

Veritas™ Cluster Server Centralized Management Guide

AIX, HP-UX, Linux, Solaris, Windows

5.0

Veritas™ Cluster Server Centralized Management Guide

Copyright © 2006 Symantec Corporation. All rights reserved.

Veritas Cluster Server 5.0

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

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

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

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

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

Third-party legal notices

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

AIX is a registered trademark of IBM Corporation.

HP-UX is a registered trademark of Hewlett-Packard Development Company, L.P.

Linux is a registered trademark of Linus Torvalds.

Solaris is a trademark of Sun Microsystems, Inc.

Windows is a registered trademark of Microsoft Corporation.

Licensing and registration

Veritas Cluster Server is a licensed product. See the *Veritas Cluster Server Installation Guide* for license installation instructions.

Technical support

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

Contents

Section I	Cluster Management Console basics	
Chapter 1	Getting acquainted with the Cluster Management Console	
	What is the Cluster Management Console?	14
	Improved enterprise-wide application availability	14
	Global failure avoidance and recovery	15
Chapter 2	Concepts, components, and architecture	
	Operational modes	18
	About Cluster Management Console software components	20
	Management server	20
	Cluster connector	21
	General deployment diagram	22
	Objects in the Cluster Management Console	22
	User accounts and user authentication	23
	User account format	23
	Supported user domain types	23
	Internal user accounts	24
	User roles	24
	Privileges and privilege levels	24
	Role type	25
	Role scope	27
	Role persistence	27
	Role-restricted navigation	28
Section II	Administration, configuration, and management	
Chapter 3	Getting started with the Cluster Management Console	
	Verifying installation integrity and other requirements	32
	Connecting to the management server	32
	Logging in to the management server	33
	Logging out of the management server	34

- Overview of the Cluster Management Console 35
 - Objects in the Cluster Management Console 35
 - Cluster Management Console layout 35
 - Icon conventions 47
 - Sorting the contents of a data table 48
 - Viewing multiple pages of a data table 49
 - Controlling view updates 49
- About online help 51
 - Online help navigation 51
 - Locating topics 51

Chapter 4 Administering users and cluster configurations

- Summaries of management server, cluster, and related data 54
 - About summary views 55
 - Summary information in state-wise distribution tables 63
- Administering users and user privileges 65
 - About user listing tables 66
 - Adding and deleting a management server user 68
 - Adding and deleting a cluster user 69
 - Adding management server users to clusters 71
 - Adding management server users and cluster users to service groups 72
 - Granting and revoking the reporting privileges 72
- Administering management servers 74
 - VCS global clusters 74
 - Migrating a site (local site disaster recovery) 75
 - Recovering a failed site (remote site disaster recovery) 76
 - Managing tags 78
 - Creating and deleting maintenance windows 79
 - Configuring a peer management server 80
 - Adding a cluster to the management server using direct connection 81
 - Removing a direct connection cluster from the management server 82
- Administering clusters 83
 - About cluster listing tables 84
 - Cluster tasks at the home and management server level 85
 - Cluster tasks at the cluster level 87
- Administering service groups 88
 - About service group listing tables 90
 - Service group tasks at the home and management server level 92
 - Service group tasks at or below the cluster level 96
- Administering systems 98
 - About system listing tables 99
 - System tasks at the home and management server level 101
 - System tasks at or below the cluster level 102

Administering resources	104
About resource listing tables	105
Resource tasks at or below the cluster level	106
Administering resource types	108
About resource type listing tables	109
Resource type tasks at or below the cluster level	110
Viewing logs	112
Chapter 5	Reporting historical data
About reporting	114
Administering report jobs	116
Viewing a list of report jobs	116
Viewing and modifying details of a report job	117
Creating a new report job	117
Modifying a report job	121
Deleting a report job	122
Running a report job to generate a report output	122
Enabling and disabling a report job	123
Cloning a report job	123
Filtering the report jobs table	124
Granting and revoking reporting privileges	125
Administering report outputs	126
Viewing a list of report outputs	126
Creating a report output	126
Viewing a report output	126
Deleting a report output	127
Linking a reinstalled cluster back to its historical data	127
Filtering report outputs	128
Understanding report types by functionality	129
Tracking VCS agents across the enterprise with reports	129
Managing cluster configurations with reports	130
Analyzing failures for trends, patterns, and problem areas	133
Managing and reporting uptime of service groups	135
Managing cluster storage with reports	136
Tracking activity using reports	136
Chapter 6	Administering notification
Events, policies, and notifications	140
Configuring SNMP consoles to receive traps	142
Notification settings	143
Viewing a list of policies	144
Viewing policy details	145

Creating a policy	145
Editing a policy	147
Deleting a policy	147
Disabling a policy	147
Enabling a policy	148
Exporting policies	148
Importing policies	149

Chapter 7 Searches

About the search feature	152
Conducting a search	152

Chapter 8 Administering the database

Viewing information about the database	156
Pruning the database	157
Backing up the database	158
Restoring the database from a backup	158
Modifying guest access to the database	159

Section III Appendixes

Appendix A Command line interface

Introduction to the command line interface	164
Notations for object names in the CLI	165
Use of qualified and unqualified names	166
Output options summary	167

Appendix B Creating custom reports

Accessing the database information	200
Database schema objects	201
Published database schema objects	202
K2VW_ENTERPRISE	202
K2VW_MServers	204
K2VW_Clusters	206
K2VW_Groups	208
K2VW_Nodes	210
K2VW_ResourceTypes	211
K2VW_Resources	213
K2VW_Schedules	215
K2VW_Logs	217
Example statements	218

	Example 1	218
	Example 2	218
	Example 3	218
Appendix C	Accessibility	
	Navigating the Cluster Management Console	222
	Accessibility features in GUI controls	223
Appendix D	Troubleshooting	
	Installation issues and recommendations	226
	Avoid concurrent installations	226
	Authentication broker installer location	226
	VCS 4.3 upgrade	226
	Installation user account role	226
	Configuration issues and recommendations	227
	Resetting the CMC_CC@CMC_SERVICES user account	227
	Cluster configuration state after cluster user addition	227
	Cluster connector, direct connection, and DNS configuration	228
	Using direct connection to manage a VCS 5.0 secure cluster	228
	Operational issues and recommendations	229
	Cluster Management Console controls not immediately active	229
	Cluster status during snapshot	229
	Log file locations	230
	Status icon reference	231
Index		235

Section



Cluster Management Console basics

Getting acquainted with the Cluster Management Console

This chapter includes the following topics:

- [“What is the Cluster Management Console?”](#) on page 14
- [“Improved enterprise-wide application availability”](#) on page 14
- [“Global failure avoidance and recovery”](#) on page 15

What is the Cluster Management Console?

The Veritas Cluster Management Console is a centralized management solution for high-availability application environments based on Veritas Cluster Server. The mission of the Cluster Management Console is *centralized cluster management*: enabling administrative tasks and analysis for all clusters in your enterprise from a single console.

The Cluster Management Console is also designed to facilitate enterprise-wide installation and configuration. The console components are installed using the native installation process for each supported operating system.

The Veritas Cluster Management Console comprises many features for managing multiple clusters, greatly extending the capabilities of Veritas Cluster Server (VCS). The Cluster Management Console is a single software interface, available using any supported Web browser, that enables you to administer multiple VCS clusters at one site or at multiple sites across your enterprise.

