet_time="0">
  <description></description>
  <object_selection type="LIST">Corp-Apache-App</
object_selection>
  <event_selection type="LIST">GRP_NOFAILOVER</
event_selection>
  <associated-job name="provisionJob">
    <variable name="@{x}">Event.GRP</variable>
  </associated-job>
</rule>

<!-- Notification Rule Definition -->
<notification_rule enabled="true" event_type="1"
isusergrp="false" name="NotifySysFault" object_type="SYSTEM"
ou="/" owner="simuser@domain" quiet_time="0">
  <description></description>
  <object_selection type="ALL"></object_selection>
  <event_selection type="LIST">SYS_FAULTED$SYS_DDNA</
event_selection>
  <task halt_on_error="false" timeout="1000" type="SEND_MAIL"
wait="0">
    <param name="%ADDRESS">admin@corp.com</param>
    <param name="%USE_OWNER_EMAIL">>false</param>
  </task>
  <task halt_on_error="false" timeout="1000" type="SNMP_TRAP"
wait="0">
    <param name="%CONSOLES">openviewsys</param>
    <param name="%USE_OWNER_SNMP">>false</param>
  </task>
</notification_rule>

<!-- Automation Settings -->
<settings SmtplibFromPath="VCSOne-Notifier" SmtplibReturnPath=""
SmtplibServer="" SecondarySmtplibServer="" SmtplibServerTimeout="10"
SmtplibWebconsole="" SnmpCommunity="public" MaxEmail="100"
SnmpTrapPort="162" DefaultSnmpConsole="" EnableScript="0"
EnableSmtplib="0" EnableSnmp="0" EnableSyslog="0">
```

```
BusinessEvalMaxThreads="10" BusinessEvalMinThreads="5"  
BusinessEvalQueueSize="100" DefaultTaskMaxThreads="10"  
DefaultTaskMinThreads="5" DefaultTaskQueueSize="100"  
EmailTaskMaxThreads="1" EmailTaskMinThreads="1"  
EmailTaskQueueSize="500" ExecutorMaxThreads="10"  
ExecutorMinThreads="5" ExecutorQueueSize="100"  
NotificationEvalMaxThreads="1" NotificationEvalMinThreads="1"  
NotificationEvalQueueSize="500" SNMPTaskMaxThreads="1"  
SNMPTaskMinThreads="1" SNMPTaskQueueSize="500"  
ScriptTaskMaxThreads="20" ScriptTaskMinThreads="10"  
ScriptTaskQueueSize="500" SleepThreads="2"  
SyslogTaskMaxThreads="1" SyslogTaskMinThreads="1"  
SyslogTaskQueueSize="500" TimeoutThreads="2" />
```

```
</bpa>
```

The prefs.xml file

This file includes user UI preferences and custom view definitions. It resides in the ext directory. The ext directory is a subdirectory of the directory where main.xml is present.

The following text is a sample prefs.xml file

```
<preferences>  
  <user name="simuser@domain">  
    <pref name="UPDATER_MODE" value="TimedRefresh"/>  
    <pref name="UPDATE_TIMER" value="01:00"/>  
    <vcsoneset name="My Objects">  
      <custom_view description="" expression="EA:/  
        VCSOneCO=Retail~grp~Customers&amp;EA:/  
        VCSOneCO=Wholesale~grp~Project" name="ProjectTree"/>  
    </vcsoneset>  
  </user>  
</preferences>
```

Attributes reference

This chapter includes the following topics:

- [About attributes](#)
- [Viewing and editing attributes](#)
- [VCS One cluster level attributes](#)
- [Composite service group attributes](#)
- [Remote cluster attributes](#)
- [System attributes](#)
- [Service group attributes](#)
- [Resource type attributes](#)
- [Resource attributes](#)
- [Role attributes](#)
- [User attributes](#)
- [Group Transition Queue attributes](#)
- [Action entry attributes](#)
- [Set name attributes](#)
- [OUname attributes](#)
- [OUvalue attributes](#)

About attributes

Attributes define how VCS One controls the associated object.

Unless otherwise noted, attributes values are case-insensitive and the value remains persistent if the Policy Master restarts.

About the data-type of attributes

Attribute values have one of the following data-types:

string	<p>String values 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 (_).</p> <ul style="list-style-type: none">■ A string consisting of only letters and numbers does not require quotes. A network interface such as <code>eth0</code> is an example. Enclosing the string in double quotes is also acceptable—<code>"eth0"</code>.■ Strings containing delimiters, such as periods in IP addresses or slashes in path names, require quotes. The IP address <code>"192.168.100.1"</code> is an example. <p>A string can contain double quotes. If the string contains double quotes, precede the string by a backslash. Within a string, represent a backslash with two forward slashes (\\).</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: <code>21471183247</code>.</p>
boolean	<p>Boolean values are integers with the possible values of 0 (false) or 1 (true).</p>

About the dimension of attributes

Attribute values have one of the following dimensions:.

scalar	<p>A scalar has only one value.</p>
vector	<p>A vector is an ordered list of values. Each value is indexed using a positive integer [zero or higher].</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.</p>

Viewing and editing attributes

Each attribute has its own set of valid values. You can define the value of an attribute in one of the following ways:

- Use the VCS One console
- Enter a command on the command line
- Edit the appropriate configuration file

The command you use to define the value of an attribute depends on the type of the attribute. Some attributes may not be modifiable.

Some attributes have an empty value. In the console, the value <BLANK_VALUE> is equivalent to an empty value. When using the command line, the value "" denotes an empty value.

To display a specific attribute of a given type and the current value using the command line

- ◆ Type the following command
hacommand -display -attribute attribute

Use the following information to replace the appropriate variables:

hacommand Use one of the following commands depending on the type of the attribute:

haclus	type cluster
hasys	type system
haframe	type frame (future functionality)
hagrp	type service group
hatype	type resource type
hares	type resource
hauser	type user
harole	type role
haset	type set

attribute Name of the specific attribute.
To display all attributes of this type, use only the -display flag

See the *Veritas Cluster Server One Command Reference Guide*.

To display a specific attribute of a given type and the current value using the VCS One console

See [“Editing VCS One cluster attributes”](#) on page 516.

VCS One cluster level attributes

[Table 36-1](#) lists VCS One cluster attributes in alphabetical order and provides definitions and information about their use.

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
AuthBrokerMap	<p>Type-dimension: string-association</p> <p>This attribute sets the VCS One cluster-wide mappings of domain type to an Authentication broker servicing that domain type. For example, each of the following commands could go to their own preferred Authentication broker to get a credential and present it to the Policy Master, without the Policy Master being an AD, NIS, or LDAP client:</p> <pre>hasys -state -user abcd@AD-domain -domaintype nt hasys -state -user abcd@nis-domain -domaintype nis hasys -state -user abcd@ldap-domain -domaintype ldap</pre> <p>These commands may be run from anywhere in the VCS One cluster.</p> <p>The Policy Master Authentication Broker and the Authentication Broker that are pointed to by this attribute should be trusted or in the same root hierarchy.</p> <p>If this attribute is not set, environment variables for command-line interface or user-selection of these values in the GUI determine the mapping.</p> <p>Change this attribute to have flexibility to add users from existing domains without the need to change the Policy Master node Authentication broker.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute with the GUI or the <code>haclus -modify</code> command.</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
ClusterAddress	<p>Type-dimension: string-keylist</p> <p>List of IP addresses and ports on which the Policy Master listens for incoming connections from the VCS One cluster. When the Policy Master updates the ClusterAddress values, it communicates the values to the VCS One client daemons, which update the values in the vcstone.conf file. Systems not running when updates occur obtain the ClusterAddress values when they reconnect to the Policy Master.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
ClusterDirs	<p>Type-dimension: string-association</p> <p>The currently defined VCS One directory variables such as VCSONE_HOME, VCSONE_CONF, and VCSONE_TRIGGERS_DIR.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
ClusterMode	<p>Type-dimension: integer-scalar</p> <p>Indicates the start mode (cold or normal) and run mode (manual or simulator) of the VCS One cluster.</p> <p>The value of this attribute does not persist when the Policy Master restarts</p> <p>Default value = 0</p> <p>You may not edit the value of this attribute.</p>
ClusterName	<p>Type-dimension: string-scalar</p> <p>User-defined label for the name of the VCS One cluster in the GUI.</p> <p>Limit this name to 128 characters.</p> <p>Default value = VCSOne</p>
ClusterState	<p>Type-dimension: integer-scalar</p> <p>Current state of the VCS One cluster.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = 1</p> <p>You may not edit the value of this attribute.</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
CompatibleClientVersion	<p>Type-dimension: string-association</p> <p>Defines the minimum version and maximum version of the client daemon that is compatible with the Policy Master.</p> <p>Default values: Minimum = 2.0 Maximum = 2.0</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
CompatibleCLIVersion	<p>Type-dimension: string-association</p> <p>Defines the minimum version and maximum version of the ha- commands, such as hagrps, that are compatible with the Policy Master.</p> <p>Default values: Minimum = 2.0 Maximum = 2.0</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
CompatibleDRVersion	<p>Type-dimension: string-association</p> <p>Defines the minimum version and maximum version of the DR Connector that is compatible with the Policy Master.</p> <p>Default values: Minimum = 1.0 Maximum = 1.0</p> <p>You may not edit the value of this attribute.</p>
CompatibleGUIVersion	<p>Type-dimension: string-association</p> <p>Defines the minimum version and maximum version of the GUI that is compatible with the Policy Master.</p> <p>Default values: Minimum = 2.0 Maximum = 2.0</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
CounterInterval	<p>Type-dimension: integer-scalar</p> <p>Interval in seconds by which the GlobalCounter is increased.</p> <p>See “GlobalCounter” on page 686.</p> <p>Default value = 30 seconds</p> <p>You may not edit the value of this attribute.</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
Created	<p>Type-dimension: integer-scalar</p> <p>Timestamp of when the VCS One cluster was created.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
CredRenewInterval	<p>Type-dimension: integer-scalar</p> <p>The number of days after which VCS One renews its credentials with the authentication broker.</p> <p>For example, the value 5 indicates that credentials are renewed every 5 days; the value 0 indicates that credentials are not renewed.</p> <p>The value of this attribute must be between 0 and 730.</p> <p>Default value = 90.</p> <p>You may edit the value of this attribute with the GUI or the <code>haclus -modify</code> command.</p>
DefaultAuthDomain	<p>Type-dimension: string-scalar</p> <p>Default authentication domain and domain type information for the VCS One cluster. Takes the following value: <code>domain_type:domain_name</code></p> <p>For example, <code>nis:ourlab.com</code> where <code>ourlab.com</code> is an NIS domain.</p> <p>If you specify both domain and domain type on the command line, this value is overridden.</p> <p>Usage: The format <code>user@domain</code> is enforced in the VCS One cluster. Modify this attribute to contain a domain type and domain name when the use of one particular domain is dominant in the environment.</p> <p>If this value is not set then the following is an example command: <code>hasys -state -user username@domain -domaintype domain_type</code></p> <p>If this value is set then the following is an example command: <code>hasys -state -user username</code></p> <p>Default value = ""</p> <p>You may edit the value of this attribute with the GUI or the <code>haclus -modify</code> command.</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
DefaultPlatform	<p>Type-dimension: string-scalar</p> <p>User-defined attribute that represents the most common platform in the VCS One cluster.</p> <p>The following values are valid for this attribute: aix, aix/rs6000, hpux, linux, linux/x86, solaris, solaris/sparc, solaris/x86, windows, windows/x86.</p> <p>Default value = linux/x86</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
DeploymentTimeout	<p>Type-dimension: integer-scalar</p> <p>Timeout window with which clients can be deploying using deployment credential.</p> <p>Default value = 0</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
DRAddress	<p>Type-dimension: string-keylist</p> <p>List of IP addresses on which the Policy Master listens for incoming connections from a remote VCS One cluster.</p> <p>You may edit the value of this attribute only by directly editing the main.xml configuration file.</p> <p>See “Changing the local cluster’s DR address value” on page 492.</p> <p>Note: You must stop the Policy Master before you edit the value of this attribute.</p>
DRListeningPort	<p>Type-dimension: integer-scalar</p> <p>Port on which the local VCS One cluster listens for incoming connections from the remote VCS One clusters.</p> <p>The value for this attribute must be between 1025 and 65535.</p> <p>Default = 14151</p> <p>You may edit the value of this attribute only by directly editing the main.xml configuration file.</p> <p>See “Changing the local cluster’s DR port value” on page 491.</p> <p>Note: You must stop the Policy Master before you edit the value of this attribute.</p>
EAMaxValidValue	<p>Type-dimension: integer-scalar</p> <p>Attribute to restrict the maximum permitted extended attribute validation values.</p> <p>The value for this attribute must be between 1 and 65536.</p> <p>Default value = 50</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
EnableFFDC	<p>Type-dimension: boolean-scalar</p> <p>Enables (1)/Disables(0) First Failure Data Capture function.</p> <p>Default value = 1</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
EngineClass	<p>Type-dimension: string-scalar</p> <p>User-defined attribute specifying the scheduling class for Policy Master.</p> <p>Default value = TS</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
EnginePriority	<p>Type-dimension: string-scalar</p> <p>User-defined attribute specifying the priority of the Policy Master engine.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
FarmUUID	<p>Type-dimension: string-scalar</p> <p>Unique universal identifier for the farm.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
FragmentationPolicy	<p>Type-dimension: string-scalar</p> <p>User-defined attribute specifying how VCS One resolves service group placement when available systems have the same Disruption Factor.</p> <p>The following values are valid for this attribute:</p> <p>BiggestAvailable. VCS One evaluates the first PrecedenceOrder key (typically, CPU) and places the group on the system with greatest Capacity value for the group's Load.</p> <p>BestFit. VCS One evaluates the first PrecedenceOrder value (typically, CPU) and places the group on the system with closest sufficient Capacity value for the group's Load.</p> <p>Heuristic. The system that is chosen is based on whether or not the service group has a local service group dependency with another service group</p> <p>Default value = BiggestAvailable</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
GlobalCounter	<p>Type-dimension: integer-scalar</p> <p>Internal use counter. The CounterInterval attribute specifies the interval at which this counter increases.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
LastConfigUpdate	<p>Type-dimension: integer-scalar</p> <p>Timestamp of when VCS One cluster object was last modified.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
LicensedCPUs	<p>Type-dimension: integer-association</p> <p>Total number of CPUs allowed to participate in the VCS One cluster.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default values:</p> <p>LinWin = 0</p> <p>Unix = 0</p> <p>You may not edit the value of this attribute.</p>
LicensedFeatures	<p>Type-dimension: integer-scalar</p> <p>Indicates VCS One features currently enabled.</p> <p>The value of this attribute does not persist when the Policy Master restarts</p> <p>Default value = 0</p> <p>You may not edit the value of this attribute.</p>
LicenseMode	<p>Type-dimension: integer-scalar</p> <p>Indicates the current license-based mode in which the VCS One cluster is running.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = 1.</p> <p>You may not edit the value of this attribute.</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
LicenseType	<p>Type-dimension: integer-scalar</p> <p>Type of license key that the Policy Master uses.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = 0</p> <p>You may not edit the value of this attribute.</p>
LockMemory	<p>Type-dimension: string-scalar</p> <p>Disables paging for Policy Master process if set to CURRENT or ALL.</p> <p>Enables paging if set to NONE.</p> <p>Default value = ALL</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
LogDbg	<p>Type-dimension: string-keylist</p> <p>Specifies which debug messages are logged.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
LogSize	<p>Type-dimension: integer-scalar</p> <p>Maximum size, in bytes, for the log files the Policy Master and the client daemon generate. Log files reaching this size roll over. For example, vcsoneclientd_A.log becomes vcsoneclientd_B.log, and vcsoneclientd_A.log becomes the new log file.</p> <p>The value for this attribute must be between 65536 and 134217728.</p> <p>Default value = 33554432</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
MaxGrpCompatMatrixSize	<p>Type-dimension: integer-scalar</p> <p>The maximum number of group combinations to allow in a single CLI instance that sets compatibility between groups using SET/OU/EA specification.</p> <p>Default value = 100</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
MsgCatID	<p>Type-dimension: integer-scalar</p> <p>Message category ID that is used for the VCS One cluster object.</p> <p>Default value = 1.</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
NodeIdCounter	<p>Type-dimension: integer-scalar</p> <p>Indicates the node ID that will be assigned to the next system that is added to the VCS One cluster.</p> <p>Default value = 1024</p> <p>You may not edit the value of this attribute.</p>
PMStartupTime	<p>Type-dimension: integer-scalar</p> <p>Indicates the startup time for the Policy Master.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
PolicyHBTimeout	<p>Type-dimension: integer-scalar</p> <p>The number of seconds for the Policy Master network module to wait before proactively killing the Policy Master if the Policy Master thread has stopped sending a heartbeat signal to the network module. The Policy Master normally sends a heartbeat signal to the network module several times in a second. This heartbeat signal may stop when the Policy Master thread hangs for any reason or encounters an unknown defect.</p> <p>The network module kills the Policy Master process to avoid being stuck in this state forever. It initiates a restart or a failover of the Policy Master daemon process.</p> <p>This behavior can be turned off by setting the PolicyHBTimeout attribute value to 0.</p> <p>Default value = 0</p> <p>You may edit the value of this attribute with the GUI or the <code>haclus -modify</code> command.</p>
PrecedenceOrder	<p>Type-dimension: string-association</p> <p>User-defined keys that refer to the aspects of system resource capacity and of corresponding service group load. The names, or keys, can be combined with a value to define capacity</p> <p>See “How you can define service group load and system capacity” on page 59.</p> <p>Administrators may delete a <code>PrecedenceOrder</code> key using <code>hagrps -modify</code> only if <i>all</i> group loads and system capacities have zero values associated with the key.</p> <p>Default values:</p> <ul style="list-style-type: none"> ■ Key1=CPU ■ Key 2=MEM <p>You may edit the value of this attribute with the GUI or the <code>haclus -modify</code> command.</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
ProcessClass	<p>Type-dimension: string-scalar</p> <p>The scheduling class for the processes that are forked off by the Policy Master.</p> <p>Default value = TS</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
ProcessPriority	<p>Type-dimension: string-scalar</p> <p>The scheduling priority for the processes that are forked off by the Policy Master.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
ProductVersion	<p>Type-dimension: integer-scalar</p> <p>VCS One product version.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = 2.0.</p> <p>You may not edit the value of this attribute.</p>
ProtocolVersion	<p>Type-dimension: integer-scalar</p> <p>A version number. The VCS One Policy Master uses this protocol version to communicate. All clients must provide a protocol version lower or equal to the Policy Master protocol version to successfully communicate.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = 1.0</p> <p>You may not edit the value of this attribute.</p>
ProxysimIPAddr	<p>Type-dimension: string-scalar</p> <p>An IP address. The simulated Policy Master uses this IP address to ping the proxysim. This IP address is updated on the Policy Master when the proxysim connects for the first time with the Policy Master.</p> <p>Default value = ""</p> <p>Do not edit the value of this attribute.</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
RestartMode	<p>Type-dimension: integer-scalar</p> <p>Determines the start mode of the VCS One cluster the next time the cluster is started.</p> <p>The value for this attribute must be between 1 and 4, which indicate the following values:</p> <ul style="list-style-type: none"> ■ 0 = Unknown ■ 1 = Normal ■ 2 = Invalid ■ 3 = Invalid ■ 4 = Cold <p>Default value = 4.</p> <p>You may not edit the value of this attribute.</p>
SiteAddress	<p>Type-dimension: string-association</p> <p>Denotes the IP address or the hostname that is associated with a site name.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
SkipCVNCheck	<p>Type-dimension: integer-scalar</p> <p>Indicates whether or not a configuration version number check is done whenever the VCS One client connects to the Policy Master.</p> <p>SkipCVNCheck = 1 indicates the check is not done.</p> <p>Default value = 0</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
SourceFile	<p>Type-dimension: string-scalar</p> <p>The name of the XML file where this object resides.</p> <p>Default value = main.xml</p> <p>You may not edit the value of this attribute.</p>
TrustedAuthBrokerID	<p>Type-dimension: string-keylist</p> <p>Lists the trusted authentication brokers' UUIDs. Includes remote authentication brokers that have trust set up with the VCS One cluster.</p> <p>Type the following command on the broker host to retrieve the broker UUID:</p> <pre># /opt/VRTSvcsone/bin/haat getbrokeruuid -b localhost:14159</pre> <p>Default value = ""</p>

Table 36-1 VCS One cluster level attributes

VCS One cluster Attribute	Definition
WebserverSubsystems	<p>Type-dimension: string-keylist</p> <p>The list of enabled subsystems in the VCS One web server.</p> <p>The following values are valid for this attribute: BPA, SEARCH, RCA</p> <p>Default value = BPA, SEARCH, RCA</p> <p>Contact Symantec support before modifying this attribute.</p>

Composite service group attributes

[Table 36-2](#) lists composite service group attributes in alphabetical order and provides definitions and information about their use.