The Central Management Console also represents an evolution of the capabilities of the Veritas CommandCentral Availability product. The Cluster Management Console builds upon the key features of CommandCentral Availability, such as detailed reporting, availability management, cluster configuration management, and user management. The following are a few of the more significant enhancements:

- Includes more bundled agents and enhanced enterprise agents
- Increases the depth of cluster management to include cluster creation and low-level cluster object configuration and manipulation.
- Expands the scope of cluster management to an entire enterprise and multiple geographic sites

Improved enterprise-wide application availability

The Cluster Management Console helps a network administrator work more efficiently by:

- Centralizing visualization, monitoring, and control for clusters
- Quickly detecting, isolating, and correcting errors
- Managing multiple clustered environments from almost anywhere using almost any operating system platform
- Centrally deploying configuration changes.
- Replacing tools that use stored historical data with out-of-the-box reporting

The Cluster Management Console provides detailed reports on historical uptime, failure analysis, and configuration analysis. These reports enable administrators to increase the availability of applications by helping them to detect, and then to correct, configurations or errors that could lead to downtime. The Cluster Management Console also monitors cluster capacity trends and analyzes cluster configurations, which can help to improve server utilization.

Global failure avoidance and recovery

The Cluster Management Console provides two significant disaster recovery (DR) features: One-click migration and failed site recovery. When configured using the VCS Global Cluster Operations (GCO) technology, a site that is experiencing failures, and even those that have unexpectedly and suddenly failed totally, can be recovered and brought online at another geographical site with a single mouse click.

Concepts, components, and architecture

This chapter includes the following topics:

- [Operational modes](#)
- [About Cluster Management Console software components](#)
- [Objects in the Cluster Management Console](#)
- [User accounts and user authentication](#)

Operational modes

The Veritas Cluster Management Console is a high-availability cluster administration and management solution. It can be configured to locally manage a single cluster or to centrally manage multiple clusters.

These two modes of operation are called *single-cluster* and *multi-cluster*. The differences between the modes are significant. Multi-cluster mode offers greater capability on a larger scale. Both modes require different installation and configuration procedures. The following table summarizes some of the differences between single-cluster and multi-cluster mode.

Operational mode	Configurational description
Local management of one cluster (single-cluster mode)	The Cluster Management Console is installed along with VCS on each node in the cluster and is configured for failover. It is integrated with VCS as part of the ClusterService service group. The Cluster Management Console offers robust cluster management capability and can be run from any supported Web browser on any system.
Centralized, comprehensive, enterprise-wide administration of multiple clusters (multi-cluster mode)	<p>One instance of the Cluster Management Console is installed outside all clusters on a standalone server. The console enables users to visually and intuitively input commands to the multi-cluster management engine, the <i>management server</i>. The management server initiates monitoring and management actions based upon those commands. The management server uses a database to store cluster configurations, cluster status, events, event policies, report jobs, report outputs, and more.</p> <p>If the management server and cluster nodes are separated by a firewall, a component called <i>cluster connector</i> is installed on each cluster node. Cluster connector enables communication between the management server and clusters through firewalls. Cluster connector also provides buffering for cluster data. If the management server goes offline and then comes back online, it can retrieve data collected during the offline period from the cluster connector buffer.</p> <p>The console offers additional capability for administering users, reports, events, and notification. If the cluster environment includes licensed VCS global clusters, disaster recovery (DR) capability is also available.</p>

The configurational differences between the operational modes mean that you cannot switch a single Cluster Management Console installation from one mode to the other. The modes are also incompatible on the same system.

Consequently, one system cannot offer both operational modes. However, the modes *can* co-exist in the same multi-cluster environment, with single-cluster-mode installations on VCS cluster nodes, and multi-cluster-mode installations on management server hosts. Such a deployment can be desirable if different IT administrators in your enterprise have different scopes of responsibility.

This user's guide describes how to use the Cluster Management Console in multi-cluster mode.

About Cluster Management Console software components

Note: This topic applies only to the Cluster Management Console configured in multi-cluster mode (configured to manage multiple clusters)

Several components comprise the Cluster Management Console. You can deploy these components in a configuration that best matches your requirements. Before using the console, you should know these fundamentals about each Cluster Management Console component:

- The component name
- The component role – the role the component plays in achieving high-availability cluster administration
- The component location – where the component resides within the Cluster Management Console framework.

Note: This guide presumes you have a thorough knowledge of managing single clusters using Veritas Cluster Server (VCS). If you are new to high-availability cluster management, Symantec recommends that you review the concepts and terminology in your existing VCS documentation before you continue.

The Cluster Management Console uses a scalable architecture consisting of the components described by the remaining sections in this topic.

Management server

The management server is the software engine that performs centralized multi-cluster management and monitoring tasks. The management server accepts and processes the operational commands and the configurational input that users enter through the Cluster Management Console. Although the Cluster Management Console and the management server are conceptually two functional components, they are inseparable. When using the Cluster Management Console to manage multiple clusters, both components are always installed together on the same physical server system.

The management server communicates with the agent manager on VCS clusters, known as the High Availability Daemon (HAD). HAD is sometimes called the *VCS engine*. The management server also communicates with a database that stores cluster configuration data, historical data gathered from cluster monitoring, and more.

One management server is capable of administering many clusters. The management server can communicate with peer management servers at other locations in a manner that enables all clusters across your enterprise to be viewed and managed from a single console. The following are the infrastructure components that support the management server:

- Database server
The Sybase ASA database Unix Daemon or NT service.
- Web server
- Authentication broker
The Cluster Management Console uses local operating system and domain user accounts; it does not require “native”, proprietary user accounts. The Cluster Management Console uses the Symantec Product Authentication Service authentication broker to securely authenticate user accounts.
- Database of configurational and historical management data.
The Cluster Management Console database is an embedded Sybase ASA database that serves as the data store for a management server. Every management server requires one database. The database includes automated maintenance such as backup, restore, and prune. Read-only access is available to external clients through ODBC and JDBC.
- Direct connection
Direct connection refers to the TCP mechanism by which the management server can connect to the VCS socket interface when no intervening firewall is present. Direct connections are made to each running VCS instance through an inbound port on the cluster.

Cluster connector

Cluster connector initiates the connection to the management server when a firewall is present between the management server and a VCS cluster. Cluster connector is an agent that is installed on the VCS cluster. Cluster connector connects to the management server through an outbound port on the cluster.

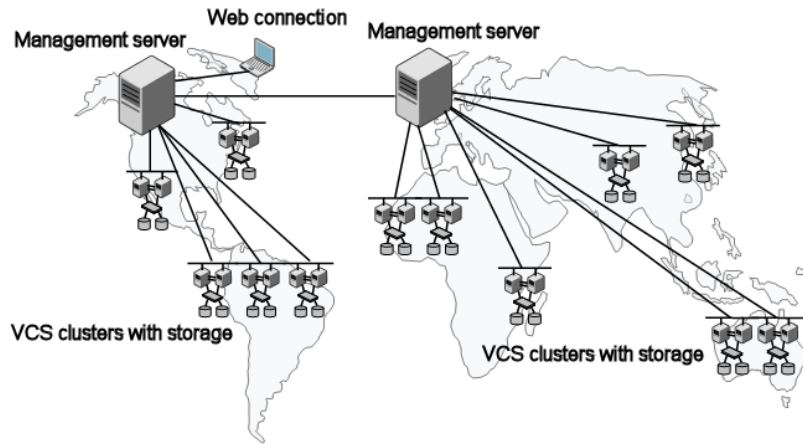
On the VCS cluster, one instance of cluster connector communicates with HAD. Like VCS, cluster connector runs on one system of the managed cluster, but is installed on each cluster node (system) and is configured for failover.