Table 36-2 Composite service group attributes

Composite service group attributes	Definition
Authority	<p>Type-dimension: boolean-scalar</p> <p>This attribute is applicable only in a VCS One global cluster environment.</p> <p>Indicates whether or not the local VCS One cluster is allowed to bring the composite service group online.</p> <p>0—the local VCS One cluster is not allowed to bring the composite service group online.</p> <p>1—the local VCS One cluster is allowed to bring the composite service group online.</p> <p>The Authority attribute prevents a composite service group from coming online in multiple sites at the same time.</p> <p>See “How VCS One resolves authority for application that spans clusters” on page 72.</p> <p>Default value = “ “</p> <p>You may not edit the value of this attribute.</p> <p>See “Requesting authority for a global CSG” on page 499.</p>
AttnInfo	<p>Type-dimension: string-association</p> <p>The names of the service groups in the composite service group that are responsible for the ATTN flag being set for the CSG, along with the reason why ATTN was set.</p> <p>The following values are valid for the reason:</p> <ul style="list-style-type: none"> ■ Unable to Online ■ Group Fault <p>The names of the CSG that are responsible for the ATTN flag being set, along with the reason why ATTN was set.</p> <p>The following values are valid for the reason:</p> <ul style="list-style-type: none"> ■ Concurrency Violation ■ State is Stale <p>Default value = ““</p> <p>You may not edit the value of this attribute.</p> <p>See “ATTN flag is set for the CSG” on page 614.</p>

Table 36-2 Composite service group attributes

Composite service group attributes	Definition
ClusterList	<p>Type-dimension: string-keylist</p> <p>This attribute is applicable only in a VCS One global cluster environment.</p> <p>Specifies the list of VCS One clusters on which the composite service group is set to run.</p> <p>You may edit the value of this attribute with the GUI or the hacsg -modify command.</p> <p>See “Configuring a global CSG” on page 498.</p>
Created	<p>Type-dimension: integer-scalar</p> <p>Timestamp of when system object was created</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>

Table 36-2 Composite service group attributes

Composite service group attributes	Definition
CSGState	<p>Type-dimension: integer-scalar</p> <p>The state of the composite service group.</p> <p>This attribute represents the collective running states of the constituent service groups of the composite service group.</p> <p>The following values are valid for this attribute:</p> <ul style="list-style-type: none"> ■ ONLINE - All the service groups in the CSG are online. ■ PARTIAL - Some groups in the CSG are offline, and the others are in the online or the partial state. Or, no groups are offline, some or all groups are partial, and the rest, if any, are online. ■ OFFLINE - All the service groups in the CSG are offline. ■ ONLINE PENDING - All groups in the CSG are online, but one or more of the constituent service groups are in transition to a different state. ■ PARTIAL PENDING - Same as PARTIAL, but some service groups are in transition to a different state. ■ PARTIAL ATTN - Same as PARTIAL, but some service groups are faulted or are unable to go online. ■ PARTIAL ATTN PENDING - Same as PARTIAL, but some service groups are faulted or unable to go online, while one or more of the remaining service groups in the CSG are in transition to a different state. ■ OFFLINE PENDING - Same as OFFLINE, but some service groups may be in transition to a different state. ■ OFFLINE ATTN - One of the following conditions is true: All service groups are faulted; all service groups are offline or faulted; all service groups are offline and some of them are unable to come online. ■ OFFLINE ATTN PENDING - Same as OFFLINE ATTN but some service groups in the CSG are in transition to a different state. <p>Default value = OFFLINE</p> <p>The ATTN modifier indicates that one or more of the service groups in the CSG are faulted or are unable to go online anywhere in the VCS One cluster.</p> <p>The PENDING modifier indicates that one or more groups in CSG are in transition.</p> <p>The value of this attribute does not persist when the Policy Master restarts. The value is re-evaluated upon each Policy Master restart.</p> <p>You may not edit the value of this attribute.</p> <p>See “How VCS One determines the state of a multi-tier application” on page 72.</p>

Table 36-2 Composite service group attributes

Composite service group attributes	Definition
GroupList	<p>Type-dimension: string-keylist</p> <p>The names of the service groups that are in the composite service group.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute with the GUI or the hacsg -modify command.</p>
InTransition	<p>Type-dimension: boolean-scalar</p> <p>Indicates whether or not the CSG state is in transition. If any service group in the CSG, or any resource in the service groups within the CSG, is in transition, the value is set to 1. If not, the value is set to 0.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
LastConfigUpdate	<p>Type-dimension: integer-scalar</p> <p>Timestamp of when CSG object was last modified.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
LastStateUpdate	<p>Type-dimension: integer-scalar</p> <p>The timestamp of when the state of the composite service group's last changed.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
MsgCatID	<p>Type-dimension: integer-scalar</p> <p>Message category ID that is used for the CST object</p> <p>Default value = 1</p> <p>You may edit the value of this attribute with the GUI or the hasys -modify command.</p>

Table 36-2 Composite service group attributes

Composite service group attributes	Definition
NotifyAttrChange	<p>Type-dimension: string-keylist</p> <p>Editable list of attribute names. If the user wants to get notified of any changes to the value of a CSG attribute, then the name of that attribute should be added as a key to the this attribute.</p> <p>Upon any changes to the value of such attributes that are listed in NotifyAttrChange, a CSG_ATTR_CHANGE event is generated.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
SourceFile	<p>Type-dimension: string-scalar</p> <p>The name of the XML file where this object resides.</p> <p>Default value = main.xml</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>

Remote cluster attributes

[Table 36-3](#) lists remote cluster attributes in alphabetical order and provides definitions and information about their use.

Table 36-3 Remote cluster attributes

Remote VCS One cluster attribute	Definition
ClusterName	<p>Type-dimension: string-scalar</p> <p>User-defined label for the name of the remote cluster.</p> <p>The name of the remote cluster must not exceed 128 characters. The name cannot start with a number or contain any special characters.</p> <p>Default value = “ ”</p> <p>You may not edit the value of this attribute.</p>
ClusterState	<p>Type-dimension: integer-scalar</p> <p>Indicates the current state of the remote VCS One cluster.</p> <p>You may not edit the value of this attribute.</p> <p>See “Cluster states in VCS One global clusters” on page 762.</p>
ConnectionRole	<p>Type-dimension: string-scalar</p> <p>Specifies whether the remote cluster initiates the connection to the local cluster or accepts the connection from the local cluster. The value of this attribute can be one of the following:</p> <ul style="list-style-type: none">■ Initiator—the remote cluster initiates the connection to the local cluster■ Acceptor—the remote cluster accepts the connection from the local cluster <p>You may not edit the value of this attribute.</p> <p>See “Determining the connection role of clusters” on page 480.</p>

Table 36-3 Remote cluster attributes

Remote VCS One cluster attribute	Definition
ConnectionTimeout	<p>Type-dimension: integer-scalar</p> <p>This attribute is applicable only on the VCS One cluster that initiates the inter-cluster connection.</p> <p>Note: If the value of the ConnectionRole attribute is Initiator, VCS One requires you to define this attribute on the remote cluster that this remote cluster object represents.</p> <p>Time-out value in seconds to initiate a connection to the remote cluster.</p> <p>If the specified value is exceeded, VCS One reports an error and retries to initiate a connection.</p> <p>The value for this attribute must be between 2 and 50.</p> <p>Default value = 5 seconds</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
ConsolidatedLinkStatus	<p>Type-dimension: string-scalar</p> <p>Indicates the consolidated status of the network links between the local and the remote clusters.</p> <ul style="list-style-type: none"> ■ DISABLED—all the network links are disabled ■ DOWN—all the network links are down ■ UP—all the network links are up ■ PARTIAL UP—at least one of the network links is up <p>You may not edit the value of this attribute.</p> <p>See “Network link states in VCS One global clusters” on page 763.</p>

Table 36-3 Remote cluster attributes

Remote VCS One cluster attribute	Definition
DRPort	<p>Type-dimension: integer-scalar</p> <p>This attribute is applicable only on the VCS One cluster that initiates the inter-cluster connection.</p> <p>Note: If the value of the ConnectionRole attribute is Initiator, VCS One requires you to define this attribute on the remote VCS One cluster that this remote VCS One cluster object represents.</p> <p>Port on which the remote VCS One cluster listens for incoming connections. The value of this remote cluster object's attribute must match the value of the cluster-level attribute DRListeningPort that you defined for the cluster at the remote site.</p> <p>The value for this attribute must be between 1025 and 65535.</p> <p>Default = 14151</p> <p>You may edit the value of the DRPort attribute with the GUI or the haclus -modify command.</p> <p>Note: You must set the value of the EnableConnections attribute to 0 before you edit the value of this attribute.</p>
EnableConnections	<p>Type-dimension: boolean-scalar</p> <p>Indicates whether VCS One on the local cluster must establish (1) or close (0) connections with the remote cluster.</p> <p>You must set the value of this attribute to 1 on both the VCS One clusters to establish the network connection.</p> <p>Default value = 0</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>

Table 36-3 Remote cluster attributes

Remote VCS One cluster attribute	Definition
LinkStatus	<p>Type-dimension: integer-association</p> <p>Indicates the status of each network link that is specified in the NetworkConnections attribute for the VCS One cluster that initiates the inter-cluster connection.</p> <p>The status of the network link between the local and the remote clusters can be UP, DOWN, or DISABLED.</p> <p>See “Network link states in VCS One global clusters” on page 763.</p> <p>The LinkStatus attribute stores the network link in the same format as you defined in the NetworkConnections attribute:</p> <p><i>destinationIP[:sourceIP]</i></p> <p>For example, you may see the following value for the LinkStatus attribute if you had defined two network links and if EnableConnection attribute is set to 1 on both the VCS One clusters:</p> <p>192.168.1.16:192.168.1.20 = UP</p> <p>192.168.2.16:192.168.2.20 = DOWN</p> <p>You may not edit the value of this attribute.</p>
MaxHeartbeatInterval	<p>Type-dimension: integer-scalar</p> <p>The maximum number of seconds to elapse without a heartbeat. If no messages are exchanged on a particular network connection for this interval, an explicit heartbeat is exchanged.</p> <p>The value for this attribute must be between 5 and 360.</p> <p>Default value = 5 seconds</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>
MissedHeartbeatThreshold	<p>Type-dimension: integer-scalar</p> <p>The maximum number of missed heartbeats that the Policy Master waits before declaring the network link as down.</p> <p>The value for this attribute must be between 2 and 50.</p> <p>Default value = 5 seconds</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>

Table 36-3 Remote cluster attributes

Remote VCS One cluster attribute	Definition
NetworkConnections	<p>Type-dimension: string-keylist</p> <p>This attribute is applicable only on the VCS One cluster that initiates the inter-cluster connection.</p> <p>Note: If the value of the ConnectionRole attribute is Initiator, VCS One requires you to define this attribute on the remote cluster that this remote cluster object represents.</p> <p>Specifies the list of network links that the local cluster uses to connect to the remote cluster.</p> <p>The value of this attribute must have the following format:</p> <p><i>destinationIP[:sourceIP]</i></p> <p>where:</p> <ul style="list-style-type: none"> ■ <i>destinationIP</i> is the IP address of the remote cluster You must specify a value for the destination IP address. ■ <i>sourceIP</i> is the IP address of the local cluster If you do not specify a source IP address, VCS One uses any of the available IP addresses on the local cluster to connect to the remote cluster. <p>For example, you can specify the value of this attribute as 192.168.1.16. In this case, VCS One uses any available IP addresses on the local cluster.</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p> <p>Note: You must set the value of the EnableConnections attribute to 0 before you edit the value of this attribute.</p>
RClusterUUID	<p>Type-dimension: string-scalar</p> <p>Unique universal identifier for the remote VCS One cluster.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
ReconnectInterval	<p>Type-dimension: integer-scalar</p> <p>This attribute is applicable only on the VCS One cluster that initiates the inter-cluster connection.</p> <p>Note: If the value of the ConnectionRole attribute is Initiator, VCS One requires you to define this attribute on the remote cluster that this remote cluster object represents.</p> <p>Number of seconds to wait before VCS One attempts to reconnect to a remote cluster.</p> <p>The value for this attribute must be between 2 and 50.</p> <p>Default value = 5 seconds</p> <p>You may edit the value of this attribute with the GUI or the haclus -modify command.</p>

Table 36-3 Remote cluster attributes

Remote VCS One cluster attribute	Definition
RunningDRVersion	Type-dimension: string-scalar Indicates the version of the DR component that is currently running on the local cluster. You may not edit the value of this attribute.
SourceFile	Type-dimension: string-scalar The name of the XML file where this object resides. Default value = main.xml You may edit the value of this attribute with the GUI or the haclus -modify command.
TransitionTimeout	Type-dimension: integer-scalar Number of seconds within which Policy Master must fail over from one node to the other in the VCS One cluster. If Policy Master successfully fails over within the TransitionTimeout value, VCS One changes the state of the remote cluster from TRANSITIONING to BUILD. Otherwise, VCS One marks the state of the remote cluster as FAULTED. The value for this attribute must be between 60 and 65535. Default value = 300 seconds You may edit the value of this attribute with the GUI or the haclus -modify command.

System attributes

[Table 36-4](#) lists system attributes in alphabetical order and provides definitions and information about their use.

Table 36-4 System level attributes

System Attribute	Definition
AgentsStopped	Type-dimension: integer-scalar AgentStopped is set to 1 when all agents on the system are stopped. Typically, the use of the hastop command to stop vcsoneclientd stops the agents. The value of this attribute does not persist when the Policy Master restarts. Default value = 0 You may not edit the value of this attribute.

Table 36-4 System level attributes

System Attribute	Definition
AgentVersionInfo	Type-dimension: string-association Displays the version information of the agents that are installed on the system. Default value = 1 You may edit the value of this attribute with the <code>hasys -modify</code> command or the GUI.
AutoDeploy	Type-dimension: integer-scalar Indicates if the system can be deployed using deployment credentials. Default value = 1 You may edit the value of this attribute with the <code>hasys -modify</code> command or the GUI.
AutoEnablePending	Type-dimension: integer-scalar The number of groups that are not fully probed on a newly joined system. When value drops to zero, the Policy Master attempts to bring online on the system those groups that are listed in the GTQ with <code>INTENTONLINE</code> entries. Default value = 0 You may not edit the value of this attribute.
AvailableCapacity	Type-dimension: integer-association Key-values pairs. These pairs contain the calculated values that are based on the <code>Capacity</code> attribute, the <code>ReserveCapacity</code> attribute, and the <code>Load</code> attribute for all the applicable service groups. See “ Capacity ” on page 704, “ ReservedCapacity ” on page 708, and “ Load ” on page 715. The value of this attribute does not persist when the Policy Master restarts When a system has the <code>DDNAState</code> attribute = 1, the value of this attribute is the last known value when the system was connected with the Policy Master. You may not edit the value of this attribute.

Table 36-4 System level attributes

System Attribute	Definition
Capacity	<p>Type-dimension: integer-association</p> <p>When adding a system to a VCS One cluster, an administrator defines a system's <code>Capacity</code> attribute by associating integer values with user-defined keys. The key-value pairs (for example, "cpu 6 memory 3096") represent the capacity of the system. The keys, such as "cpu" and "memory" (see "PrecedenceOrder" on page 688), are initially defined in the VCS One cluster attribute <code>PrecedenceOrder</code>. Users may define up to four keys.</p> <p>The service group level attribute <code>Load</code> that the administrator defines when creating a service group corresponds to the system <code>Capacity</code> attribute. For example, a group's <code>Load</code> attribute may be "cpu 2 memory 1028" and a system's <code>Capacity</code> attribute may be "cpu 6 memory 3096". A service group whose <code>Load</code> exceeds a system's <code>Capacity</code> cannot be brought online on that system. See information about "Load" on page 715.</p> <p>The Policy Master reserves capacity on a system where it plans to online a service group. The <code>ReservedCapacity</code> attribute contains the key-value pairs reflecting the reserved capacity. See "ReservedCapacity" on page 708.</p> <p>The system maintains an attribute that is called <code>AvailableCapacity</code>, which reflects the initial <code>Capacity</code> of a system minus <code>ReservedCapacity</code> and the <code>Load</code> it currently bears. See "AvailableCapacity" on page 703.</p> <p>You may edit the value of this attribute with the GUI or the <code>hasys -modify</code> command.</p>
CPUBinding	<p><i>CPUBinding is not supported in VCS One 2.0</i></p> <p>Type-dimension: string-association</p> <p>Binds the HAD process to the specified CPU. Set this attribute to prevent HAD from getting interrupted.</p> <p>The <code>CPUBinding</code> attribute has two key-value pairs, <code>BindTo = binding</code> and <code>CPUNumber = number</code>.</p> <p>The <code>BindTo</code> key has the following values for <i>binding</i>:</p> <ul style="list-style-type: none"> NONE, indicating that <code>CPUBinding</code> is not used ANY, indicates that HAD is to bind any CPU CPUNUM indicates that HAD is to bind to CPU specified in the <code>CPUNumber</code> key. <p>The <code>CPUNumber</code> key has the value <i>number</i>, which specifies the number of the CPU.</p> <p>Default value = " " (disabled)</p> <p>You may edit the value of this attribute with the GUI or the <code>hasys -modify</code> command.</p>

Table 36-4 System level attributes

System Attribute	Definition
Created	Type-dimension: integer-scalar Timestamp of when system object was created Default value = "" You may not edit the value of this attribute.
DDNAPingInterval	Type-dimension: integer-scalar The interval in seconds to wait before Policy Master investigates current status of a system in the DDNA (Daemon Dead Node Alive) state. The value of this attribute must be between 10-360. Default value = 20 You may edit the value of this attribute with the GUI or the hasys -modify command.
DDNAState	Type-dimension: integer-scalar DDNA (Daemon Dead Node Alive) state of 1 indicates the vcsoneclientd process on the system, which is still alive, does not send heartbeats to the Policy Master. Default value = 0 You may not edit the value of this attribute.
EnableFFDC	Type-dimension: boolean-scalar Indicates if First Failure Data Capture (FFDC) functionality is enabled for the VCS One client running on this system. See “About the first failure data capture (FFDC) log” on page 587. Enabled = 1; Disabled = 0 Default value = 1 You may edit the value of this attribute with the GUI or the haclus -modify command.
FirstTimeConnect	Type-dimension: integer-scalar Indicates whether or not the system has connected to the Policy Master since the time a fresh configuration was loaded into the configuration database. Default value = 1 You may not edit the value of this attribute.

Table 36-4 System level attributes

System Attribute	Definition
Frozen	<p>Type-dimension: boolean-scalar</p> <p>Indicates if service groups can be brought online on the system. Groups cannot be brought online if the attribute value is 1.</p> <p>Default value = 0.</p> <p>The Policy Master sets the value of this attribute in response to Freeze or Unfreeze menu items in the GUI, or the <code>hasys -freeze -unfreeze</code> command.</p> <p>The user may not directly edit this attribute.</p>
GroupList	Internal use only.
InternalSysFlag	Internal use only.
LastConfigUpdate	<p>Type-dimension: integer-scalar</p> <p>Timestamp of when system object was last modified.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
LastStateUpdate	<p>Type-dimension: integer-scalar</p> <p>The timestamp of when system's state last changed.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
LogDbg	<p>Type-dimension: string-keylist</p> <p>Specifies which debug messages are written to the <code>vsoneclientd</code> log file.</p> <p>Default value = ""</p>
MaxHeartbeatInterval	<p>Type-dimension: integer-scalar</p> <p>Interval in seconds that determines how often a system should send a heartbeat to the Policy Master.</p> <p>The value for this attribute must be between 5 and 360.</p> <p>Default value = 10</p> <p>You may not edit the value of this attribute.</p>

Table 36-4 System level attributes

System Attribute	Definition
MissedHeartbeatThreshold	Type-dimension: integer-scalar A number that denotes how many missed heartbeats the Policy Master waits before investigating the system missing heartbeats. The value for this attribute must be between 2 and 50. Default value = 3 You may edit the value of this attribute with the GUI or the <code>hasys -modify</code> command.
MsgCatID	Type-dimension: integer-scalar Message category ID that is used for the system object Default value = 1 You may edit the value of this attribute with the GUI or the <code>hasys -modify</code> command.
NodeId	Type-dimension: integer-scalar The node ID of the system. The Policy Master assigns this node ID. Default value = -1 You may not edit the value of this attribute.
NotifyAttrChange	Type-dimension: string-keylist The value of this attribute is a list of attributes. Whenever any of the attributes in this list is modified, the <code>SYS_ATTR_CHANGE</code> event is generated. Use this attribute to monitor changes in system attributes. Default value = ""
NumMissedHeartbeat	Type-dimension: integer-scalar Number of heartbeats the specific system has missed. When the <code>NumMissedHeartbeats</code> crosses the <code>MissedHeartbeatThreshold</code> value, the Policy Master starts investigating the system. Default value = 0 You may not edit the value of this attribute. The value of this attribute does not persist when the Policy Master restarts.

Table 36-4 System level attributes

System Attribute	Definition
OnGrpCnt	<p>Type-dimension: integer-scalar</p> <p>The number of groups online or partially online on the system. This number does not include the number of groups that are planned to be brought online.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>When a system has the DDNAState attribute = 1, the value of this attribute is the last known value when the system was connected with the Policy Master.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
PlatformName	<p>Type-dimension: string-scalar</p> <p>Name of the platform in use on the system.</p> <p>The following values are valid for this attribute: aix, aix/rs6000, hpux, linux, linux/x86, solaris, solaris/sparc, solaris/x86, windows, and windows/x86.</p> <p>Default value = ""</p> <p>You may modify the value of this attribute with the hasys -modify command or the GUI.</p>
ReservedCapacity	<p>Type-dimension: integer-association</p> <p>Key-values pairs. The Policy Master defines these pairs and designates the reserve capacity on the system.</p> <p>For example, if the Policy Master plans to fail over G1 to system S2, the ReserveCapacity attribute on system S2 includes the capacity that is required for G1. As G1 is brought online on S2, the Policy Master removes the capacity that G1 requires from the ReserveCapacity attribute value.</p> <p>See “Capacity” on page 704.</p> <p>When a system has the DDNAState attribute = 1, the value of this attribute is the last known value when the system was connected with the Policy Master.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
SourceFile	<p>Type-dimension: string-scalar</p> <p>The name of the XML file where this object resides.</p> <p>Default value = main.xml</p> <p>You may edit the value of this attribute with the GUI or the hasys -modify command.</p>

Table 36-4 System level attributes

System Attribute	Definition
StaleSysState	<p>Type-dimension: boolean-scalar</p> <p>Denotes whether or not the state of the system is based on an old value from the database which has not as yet been determined accurately by the Policy Master.</p> <p>Default value = 0</p> <p>You may not edit the value of this attribute.</p>
SysInfo	<p>Type-dimension: string-association</p> <p>Indicates the system-specific information by key–value pairs. This attribute is updated each time the VCS One client daemon connects to the Policy Master.</p> <p>Default value = MemoryReal = "" MemoryVirt= "" OsType = "" OsVersion = "" CpuCount = "" CpuArch = "" CpuSpeed = ""</p> <p>You may not edit the value of this attribute.</p>
SysName	<p>Type-dimension: string-scalar</p> <p>Indicates the system's name.</p> <p>The value of this attribute does not persist when the Policy Master restarts</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
SysState	<p>Type-dimension: integer-scalar</p> <p>Indicates the system's state:</p> <p>1 = UNKNOWN 8 = LOCAL_BUILD 11 = RUNNING 12 = LEAVING 14 = EXITED 15 = FAULTED</p> <p>Default value = 1</p> <p>You may not edit the value of this attribute.</p>

Table 36-4 System level attributes

System Attribute	Definition
SystemConfigVersion	<p>Type-dimension: integer-scalar</p> <p>Indicates whether the Policy Master is to push fresh configuration information to the system when the system's vcsoneclientd connects to the Policy Master.</p> <p>Default value = 0</p> <p>You may not edit the value of this attribute.</p>
SystemIPAddr	<p>Type-dimension: string-vector</p> <p>Value specifies the IP address(es) configured for the system. The Policy Master uses the list to ping the system in case of a fault.</p> <p>Every time the system's vcsoneclientd daemon starts, the daemon updates the value of the attribute.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
SystemMode	<p>Type-dimension: string-scalar</p> <p>Indicates whether this system is an actual system (Real) or a simulated system (Simulated).</p> <p>Default value = Real</p> <p>You may not edit the value of this attribute.</p>
SystemSequenceNumber	<p>Type-dimension: integer-scalar</p> <p>Specifies whether the Policy Master is to probe all resources on the system when the system's vcsoneclientd connects to the Policy Master. Values are Yes (1) and No (0).</p> <p>Default value = 0</p> <p>You may not edit the value of this attribute.</p>
SystemVersion	<p>Type-dimension: string-association</p> <p>Version of the vcsoneclientd (VCS One client system daemon) running on the system.</p> <p>Default values are:</p> <p>DaemonVersion = ""</p> <p>ProductVersion = ""</p> <p>BuildDate = ""</p> <p>PSTAMP = ""</p> <p>ProtocolVersion = ""</p> <p>You may not edit the value of this attribute.</p>

Table 36-4 System level attributes

System Attribute	Definition
SysUserName	Type-dimension: string-scalar The user name that is associated with a system. The privileges that are granted to this user determine the operations that the root user on that system can perform within the VCS One cluster. Default value = "" You may not edit the value of this attribute.
SystemUUID	Type-dimension: string-scalar Specifies the System UUID, a unique identifier for the system. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
TransitionOffline	Type-dimension: integer-scalar When user issues <code>hastop -sys</code> command without the <code>-evacuate</code> option, Policy Master sets value of <code>TransitionOffline</code> to 1 for a brief time. The value of this attribute does not persist when the Policy Master restarts. Default value = 0 You may not edit the value of this attribute.
TransitionOnline	Type-dimension: integer-scalar When user issues <code>hastop -sys</code> command with the <code>-evacuate</code> option, Policy Master sets value of <code>TransitionOnline</code> to 1 for a brief time. The value of this attribute does not persist when the Policy Master restarts. Default value = 0 You may not edit the value of this attribute.
UsePMIPAddr	Type-dimension: string-keylist Specifies the list of IP addresses (and ports) that the client system uses to connect to the Policy Master. This list must be a subset of the IP addresses that the Policy Master listens on. The cluster attribute <code>ClusterAddress</code> specifies on which IP addresses the Policy Master listens. Default value = ""

Service group attributes

[Table 36-5](#) lists service group attributes in alphabetical order and provides definitions and information about their use:

Table 36-5 Service group attributes

Service Group Attribute	Definition
ActiveCount	Internal use only.
AutoEnableWait	<p>Type-Dimension: boolean-scalar</p> <p>For internal use. If set to 1 it indicates Policy Master is waiting to probe a group on this newly joined system. Once the group is probed this value is set to 0 and AutoEnablePending for the system decrements by 1.</p> <p>Default value = 0.</p> <p>You may not edit the value of this attribute.</p>
CompatibleGroups	<p>Type-dimension: string-keylist</p> <p>A list of the service groups that are compatible with the current group. This attribute does not have a value if the IncompatibleGroups attribute has a value.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
ContainerInfo	<p>Type-Dimension: string-association</p> <p>Used in operating system virtualization technology environments. Describes the Container information and whether that information is passed to the agent framework.</p> <p>Can only be modified if all resources in the group are in a clean OFFLINE state.</p> <p>Has the following keys:</p> <p>NAME: Name of the Container in free-form non-null text</p> <p>TYPE: Type of the Container. Valid values are ZONE and WPAR. The XRM option is not supported.</p> <p>ENABLED: Valid values are 0 and 1. Indicates if the Policy Master does (1) or does not (0) pass ContainerInfo to the agents managing resources in a group. (Target group must have the value 1 set for either the RunInContainer key or the PassCInfo key in the resource attribute ContainerOpts.)</p> <p>By default, this attribute is NULL, indicating the service group is not associated with a Container.</p> <p>Default value = ""</p>

Table 36-5 Service group attributes

Service Group Attribute	Definition
Created	<p>Type-dimension: integer-scalar</p> <p>Timestamp of when group object was created</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
CSGName	<p>Type-Dimension: string-scalar</p> <p>Denotes the name of the composite service group to which this group belongs. A blank value indicates this group does not belong to a composite service group.</p> <p>This attribute remains persistent across Policy Master reboots.</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p> <p>Default value = ""</p>
CurrentCount	<p>Type-Dimension: integer-scalar</p> <p>Internal use only. Number of systems on which the service group is active. The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
Enabled	<p>Type-Dimension: boolean-scalar</p> <p>Indicates if a group can be failed over or brought online. If any of the local values are disabled, the group is disabled.</p> <p>Default value = 1 (enabled)</p> <p>You may only edit the value of this attribute if the group's SystemList attribute is non-empty.</p> <p>You may edit the value of this attribute with the <code>hagrp -enable</code> or <code>hagrp -disable</code> command or the GUI.</p> <p>You may edit the value of this attribute for an individual group instance by editing the <code>main.xml</code> configuration file directly.</p>
Evacuate	<p>Type-Dimension: boolean-scalar</p> <p>Indicates if VCS One initiates an automatic failover when user issues the command <code>hastop -local -evacuate</code>.</p> <p>Default value = 1</p>

Table 36-5 Service group attributes

Service Group Attribute	Definition
Frozen	<p>Type-Dimension: boolean-scalar</p> <p>Disables all actions on the service group except for the monitor actions that the agents perform.</p> <p>Examples of disabled actions are autostart, online, offline, and failover.</p> <p>All agents that are bundled with VCS One observe this convention.</p> <p>Default value = 0 (not frozen)</p> <p>The Policy Master sets the value of this attribute in response to Freeze or Unfreeze menu items in the GUI, or the <code>hagrp -freeze -unfreeze</code> command.</p> <p>The user may not directly edit this attribute.</p>
GrpFaultPolicy	<p>Type-Dimension: string-scalar</p> <p>specifies whether VCS One fails over or does not fail over a faulted service group. Also indicates which VCS One product is in use. The following values are valid for this attribute:</p> <ul style="list-style-type: none"> ■ Failover ■ NoFailover <p>See “Service group level control” on page 230.</p> <p>To specify VCS One Start functional mode (license), set the following values:</p> <ul style="list-style-type: none"> ■ GrpFaultPolicy = NoFailover ■ NodeFaultPolicy = NoFailover <p>Default value = Failover</p>
GTQDisplayName	<p>Type-Dimension: string-scalar</p> <p>Default value = “”</p> <p>You may not edit the value of this attribute.</p>
IncompatibleGroups	<p>Type-dimension: string-keylist</p> <p>A list of the service groups that are incompatible with the current group. This attribute does not have a value if the CompatibleGroups attribute has a value.</p> <p>Default value = “”</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
LastConfigUpdate	<p>Type-dimension: integer-scalar</p> <p>Timestamp of when group object was last modified.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = “”</p> <p>You may not edit the value of this attribute.</p>

Table 36-5 Service group attributes

Service Group Attribute	Definition
LastRestartTime	<p>Type-dimension: integer-scalar</p> <p>Timestamp of when group last restarted.</p> <p>Default value = 0</p> <p>You may not edit the value of this attribute.</p>
LastStateUpdate	<p>Type-dimension: integer-scalar</p> <p>Timestamp of when group's state last changed.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
Load	<p>Type-Dimension: integer-association</p> <p>Integer value expressing total system Load that this group exerts on a system.</p> <p>For example, the administrator may assign a value of 100 to a large production SQL and 15 to a Web server.</p> <p>When creating a service group, an administrator defines a group's Load attribute by associating integer values with user-defined keys. The key-value pairs (for example, "cpu 4 memory 1028") represent the load a service group places on a system's resources.</p> <p>The keys, such as "cpu" and "memory" (see "PrecedenceOrder" on page 688) are initially defined in the cluster attribute</p> <p><code>PrecedenceOrder</code>. Users may define up to four keys.</p> <p>The system level attribute, <code>Capacity</code>, which the administrator defines when adding a system, corresponds to the Load attribute. For example, a system's <code>Capacity</code> attribute may be "cpu 6 memory 3046" and a service group Load attribute may be "cpu 2 memory 1028". See information about "Capacity" on page 704.</p> <p>The <code>hagrp -changeload</code> command enables users to change the Load attribute definition for an online service group.</p> <p>Default value = 0</p>
ManualOps	<p>Type-Dimension: boolean-scalar</p> <p>Indicates if manual operations are allowed on the service group. If set to 0 then online, offline and switch operations are not permitted.</p> <p>Default value = 1 (enabled)</p>
MasterGroup	For future use.

Table 36-5 Service group attributes

Service Group Attribute	Definition
MsgCatID	<p>Type-dimension: integer-scalar</p> <p>Message category ID that is used for the group object</p> <p>Default value = 1</p>
NodeFaultPolicy	<p>Type-Dimension: string-scalar</p> <p>Specifies whether or not to fail over the service group when the application node on which it runs faults. The following values are valid for this attribute:</p> <ul style="list-style-type: none"> ■ Failover - VCS One fails over the group to the best available target node. ■ NoFailover - VCS One does not fail over the group. <p>See “System level control” on page 231.</p> <p>To specify VCS One Start functional mode (license), set the following values:</p> <ul style="list-style-type: none"> ■ GrpFaultPolicy = NoFailover ■ NodeFaultPolicy = NoFailover <p>Default value = Failover</p>
NotifyAttrChange	<p>Type-dimension: string-keylist</p> <p>The value of this attribute is a list of attributes. Whenever any of the attributes in this list is modified, the GRP_ATTR_CHANGE event is generated.</p> <p>Use this attribute to monitor changes in group attributes.</p> <p>Default value = ““</p>
OffHostResource	<p>Type-dimension: string-keylist</p> <p>A list of the off-host resources that use this group as a control group.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ““</p> <p>You may not edit the value of this attribute.</p>
Parallel	<p>Type-Dimension: integer-scalar</p> <p>Indicates if the service group is failover (0) or parallel (1).</p> <p>Default value = 0</p>
PathCount	<p>Type-Dimension: integer-scalar</p> <p>For internal use only. Number of resources in path not yet taken offline. When this number drops to zero, the engine may take the entire service group offline if critical fault has occurred.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>You may not edit the value of this attribute.</p>

Table 36-5 Service group attributes

Service Group Attribute	Definition
PlatformName	<p>Type-dimension: string-scalar</p> <p>Name of system platform for which service group is configured to run.</p> <p>If a default platform name has not been set for the VCS One cluster, then specify the platform when creating the service group. If this attribute has been set for the VCS One cluster, it is used by default for a new group unless you explicitly set the platform.</p> <p>The following values are valid for this attribute: aix, aix/rs6000, hpux, linux, linux/x86, solaris, solaris/sparc, solaris/x86, windows, and windows/x86.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute with the <code>hagrp -modify</code> command or the GUI.</p>
Priority	<p>Type-Dimension: integer-scalar</p> <p>Indicates the priority of the service group, ranging from highest (1) to lowest (5). Higher priority groups take precedence over lower priority groups when the groups contend for resources. Low priority groups may be kicked out of a system in favor of a higher priority group. The value for this attribute must be between 1 and 5.</p> <p>Default value = 5</p> <p>You may edit the value of this attribute with the <code>hagrp -modify</code> command.</p>
Probed	<p>Type-Dimension: boolean-scalar</p> <p>Probed = 1 indicates one of the following conditions:</p> <ul style="list-style-type: none"> ■ Agents have detected all enabled resources in the group. ■ A group with no resources or no enabled resources is detected when Policy Master starts or restarts. <p>Probed = 0 indicates one of the following conditions:</p> <ul style="list-style-type: none"> ■ Agents have not detected all enabled resources in the group. ■ A new group is added with no resources or no enabled resource while the Policy Master is running. <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
ProbesPending	<p>Type-Dimension: integer-scalar</p> <p>The number of resources that the agent has not yet detected on each system.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>

Table 36-5 Service group attributes

Service Group Attribute	Definition
Responding	<p>Type-Dimension: integer-scalar</p> <p>For internal use only. Indicates the engine is responding to a failover event and is in the process of bringing the service group online or failing over the node. The value of this attribute does not persist when the Policy Master restarts.</p> <p>You may not edit the value of this attribute.</p>
SourceFile	<p>Type-Dimension: string-scalar</p> <p>The name of the XML file where this object resides.</p> <p>Default value = main.xml</p>
StandbyGroup	For future use.