Cluster connector also provides buffering for VCS information. This feature is useful in the event that cluster connector loses the connection to the management server. When the connection is reestablished, the management server retrieves the status and event information that was generated during the disruption from the cluster connector buffer. It can then make that information available in the Cluster Management Console.

General deployment diagram

The following diagram shows two peer management servers that manage clusters on different continents. The notebook computer represents a web connection to the Cluster Management Console, which runs as part of the management server on the management server host system.

Figure 2-1 Centralized cluster management



Objects in the Cluster Management Console

In the Cluster Management Console, an object is a representation of a physical element, application data structure, or other collection of data that is related to the administration or function of a cluster. Objects can be created, manipulated, stored, and deleted. Most objects persist from one console session to the next.

The Cluster Management Console enables you to administer two types of objects: *management server objects* and *cluster objects*. Management server objects are not directly part of a cluster but support cluster operation and administration. Examples of management server objects are users, management servers, alert policies, report jobs, tags, and searches. Cluster objects are part of a cluster and participate directly in making your applications highly available. Examples of cluster objects are systems, clusters, service groups, and resources.

User accounts and user authentication

The Cluster Management Console uses operating system user accounts. The management server uses a Symantec Product Authentication Service authentication broker to authenticate users. The authentication broker requires a root broker.

An authentication broker is always installed on the management server host system. The root broker can also be installed on the management server host, or the authentication broker can be configured to use another (remote) root broker. See the *Veritas Cluster Server 5.0 Installation Guide* for more information about authentication brokers, root brokers, and security requirements.

Note: Symantec recommends that only one root broker be configured per enterprise. One or more authentication brokers can be configured to use one root broker. One authentication broker is required for each operating system in an enterprise. Configuring all authentication brokers to use one root enables authentication across all operating system platforms.

User account format

Cluster user accounts are of the form *cluster_user_name@domain*.
Management server user accounts are of the form
management_server_user_name@domain@domain_type

Supported user domain types

The user domain type is always one of:

- Windows
- UNIX NIS
- UNIX NIS+
- UNIX Password (the Unix system password)
- Veritas (VCS security services)
- Lightweight Directory Access Protocol (LDAP)
- VCS (VCS user identifiers, used to authenticate users for non-secure clusters)

Internal user accounts

The management server maintains three internal “user” accounts for secure communication among Cluster Management Console components:

- `CMC@CMC_SERVICES`
This account is required for the management server to start.
- `CMC_CC@CMC_SERVICES`
This account is required for cluster connector to connect to the management server.
- `CMC_HAD@CMC_SERVICES`
This account is required for cluster connector to connect to the VCS engine, HAD.
- `CMC_CLI@CMC_SERVICES`
This account is required for the CLI to connect to management server.

User roles

The management tasks and data that are available to a user are determined by the user’s role. You can use the Cluster Management Console to assign roles to users. Users can have more than one role, and more than one user can have the same role.

A user’s role is defined by *privileges*. Privileges specify the tasks a user can perform and the data a user can view.

A role specifies two things: a *role type* and a *privilege level*.

Privileges and privilege levels

A privilege is the authorization to:

- perform a specific task upon a managed object
- view specific data about a managed object

When a role is assigned to a user, the user assumes the privileges specified in that role; the role is also said to *grant* the privileges it specifies to a user.

The set of privileges a role specifies is called a *privilege level*. Privilege levels are predefined. The following are general definitions of the available privilege levels:

- Administrator (admin) – A role with a privilege level of administrator grants a user maximum privileges on a managed object. An administrator has full control of specific objects, including privileges to perform tasks on those objects and to change object configurations. In the Cluster Management

Console, tasks that are listed in either an Operations or a Configuration task panel are available to admins. See “[About the task pane](#)” on page 37 for information on task panels.

- **Operator** – A role with a privilege level of operator grants a user only limited privileges on a managed object. An operator can perform some tasks on specific objects, but does not have privileges to perform all tasks or to change object configurations. In the Cluster Management Console, a task must be listed in an Operations task panel to be available to operators. Even then, some tasks in an Operations task panel may still be reserved for admins. Tasks that are listed in a Configuration task panel are not available to operators.
- **Guest** – A role with a privilege level of guest grants a user read-only privilege on all objects. A guest can view managed objects, but does not have privileges to perform tasks on them or to change object configurations. In the Cluster Management Console, no tasks that are listed in either an Operations or a Configuration task panel are available to a guest. Tasks that are listed in a view Filters panel *are* available to guests.

Role type

Two types of roles exist in the Cluster Management Console: *management server roles* and *cluster roles*. These roles are distinct in many ways.

The privilege level in a management server role specifies privileges that enable a user to perform management server tasks on management server objects. A user that is assigned a management server role is called a *management server user*.

The privilege level in a cluster role specifies privileges that enable a user to perform cluster tasks on cluster objects. A user that is assigned a cluster role is called a *cluster user*.

Management server roles and cluster roles do not share privileges even though they may share a privilege level name. For example, the role of management server admin has the same privilege level as the role of cluster admin, but each role represents a different set of privileges.

A management server role can grant the privilege levels of either admin or guest. So, a management server user can assume the role of management server admin or management server guest.

A cluster role can grant the privilege levels of admin, operator, or guest. So, a cluster user can assume the role of cluster admin, cluster operator, or cluster guest. (A subgroup of cluster roles, called service group roles, can grant the privilege levels of admin and operator. So, a cluster user can also assume the role of service group admin or service group operator.)

Users with management server roles are primarily concerned with administering management servers, users, report jobs, tags, notification, and the database. Users with cluster roles are primarily concerned with administering clusters, service groups, and other cluster objects.

This guide primarily covers the tasks and data that are pertinent to management server administrators. For more information about the tasks and data pertinent to cluster administrators, see your *Veritas Cluster Server 5.0 User's Guide*.

More about management server roles and users

The following is a list of generally useful information regarding management server roles:

- When created, management server users are not associated with any cluster, but are assigned the role of cluster guest (read-only privileges) for all managed clusters.
- Management server roles include the management server guest and management server admin roles only. No management server operator role can be assigned.
- A management server admin can assign the roles of cluster admin, cluster operator, or cluster guest for a specific cluster to any management server user, including himself. A management server admin can also add users, change users' roles (including his own), and delete users (if they have no role on any cluster).
- A management server admin can configure and run reports, configure notification, administer the database, and assign roles to both management server and cluster users.

More about cluster roles and users

The following is a list of generally useful information regarding cluster roles:

- Cluster user information is *not* maintained in the management server database. Cluster user information is kept *on the cluster*, whether the cluster user was created in the Cluster Management Console or in VCS. If a user attempts to modify a cluster, role information for that user is communicated from the cluster to the management server at that time.
- For users of VCS clusters configured in secure mode:
 - These users must be explicitly added as management server users in the Cluster Management Console so that they can log in to the management server.
 - These users retain their original roles on their original clusters.

- These users are authenticated against a Symantec Product Authentication Service authentication broker.
- Users of VCS clusters not configured in secure mode cannot log in to the management server.

Role scope

Management server roles and cluster roles each have a range of influence, or *scope*. The scope of a user's role limits the objects to which a user's privileges extend.

The scope of a management server role includes the management server objects configured under one management server. The scope of a cluster role includes the cluster objects configured in one cluster.

The scopes of management server roles and cluster roles do not overlap. Users with management server roles cannot “reach beyond their scope” to include cluster objects because their roles lack cluster privileges. Likewise, users with cluster roles cannot “reach beyond their scope” to include management server objects because their roles lack management server privileges.