State	<p>Type-Dimension: integer-scalar</p> <p>Group state on each system. The following states are the possible values:</p> <p>OFFLINE All non-persistent resources are offline.</p> <p>ONLINE All resources whose AutoStart attribute is equal to 1 are online.</p> <p>FAULTED At least one critical resource in the group is faulted or is affected by a fault.</p> <p>PARTIAL At least one, but not all, resources with Operations=OnOff is online, and not all AutoStart resources are online.</p> <p>STARTING Group is attempting to go online.</p> <p>STOPPING Group is attempting to go offline.</p> <p>A group state can be a combination of multiple states. For example,</p> <p>OFFLINE FAULTED</p> <p>OFFLINE STARTING</p> <p>PARTIAL FAULTED</p> <p>PARTIAL STARTING</p> <p>PARTIAL STOPPING</p> <p>ONLINE STOPPING</p> <p>Default value = 1</p> <p>The value of this attribute does not persist when the Policy Master restarts</p> <p>You may not edit the value of this attribute.</p>

Table 36-5 Service group attributes

Service Group Attribute	Definition
SystemList	<p>Type-Dimension: integer-association</p> <p>List of systems on which the service group is configured to run. Each system has an associated value reflecting its priority. Lower priority numbers indicate a preference for the system as a failover target.</p> <p>A service group must not be online on the systems to be deleted from its SystemList.</p> <p>Default value = ""</p>
SystemListExpr	<p>Type-dimension: string-association</p> <p>Expression that is used to derive the value of the SystemList attribute for a service group. Used when user performs the refresh for the SystemList.</p> <p>Default values are: OU = "" EA = ""</p>
SystemZones	<p>Type-Dimension: integer-association</p> <p>Indicates the virtual sublists within the SystemList attribute that grant priority in failing over. Values are string/integer pairs. The string key is the name of a system in the SystemList attribute, and the integer is the number of the zone. Systems with the same zone number are members of the same zone. If a service group faults on one system in a zone, it is granted priority to fail over to another system within the same zone.</p> <p>Default value = ""</p>
TriggerResStateChange	<p>Type-Dimension: boolean-scalar</p> <p>Determines whether or not to invoke the <code>resstatechange</code> trigger if resource state changes.</p> <p>Default value = 0 (disabled)</p>

Resource type attributes

Resource type attributes apply to all resources of that specific type. The table in this section describes these static attributes. More information is available about resource type attributes.

See the *Veritas Cluster Server One Agent Developer's Guide*.

Specific resource types that have defined values are listed in the file `vcson.xml`. Unless otherwise notes, you may override the value of these attributes at the resource level.

Overriding static resource type attributes

Users can override the values of some predefined, static attributes for a specific resource without affecting the values of the attributes for other resources of that type. The table that follows identifies the attributes that can be overridden.

Users can override the values of specific resource attribute by:

- Explicitly defining the attribute for the resource in the `main.xml` configuration file
- Using the `hares` command from the command line with the `-override` option

Also, users can:

- View the values of the overridden attributes by using the `hares -display` command.
- Remove overridden values of static attributes by using the `hares -undo_override` option from the command line.

[Table 36-6](#) lists resource type attributes in alphabetical order and provides definitions and information about their use:

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
ActionTimeout	Type-Dimension: integer-scalar Timeout value in seconds for the Action entry point. The valid values of this attribute are in the range of 4-315360000. Default value = 30

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
AgentClass	<p>Type-Dimension: string-scalar</p> <p>Indicates the scheduling class for the VCS One agent process. The following values are valid:</p> <ul style="list-style-type: none"> ■ RT (Real Time) ■ TS (Time Sharing) ■ SHR (Solaris only) <p>You may use only one of the following sets of attributes to configure scheduling class and priority for VCS One:</p> <ul style="list-style-type: none"> ■ AgentClass, AgentPriority, ScriptClass, ScriptPriority ■ OnlineClass, OnlinePriority, EPClass, EPPriority <p>This attribute is in use if the values of the following attributes is -1: OnlineClass, OnlinePriority, EPClass, and EPPriority</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = TS</p>
AgentDirectory	<p>Type-dimension: string-scalar</p> <p>Specifies the path to a working directory for an agent and the directory from which script entry points are run.</p> <p>If users do not set the <code>AgentDirectory</code> attribute, the agent uses the default directory <code>\$VCSONE_HOME/bin/resource_type</code>. If the default directory does not exist, the agent uses the common agents directory <code>/opt/VRTSagents/ha/bin/resource_type</code>. If the agent cannot find any of the directories, the agent fails.</p> <p>Default = ""</p>
AgentFailedOn	<p>Type-Dimension: string-keylist</p> <p>A list of systems on which the agent for the resource type has failed. The value of this attribute does not persist when the Policy Master restarts</p> <p>You may not override this value at the individual resource level.</p> <p>Default value is not applicable to this attribute.</p> <p>You may not edit the value of this attribute.</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
AgentFile	<p>Type-dimension: string-scalar</p> <p>Specifies the path to an agent binary for a resource type.</p> <p>If the AgentFile attribute is not set, the vcstoneclntd process uses the agent in the agent file in following locations, in the order specified:</p> <ul style="list-style-type: none"> ■ AgentDirectory attribute ■ /opt/VRTSvcsone/bin/resource_type ■ /opt/VRTSagents/ha/resource_type <p>If the vcstoneclntd cannot find an agent file, the agent fails.</p>
AgentPriority	<p>Type-Dimension: string-scalar</p> <p>Indicates the priority in which the agent process runs.</p> <p>You may use only one of the following sets of attributes to configure scheduling class and priority for VCS One:</p> <ul style="list-style-type: none"> ■ AgentClass, AgentPriority, ScriptClass, ScriptPriority ■ OnlineClass, OnlinePriority, EPClass, EPPriority <p>This attribute is in use if the values of the following attributes is -1: OnlineClass, OnlinePriority, EPClass, and EPPriority</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = 0</p>
AgentReplyTimeout	<p>Type-Dimension: integer-scalar</p> <p>The number of seconds the engine waits to receive a heartbeat from the agent before restarting the agent.</p> <p>You may not override this value at the individual resource level.</p> <p>The valid values of this attribute are in the range of 4-315360000.</p> <p>Default value = 130</p>
AgentStartTimeout	<p>Type-Dimension: integer-scalar</p> <p>The number of seconds after starting the agent that the engine waits for the initial agent “handshake” before restarting the agent.</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = 60</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
AllowedOnlineOps	<p>Type-Dimension: string-keylist</p> <p>Defines whether or not an online resource can be deleted or modified.</p> <p>The following values are valid for this attribute:</p> <ul style="list-style-type: none"> ■ "" (null value) The resource must be offline before it can be deleted. ■ delete An online resource can be deleted. ■ modify An online resource can be modified. ■ delete modify An online resource can be deleted or modified. <p>Default value = ""</p>
ArgList	Internal use only.
AttrChangedTimeout	<p>Type-Dimension: integer-scalar</p> <p>Maximum time (in seconds) within which the attr_changed entry point must complete or be terminated.</p> <p>The valid values of this attribute are in the range of 4-315360000.</p> <p>Default value = 60 seconds</p>
AutoStart	<p>Type-Dimension: boolean-scalar</p> <p>Specifies whether the resource is brought online when the service group is brought online;</p> <p>Default value = 1 second</p>
CleanRetryLimit	<p>Type-Dimension: integer-scalar</p> <p>Number of times to retry clean before moving a resource to ADMIN_WAIT state. If set to 0, clean is re-tried indefinitely.</p> <p>The valid values of this attribute are in the range of 0-1024.</p> <p>Default value = 0</p>
CleanTimeout	<p>Type-Dimension: integer-scalar</p> <p>Maximum time (in seconds) within which the clean entry point must complete or else be terminated.</p> <p>The valid values of this attribute are in the range of 4-315360000.</p> <p>Default value = 60</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
CloseTimeout	<p>Type-Dimension: integer-scalar</p> <p>Maximum time (in seconds) within which the close entry point must complete or else be terminated.</p> <p>The valid values of this attribute are in the range of 4-315360000.</p> <p>Default value = 60</p>
ConfInterval	<p>Type-Dimension: integer-scalar</p> <p>When a resource has remained online for the specified number of seconds, the agents ignore previous faults and restart attempts when evaluating other attributes, such as the ToleranceLimit attribute and the RestartLimit attribute.</p> <p>Default value = 600 seconds</p>
ContainerOpts	<p>Type-Dimension: integer-association</p> <p>Used in operating system virtualization technology environments. Indicates the options that may be passed to the agent framework so that Container behavior can be controlled at a resource level.</p> <p>This attribute cannot be modified if resources of this type are in use, unless you override for the specific resource you want modified. If you override this attribute, it can only be modified if the resource is in a clean OFFLINE state.</p> <p>Note: A Mount resource type does not have this attribute. In order for a Mount resource to be brought up inside a Container, you must override this attribute at the resource level and set RUNINCONTAINER to 1.</p> <p>Has the following keys:</p> <p>RUNINCONTAINER: Valid values are 0 and 1. Assign the value to 1 if you want the resource to be managed inside a Container. Group level attribute ContainerInfo must be set in order for this value to be effective.</p> <p>PASSCINFO: Valid values are 0 and 1. If set to 1, the agent framework sends the Container Information to the resource (agent entry points). Group level attribute ContainerInfo must be set in order for this value to be effective.</p> <p>PASSLOADINFO - Valid values are 0 and 1. If set to 1, the service group's Load values are passed on to the resource verbatim.</p> <p>Note: Load values must be set or changed when service group is in the OFFLINE state for a zone-enabled service group. Specifically, you may not use the hagrps -changeload command unless the zone-enabled service group is in the OFFLINE state.</p> <p>Default value = ""</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
Created	<p>Type-Dimension: integer-scalar</p> <p>Timestamp of when resource type object was created</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
EPClass	<p>Type-Dimension: string-scalar</p> <p>Configures the scheduling class for all entry points except online entry point. The following values are valid for this attribute:</p> <ul style="list-style-type: none">■ RT (Real Time)■ TS (Time Sharing)■ SHR (Solaris only) <p>You may use only one of the following sets of attributes to configure scheduling class and priority for VCS One:</p> <ul style="list-style-type: none">■ AgentClass, AgentPriority, ScriptClass, ScriptPriority■ OnlineClass, OnlinePriority, EPClass, EPPriority <p>If the value of the EPPriority attribute is -1, this attribute is not in use and the following attributes are in effect: AgentClass, AgentPriority, ScriptClass, ScriptPriority</p> <p>See “How to control the scheduling class and scheduling priority of agent operations” on page 61.</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = -1</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
EPPriority	<p>Type-Dimension: string-scalar</p> <p>Configures the scheduling priority for all entry points except the online entry point. You may use only one of the following sets of attributes to configure scheduling class and priority for VCS One:</p> <ul style="list-style-type: none"> ■ AgentClass, AgentPriority, ScriptClass, ScriptPriority ■ OnlineClass, OnlinePriority, EPClass, EPPriority <p>If the value of this attribute is -1, this attribute is not in use and the following attributes are in effect: AgentClass, AgentPriority, ScriptClass, ScriptPriority</p> <p>If the value of this attribute is 0, it indicates the base operating system priority for the configured scheduling class.</p> <p>For example:</p> <ul style="list-style-type: none"> ■ (Solaris) If the EPClass attribute is set to TS*, and the value of the EPPriority attribute is set to 0, then the base priority for entry points is set to 59, as that is the default value set by the operating system. ■ (Solaris) If the EPClass attribute is set to TS*, and the value of the EPPriority attribute is set to -20, then the scheduling priority of the entry point would be 39 (59 base value and - 20 configured value) ■ (Solaris) If the EPClass attribute is set to RT*, and the value of the EPPriority attribute is set to 0, then the base priority for entry points is set to 100 by the operating system. <p>See “How to control the scheduling class and scheduling priority of agent operations” on page 61.</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = -1</p>
FaultOnMonitorTimeouts	<p>Type-Dimension: integer-scalar</p> <p>When a monitor times out as many times as the value specified, the corresponding resource is brought down by calling the clean entry point. The resource is then marked FAULTED, or it is restarted, depending on the value of the RestartLimit attribute.</p> <p>When FaultOnMonitorTimeouts is set to 0, monitor failures are not considered indicative of a resource fault. A low value may lead to spurious resource faults, especially on heavily loaded systems.</p> <p>The valid values of this attribute are in the range of 0-2147483647.</p> <p>Default value = 4</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
FireDrill	Type-Dimension: boolean-scalar Specifies whether or not fire drill is enabled for the resource type. If set to 1, fire drill is enabled. If set to 0, it is disabled. You may not override this value at the individual resource level. Default value = 0

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
IMF	<p>Type-Dimension: integer-scalar</p> <p>Enables the use and control of type-level monitoring for a resource. By setting this attribute, the agent developer can switch between type-level monitoring and monitoring a resource using the monitor entry point.</p> <p>The IMF attribute has the following four keys:</p> <ul style="list-style-type: none"> ■ Mode-This key can take values from 0 to 3. Default value is 3. <ul style="list-style-type: none"> 0 - Set the Mode to 0 to disable type-level monitoring. When the Mode is set to 1, the agent monitors all resource using the monitor entry point. 1- Set the Mode to 1 to enable type-level monitoring for all offline resources. When the Mode is set to 1, the agent monitors all the offline resources using type-level monitoring, whereas it monitors all the online resources using the monitor entry point. 2- Set the Mode to 2 to enable type-level monitoring for all online resources. When the Mode is set to 2, the agent monitors all online resources using type-level monitoring, but it monitors all the offline resources using the monitor entry point. 3- Set the mode to 3 to enable type-level monitoring for both online and offline resources. ■ MonitorFreq-Specifies the frequency at which the monitor entry point is invoked, after type-level monitoring has been enabled for a module. The value of this key is an integer. <p>If you enable type-level monitoring, the monitor entry point is invoked every (MonitorFrequency x MonitorInterval) number of seconds, where MonitorInterval is a type-level static attribute.</p> <p>If the MonitorFreq is set to 0 (zero), the resource is monitored periodically using the monitor entry point.</p> <p>Default value is 100.</p> ■ RegisterRetryLimit-When the Mode key is set to 1, 2 or 3, the VCSAgEPIMFRegister entry point is invoked for some of the resources to register them with the type-level monitoring module. If the registration fails for a resource, the agent framework re-tries to register each resource depending upon the value of RegisterRetryLimit set. If it cannot register the resource, it continues monitoring the resource using the monitor entry point. <p>Default value: 100</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
InfoInterval	<p>Type-Dimension: integer-scalar</p> <p>Duration (in seconds) after which the agent framework invokes the info entry point for ONLINE resources of the particular resource type.</p> <p>If set to 0, the agent framework does not periodically invoke the info entry point. To manually invoke the info entry point, use the command <code>hares -refreshinfo</code>. If the value you designate is 30, for example, the entry point is invoked every 30 seconds for all ONLINE resources of the particular resource type.</p> <p>The valid values of this attribute are in the range of 0-315360000.</p> <p>Default value = 0</p>
InfoTimeout	<p>Type-Dimension: integer-scalar</p> <p>Timeout value for info entry point. If entry point does not complete by the designated time, the agent framework cancels the entry point's thread.</p> <p>The valid values of this attribute are in the range of 4-315360000.</p> <p>Default value = 30 seconds</p>
LastConfigUpdate	<p>Type-Dimension: integer-scalar</p> <p>Timestamp of when type object was last modified</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
LevelTwoMonitorFreq	<p>Type-Dimension: integer-scalar</p> <p>Specifies the frequency with which the agent for this type performs second-level monitoring. Default is 1, which means every monitor cycle would also do second-level monitoring.</p> <p>The valid values of this attribute are in the range of 0-1024.</p> <p>Default value = 1</p> <p>You may edit the value of this attribute with the <code>hares -modify</code> command or the GUI.</p>
LogDbg	<p>Type-Dimension: string-keylist</p> <p>Indicates the debug severities that are enabled for the resource type or agent framework. The debug severities that are used by the agent entry points are in the range of <code>DBG_1-DBG_21</code>. The debug messages from the agent framework are logged with the severities <code>DBG_AGINFO</code>, <code>DBG_AGDEBUG</code>, AND <code>DBG_AGTRACE</code>, representing the least to most verbose.</p> <p>Default value = ""</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
LogFileSize	<p>Type-Dimension: integer-scalar</p> <p>Specifies the size (in bytes) of the agent log file.</p> <p>You may not override this value at the individual resource level.</p> <p>The valid values of this attribute are in the range of 65536 (64 KB) -134217728 (128 MB).</p> <p>Default value = 33554432 (32 MB)</p>
MinCompatAgentVersion	<p>Type-Dimension: string-scalar</p> <p>Specifies the lowest version of an agent for this resource type that can work with this version of the Type definition. The TypeDefinitionVersion attribute gives the version of this Type definition.</p> <p>Default value = UNKNOWN</p> <p>Do not edit the value of this attribute.</p>
MonitorInterval	<p>Type-Dimension: integer-scalar</p> <p>Duration (in seconds) between two consecutive monitor calls for an ONLINE or transitioning resource.</p> <p>The valid values of this attribute are in the range of 1-315360000.</p> <p>Default value = 60 seconds</p> <p>A lower value may affect performance if many resources of the same type exist. A higher value may delay detection of a faulted resource.</p>
MonitorMethod	<p>Type-Dimension: string-scalar</p> <p>Specifies the method of monitoring the resource uses. Default value indicates a monitor function is run periodically to check the health of the resource.</p> <p>The value of this attribute does not persist when the Policy Master restarts</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = Traditional</p> <p>You may not edit the value of this attribute.</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
MonitorStatsParam	<p>Type-Dimension: integer-association</p> <p>Stores the required parameter values for calculating monitor time statistics. The following values are valid for this attribute:</p> <p><i>Frequency</i>: Defines the number of monitor cycles after which the average monitor cycle time should be computed and sent to the engine. The configured value for this attribute must be between 1 and 30. Default value = 0.</p> <p><i>ExpectedValue</i>: The expected monitor time in milliseconds for all resources of this type. Default value = 100.</p> <p><i>ValueThreshold</i>: The acceptable percentage difference between the expected monitor cycle time (ExpectedValue) and the actual monitor cycle time. Default value = 100.</p> <p><i>AvgThreshold</i>: The acceptable percentage difference between the benchmark average and the moving average of monitor cycle times. Default value = 40.</p>
MonitorTimeout	<p>Type-Dimension: integer-scalar</p> <p>Maximum time (in seconds) within which the monitor entry point must complete or else be terminated.</p> <p>The valid values of this attribute are in the range of 4-315360000.</p> <p>Default value = 60 seconds</p>
MsgCatID	<p>Type-dimension: integer-scalar</p> <p>Message category ID that is used for the resource type object.</p> <p>Default value = 1</p>
NumThreads	<p>Type-Dimension: integer-scalar</p> <p>Limits the number of threads an agent can create.</p> <p>For the efficient management of system and process resources, the agent framework uses a threads-on-demand method to create and remove service threads: an agent adds threads dynamically for a given resource and the agent framework removes threads no longer needed, freeing them for use by other agents. A significantly large number of threads (over 30, for example) can degrade system and process performance.</p> <p>A value of 1 prevents the creation of multiple threads. This limit does not include the threads that are used for other internal purposes.</p> <p>You may not override this value at the individual resource level.</p> <p>Default= 10</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
OfflineMonitorInterval	<p>Type-Dimension: integer-scalar</p> <p>Duration in seconds between two consecutive monitor calls for an OFFLINE resource. If set to 0, OFFLINE resources are not monitored.</p> <p>With a value of 0, concurrency violations are not detected. If an application that is supposed to be in the offline state on a node is brought to the online state outside of VCS One control, the application continues to run. This behavior is because VCS One cannot detect this state change. Data is protected using I/O fencing. As mentioned, to avoid this, one can set OfflineMonitorInterval to a non-zero value (apart from overriding it for a specific resource).</p> <p>The valid values of this attribute are in the range of 0-315360000.</p> <p>Default value = 0</p>
OfflineTimeout	<p>Type-Dimension: integer-scalar</p> <p>Maximum time (in seconds) within which the offline entry point must complete or else be terminated.</p> <p>The valid values of this attribute are in the range of 4-315360000.</p> <p>Default value = 300 seconds</p>
OfflineWaitLimit	<p>Type-Dimension: integer-scalar</p> <p>Number of monitor intervals to wait after the offline process is completed, and before the resource is taken offline.</p> <p>The valid values of this attribute are in the range of 0-1024.</p> <p>Default value = 0</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
OnlineClass	<p>Type-Dimension: string-scalar</p> <p>Configures the scheduling class for the online entry point. The following values are valid for this attribute:</p> <ul style="list-style-type: none">■ RT (Real Time)■ TS (Time Sharing)■ SHR (Solaris only) <p>You may use only one of the following sets of attributes to configure scheduling class and priority for VCS One:</p> <ul style="list-style-type: none">■ AgentClass, AgentPriority, ScriptClass, ScriptPriority■ OnlineClass, OnlinePriority, EPClass, EPPriority <p>If the value of the OnlinePriority attribute is -1, this attribute is not in use and the following attributes are in effect: AgentClass, AgentPriority, ScriptClass, ScriptPriority</p> <p>See “How to control the scheduling class and scheduling priority of agent operations” on page 61.</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = -1</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
OnlinePriority	<p>Type-Dimension: string-scalar</p> <p>Configures the scheduling priority for the online entry point.</p> <p>You may use only one of the following sets of attributes to configure scheduling class and priority for VCS One:</p> <ul style="list-style-type: none"> ■ AgentClass, AgentPriority, ScriptClass, ScriptPriority ■ OnlineClass, OnlinePriority, EPClass, EPPriority <p>If the value of this attribute is -1, this attribute is not in use and the following attributes are in effect: AgentClass, AgentPriority, ScriptClass, ScriptPriority</p> <p>If the value of this attribute is 0, it indicates the base operating system priority for the configured scheduling class.</p> <p>For example:</p> <ul style="list-style-type: none"> ■ (Solaris) If the EPClass attribute is set to TS*, and the value of the EPPriority attribute is set to 0, then the base priority for entry points is set to 59, as that is the default value set by the operating system. ■ (Solaris) If the EPClass attribute is set to TS*, and the value of the EPPriority attribute is set to -20, then the scheduling priority of the entry point would be 39 (59 base value and - 20 configured value) ■ (Solaris) If the EPClass attribute is set to RT*, and the value of the EPPriority attribute is set to 0, then the base priority for entry points is set to 100 by the operating system. <p>See “How to control the scheduling class and scheduling priority of agent operations” on page 61.</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = -1</p>
OnlineRetryLimit	<p>Type-Dimension: integer-scalar</p> <p>Number of times to retry online if the attempt to bring a resource online is unsuccessful.</p> <p>The value for this attribute must be between 0 and 1024.</p> <p>Default value = 0</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
OnlineTimeout	<p>Type-Dimension: integer-scalar</p> <p>Maximum time (in seconds) within which the online entry point must complete or else be terminated.</p> <p>The valid values of this attribute are in the range of 4-315360000.</p> <p>Default value = 300 seconds</p> <p>Modification notes: Increase only if resource is likely to take a longer time to come online.</p>
OnlineWaitLimit	<p>Type-Dimension: integer-scalar</p> <p>Number of monitor intervals to wait after completing the online procedure, and before the resource becomes online.</p> <p>The valid values of this attribute are in the range of 0-2147483647.</p> <p>Default value = 2</p>
OpenTimeout	<p>Type-Dimension: integer-scalar</p> <p>Maximum time (in seconds) within which the open entry point must complete or else be terminated.</p> <p>The valid values of this attribute are in the range of 4-315360000.</p> <p>Default value = 60 seconds</p>
Operations	<p>Type-Dimension: string-scalar</p> <p>Indicates the valid operations of the resources of the resource type.</p> <p>Values are OnOnly (can online only), OnOff (can online and offline), None (cannot online or offline).</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = OnOff</p> <p>You may modify the value of this attribute when a resource of that type is not configured.</p>
RestartLimit	<p>Type-Dimension: integer-scalar</p> <p>Number of times to retry bringing a resource online when it is taken offline unexpectedly and before VCS One declares it <code>FAULTED</code>.</p> <p>The valid values of this attribute are in the range of 0-2147483647.</p> <p>Default value = 0</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
ScriptClass	<p>Type-Dimension: string-scalar</p> <p>Indicates the scheduling class of the script processes created by the agent. The online script is an example of a script process affected by this scheduling class. The following values are valid for this attribute:</p> <ul style="list-style-type: none"> ■ RT (Real Time) ■ TS (Time Sharing) ■ SHR (Solaris only) <p>You may use only one of the following sets of attributes to configure scheduling class and priority for VCS One:</p> <ul style="list-style-type: none"> ■ AgentClass, AgentPriority, ScriptClass, ScriptPriority ■ OnlineClass, OnlinePriority, EPClass, EPPriority <p>This attribute is in use if the values of the following attributes is -1: OnlineClass, OnlinePriority, EPClass, and EPPriority</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = TS</p>
ScriptPriority	<p>Type-Dimension: string-scalar</p> <p>Indicates the priority of the script processes created by the agent.</p> <p>You may use only one of the following sets of attributes to configure scheduling class and priority for VCS One:</p> <ul style="list-style-type: none"> ■ AgentClass, AgentPriority, ScriptClass, ScriptPriority ■ OnlineClass, OnlinePriority, EPClass, EPPriority <p>This attribute is in use if the values of the following attributes is -1: OnlineClass, OnlinePriority, EPClass, and EPPriority</p> <p>You may not override this value at the individual resource level.</p> <p>Default value = 0</p>
SourceFile	<p>Type-Dimension: string-scalar</p> <p>The name of the XML file where this object resides.</p> <p>Default value = types.xml</p>
SupportedActions	<p>Type-Dimension: string-keylist</p> <p>Valid action tokens for resource.</p> <p>You may not override the value of this attribute at the individual resource level.</p> <p>Default value = ""</p>

Table 36-6 Resource type attributes

Resource Type Attribute	Definition
ToleranceLimit	<p>Type-Dimension: integer-scalar</p> <p>Number of times the monitor entry point should return OFFLINE before declaring the resource FAULTED.</p> <p>The valid values of this attribute are in the range of 0-2147483647.</p> <p>Default value = 0</p> <p>Modification note: A large value could delay detection of a genuinely faulted resource.</p>
TypeDefinitionVersion	<p>Type-Dimension: string-scalar</p> <p>Specifies the version of the type-definition in use by all the agents of this type on a given platform. The type-definition version for a given resource type could be different on different platforms.</p> <p>See “About the types file” on page 568.</p> <p>Default value = UNKNOWN</p> <p>Do not edit the value of this attribute.</p>

Resource attributes

[Table 36-7](#) lists resource attributes in alphabetical order and provides definitions and information about their use:

Table 36-7 Resource attributes

Resource Attribute	Definition
ArgListValues	<p>Type-Dimension: string-vector</p> <p>List of arguments that are passed to the resource’s agent on each system. This attribute is resource-specific and system-specific, which means that the list of values that are passed to the agent depend on which system and resource they are intended.</p> <p>Default value is not applicable to this attribute</p> <p>You may not edit the value of this attribute.</p>
AutoStart	<p>Type-Dimension: boolean-scalar</p> <p>Indicates the resource is brought online when the service group is brought online.</p> <p>Default value = 1</p>

Table 36-7 Resource attributes

Resource Attribute	Definition
ComputeStats	<p>Type-Dimension: boolean-scalar</p> <p>Indicates to agent framework whether or not to calculate the resource's monitor statistics.</p> <p>Default value = 0</p>
ConfidenceLevel	<p>Type-Dimension: integer-scalar</p> <p>Indicates the level of confidence [percentage] in an online resource.</p> <p>The value for this attribute ranges from 0-100. Note that some VCS One agents may not take advantage of this attribute and may always set it to 0. Set the level to 100% if the attribute is not used.</p> <p>Default value = 0.</p> <p>You may not edit the value of this attribute.</p>
ConfidenceMsg	<p>Type-Dimension: string-scalar</p> <p>Indicates the reason why the level of confidence of an online resource is not 100%.</p> <p>The values for this attribute are specific to the agent that manages the resource.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
ControlGroup	<p>Type-Dimension: string-scalar</p> <p>This attribute indicates whether or not a resource is an off-host resource. The following values are valid for this attribute:</p> <ul style="list-style-type: none"> ■ ControlGroup value = "" (null) indicates the resource is a local resource. ■ ControlGroup value = <i>name of the control group</i> indicates the resource is an off-host resource. <p>The control group is located on the control system.</p> <p>Only resources of type NetAppExport can be configured as off-host resources.</p>
ControlMode	<p>Type-Dimension: boolean-scalar</p> <p>Indicates whether (1) or not(0) it is necessary to provide values for required attributes in order for a resource in the control group to online completely.</p> <p>Use ControlMode = 1 when the resource is running as part of the control group and it is not necessary to provide values for the required attributes of the resource. Tells the agent that the off-host resource provides this resource the list of arguments.</p> <p>Only resources of type NetAppExport can be configured as off-host resources.</p> <p>Default value = 1</p>

Table 36-7 Resource attributes

Resource Attribute	Definition
Enabled	<p>Type-dimension: boolean-scalar</p> <p>Indicates that agents monitor the resource. If a resource is created dynamically while VCS One is running, you must enable the resource before VCS One monitors it.</p> <p>When Enabled = 0, the resource is disabled. A disabled resource is not brought online.</p> <p>Default value = 1 if the resource is in main.xml before starting VCS One, otherwise the default value is 0.</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
Flags	<p>Type-Dimension: integer-scalar</p> <p>Provides additional information for the state of a resource. Primarily this attribute raises flags pertaining to the resource.</p> <p>Values:</p> <p>NORMAL indicates standard working order.</p> <p>RESTARTING indicates the resource has faulted and the agent is attempting to restart the resource on the same system.</p> <p>STATE UNKNOWN indicates the latest monitor call by the agent could not determine if the resource was online or offline.</p> <p>MONITOR TIMEDOUT indicates the latest monitor call by the agent was terminated because it exceeded the maximum time that is specified by the static attribute MonitorTimeout.</p> <p>UNABLE TO OFFLINE indicates the agent attempted to offline the resource but the resource did not go offline. This flag is also set when a resource faults and the clean entry point completes successfully, but the subsequent monitor hangs or is unable to determine resource status.</p> <p>Default value is not applicable to this attribute.</p> <p>You may not edit the value of this attribute.</p>
Group	<p>Type-Dimension: string-scalar</p> <p>The name of the group to which the resource belongs.</p> <p>This attribute only displays using the CLI, for example, the hares -display command.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>

Table 36-7 Resource attributes

Resource Attribute	Definition
IState	<p>Type-Dimension: integer-scalar</p> <p>Indicates the internal state of a resource. In addition to the State attribute, this attribute shows to which state the resource is transitioning.</p> <p>Values:</p> <p>NOT WAITING – Resource is not in transition.</p> <p>WAITING TO GO ONLINE – Agent has been notified to bring the resource online but the procedure is not yet complete.</p> <p>WAITING FOR CHILDREN ONLINE – Resource is to be brought online, but the resource depends on at least one offline resource. Resource transitions to WAITING TO GO ONLINE state when all children are online.</p> <p>WAITING TO GO OFFLINE – Agent has been notified to take the resource offline but the procedure is not yet complete.</p> <p>WAITING TO GO OFFLINE (propagate) – Agent has been notified to take the resource offline but the procedure is not yet complete. When the process is complete, the resource’s children are also offline.</p> <p>WAITING TO GO ONLINE (reverse) – Resource is waiting to be brought online, but when it is online it attempts to go offline. Typically this is the result of an offline command that is issued while the resource waits to go online.</p> <p>WAITING TO GO OFFLINE (reverse/propagate) – Resource is waiting to be brought online, but when it is online it attempts to go offline, and the resource propagates the offline action.</p> <p>Default value = NOT WAITING</p> <p>You may not edit the value of this attribute.</p>
LastOnline	<p>Type-Dimension: string-scalar</p> <p>Indicates the system name on which the resource was last online. The Policy Master sets this attribute.</p> <p>Default value is not applicable to this attribute.</p> <p>You may not edit the value of this attribute.</p>
MonitorOnly	<p>Type-dimension: boolean-scalar</p> <p>A value of 0 indicates a resource can be taken offline and brought online. If the resource can be monitored only, the value is 1.</p> <p>The hagr -freeze command modifies the value of this attribute.</p> <p>Default value = 0</p> <p>You may not edit the value of this attribute.</p>

Table 36-7 Resource attributes

Resource Attribute	Definition
MonitorTimeStats	Type-dimension: string-association Keys are Average and TS. The values indicate the Average time that is taken by the monitor entry point since the time that is indicated by the timestamp (TS) that Average was updated. Default value = Average = 0; TS = "" You may not edit the value of this attribute.
Name	Type-Dimension: string-scalar Name of the resource. The value of this attribute does not persist when the Policy Master restarts. Default value = "" You may not edit the value of this attribute.
NotifyAttrChange	Type-Dimension: string-keylist The value of this attribute is a list of attributes. Whenever any of the attributes in this list is modified, the RES_ATTR_CHANGE event is generated. Use this attribute to monitor changes in resource attributes. Default value = ""
Path	Type-Dimension: string-scalar Set to 1 to identify a resource as a member of a path in the dependency tree to be taken offline on a specific system after a resource faults. Default value = 0. You may not edit the value of this attribute.
PlatformName	Type-Dimension: string-scalar The name of the platform of the group to which the resource belongs. See " PlatformName " on page 717. This attribute only displays using the CLI, for example, the hares -display command. Default value = "" You may not edit the value of this attribute.
Probed	Type-Dimension: integer-scalar Indicates whether the agent has detected the resource. Default value = 0. You may not edit the value of this attribute.

Table 36-7 Resource attributes

Resource Attribute	Definition
ResCreated	Type-Dimension: integer-scalar Default value = "" You may not edit the value of this attribute.
ResFaultPolicy	Type-Dimension: string-scalar Controls the behavior of a resource in the event of a fault. The following values are valid for this attribute: <ul style="list-style-type: none"> ■ FaultPropagateAll ■ FaultPropagateParent ■ FaultHold ■ FaultNone See "Resource level control" on page 228. See "Faulted resource state not reflected in service group state" on page 593. Default value = FaultPropagateAll
ResLastConfigUpdate	Type-Dimension: integer-scalar The value of this attribute does not persist when the Policy Master restarts. Default value = "" You may not edit the value of this attribute.
ResLastStateUpdate	Type-Dimension: integer-scalar The value of this attribute does not persist when the Policy Master restarts. Default value = "" You may not edit the value of this attribute.
ResourceInfo	Type-Dimension: string-association Indicates information about the resource as it is populated by the info entry point. This attribute has three predefined keys: State: Values are Valid, Invalid, or Stale Msg: Output of the info entry point captured on stdout by the agent framework TS: Timestamp that indicates when the agent framework updated the ResourceInfo attribute. Defaults: State = Valid Msg = "" TS = ""

Table 36-7 Resource attributes

Resource Attribute	Definition
Signaled	<p>Type-Dimension: integer-association</p> <p>Used when you bring a service group online or take it offline. This attribute indicates whether or not a resource has been traversed. The following values are valid for this attribute: online, offline, clear, visited.</p> <p>The value of this attribute does not persist when the Policy Master restarts.</p> <p>Default values:</p> <p>online = 0</p> <p>offline = 0</p> <p>clear = 0</p> <p>visited = 0</p> <p>You may not edit the value of this attribute.</p>
SourceFile	<p>Type-Dimension: string-scalar</p> <p>The name of the XML file where this object resides.</p> <p>Default value = ""</p>
Start	<p>Type-Dimension: integer-scalar</p> <p>Indicates whether a resource was started (the process of bringing it online was initiated) on a system.</p> <p>Default value = 0.</p> <p>You may not edit the value of this attribute.</p>

Table 36-7 Resource attributes

Resource Attribute	Definition
State	<p>Type-Dimension: integer-scalar</p> <p>Displays the state of the resource and the flags that are associated with the resource. This attribute and the Flags attribute present a comprehensive view of the resource's current state.</p> <p>Values:</p> <p>ONLINE</p> <p>OFFLINE</p> <p>FAULTED</p> <p>ONLINE STATE UNKNOWN</p> <p>ONLINE MONITOR TIMEOUT</p> <p>ONLINE UNABLE TO OFFLINE</p> <p>ONLINE ADMIN_WAIT</p> <p>OFFLINE STATE UNKNOWN</p> <p>FAULTED RESTARTING</p> <p>A faulted resource is physically offline, though unintentionally.</p> <p>Default value = OFFLINE.</p> <p>You may not edit the value of this attribute.</p>
Type	<p>Type-Dimension: string-scalar</p> <p>The resource type of the resource.</p> <p>This attribute only displays using the CLI, for example, the hares -display command.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
WorkLoad	<p>Type-Dimension: integer-association</p> <p>Group's load is passed to this resource when PassLoadInfo in ContainerOpts attribute for this resource type is set to 1. Group's load is stored verbatim in this attribute.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>

Role attributes

[Table 36-8](#) lists role attributes in alphabetical order and provides definitions and information about their use.