A fundamental premise underlies the concept of role scope: *a user does not have a role on a management server or cluster until that user is explicitly assigned a role on that management server or cluster*. For example, a management server admin on management server X is not by default a cluster admin on cluster Y, even if cluster Y is configured under X. Furthermore, a cluster admin on cluster Y is not a cluster admin on cluster Z, a peer cluster under X.

Role persistence

Roles are persistent; a role remains assigned to a user even if that user also operates in other capacities using different roles. Role persistence is a necessary result of limiting role scope to one management server or one cluster; otherwise, a user could not have privileges on more than one management server or cluster.

For example, if a cluster admin is assigned a role on a management server, he retains his administrator privileges on the cluster. More generally, all users retain their same role for any explicitly-assigned management server or cluster, even when operating in a context different from the one in which they were assigned that role. In a centralized cluster management environment, the possible contexts in which users can operate are:

- The VCS Java Console, the Cluster Management Console, or the command line interface, which are the interfaces that are local to (installed on) a cluster. In this context, users can be assigned only cluster roles.

- The Cluster Management Console or the command line interface, which are the interfaces that are local to the management server. In this context, users can be assigned management server roles or cluster roles.

Role-restricted navigation

Roles determine the objects and tasks available to a user. Some views may not be available to some users because of their role. If the privileges granted by a user's role do not apply to the objects, data, and tasks in a particular view, that view is restricted for that particular user. Users may not be able to navigate to restricted views; if they can, some or all of the task choices may not be offered.

Section



Administration,
configuration,
and management

Getting started with the Cluster Management Console

This chapter includes the following topics:

- [Verifying installation integrity and other requirements](#)
- [Connecting to the management server](#)
- [Logging in to the management server](#)
- [Overview of the Cluster Management Console](#)
- [About online help](#)

Verifying installation integrity and other requirements

Before you can use the Cluster Management Console, you must install the management server, and then either install cluster connector on the VCS clusters to be managed, or configure direct connection. Also, the local system (the system you use to run the Cluster Management Console) must be running a supported web browser (Microsoft Internet Explorer 6.0 or newer and FireFox 1.5 or newer with Macromedia Flash Plugin v8.0).

Ensure that your network and DNS configuration provide proper name resolution. Otherwise, one of the following occurs:

- If using cluster connector, cluster connector cannot resolve the management server hostname when attempting to connect to the management server. The initial handshake connection fails.
- If using direct connection with secure clusters, the management server cannot resolve cluster hostnames when attempting to connect to the clusters. The initial handshake connections to secure clusters fail.

Improperly configured network and name resolution services can create similar issues in the Cluster Management Console and other Storage Foundation and High Availability Solutions 5.0 products.

For information about browser support, how to verify console installation, and other prerequisite conditions, see your *Veritas Cluster Server 5.0 Installation Guide*.

Connecting to the management server

To use the Cluster Management Console, you must first connect to a management server and then log in. Connecting to a management server requires that you specify the management server host system in the address box of a supported web browser. In some installations, you can also connect through a desktop icon.

To connect to a management server

- ◆ In the address box of your Internet browser, enter the URL address of the management server. You can enter either:

`http://System:8181/cmc/`

or

`https://System:8443/cmc/`

Replace *System* with either the system name or the IP address of the management server host system.

On Windows platforms, you can click **Start>Programs>VERITAS Cluster Management Console** to connect.

If the connection is successful, the web browser presents the Veritas Cluster Management Console login screen.

Logging in to the management server

Logging in to a management server requires that you provide a management server user name and password, a domain, and a domain type at the Veritas Cluster Management Console login screen. The user account information that you enter must be valid for the authentication broker that validates the login. See “[User accounts and user authentication](#)” on page 23 for information on management server user accounts, authentication brokers, and other security requirements.

After logging in, the Cluster Management Console enables you to view and manage any clusters that have been configured under any management server, including clusters at locations other than your own.

Note: The operating system administrator-level user that installed the management server is the only user that can perform the first login after installation. This condition is true whether the management server is a new installation or is an upgrade from CommandCentral Availability.

After the first login, any users with the role of management server administrator can add more management server users in the Administration:Users view.

To log in to a management server

- 1 Connect to the management server
- 2 Under **Please enter a web-admin user name and password to continue**, select a language from the drop-down menu.
- 3 Enter the user name and password of the default administrator-level user account for the management server.

On Solaris, the default account is the local root account. On Windows, the default account is the account that was used to perform the management server installation.

See “[User accounts and user authentication](#)” on page 23 for information on management server user accounts, authentication brokers, and other security requirements.

- 4 Enter the domain name associated with the user account into the **Domain** box. If the user account is *not* a domain account, enter the fully-qualified system name of the management server host. (The management server host is the system running the Cluster Management Console, and is also called the local host in the login menus).
- 5 Do one of the following:
 - If you are logging in using the authentication broker on the management server host, click **Login**. This action accepts the default setting for **Domain Type** and **Authentication Broker** for the system. For Solaris, the default settings are **Automatic** for **Domain Type** and **localhost:2821** for **Authentication Broker**. For Windows, the default settings are **Automatic** for **Domain Type** and **127.0.0.1:2821** for **Authentication Broker**.
 - If you are logging in using a remote authentication broker, specify the following details for the remote authentication broker host system and then click **Login**:
 - On the **Domain Type** drop-down menu, select the domain type of the remote broker host.
 - In the **Authentication Broker** box, enter the remote host name, a : (colon), and then the port number used by the remote authentication broker.

To log in to a management server using the command line

◆ # `galogin`

The Management Servers pane of the Cluster Management Console indicates the management server to which you are connected.

Logging out of the management server

To log out of a management server

- ◆ Do one of the following
 - On the title bar of the Cluster Management Console, click **Logout**.
 - At the command prompt, type the following command:
`galogout`

Overview of the Cluster Management Console

The Cluster Management Console comprises several *views*. A view is an HTML page that displays:

- Objects and information about objects in your high availability environment
- Familiar mouse- or keyboard-accessible controls, such as buttons, menu items, check boxes, and text boxes, that enable you to issue commands or specify options
- Links to other views or task wizards

Use this material to familiarize yourself with the startup view, general view contents, view organization, and the view navigation methods used in the console.

Note: If you are a user with a guest or operator role, certain Cluster Management Console tabs and their corresponding views may not be displayed. Users with the role of management server administrator have access to all views.

Objects in the Cluster Management Console

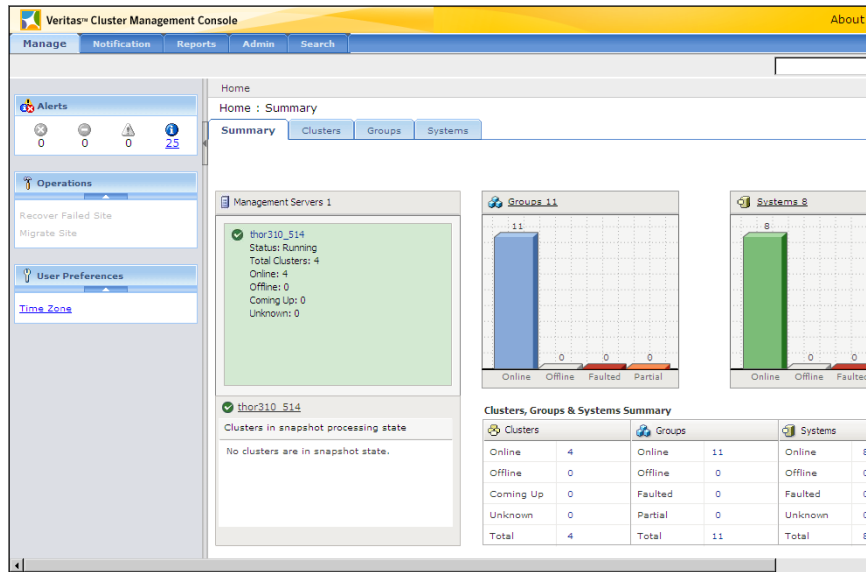
Views display objects and information about objects. In the Cluster Management Console, an object is a representation of a physical element, application data structure, or other collection of data that is related to the administration or function of a cluster. Objects can be created, manipulated, stored, and deleted. Most objects persist from one console session to the next.