Note: Role attributes that correspond to virtualization are visible to the user. This capability is not supported in the current release, but will be available in the future.

Table 36-8 Role attributes

Role attribute	Definition
AutomationPrivileges	Type-Dimension: integer-scalar The business policy automation privileges that a role contains. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
Category	Type-Dimension: integer-scalar Denotes certain characteristics of a role. Default value = 0. You may edit the value of this attribute only by editing the configuration file directly.
Count	Internal use only.
Created	Type-Dimension: integer-scalar Timestamp of when role was created Default value = "" You may not edit the value of this attribute.
Description	Type-Dimension: string-scalar Text that describes the role. Default value = ""
FarmPrivileges	Type-Dimension: integer-scalar The farm level privileges that a role contains. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
FramePrivileges	Type-Dimension: integer-scalar The frame level privileges that a role contains. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.

Table 36-8 Role attributes

Role attribute	Definition
GroupPrivileges	Type-Dimension: integer-scalar The group level privileges that a role contains. Default value = "" You may edit the value of this attribute only by editing the configuration file directly
LastConfigUpdate	Type-Dimension: integer-scalar Timestamp of when role was last modified. The value of this attribute does not persist when the Policy Master restarts. Default value = "" You may not edit the value of this attribute.
MsgCatID	Type-Dimension: integer-scalar Message category ID used for the role object. Default value = 1
NotifierPrivileges	Type-Dimension: integer-scalar The Notifier Privileges that a role contains. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
ObjectPrivileges	Type-Dimension: integer-scalar The object level privileges that a role contains. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
OTPrivileges	Type-Dimension: integer-scalar The OrgTree privileges that a role contains. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
ResourcePrivileges	Type-Dimension: integer-scalar The resource privileges that a role contains. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
rollback_state	Internal use only.

Table 36-8 Role attributes

Role attribute	Definition
SourceFile	Type-Dimension: string-scalar The name of the XML file where this object resides. Default value = main.xml
SystemPrivileges	Type-Dimension: integer-scalar The system privileges that a role contains. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
Type	Type-Dimension: integer-scalar Denotes the type of this role. Possible values are Object, System, Group, Resource, User, OT, Notifier, Frame, Farm, or Automation. The value for this attribute must be between -1 and 9. Default value = -1. You may edit the value of this attribute only by editing the configuration file directly.
UserPrivileges	Type-Dimension: integer-scalar The user privileges that a role contains. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
ValidPrivBits	Internal use only.

User attributes

[Table 36-9](#) lists user and usergroup attributes in alphabetical order and provides definitions and information about their use.

Note: User attributes that correspond to virtualization are visible to the user. This capability is not supported in the current release, but will be available in the future.

Table 36-9 User and usergroup level attributes

User Attribute	Definition
CanImpersonate	Internal use only.

Table 36-9 User and usergroup level attributes

User Attribute	Definition
Created	Type-Dimension: integer-scalar Timestamp of when user object was created Default value = "" You may not edit the value of this attribute.
EffectiveFarmPrivs	Internal use only.
EffectiveFramePrivs	Internal use only.
EffectiveGrpPrivs	Internal use only.
EffectiveNotifierPrivs	Internal use only.
EffectiveObjPrivs	Internal use only.
EffectiveOTPrivs	Internal use only.
EffectiveOUAutomationPrivs	Internal use only.
EffectiveOUFramePrivs	Internal use only.
EffectiveOUGrpPrivs	Internal use only.
EffectiveOUObjPrivs	Internal use only.
EffectiveOUSysPrivs	Internal use only.
EffectiveOUUsrGrpPrivs	Internal use only.
EffectiveOUUsrPrivs	Internal use only.
EffectiveResPrivs	Internal use only.
EffectiveSysPrivs	Internal use only.
EffectiveUsrGrpPrivs	Internal use only.
EffectiveUsrPrivs	Internal use only.
Email	Type-dimension: string-scalar The user's email address that is used for notification. Default = ""

Table 36-9 User and usergroup level attributes

User Attribute	Definition
Enabled	Type-dimension: boolean-scalar Specifies whether user is enabled, that is, capable of performing privileged operations. Default value = 1. You may edit the value of this attribute only by editing the configuration file directly.
FarmRoles	Type-Dimension: string-association The roles that are assigned to the user for the VCS One cluster. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
FirstName	Type-Dimension: string-scalar The first name of the user. Default value = ""
FrameRoles	Type-Dimension: string-association List of frames and the frame roles that are assigned on them to the user. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
GroupRoles	Type-dimension: string-association List of service groups and the respective group roles that are assigned to user. Default = "" You may edit the value of this attribute only by editing the configuration file directly.
LastConfigUpdate	Type-Dimension: integer-scalar Timestamp of when user object was last modified The value of this attribute does not persist when the Policy Master restarts. Default value = "" You may not edit the value of this attribute.

Table 36-9 User and usergroup level attributes

User Attribute	Definition
LastLogin	<p>Type-Dimension: integer-scalar</p> <p>Denotes the last time the user logged on to the VCS One cluster using the GUI.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
LastMessageSent	Internal use only.
LastName	<p>Type-Dimension: string-scalar</p> <p>The last name of the user.</p> <p>Default value = ""</p>
MsgCatID	<p>Type-Dimension: integer-scalar</p> <p>Message category ID used for the user object.</p> <p>Default value = 1</p>
NotifierRoles	<p>Type-Dimension: string-association</p> <p>The list of notifier roles that are assigned to the user.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
ObjectRoles	<p>Type-Dimension: string-association</p> <p>A list of objects and the respective object roles that are assigned to the user on the VCS One cluster.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
OTRoles	<p>Type-Dimension: string-association</p> <p>A list of OUValuePaths and the respective OT roles that are assigned on them to the user.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>

Table 36-9 User and usergroup level attributes

User Attribute	Definition
OUAutomationRoles	Type-Dimension: string-association A list of OUValuePaths and the respective automation roles that are assigned on them to the user. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
OUFrameRoles	Type-Dimension: string-association A list of OUValuePaths and the respective frame roles that are assigned on them to the user. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
OUGroupRoles	Type-Dimension: string-association A list of OUValuePaths and the respective group roles that are assigned on them to the user. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
OUObjectRoles	Type-Dimension: string-association A list of OUValuePaths and the respective object roles that are assigned on them to the user. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.
OUSystemRoles	Type-Dimension: string-association A list of OUValuePaths and the respective system roles that are assigned on them to the user. Default value = "" You may edit the value of this attribute only by editing the configuration file directly.

Table 36-9 User and usergroup level attributes

User Attribute	Definition
OUUserGroupRoles	<p>Type-Dimension: string-association</p> <p>A list of OUValuePaths and the respective usergroup roles that are assigned on them to the user.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
OUUserRoles	<p>Type-Dimension: string-association</p> <p>A list of OUValuePaths and the respective user roles that are assigned on them to the user.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
ResourceRoles	<p>Type-dimension: string-association</p> <p>List of resources and the respective resource roles that are assigned on them to the user.</p> <p>Default = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
SnmAddress	<p>Type-dimension: string-scalar</p> <p>IP address of console where SNMP traps are to be sent for the user.</p> <p>Default = ""</p>
SourceFile	<p>Type-dimension: string-scalar</p> <p>The name of the XML file where this object resides.</p> <p>Default value = main.xml</p>
SystemRoles	<p>Type-dimension: string-association</p> <p>List of systems and the respective system roles that are assigned on them to user.</p> <p>Default = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>

Table 36-9 User and usergroup level attributes

User Attribute	Definition
UserGroupRoles	<p>Type-Dimension: string-association</p> <p>List of user groups and the respective user group roles that are assigned on them to user.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
UserPref	<p>Type-Dimension: integer-scalar</p> <p>Denotes if this User object is a User Preference object.</p> <p>Default value = 0.</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
UserRoles	<p>Type-dimension: string-association</p> <p>List of users and the respective user roles that are assigned on them to user.</p> <p>Default = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
VCSOneClientName	<p>Type-dimension: string-vector</p> <p>A special attribute of a VCSOneClient user that denotes the name of the client system of the particular VCS One Client process.</p> <p>Default = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
WebUser	<p>Type-dimension: integer-scalar</p> <p>A flag denoting that the user is a special Web server user.</p> <p>Default value = ""</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>

Group Transition Queue attributes

[Table 36-10](#) lists GTQ attributes in alphabetical order and provides definitions and information about their use.

Table 36-10 Group transition queue attributes

GTQ entry attribute	Definition
CompatibleGroups	<p>Type-Dimension: string-keylist</p> <p>List of the group names that are compatible with the group represented by this GTQ entry. If this attribute has a value, the group's IncompatibleGroups attribute may not have a value. A group must be compatible with groups with which it has a dependency relationship.</p> <p>Default= none</p> <p>You may edit the value of this attribute only by editing the main.xml configuration file directly.</p>
ContextIdList	Internal use only.
GroupNameList	<p>Type-Dimension: string-keylist</p> <p>List of the group names that this GTQ entry represents.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
IncompatibleGroups	<p>Type-Dimension: string-keylist</p> <p>List of the group names that are incompatible with current group. If the attribute has a value, the group's CompatibleGroups attribute may not have a value, and vice versa. A group must be compatible with groups with which it has a dependency relationship.</p> <p>Default value = none</p> <p>You may edit the value of this attribute only by editing the configuration file directly.</p>
Load	<p>Type-Dimension: integer-association</p> <p>Load of all the groups for which the target system is to be decided.</p> <p>Default value = ""</p> <p>You may not edit the value of this attribute.</p>
MsgCatID	<p>Type-Dimension: integer-scalar</p> <p>Message category ID used for the GTQ entry object</p> <p>Default value = 1</p>

Table 36-10 Group transition queue attributes

GTQ entry attribute	Definition
Priority	Type-Dimension: integer-scalar Priority of the groups that this GTQ entry represents. Default value = "" You may not edit the value of this attribute.
RollbackCopy	Internal use only.
SourceFile	Type-Dimension: string-scalar The name of the XML file where this object resides. Default value = main.xml
TargetCriteria	Type-Dimension: integer-scalar Criteria for the decision of the target system. Default value = "" You may not edit the value of this attribute.
TargetFlag	Type-Dimension: integer-scalar A flag that is specific to this GTQ entry indicating if this is <code>INTENTONLINE</code> <code>GTQEntry</code> , if target is yet to be decided, or if target decision is already made. Default value = "" You may not edit the value of this attribute.
TargetSystem	Type-Dimension: string-scalar The system where the service group is targeted to go online. Default value = "" You may not edit the value of this attribute.

Action entry attributes

Action entry attributes are part of the GTQ functionality.

[Table 36-11](#) lists action entry attributes in alphabetical order and provides definitions and information about their use:

Table 36-11 Action entry attributes

Action entry attribute	Definition
DependentActionList	Type-Dimension: string-keylist List of the action names on which this action depends. Default value = "" You may not edit the value of this attribute.
DependentKickoutActionList	Type-Dimension: string-keylist List of the dependent action names that are specific to target system. Examples are: offline action for a group that is to be kicked out, or online of a child group on which this group depends. This list is always cleared before redeciding target. Default value = "" You may not edit the value of this attribute.
GroupName	Type-Dimension: string-scalar Name of the group. Default value = "" You may not edit the value of this attribute.
MsgCatID	Type-Dimension: integer-scalar Message category ID that is used for the actionentry object Default value = 1
NextActionList	Type-Dimension: string-keylist Next action to be executed in the plan sequence. The value of this attribute does not persist when the Policy Master restarts. Default value = "" You may not edit the value of this attribute.
OpCode	Type-Dimension: integer-scalar Operation code. Valid values are: online, offline, and intent-online Default value = "" You may not edit the value of this attribute.

Table 36-11 Action entry attributes

Action entry attribute	Definition
RollbackCopy	Type-Dimension: integer-scalar For internal use. The value of this attribute does not persist when the Policy Master restarts Default value = "" You may not edit the value of this attribute.
SourceFile	Type-Dimension: string-scalar The name of the XML file where this object resides. Default value = main.xml
SourceSystem	Type-Dimension: string-scalar Source system name that is applicable for online ActionEntry only when doing a failover. For example, the system name on which the service group faulted. Default value = "" You may not edit the value of this attribute.
Status	Type-Dimension: integer-scalar Operation-related status. Valid values are started, not started, completed, and on_hold. Default value = "" You may not edit the value of this attribute.
System	Type-Dimension: string-scalar System name on which to perform the operation. Default value = "" You may not edit the value of this attribute.
TimeStarted	Type-Dimension: integer-scalar Time when the operation started. Set in terms of the global counter. Default value = "" You may not edit the value of this attribute.

Set name attributes

[Table 36-12](#) lists set name attributes in alphabetical order and provides definitions and information about their use:

Table 36-12 Set name attributes

Set name attribute	Definition
Description	Type-Dimension: string-scalar The text of the set name. Default value = ""
EExpression	Type-Dimension: string-scalar The extended attributes expression that is used to create the set. Default value = ""
MsgCatID	Type-Dimension: integer-scalar Message category ID that is used for the object. Default value = 1
OUExpression	Type-Dimension: string-scalar The organization unit expression that is used to create the set. Default value = ""
SourceFile	Type-Dimension: string-scalar The name of the XML file where this object resides. Default value = ""

OUname attributes

OUname attributes are part of the Organization Tree functionality.

[Table 36-13](#) lists OUname attributes in alphabetical order and provides definitions and information about their use:

Table 36-13 OUname attributes

OUname attribute	Definition
Description	Type-Dimension: string-scalar The text of the ouname description. Default value = ""
MsgCatID	Type-dimension: integer-scalar Message category ID that is used for the ouname object. Default value = 1
SourceFile	Type-Dimension: string-scalar The name of the XML file where this object resides. Default value = orgtree.xml

OUvalue attributes

OUvalue attributes are part of the Organization Tree functionality.

[Table 36-14](#) lists OUvalue attributes in alphabetical order and provides definitions and information about their use:

Table 36-14 OUvalue attributes

OUvalue attribute	Definition
Description	Type-Dimension: string-scalar The text of the ouvalue description. Default value = ""
MsgCatID	Type-dimension: integer-scalar Message category ID that is used for the ouvalue object. Default value = 1
SourceFile	Type-Dimension: string-scalar The name of the XML file where this object resides. Default value = orgtree.xml

State reference

This chapter includes the following topics:

- [Cluster states in VCS One global clusters](#)
- [Network link states in VCS One global clusters](#)

Cluster states in VCS One global clusters

In a global cluster environment, VCS One uses the network connections between the VCS One clusters to monitor and maintain the “health” of the remote VCS One clusters. The primary link is used for inter-cluster communication and exchange of cluster information. The heartbeating occurs on all network links. When you enable network connection between the VCS One clusters, the heartbeating between the VCS One clusters is also enabled. VCS One monitors the state of remote clusters using the heartbeats. The state is then communicated to the VCS One engine, which takes appropriate action when required based on the information.

See “[How global clusters work](#)” on page 69.

[Table 37-1](#) provides a list of VCS One remote cluster states and their descriptions.

Table 37-1 VCS One cluster state definitions

State	Definition
INIT	The initial state of the VCS One cluster. This is the default state. The VCS One clusters do not have any connections established at this point.
BUILD	The local and the remote VCS One clusters have established connection. The VCS One clusters exchange the initial snapshot information.
EXITED	The connections between the local and the remote VCS One clusters are closed.
EXITING	The local or the remote VCS One cluster is closing the connections.
TRANSITIONING	The Policy Master in the remote VCS One cluster is failing over from one node to the other in the Policy Master cluster.
FAULTED	The local VCS One cluster has lost connectivity with the remote VCS One cluster.
LINK_FAILOVER	The primary link that is used for inter-cluster communication is down. The VCS One cluster that initiates the connection request (Initiator) is failing over the communication link to an active secondary link that is available between the VCS One clusters.
RUNNING	The VCS One clusters are successfully connected, and have completed exchanging the snapshot information.

Examples of VCS One cluster state transitions

- If a network connection is established between the VCS One clusters, the clusters exchange initial snapshot information. The state of the remote cluster in view of the local cluster transitions from INIT to BUILD state.
INIT -> BUILD
- If a network connection is reestablished between the VCS One clusters, the state of the remote cluster in view of the local cluster transitions from EXITED/FAULTED to BUILD state.
EXITED -> BUILD
FAULTED -> BUILD
- If the exchange of snapshot between the clusters is complete, the state of the remote cluster in view of the local cluster transitions from BUILD to RUNNING state.
BUILD -> RUNNING
- If the local VCS One cluster loses all network connections to a remote VCS One cluster in the BUILD/RUNNING state when the snapshots are exchanged, VCS One transitions the remote cluster state to FAULTED.
BUILD -> FAULTED
RUNNING -> FAULTED
- If the value of the EnableConnections attribute is set to 0 when the remote cluster is in BUILD/RUNNING state, VCS One transitions the remote cluster state to EXITED after all connections are closed.
BUILD -> EXITED
RUNNING -> EXITED

Network link states in VCS One global clusters

In a VCS One global cluster environment, the local and the remote clusters communicate using the network connection details that you define in the NetworkConnections attribute on the VCS One cluster that initiates the connection request. The LinkStatus attribute indicates the status of each network link between the local and the remote clusters. The status of the network connections depends on the value of the EnableConnections attribute. See [“Remote cluster attributes”](#) on page 697.

[Table 37-2](#) provides a list of the individual link status for each network link between the local and the remote clusters and their description.

Table 37-2 Individual links status for network connections

State	Definition
DOWN	<p>The network connection is not established between the local and the remote cluster.</p> <p>The status of a network link can be DOWN in the following cases:</p> <ul style="list-style-type: none"> ■ VCS One has not attempted to establish connection. ■ VCS One cannot establish connection between the VCS One clusters due to a link failure. ■ VCS One is gracefully shut down.
UP	The network connection is established between the local and the remote cluster.
DISABLED	<p>The network connection is disabled between the local and the remote VCS One clusters.</p> <p>The network connection cannot be established because the value of the EnableConnections attribute is set to 0 on the local or the remote cluster.</p>

[Table 37-3](#) provides a list of the consolidated status of all the network links between the local and the remote clusters and their description.

Table 37-3 Consolidated link status for network connections

State	Definition
DOWN	All the individual network links between the VCS One clusters are down.
UP	All the individual network links between the VCS One clusters are up.
PARTIAL UP	At least one individual network link between the VCS One clusters is up.
DISABLED	All the individual network links between the VCS One clusters have the connection disabled.
DISABLED DOWN	At least one network link between the VCS One clusters is down while while all other network links have the connection disabled.

Examples of network link state transitions

- If the value of the EnableConnections attribute is set to 0 on the VCS One cluster to which VCS One initiates a network connection, then the network connection status transitions to DISABLED state.
 Empty -> DISABLED
- If the value of the EnableConnections attribute is set to 1 on both the VCS One clusters and if VCS One establishes a network connection, then the network connection status transitions to UP state.
 Empty -> UP
 The state of the remote cluster in view of the local cluster transitions to BUILD/RUNNING state.
- If the value of the EnableConnections attribute is set to 0 on one or both the clusters and the network connections are already established, then the network connection status transitions from UP to DISABLED state.
 UP -> DISABLED
 The state of the remote cluster in view of the local cluster transitions from BUILD/RUNNING state to EXITING/EXITED.
- If the value of the EnableConnections attribute is set to 0 on one or both the clusters and the network connections are down, then the network connection status transitions from DOWN to DISABLED state.
 DOWN -> DISABLED
 The state of the remote cluster in view of the local cluster transitions to EXITING/EXITED.
- If the network connections are already established and one of the links goes down, the connection status transitions from UP to PARTIAL UP state.
 UP -> PARTIAL UP
 - If the primary link goes down:
 The state of the remote cluster in view of the local cluster transitions from BUILD/RUNNING state to LINK_FAILOVER to BUILD/RUNNING.
 - If any of the links other than the primary link go down:
 The state of the remote cluster in view of the local cluster remains as BUILD/RUNNING state.
- If the network connections are already established and all of the links go down, the connection status transitions from UP to DOWN state.
 UP -> DOWN
 The state of the remote cluster in view of the local cluster transitions from BUILD/RUNNING state to FAULTED.

- If the links between the clusters are DISABLED and one or more links go down, then the link state transitions from DISABLED to DISABLED DOWN if at least one link is UP.

DISABLED -> DISABLED DOWN

- If the links between the clusters are DISABLED and if the value of the EnableConnections attribute is set to 1 on both the clusters, the link state transitions from DISABLED to UP.

DISABLED -> UP

Glossary

AB

See [authentication broker](#).

active/active configuration

A failover configuration where each system runs a number of service groups. If either system fails, the other system takes over and runs both system's service groups. Also known as a symmetric configuration.

active/passive configuration

A failover configuration consisting of a number of service groups on a primary system, and one dedicated target failover system in case the primary system fails. Also known as an asymmetric configuration.

administrative IP address

The operating system controls certain IP addresses and brings them up even before VCS One or VCS brings applications online. An administrative IP address can be used to access a specific system over the network for doing administrative tasks. Examples of these tasks are examining logs to troubleshoot issues or cleaning up temp files to free space. Typically, there is one administrative IP address per node per subnet.

advanced workload management

The feature in VCS One that uses attributes such as service group Priority, Capacity, Load, and CompatibleGroups to choose the best possible target system to host a service group during start up or automated failover.

agent

A process that starts, stops, monitors and reports status of resources as well as cleans up after resource faults.

agent framework

A set of common, predefined functions compiled into each agent. These functions include the ability to connect to the Policy Master (or HAD on the Policy Master cluster), and to understand common configuration attributes.

asymmetric configuration

See [active/passive configuration](#).

AT

Veritas Product Authentication Service.

authentication broker

A component of Veritas Product Authentication Services that serves as an intermediate registration authority and a certification authority. Used to authenticate VCS One users when they log to the VCS One cluster. The authentication broker is one level beneath the root broker. See [root broker](#).

AWM

See [advanced workload management](#).

base IP address

The IP address of the physical network interface brought up by the operating system. It can be used as an [administrative IP address](#).

business rule

The definition of what actions occur in response to event policy configured.

CLI

Command line interface.

cluster

A cluster is two or more computers linked together for some combination of failover, load balancing, multiprocessing, or improved manageability.

Cluster Manager (Java Console)

A Java-based graphical user interface to manage the Policy Master cluster. It provides complete administration capabilities, and can run on any system inside or outside the cluster, on any operating system that supports Java.

Cluster Manager (Web Console)

A Web-based graphical user interface for monitoring and administering the Policy Master cluster.

Disaster Recovery

A solution that supports failover of an application to a cluster in a remote location in the event that the local cluster becomes unavailable. Disaster recovery is based on high availability and data replication technologies.

See also [global cluster](#).

entry point

The functions an agent performs, such as online, offline and monitor. The code sections that carry out these functions can be compiled into the agent itself or implemented as individual Perl scripts.

See *Veritas Cluster Server One Agent Developer's Guide*.

failover

A failover is the VCS One-initiated movement of a service group to another system. See also [switch](#).

floating IP address

See [virtual IP address](#).

gateway

The process that runs on the Policy Master node that executes the GUI and Command Line Interface (CLI) processing for the Policy Master.

global cluster

A group of geographically dispersed clusters that connect and communicate with each other to provide application availability in the event of a disaster.

See also [Disaster Recovery](#).

group

See [service group](#).

group transition queue

An internal data structure used by [advanced workload management](#) to create a prioritized list of service groups and the actions planned for them. Can be in manual or automatic mode.

GTQ

See [group transition queue](#)

GUI

Graphical User Interface

logical IP address

See [virtual IP address](#).

main.xml / main.cf .extension files

The main.xml file is the file that contains the VCS One object instances like service group, systems, etc. and their attributes.

The main.cf file is the file in which the Policy Master VCS-based cluster configuration is stored.

NIC bonding

Combining two or more NICs to form a single logical NIC, which creates higher bandwidth and a more resilient connection to a network switch.

node

A physical host or system in the Policy Master cluster.

notification rule

The definition of which users receive notice of certain events of a specified severity concerning VCS One objects, and how the notice is sent and received.

notifier

A core function that enables authorized users to receive notice when events of a certain type and severity occur.

NTP

Network Time Protocol. Typically used to keep the clocks on VCS One cluster client systems synchronized with each other.

Policy Master

A single highly available specialized application that provides the central logic of the VCS One cluster. Also known as the Policy Master daemon or vcsd, it is responsible for all configuration and management of the VCS One environment. Runs in the Policy Master cluster.

plumb

Term used in some operating systems to make a physical NIC ready to bring up an IP address.

PM

See [Policy Master](#).

RB

See [root broker](#).

resource

Individual components that work together to provide an application service. A resource may be a physical component such as a disk or network interface card, a software component such as Oracle8i or a Web server, or a configuration component such as an IP address or mounted file system.

resource dependency

Resource dependencies indicate resources that depend on each other because of application or operating system requirements. Resource dependencies are graphically depicted in a hierarchy, also called a tree, where the resources higher up (parent) depend on the resources lower down (child).

resource types

Each resource in a VCS One cluster is identified by a unique name and classified according to its type. VCS One includes a set of predefined resource types for storage, networking, and application services.

root broker

The main registration and certification authority for Veritas Product Authentication Services. Usually there is only one root broker per domain. See [authentication broker](#).

seeding

A cluster is seeded if the number of cluster systems declared in the `/etc/gabtab` file in the Policy Master cluster equals the number of systems actually running in the Policy Master cluster. Seeding is not relevant in the VCS One cluster.

segment

A local groupings of systems in the VCS One cluster.

service group

A service group is a collection of resources working together to provide application services. It typically includes multiple hardware-based and software-based resources working together to provide a single service.

service group dependency

A service group dependency provides a mechanism by which two service groups can be linked by a dependency rule, similar to the way resources are linked.

shared storage

Storage devices that are connected to and used by two or more systems.

SMTP notification

Simple Mail Transport Protocol (SMTP) can be used to notify specific VCS One users via email of VCS One cluster events.

SNMP notification

Simple Network Management Protocol (SNMP) developed to manage nodes on an IP network. In VCS One, users can use SNMP to receive notification at a specific console concerning specific events.

state

The current activity status of a resource, group or system. Resource states are given relative to all systems.

switch

A manual operator-initiated process of moving a service group from one system to another. A switch can be done either from the GUI or the command line. See [failover](#).

symmetric configuration

See [active/active configuration](#).

system

The physical system on which applications and service groups reside. When a system is managed by VCS One, it becomes part of the VCS One cluster.

test IP address

IP addresses to help determine the state of a link by sending out a ping probe to another NIC (on another system.) Requires a return ping to complete the test. Test IP addresses can be the same as base IP addresses.

types.extension.xml and types.cf file

The types.xml file describes standard resource types to the VCS One engine; specifically, the data required to control a specific resource.

The types.cf file describes the same to the high availability daemon running in the Policy Master cluster.

virtual IP address

IP addresses that can move from one NIC to another or from one system to another. These IP addresses move with the service group. Sometimes called a logical or floating IP address.

vcsonelientd

A stateless daemon that is responsible for communication between the client systems and the Policy Master, as well as the starting and stopping of agents on the local system. Contained in the VRTSvcsonecd package.

vcsoned

The Policy Master daemon. Equivalent to the Policy Master. Provides the central logic of the VCS One cluster. Responsible for all configuration and management of the VCS One environment.

VxDBMS

A Veritas proprietary relational database management system used for the Policy Master configuration database.

Index

A

- ActionTimeout attribute 720
- ActiveCount attribute 712
- adding
 - remote clusters 478
 - resources 380
 - roles 534
 - service groups 315
 - system from command line 294, 295
 - system from console 293
 - systems 292
 - usergroup 530
 - users 530
 - variables in resource attributes 393
- adding a Simulator instance 181
- administration section
 - about 162
- AgentClass attribute 721
- AgentDirectory attribute 721
- AgentFailedOn attribute 721
- AgentFile attribute 722
- AgentPriority attribute 722
- AgentReplyTimeout attribute 722
- agents
 - about 52
 - custom 53
- AgentStartTimeout attribute 722
- AgentStopped attribute 702
- application management
 - about 273
 - advanced configuration 275
 - basic configuration 274
 - basic failover configuration 275
 - choosing best system with dependencies 284
 - choosing best system without dependencies 285
 - configurations 274
 - decision making 282
 - disruption factor 277
 - Group Transition Queue 283
 - load and capacity 280
 - manual switchover configuration 275
 - service group compatibility 278
- application placement
 - viewing 406
- applications
 - managed 245
- ArgList attribute 723
- ArgListValues attribute 737
- assigning roles 533
- AT
 - see Symantec Product Authentication Service 63, 578
- AttrChangedTimeout attribute 723
- attributes
 - composite service group
 - Authority 692
 - ClusterList 693
 - data type and dimensions 678
 - for cluster 680
 - for fault management 228
 - how control where applications run 276
 - naming requirements 209
 - overriding 720
 - remote cluster 692, 697
 - ClusterName 697
 - ClusterState 697
 - ConnectionRole 697
 - ConnectionTimeout 698
 - ConsolidatedLinkStatus 698
 - DRPort 699
 - EnableConnections 699
 - LinkStatus 700
 - MaxHeartbeatInterval 700
 - MissedHeartbeatThreshold 700
 - NetworkConnections 701
 - RClusterUUID 701
 - ReconnectInterval 701
 - RunningDRVersion 702
 - SourceFile 702
 - TransitionTimeout 702
- authenticating users
 - about 543

- using environment variables 545
- using halogin 545
- using switches 544
- authentication issues 616
- Authority attribute 692
- AutoDisabled attribute 703
- AutoEnablePending attribute 703
- AutoEnableWait attribute 712
- AutoStart attribute 723, 737
- AvailableCapacity attribute 703

B

- back up 575
- backing up
 - Symantec Product Authentication Service 578
- backing up configuration database 575
 - full backup 577
 - incremental backup 577
 - to an XML file 576
- Backing up configuration information 578
- backing up VCS One data 575
- best practice
 - communications 84, 96
 - coordinator disks 88
- bringing online
 - global CSG 500
- bringing selected resources online 349

C

- Capacity attribute 704
- categories in roles 629
- changing
 - DR address on local cluster 492
 - DR port on local cluster 491
- changing browser settings 103
- changing database password 574
- child resource 37
- clean entry point 53
- cleaning configuration database 571
- CleanTimeout attribute 723
- clearing
 - resource fault 388
 - service group fault 344
- cli_prompt 179
- client daemon
 - about 52
- client logs 583
- CloseTimeout attribute 724

- cluster
 - networking 47
 - role type 629
 - viewing configuration tasks 170
- cluster interconnect 81
- cluster level attributes 680
- cluster states 762
- ClusterAddress attribute 681
- ClusterDirs attribute 681
- ClusterList attribute 693
- ClusterMode attribute 681
- ClusterName attribute 681, 697
- ClusterState attribute 681, 697
- cold start up mode 54, 55
- command line interface 102
- communications 81
 - about secure 63
 - best practice 96
 - handling failures 58
- CompatibleGroups attribute 754
- composite service groups section
 - about 139
 - configuration 140
 - operations 140
 - view 141
- ComputeStats attribute 738
- ConfidenceLevel attribute 738
- configuration
 - about 566
 - extended attributes 167
 - major steps of 213
 - organization units 165
 - roles 164
 - sets 168, 169
 - users and user groups 163
- configuration database
 - about 566
 - changing password 574
 - cleaning 571
 - initializing 574
 - restarting 573
 - seeding from existing database 572
 - seeding from XML file 572
 - starting 571
 - stopping 573
 - verifying 572
 - viewing status 573
- configuration version number 59
- configurations in dependency 251

- configured information 219
- configuring
 - global CSG 498
 - notification SMTP settings 523
 - notification SNMP settings 523
- ConfInterval attribute 724
- ConnectionRole attribute 697
- ConnectionTimeout attribute 698
- console ports
 - about 108
- consolidated network link states 763
- ConsolidatedLinkStatus attribute 698
- coordinator disks 87, 89
- CounterInterval attribute 682
- CPUBinding attribute 704
- credentials 63
- CredRenewInterval attribute 683
- CurrentCount attribute 713
- custom agent 53
- custom agents
 - in zones 455
- customer systems 46
- CVN
 - see configuration version number

D

- daemon
 - about client 52
 - high availability 80
- Daemon Dead Node Alive 58
- data protection
 - with membership arbitration 91
- DDNA
 - see Daemon Dead Node Alive
- DDNAPingInterval attribute 705
- DDNAState attribute 705
- default Simulator
 - starting 180
- DefaultPlatform attribute 684
- defining compatibility 400
- defining group fault policy 402
- defining incompatibility 400
- defining load and capacity 404
- defining priority 400
- defining service group load 405
- defining system capacity 405
- defining SystemList 398
- deleting
 - a role 537

- a user 532
 - remote clusters 484
 - resources 381
 - service groups 326
 - systems 298
- dependencies
 - for resources 38
- dependencies in service groups 247
- dependency configurations 251
- dependency types
 - firm 251
 - global 250
 - hard 251
 - local 250
 - soft 250
- dependency view
 - about 135
- determining
 - cluster connection role 480
 - remote cluster connection role 480
- diagnostics 587
- disabled menu items
 - about 111
- disabling
 - a user 540
 - resources 384
 - service group resources 348
 - service groups 342
- disaster recovery 66
- disaster recovery section
 - about 148
 - configuration 150
 - operations 149
 - simulating operations 151
- disgnostics
 - hagetcf utility 622
- disruption factor 277
- DRPort attribute 699

E

- editing
 - remote cluster attributes 483
- Email attribute 748
- email, maximum limit setting 525
- EnableConnections attribute 699
- Enabled attribute 713, 749
 - for service groups 713
- EnableFFDC attribute 685
- enabling

- a user 539
- resources 383
- service group resources 347
- service groups 342
- EngineClass attribute 685
- EnginePriority attribute 685
- Evacuate attribute 713
- extended attributes
 - viewing 167
- extended attributes section
 - about 166
 - inherited 167
 - locally-defined 167

F

- Failover attribute 231
- Failover attribute (system) 231
- failover service groups 245
- fault management
 - about 227
 - related attributes 228
 - resource level attributes 228
 - service group level attributes 230
 - system level attributes 231
- fault management attributes
 - Failover 231
 - Failover attribute (system) 231
 - FaultHold 229
 - FaultNone 230
 - FaultPropagateAll 229
 - NoFailover 231
 - NoFailover (system) 231
- FaultHold attribute 229
- faulting a resource 387
- faulting a service group 343
- faulting a system 305
- FaultNone attribute 230
- FaultOnMonitorTimeouts attribute 726
- FaultPropagateAll attribute 229
- fencing 87
 - start up process 88
- FFDC log 587
- Figure 223
- figuring 454
- filtering systems 129
- FireDrill attribute 727
- firm dependency 251
- Flags attribute 739
- flushing

- service groups 337
- FragmentationPolicy attribute 406, 685
- freezing
 - service group 339
 - systems 300
- Frozen attribute 706, 714
 - for service groups 714

G

- GAB 82
- global clusters 66
 - application failover 71
 - building blocks
 - global CSG 67
 - remote cluster objects 67
 - replication agents 67
 - changing DR address value 492
 - changing DR port value 491
 - changing DRAddress 492
 - changing DRListeningPort 491
 - cluster states 762
 - BUILD 762
 - examples 763
 - EXITED 762
 - EXITING 762
 - FAULTED 762
 - INIT 762
 - LINK_FAILOVER 762