The Cluster Management Console enables you to administer two types of objects: management server objects and cluster objects. Management server objects are not directly part of a cluster but support cluster operation and administration. Management server objects include management servers, users, alert policies, and report jobs. Cluster objects are part of a cluster and help make your applications highly available. Cluster objects include systems, clusters, service groups, and resources.

Cluster Management Console layout

Logging in to the management server starts the Cluster Management Console. The startup view is the Home:Summary view.

Figure 6-1 Cluster Management Console startup view



All views in the Cluster Management Console are divided into areas called bars, panes, panels, and tables.

About the title bar

The title bar contains the product name and three links: About, Logout, and Help.

Figure 6-2 Title bar



Click About to see information about the Cluster Management Console; click Logout to end a console session; click Help to access online help for using the console.

About the main tab bar

The main tab bar contains a tab, representing a set of views, for each category of operations available in the Cluster Management Console. The tabs are: Manage (management) for object configuration and manipulation; Notification for event monitoring, policies, and filters; Reports for historical data reporting; Admin (Administration) for user and management server administration, tag

definition, and cluster configuration for direct connection (without cluster connector); and Search for conducting and saving character-based or tag-based searches on management server and cluster objects.

Figure 6-3 Main tab bar



Clicking a tab takes you to the initial view for that tab. The main tab bar always contains the same tabs.

About the search bar

The search bar contains a text edit box next to a Search button:

Figure 6-4 Search bar

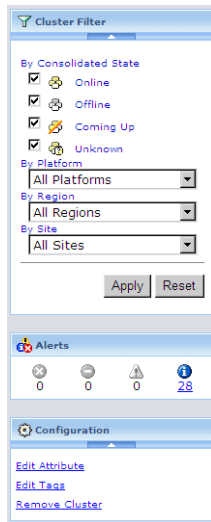


The search bar enables you to find any management server object or cluster object in the management server database.

About the task pane

The left pane of the console is the task pane. Depending on the view you select, the task pane contains one or more task panels. In the startup view, the task pane contains the Alerts and Configuration task panels. The task pane can contain as many as four task panels.

Figure 6-5 Task panels in the task pane



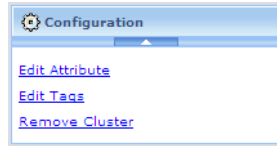
The task pane contains a narrow button on the border that separates it from the status pane on the right. This button toggles the task pane between maximum and minimum size. In the startup view, click this button to minimize the task pane. Minimizing the task pane hides the Operations and Configuration task panels and enlarges the status pane, enabling you to view information that might have been partially off the screen.

Click the narrow button again to maximize the task pane. Even with the task pane maximized, you can still display off-screen information in the status pane using the scroll bar located along the bottom border of the default view.

About task panels

The task panels in the task pane list specific operations that you can perform in each view of the Cluster Management Console. For views that list specific objects (management servers, clusters, service groups, systems, users, notification policies, reports, and so on), the task panels list all the possible tasks that you can perform on those objects. Tasks related to object management are usually divided between two task panels named Operations and Configuration.

The name of a task panel indicates the type of tasks listed in that panel. Underlined tasks indicate a link that performs an action directly or which starts a task wizard (sequence of screens that help you to perform a task).

Figure 6-6 Task panel links

For views that show details for a specific object, some tasks may not be linked (underlined). Unlinked tasks can indicate one or both of the following:

- The tasks cannot be performed on the object or objects that you are viewing
- Your current user role does not authorize you to perform those tasks.

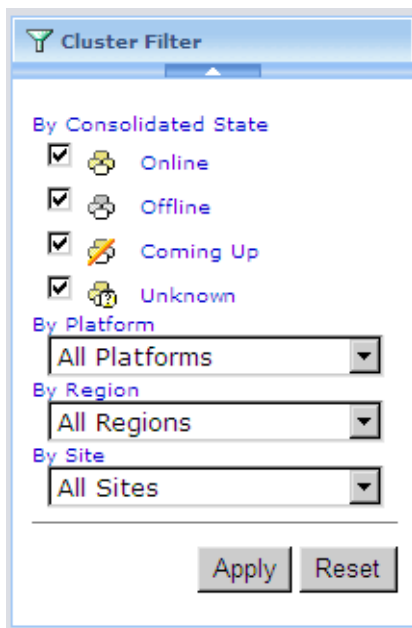
About filter panels

Many views contain a filter panel in the task pane. A filter panel enables you to view only those objects that meet the criteria you specify. You specify the filter criteria using controls such as check boxes or drop-down menus. If you want to perform a task on only certain objects, you can first filter the view for those objects and then select the task. The following are the possible filter names and settings:

- By Consolidated State – shows objects with the following values for the ConsolidatedState attribute:
 - Online - shows responsive, functioning objects
 - Offline - shows unresponsive, non-functioning objects
 - Coming up - shows objects in the process of coming online
 - Partial - shows objects (clusters or service groups) in which one or more, but not all, member objects have experienced a fault
 - Faulted - shows objects that have experienced a fault
 - Unknown - shows objects in an undetermined consolidated state
- By Platform – shows objects with the following values for the Platform attribute:
 - Solaris
 - Windows
 - Linux
 - HP
 - AIX
 - All Platforms (default)

- By Department – shows objects with the specified value for the Department attribute. This menu is populated with the currently defined values for the Department attribute and the value All Departments. All Departments is the default value.
- By Line of Business – shows objects with the specified value for the LOB attribute. This menu is populated with the currently-defined values for the LOB attribute and the value All Lines of Business. All Lines of Business is the default value.
- By Site – shows objects with the specified value for the Site attribute. This menu is populated with the currently-defined values for the Site attribute. Site has no default value.
- Global Groups – shows service groups configured using VCS GCO features.

Figure 6-7 Sample filter panel showing criteria selections

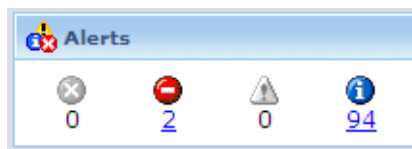


About the Alerts panel

The Alerts panel is a special panel in the task pane that provides current counts of active alerts, categorized by severity. The Alerts panel is in the task pane of every view in the Cluster Management Console.

Table 6-1 Alert severity icons

	Critical
	Error
	Warning
	Information

Figure 6-8 Alerts panel

The number below each alert indicates the current number of alerts for that particular alert severity. This number is also a navigation link to a filtered list of those alerts only. For example, to view informational alerts, click the number below the information alert icon. This link takes you to the Notifications:Logs view, which contains a table that lists the active informational alerts.