 - RUNNING 762
 - TRANSITIONING 762
 - communication 69
 - ConnectionRole
 - Acceptor 69
 - Initiator 69
 - consolidated network link states 763
 - DISABLED 764
 - DISABLED DOWN 764
 - DOWN 764
 - PARTIAL UP 764
 - UP 764
 - CSG flags 72
 - CSG states 72
 - determining connection role 480
 - disabling connections 485
 - disaster recovery 73
 - enabling connections 485
 - failover and recovery 73
 - failure
 - complete network link failure 77

- partial network link failure 77
 - partial site failure 75, 76
 - Policy Master node failure 76
 - replication link failure 77
 - total site failure 75
- failure diagnosis 73
- global CSG
 - authority 72
- how clusters communicate 69
- managing global CSG 498
- managing remote clusters 478
- network link states 763
 - DISABLED 764
 - DOWN 764
 - examples 765
 - UP 764
- Policy Master
 - warm mode 72
- setting up 470, 471
 - application 471
 - clusters 472
 - CSGs 473
 - global CSGs 473
 - replication 471
 - service groups 473
- setup workflow 470
- simulate
 - clear simulated cluster fault 493
 - clear simulated link fault 494
 - link fault 493
 - remote cluster fault 492
- testing setup 474
- typical setup 68
- viewing cluster state 488
- global CSG 67
 - bringing online 500
 - configuring 498
 - managing 498
 - requesting authority 499
 - switching 502
 - taking over 503
- global dependency 250
- GlobalCounter attribute 686
- Group Dependency View
 - locating 323
- group dependency view 135
- group fault policy 402
- Group Membership Services/Atomic Broadcast 81, 82
- Group Transition Queue
 - about 283
 - events that change entries 286
- GroupRoles attribute 749
- GrpFaultPolicy attribute 714
- GTQ
 - about 283
 - events that change entries 286
- H**
- HAD 80, 81
- hagetcf utility 622
- halogin 545
- hamultisim 179
- hard dependency 251
- hardware
 - requirements and recommendations 206, 208
- hasim
 - Simulator
 - hasim 179
- hastart command 54
- heartbeat 83
 - in policy master cluster 84
- high availability daemon 80
- History menu
 - about 117
- how to
 - add a resource 380
 - add a service group 315
 - add a system 292
 - add a user 530
 - add a usergroup 530
 - add a variable in a resource attribute 393
 - add roles 534
 - assign roles to a user 533
 - bring a service group online 329
 - bring resources online 384
 - bring selected resources online 349
 - change browser settings for the console 103
 - change service group load 352
 - change service group priority 351
 - change service group system list 353
 - change the database password 574
 - clean configuration database 571
 - clear a resource fault 388
 - clear service group fault 344
 - clone service groups 350
 - configure SMTP notification settings 523
 - configure SNMP notification settings 523

- create an off-host resource 357
- define a SystemList 398
- define compatibility 400
- define FragmentationPolicy attribute 406
- define group fault policy 402
- define incompatibility 400
- define load and capacity 404
- define priority 400
- define service group load 405
- define system capacity 405
- delete a user 532
- delete resources 381
- delete roles 537
- delete service groups 326
- delete systems 298
- disable a user 540
- disable resources 384
- disable service group resources 348
- disable service groups 342
- edit service group attributes 324
- edit system attributes 297
- enable a user 539
- enable resources 383
- enable service group resources 347
- enable service groups 342
- enable syslog notifications 526
- flush service groups 337
- freeze a system 300
- freeze service groups 339
- global clusters
 - add remote clusters 478
 - bring global online 500
 - change DR address on local cluster 492
 - change DR port on local cluster 491
 - change DRAddress value 492
 - change DRListeningPort value 491
 - configure global CSG 498
 - determine connection role 480
 - request authority for global CSG 499
 - switch global CSG 502
 - take over global CSG 503
 - view cluster state 488
- initialize database configuration 574
- link resources 390
- link service groups 345
- log off from the VCS One console 106
- log on to the console 104
- modify service groups 327
- modify user attributes 538
- modify user settings 538
- move service groups 327
- offline a service group and propagate the command 333
- online a service group and propagate the command 329
- probe resources 386
- probe service group resources 349
- remote clusters
 - delete 484
 - determine connection role 480
 - disable connections 485
 - edit attributes 483
 - enable connections 485
 - modify configuration 488
 - view 481
 - view cluster state 488
 - view network link status 486
 - viewing consolidated network link status 487
 - viewing details 482
- restart configuration database 573
- seed configuration database from existing database 572
- seed configuration database from XML file 572
- set PrecedenceOrder 404
- simulate adding a system 297
- simulate DDNA state 309
- simulate resource faults 387
- simulate resource repair 388
- simulate service group faults 343
- simulate system faults 305
- simulate system heartbeat failure 310
- simulate system heartbeat recovery 311
- simulate system offline operation 309
- simulate system repair 306
- start configuration database 571
- stop configuration database 573
- stop Simulator 199, 200
- switch service groups 336
- take a service group offline 333
- take resources offline 385
- take selected resources offline 350
- test SMTP notification settings 528
- unfreeze a system 302
- unfreeze service groups 340
- unlink resources 392
- unlink service groups 346
- update privilege 536

- verify configuration database 572
- view database status 573
- view service group attributes 324
- view system attributes 296
- view user settings 541
- viewing selected list of systems 308

I

- I/O fencing
 - algorithm 92
 - examples 93, 94
- IMF attribute 728
- implementation, major steps in 212
- IncompatibleGroups attribute 754
- InfoInterval attribute 729
- InfoTimeout attribute 729
- inherited extended attributes 167
- initializing configuration database 574
- installation
 - preparation 211
- interpreting log messages 587
- issuing commands
 - through script 546
 - using environment variables 545
 - using halogin 545
 - using switches 544
- IState attribute 740

J

- Java Keytool utility
 - about 109
- jobs section
 - about 151
 - configuration 153
 - operations 152

L

- LicensedCPUs attribute 686
- LicensedFeatures attribute 686
- LicenseType attribute 687
- linking
 - resources 390
 - service groups 345
- LinkStatus attribute 700
- LLT 82, 83
- load and capacity 280, 404
- Load attribute 715

- local dependency 250
- locally-defined extended attributes 167
- LockMemory attribute 687
- LogDbg attribute 729
- LogFileSize attribute 730
- logging off from the VCS One console 106
- logging on 104, 105
- logs 582
 - about 582
 - client 583
 - first failure data capture 587
 - interpreting log messages 587
 - Policy Master 583
 - searching 158, 160, 161
 - Simulator 584
 - Symantec Product Authentication services
 - logs 584
 - Symantec Web server logs 584
 - viewing 157, 159, 160
- logs section
 - about 156
 - logs 157, 159, 160
- LogSize attribute 687
- Low Latency Transport 82, 83

M

- managed applications
 - about 36
 - see also application management
- managing applications 273
- managing faults in VCS One 227
- managing global CSG 498
- managing remote clusters 478
- ManualOps attribute 715
- MaxHeartbeatInterval attribute 700, 706
- membership
 - in VCS One cluster 58
- membership arbitration 87
 - and data protection 91
 - process 89
- menu items, disabled
 - about 111
- MissedHeartbeatThreshold attribute 700, 707
- modifying
 - remote cluster configuration 488
- monitor entry point 53
- MonitorInterval attribute 730
- MonitorOnly attribute 740
- MonitorStartParam attribute 731

MonitorTimeout attribute 731
 MonitorTimeStats attribute 741

N

NetApp Filer
 off-host resource 358
 network link states 763
 examples 765
 NetworkConnections attribute 701
 networking
 in cluster 47
 NetworkTimeout attribute 688
 NodeFaultPolicy attribute 716
 NodeId attribute 707
 NodeIdCounter attribute 688
 NoFailover attribute 231
 NoFailover attribute (system) 231
 normal start up mode 54
 notification
 configuring SMTP notification settings 523
 configuring SNMP notification settings 523
 enabling syslog notifications 526
 testing SMTP settings 528
 notifications, halted 525
 notifications, maximum limit setting 525
 notifier role type 638
 NumMissedHeartbeat attribute 707
 NumThreads attribute 731

O

off-host resource 357
 NetApp Filer 358
 off-host resources
 about 260
 internals 261
 multiple control groups 263
 optimizing setup 263
 user privileges 264
 offline entry point 53
 OfflineMonitorInterval attribute 732
 OfflineTimeout attribute 732
 OnGrpCnt attribute 708
 online entry point 53
 OnlineRetryLimit attribute 734
 OnlineTimeout attribute 735
 OnlineWaitLimit attribute 735
 OpenTimeout attribute 735
 Operations attribute 735

optimizing
 off-host resource setup 263
 organization tree
 filtering objects 116
 naming requirements 209
 organization unit role type 637
 organization units section
 about 165
 viewing 165

P

Parallel attribute 716
 parallel service groups 245
 parent resource 37
 PathCount attribute 716
 planning
 for failover environments 244
 managed applications 242
 planning attribute names 209
 planning object name 209
 PlatformName attribute 708
 PMSG
 see policy master service group
 policy master
 about 47
 about daemon 47
 cluster communications 80
 components 48
 handling communication failures 58
 how controls resources 52
 service group 49
 start up actions 54
 start up modes 54
 policy master cluster
 about 47
 communications 80
 heartbeat 83, 84
 membership 85, 86
 membership arbitration 87
 policy master cluster membership arbitration
 components 87
 policy master daemon 47
 Policy Master logs 583
 policy master service group 49
 policy master start up modes 54
 ports, console
 about 108
 precedence order 170
 PrecedenceOrder attribute 404, 688

- preparation for installation 211
- Priority 400
- Priority attribute 717
- privileges
 - updating 536
- Probed attribute 717
 - for service groups 717
- ProbesPending attribute 717
- probing
 - resources 386
 - service group resources 349
- ProcessClass attribute 689
- ProcessPriority attribute 689
- ProductVersion attribute 689
- ProtocolVersion attribute 689
- ProxySimIPAddr attribute 689

Q

- QUIESCE state 59

R

- RClusterUUID attribute 701
- ReconnectInterval attribute 701
- remote cluster attributes 692, 697
- remote cluster objects 67
- remote clusters
 - adding 478
 - deleting 484
 - determining connection role 480
 - disabling connections 485
 - editing attributes 483
 - enabling connections 485
 - managing 478
 - modifying configuration 488
 - viewing 481
 - viewing cluster state 488
 - viewing consolidated network link status 487
 - viewing details 482
 - viewing network link status 486
- removing a Simulator instance 200
- replicated state machine 81
- requesting authority
 - global CSG 499
- requirements and recommendations
 - hardware 206, 208
- ReservedCapacity attribute 708
- ResFaultPolicy attribute 742
- resource

- actions on 53
- child definition 37
- clean entry point 53
- dependency tree 38
- monitor entry point 53
- offline entry point 53
- online entry point 53
- parent definition 37
- restart 53
- resource dependencies
 - about 37
- resource dependency tree 38
- resource dependency view 135
- resource role type 636
- resource section
 - operations 146
- resource type attributes
 - overriding 720
- resource types section
 - about 392
- resource variables 393
- ResourceInfo attribute 742
- ResourceRoles attribute 752
- resources
 - adding 380
 - adding variables in resource attributes 393
 - bringing online 384
 - clearing fault 388
 - deleting 381
 - disabling 384
 - enabling 383
 - how controlled by policy master 52
 - linking 390
 - probing 386
 - related views 379
 - resource dependency view 379
 - simulating faults 387
 - simulating repair operation 388
 - taking offline 385
 - unlinking 392
 - variables 393
- resources section
 - about 145
- Responding attribute 718
- restart resource 53
- restarting configuration database 573
- RestartLimit attribute 735
- RestartMode attribute 690
- restore 575

- restoring
 - Symantec Product Authentication Service 578
- restoring configuration information 578
- restoring the configuration database 577
- restoring VCS One data 575
- role types
 - cluster 629
 - notifier 638
 - organization unit 637
 - resource 636
 - system 632, 633, 635
 - user 637, 641
- roles
 - about 43
 - adding 534
 - categories 629
 - deleting 537
 - updating privilege 536
- roles section
 - about 164
- rules section
 - configuration 155
 - operations 154
- RunningDRVersion attribute 702

S

- ScriptClass attribute 736
- ScriptPriority attribute 736
- SCSI-3
 - in Policy Master cluster 91
 - in the cluster 80
 - on coordinator disks 88
- search section
 - about 172
- searching
 - logs 158, 160, 161
- security
 - about 63
- seeding configuration database from existing
 - database 572
- seeding configuration database from XML file 572
- service group
 - about 38
 - adding 315
 - bringing online 329
 - bringing online and propagating 329
 - bringing selected resources online 349
 - changing load 352
 - changing priority 351

- changing system list 353
- clearing fault 344
- cloning 350
- compatibility 278
- components of 243
- creating an off-host resource 357
- deleting 326
- dependency 40
- dependency levels 244
- disabling 342
- disabling resources 348
- editing attributes 324
- enabling 342
- enabling resources 347
- flushing 337
- freezing 339
- kickout 277
- linking 345
- modifying 327
- moving 327
- policy master 49
- probing resources 349
- sample 38
- simulating faults 343
- switching 336
- taking offline 333
- taking offline and propagating 333
- taking selected resources offline 350
- unfreezing 340
- unlinking 346
- viewing attributes 324
- service group dependencies 40
- service group dependency
 - configurations 251
 - firm 251
 - global 250
 - hard 251
 - local 250
 - rules of 247
 - soft 250
 - types 249
- service groups
 - dependencies 247
 - failover 245
 - parallel 245
- service groups section
 - about 130
 - configuration 132
 - operations 134

- simulating operations 138
- sets section
 - about 168
- setting PATH for CLI 102
- settings section
 - about 169
- shared storage 47
- simulating
 - DDNA state 309
 - global clusters
 - clear simulated cluster fault 493
 - clear simulated link fault 494
 - link fault 493
 - remote cluster fault 492
 - resource faults 387
 - resource repair 388
 - service group faults 343
 - system addition 297
 - system faults 305
 - system heartbeat failure 310
 - system heartbeat recovery 311
 - system offline operation 309
 - system repair 306
- Simulator 32
 - about 174
 - accessing the command line 190
 - accessing the GUI 189
 - adding an instance 181
 - changing a configuration 186
 - cli_prompt 179
 - commands 179
 - components of 176
 - creating a custom configuration 192
 - displaying instance status 192
 - hamultisim 179
 - hamultisim command usage 179
 - hasim command usage 179
 - instances 178
 - listing instances 193
 - listing port information 194
 - loading a configuration 186
 - logging on 189
 - multiple instances 178
 - ports 183
 - removing an instance 200
 - scripts 179
 - starting 182
 - starting in read-only mode 183
 - starting with non-default ports 183
 - startsim 179
 - start-up modes 177
 - stopping 199, 200
 - stopping an instance 199
 - stopsim 179
- Simulator logs 584
- soft dependency 250
- SourceFile attribute 690, 702, 708, 718, 736, 743, 752
 - for resource types 736
 - for service groups 718
- SSL certificates
 - managing 108
- StaleSysState attribute 709
- Start attribute 743
- start up mode
 - cold 55
- starting configuration database 571
- starting the default Simulator 180
- starting the Simulator 182
- starting vcsoneclientd 303
- startsim 179
- State attribute 718, 744
 - for service groups 718
- stopping a Simulator instance 199
- stopping configuration database 573
- stopping the Simulator 199, 200
- stopping vcsoneclientd 303
- stopsim 179
- storage
 - shared 47
- summary section
 - about 118
 - viewing objects that need attention 119
 - viewing service group status 118
 - viewing system load 118
- SupportedActions attribute 736
- switching
 - global CSG 502
 - switching service groups 336
- Symantec Product Authentication Service 63
 - backing up 578
 - restoring 578
 - troubleshooting 616
- Symantec Product Authentication services server
 - logs 584
- Symantec technical support 623
- Symantec Web server logs 584
- SysInfo attribute 709

- SysName attribute 709
- SysState attribute 709
- system role type 632, 633, 635
- SystemConfigVersion attribute 710
- SystemIPAddr attribute 710
- SystemList attribute 719
- SystemMode attribute 710
- SystemRoles attribute 752
- systems
 - adding 292
 - customer 46
 - deleting 298
 - editing attributes 297
 - freezing 300
 - locating 295
 - simulating DDNA state 309
 - simulating faults 305
 - simulating heartbeat failure 310
 - simulating heartbeat recovery 311
 - simulating offline operation 309
 - simulating system addition 297
 - simulating system repair 306
 - unfreezing 302
 - viewing a selected list 308
 - viewing attributes 296
- systems section
 - about 142
 - configuration 143
 - operations 143
 - simulating operations 144, 148
- SystemSequenceNumber attribute 710
- SystemVersion attribute 710
- SystemZones attribute 719
- SysUserName attribute 711

T

- tab bar
 - about 110
- table views
 - configuring 115
- tables
 - changing settings 114
 - configuring views 115
 - filtering results 115
 - selecting objects 113
 - sorting contents 113
- taking over
 - global CSG 503
- taking selected resources offline 350

- testing
 - notification SMTP settings 528
- ToleranceLimit attribute 737
- TransitionOffline attribute 711
- TransitionOnline attribute 711
- TransitionTimeout attribute 702
- TriggerResStateChange attribute 719
- troubleshooting
 - authentication
 - troubleshooting 616
 - hagetcf utility 622
 - logs 582

U

- unfreezing
 - service group 340
 - systems 302
- unlinking
 - resources 392
 - service groups 346
- user
 - role types 637, 641
- usergroup
 - adding 530
- UserRoles attribute 753
- users 219
 - about 43
 - adding 530
 - assigning roles 533
 - authenticating 543
 - deleting 532
 - disabling 540
 - enabling 539
 - modifying attributes 538
 - modifying settings 538
 - viewing 163
 - viewing settings 541
- users section
 - about 162
 - viewing 163

V

- variables
 - resources 393
- VCS One
 - global clusters 66
- VCS One cluster membership 58
- VCS One console

- about 101
- changing browser settings 103
- logging off 106
- logging on 104, 105
- prerequisite 102
- starting 104
- VCS One replication agents 67
- vcsonclientd
 - diagnostics 587
 - starting 303
 - stopping 303
- VCSoneClientName attribute 753
- vcsoned
 - about 47
 - diagnostics 587
- verifying configuration database 572
- Veritas Cluster Server 49, 80
- Veritas Product Authentication Service 63
- viewing
 - cluster state 488
 - extended attributes 167
 - faulted groups from the workload section 124
 - faulted objects 119
 - global clusters
 - consolidated network link status 487
 - network link status 486
 - logs 157, 159, 160
 - objects that need attention 119
 - offline groups from the workload section 124
 - organization units 165
 - remote cluster details 482
 - remote clusters 481
 - service group status 118
 - system load 118
 - systems by dimension 128
 - user settings 541
 - users 163
 - waiting groups 123
- viewing database status 573
- vxfen. See fencing module

W

- WebUser attribute 753
- workload section
 - about 121
 - filtering systems 129
 - finding service groups 130
 - finding systems 130
 - menu icons 129

- selecting systems for display 128
- service group operations 125
- system and service group tasks 121
- system operations 126
- viewing faulted groups 124
- viewing offline groups 124
- viewing service group information 123, 124
- viewing service group load 122, 123
- viewing system capacity 122, 123
- viewing system information 123, 124
- viewing waiting groups 123

X

- XML backup of database 576

Z

- zone root 455
- zones
 - about 434
 - configuring a service group 439
 - configuring communication with Policy
 - Master 440
 - creating a root on local disk 456
 - creating a root on shared disk 457
 - creating a zone 436
 - installing an application 438
 - prerequisites 454
 - service group attributes 265, 270
 - setting zone root 455
 - supported operations 442
 - using custom agents 455