Collapsing and expanding panels in the task pane

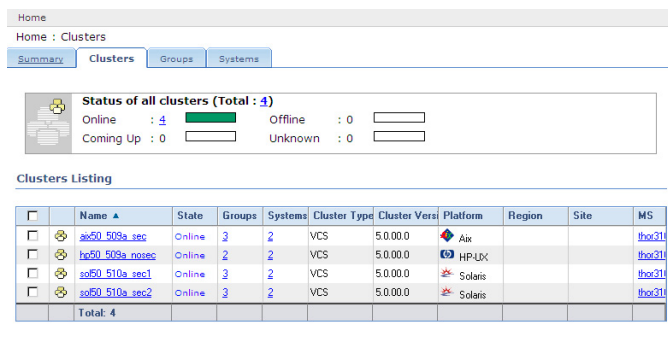
Clicking the up arrow in the center top of each task or filter panel collapses the panel to show only the heading.

When a panel is collapsed, the up arrow changes to a down arrow. When you click the down arrow, the panel expands to show the panel contents.

About the status pane

The status pane can contain many different panels and tables depending upon the view selected. These panels and tables contain status information about the management server objects or cluster objects detailed by the selected view. In the startup view, the status pane contains panels labeled Management Servers, Groups, and Systems, and a table labeled Clusters, Groups & Systems Summary.

Figure 6-9 Status pane in the startup (Home:Summary) view



Main tabs, secondary tabs, and view hierarchies

Each tab on the main tab bar represents a different category of tasks and information: management, notification, reporting, administration, and searching. Each of these tabs also marks the beginning of a multi-level navigation path, or *view hierarchy*, for that category. Each main tab “branches down” into a set of levels, and each level contains a set of views.

Under the Manage tab, the first level “down” is called *home*. The home level under the Manage tab indicates that you are viewing your enterprise-wide cluster environment at the highest level possible. From the home level, you can navigate to views that contain information about any configured management server or any cluster object.

Each level in the view hierarchy contains a set of views. You can navigate to these views using the secondary tab bar. The secondary tab bar is located along the top of the status pane and contains a row of one or more tabs. Each tab represents a view at a level in the view hierarchy.

Figure 6-10 Secondary tab bar on the Home:Summary view



On the Manage tab, the view hierarchy levels are home, management server, cluster, service group, system, resource, and resource type. Each level contains views represented by the tabs on the secondary tab bar.

Table 6-2 Levels and views in the Management view hierarchy

Level in the Management tab view hierarchy	Views available at this level (tabs on the secondary tab bar)
Home	Summary, Clusters, Groups, Systems
Management server	Summary, Clusters, Groups, Systems, Logs
Cluster	Summary, Groups, Systems, Attributes, Resources, Service Group Dependency, Resource Types, DR Alerts, Cluster Heartbeats, Users, Logs
Service group	Summary, Attributes, Resources, Logs
System	Summary, Attributes, Logs
Resource	Summary, Resource Dependency, Attributes, Logs
Resource type	Attributes

On the secondary tab bar, one tab is always active (selected); that tab represents your position at current level in the view hierarchy. For example, if you are at the startup view, Home:Summary, the Summary tab is active. According to the table, you are in the first position at the home (first, highest) level. If you are at the Cluster:Groups view, the Groups tab is active. According to the table, you are at the second position at the cluster (third) level.

As you “drill down” into lower and lower view levels (using tabs and other links), the number and variety of the objects and tasks available to you generally becomes fewer and fewer.

About the navigation bar

The navigation bar is located along the top of the status pane and indicates two things:

- Your current level in the current view hierarchy.
- The object “lineage” of the object detailed in your current view.

For example, assume that you are at the startup view, the Home:Summary view. The navigation bar shows “Home”, indicating that you are at the home level of views.

Now assume that you perform the following actions in order (If you are currently running the console, follow along.):

- Click the Clusters tab
- Click a cluster name in the table

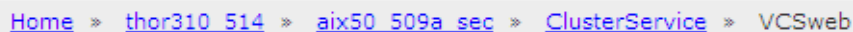
- Click the Groups tab
- Click a service group name in the table
- Click the Resources tab
- Click a resource name in the table

You arrive at a Resource:Summary view. The navigation bar shows a list of the objects that you selected to navigate to this view. The object names are shown in the following format:

Home >> Management Server >> Cluster >> Service Group >> Resource

These objects are also the parent objects of the resource you selected. The navigation trail ends with the selected resource name. This tells you that you are at the resource level of views.

Figure 6-11 Navigation bar with a resource selected.



Home > thor310_514 > aix50_509a_sec > ClusterService > VCSweb

The path on the navigation bar is also called a navigation *trail*. Object names higher up (listed nearer the beginning) of the trail are underlined, indicating that they are a navigation link to the level of views for those objects. You can move quickly up and down a view hierarchy by clicking linked object names.

About the view name

The view name appears immediately below the navigation trail. The view name is a unique name for the current view that also indicates:

- Your current level in the view hierarchy, as indicated by the navigation trail
Your “current level” is the level that the current view occupies in the view hierarchy, such as cluster, group, or resource.
- Your current position within the current level, as indicated by the secondary tab bar
Your “current position” is the position that the current view occupies within the current level. The position is the name of whichever tab is selected on the secondary tab bar, such as Summary, Attributes, or Logs.

For example:

- According to the table “[Levels and views in the Management view hierarchy](#)” on page 43, the view name Cluster:Resources indicates that this view is the fifth view at the cluster level. It contains cluster-level information about resources and enables you to view the status of resources that are members of a selected cluster.

- The view name Cluster:Summary indicates that this view is the first view at the cluster level. It contains summary information for a selected cluster and enables you to view a composite status of the cluster.
- The view name Group:Resources indicates that this view is the third view at the service group level. This view contains service-group-level information about resources and enables you to view the status of resources that are members of a selected service group.


Figure 6-12 View name example

Resource : Summary

About quick navigation links

In many views, the status pane contains linked (underlined) object names. For example, the name of the management server in the Home:Summary view links to a summary view for the clusters and systems configured under that management server. Likewise, clicking other underlined objects in the status panel takes you to summary views for those objects.

Figure 6-13 Three quick-navigation links in the status pane





A resource summary card for 'VCSweb'. It features a server icon on the left and four key-value pairs on the right: Resource Name (VCSweb), State (Online on thoribm301), Group (ClusterService), and Resource Type (VRTSWebApp). The Resource Type value is underlined and blue, indicating it is a quick navigation link.

Resource Name	: VCSweb
State	: Online on thoribm301
Group	: ClusterService
Resource Type	: VRTSWebApp

Important attributes for resource VCSweb

Attribute Name ▲	Attribute
AppName	cmc
InstallDir	/opt/VRTS
TimeForOnline	5

State information on member Systems

System Name ▲	State
 thoribm301	Online
 thoribm303	Offline

Icon conventions

The Cluster Management Console uses the following icons to represent cluster objects:

Table 6-3 Object icons

	Management server
	Cluster
	Group
	System
	Resource
	Resource type

General status indicators are applied to the basic object icons to create status icons. Status icons indicate both the type and the state of the object. The following are the status indicators:

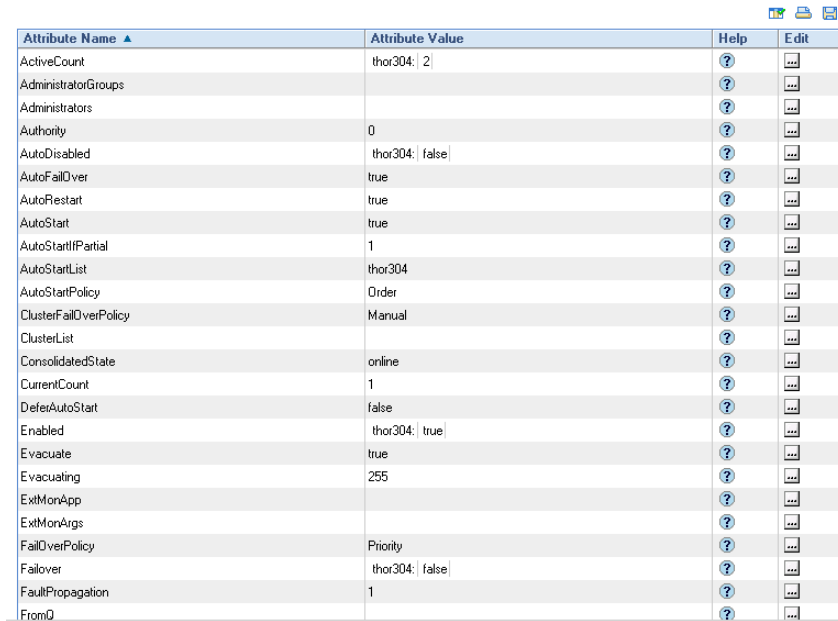
- Color icons indicate objects that are in a healthy, running condition.
- Gray icons indicate objects that are offline.
- Icons with orange lines indicate objects that are partially online with only some member (contained) objects online.
- Icons with red lines indicate faulted objects.
- Icons with a question mark indicate objects whose status is unknown.
- Icons with a red lock indicate objects in a frozen state.
- Icons with a red circle and white cross bar indicate objects in an autodisabled state.

See “[Status icon reference](#)” on page 231 for a comprehensive list of status icons.

Sorting the contents of a data table

You can sort the rows in the Cluster Management Console tables by any column that contains an up or down triangle beside the column name. [Figure 6-14](#) shows the sortable column Attributes in an attribute-value table.

Figure 6-14 Example of a sortable column in a table



Attribute Name ▲	Attribute Value	Help	Edit
ActiveCount	thor304: 2	?	...
AdministratorGroups		?	...
Administrators		?	...
Authority	0	?	...
AutoDisabled	thor304: false	?	...
AutoFailOver	true	?	...
AutoRestart	true	?	...
AutoStart	true	?	...
AutoStartIfPartial	1	?	...
AutoStartList	thor304	?	...
AutoStartPolicy	Order	?	...
ClusterFailOverPolicy	Manual	?	...
ClusterList		?	...
ConsolidatedState	online	?	...
CurrentCount	1	?	...
DeferAutoStart	false	?	...
Enabled	thor304: true	?	...
Evacuate	true	?	...
Evacuating	255	?	...
ExtMonApp		?	...
ExtMonArgs		?	...
FailOverPolicy	Priority	?	...
Failover	thor304: false	?	...
FaultPropagation	1	?	...
FromD		?	...

To sort rows in a table by data in a column

- 1 In the table, locate a sortable column you want to use to sort the data.
- 2 Click the column heading.
The list is sorted by the values in that column, in ascending order. A triangle (pointing up) displays in that column heading.
- 3 If desired, click the column heading a second time.
The list is sorted by the values in that column, in descending order. A triangle (pointing down) displays in that column heading.

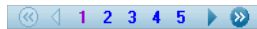
Viewing multiple pages of a data table

Tables in Cluster Management Console views may contain multiple pages. You can view subsequent pages of a table using the go-to-page bar.

To access pages in a table

- ◆ In a table with multiple pages, locate the go-to-page bar just below the table.

Figure 6-15 Go-to-page bar



Click the controls on the go-to-page bar to move forward and backward through the table pages. The following are the controls on the go-to-page bar and their meaning:

Numerals (1,2,3...)	Go to that page number
Single right arrow	Go to next page
Single left arrow	Go to previous page
Double right arrow	Go to last page
Double left arrow	Go to first page

Controlling view updates

As you use the Cluster Management Console, the status of clusters, systems, and applications changes. Devices go online and offline, alerts are generated, and data fluctuates. You can control when and how the information in your console display updates (refreshes) to reflect the latest data.

Update (refresh) mode settings and icons

An update icon near the top right-hand corner of the Cluster Management Console indicates the current update mode and the state of the information displayed in the console. Clicking the update icon enables you to set the update mode. The appearance of the update icon changes according to the following update mode settings:

- **Disabled**

Provides no indication of available updates (disables update notification). Use the refresh function in your web browser to update the console information.

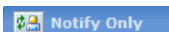
Figure 6-16 Disabled setting icon



■ **Notify Only**

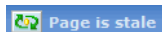
Indicates when data updates are available. This is the default setting. This icon changes to the Page is Stale icon when data updates are available.

Figure 6-17 Notify Only setting icon



For the **Notify Only** setting, when data is no longer current, the Refresh Notification icon appears. Click this icon to update the console information.

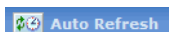
Figure 6-18 Page is Stale icon (Notify Only setting)



■ **Auto Refresh**

Automatically updates the console information when it is no longer current.

Figure 6-19 Auto Refresh setting icon



To change the refresh mode

- ◆ Click the update icon to cycle among the refresh modes. You can select any mode except **Page is Stale**.

About online help

The Cluster Management Console has a cross-platform, browser-based online help system. You can access the help system by clicking Help in the upper-right corner of the console window. You can view the Cluster Management Console online help system using a supported web browser.

Online help navigation

Navigation tools appear at the top of all Cluster Management Console help pages. Roll the mouse pointer over a tool to see the name of the tool.

- The Show Navigation tool displays the Table of Contents. This tool also displays the Show in Contents tool.
- The Show in Contents tool shows the location of the current help page in the Table of Contents.
- The Next and Previous tools (right and left arrows) enable you to navigate help topics from the current help page. These tools take you to the next or previous topic in the order that it appears in the Table of Contents.
- The Print tool enables you to print the current help topic.
- The Bookmark tool enables you to add the current help topic to your Favorite's list in your web browser.

Locating topics

Cluster Management Console online help offers several options for locating topics. When you click the Help button in the upper-right corner of the screen, the help system opens in context to the current view. Clicking the Show in Contents tool shows the Table of Contents location of the current help page. You can also access the Index and Search features to find a topic.

To use the Index feature

- ◆ In the help viewer window, click the **Index** tab.
The index opens in the task pane, enabling you to browse topics. If you select index entries with more than one reference, a list of options for that term displays. Select a reference that seems most relevant to navigate to the corresponding topic page.

To use the Search feature

- 1 In the help viewer window, click the **Search** tab.
- 2 Enter the term to be searched in the box provided. The Cluster Management Console help system displays all matches for this term.
- 3 Select an item to display the help topic for that item.

Administering users and cluster configurations

This chapter includes the following topics:

- [Summaries of management server, cluster, and related data](#)
- [Administering users and user privileges](#)
- [Administering management servers](#)
- [Administering clusters](#)
- [Administering service groups](#)
- [Administering systems](#)
- [Administering resources](#)
- [Administering resource types](#)
- [Viewing logs](#)

Summaries of management server, cluster, and related data

The startup view in the Cluster Management Console is the Home:Summary view. The Home:Summary view is one of five “home-level” views. “Home” indicates that you are at the highest, broadest, most inclusive level of views in the Cluster Management Console. You can navigate to the home-level views at any time by clicking Home in the navigation bar and then using the Summary, Clusters, Groups, Systems, or Logs tabs on the secondary tab bar.

The home-level views are named according to the tabs that navigate to them—Home:Summary, Home:Clusters, Home:Groups, Home:Systems, and Home:Logs. The first four views contain information about the state of clusters, service groups, and systems currently configured across all management servers. State information about resources and resource types is available by following links in the Home:Clusters and Home:Groups views. The fifth view, Home:Logs, lists log entries about events generated by cluster objects and management server objects across all management servers.

Note: In the Cluster Management Console, the terms “home”, “home-level”, and “all-management-servers-level” are sometimes used interchangeably.

If you click a management server name in the Management Servers panel of the Home:Summary view, you go to the management-server-level of views, which is represented by five tabs on the secondary tab bar; these tabs are named identically to those at the home level (Summary, Clusters, Groups, Systems, and Logs).

The only difference between the views at the management server level and those at the home level are the number of management servers involved. The management-server-level views display the current status information about the objects configured under (managed by) *one specific* management server. The home-level views display the same information for *all* management servers.

Summary information in the Home:Summary and Management Server:Summary views enables you to quickly see:

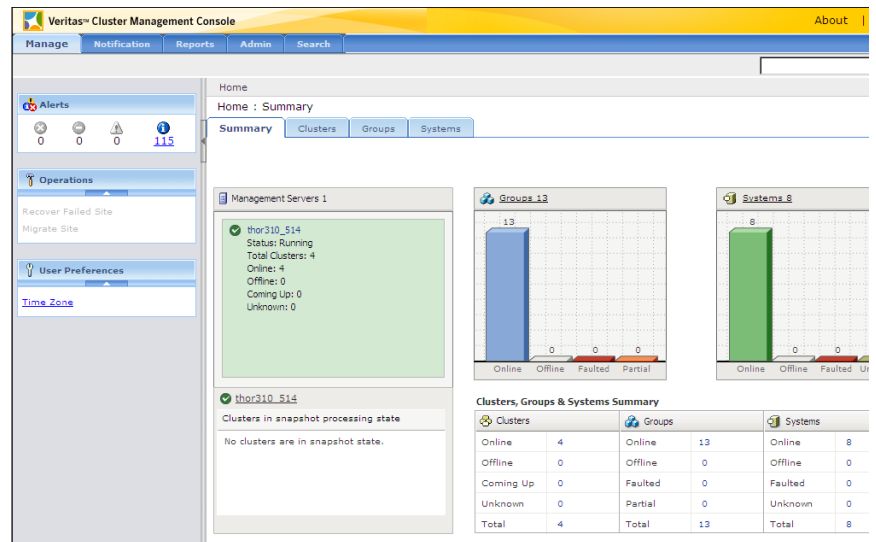
- how many clusters are in each possible cluster state (online, offline, faulted, partial, coming up),
- how many service groups are in each possible service group state (online, offline, faulted, partial, coming up)
- how many systems are in each possible system state (online, offline, faulted)
- how many service groups and systems are configured under each management server

The Home:Summary and Management Server:Summary views also provide links to other views at the same level and to summary views at lower levels.

For example,:

- In the Home:Summary view, click the linked title of the Groups or Systems panel to go to the Home:Groups view or the Home:Systems view. These views contain information about service groups or systems configured under all management servers.
- In the Management Server:Summary view, click the Groups or Systems links to go to the Management Server:Groups and the Management Server:Systems views. These views contain information about service groups and systems configured under a specific management server.
- In the Home:Summary view, click the linked numbers in the Clusters, Groups, and Systems Summary table to go to the summary views for those cluster objects.

Figure 7-1 Home:Summary view



About summary views

Every level of views in the Cluster Management Console, except for the resource type level, has a summary view. This section explains the contents of the six Cluster Management Console summary views— Home:Summary, Management

Server:Summary, Cluster:Summary, Group:Summary, System:Summary, and Resource:Summary.

Home:Summary view

The Home:Summary view is the first view at the home (all management servers) level and contains the following panels and tables:

- Management Servers panel
Contains the linked name of each configured management server. Any management servers in a faulted state are not listed. A status icon to the left of the management server name indicates the current health of the management server system.
See “[Icon conventions](#)” on page 47 for information on status icons.
- Groups panel
Contains a bar graph and numeric totals that indicate service groups in each available state: online, offline, faulted and partial. The table title is followed by a total indicating the total number of service groups across all all management servers. Click the table title “Groups” to navigate to the Home:Groups view.
- Systems panel
Contains a bar graph and numeric totals that indicate systems in each available state: RUNNING, OFFLINE, FAULTED, and UNKNOWN. The table title is followed by a numeric total indicating the total number of systems configured under all management servers. Click the table title “Systems” to navigate to the Home:Systems view.
- Clusters, Groups, and Systems Summary table
Contains the information shown in “[Data descriptions in the Clusters, Groups, and Systems Summary table](#)” on page 57.

Table 7-1 Data descriptions in the Clusters, Groups, and Systems Summary table

Clusters		Groups		Systems	
Running	Number of clusters running and functional	Faulted	Number of service groups reporting a fault event	Running	Number of systems running and functional
Exited	Number of clusters in an exited state	Partial	Number of service groups in a partially up state	Offline	Number of offline, non-operational systems
Faulting	Number of clusters currently faulting	Online	Number of online, operational service groups	Faulted	Number of systems reporting a fault event
Initing	Number of clusters being brought online	Offline	Number of offline, non-operational service groups		
Total	Total of all clusters	Total	Total of all service groups	Total	Total of all systems

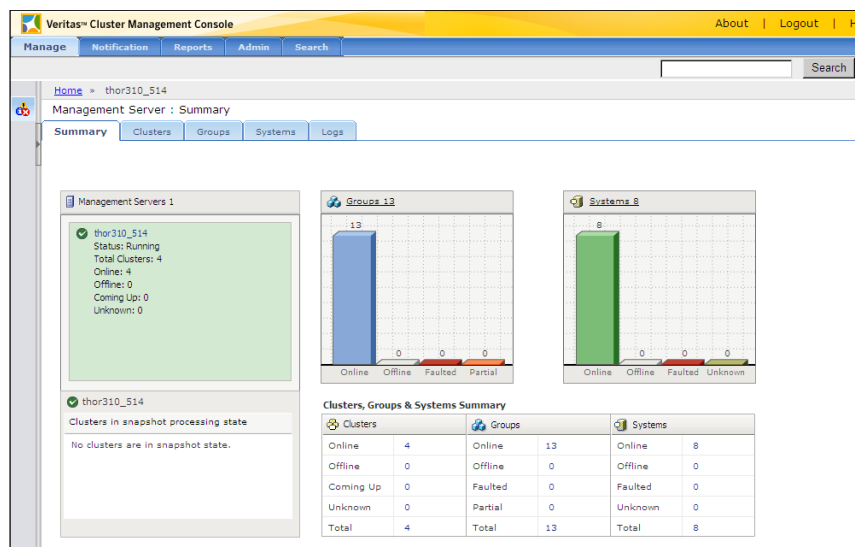
Management Server:Summary view

The Management Server:Summary view is the first view at the management server level. It is almost identical to the Home:Summary view. Both views have panels and tables that behave identically and which present similar data in identical formats. The only difference between these two summary views is how each view calculates numeric totals:

- For the Home:Summary view, all numeric totals represent objects “across all management servers.”
- For the Management Server:Summary view, all numeric totals represent objects “configured under one management server.”

See “[Home:Summary view](#)” on page 56.

Figure 7-2 Management Server:Summary view



Cluster:Summary view

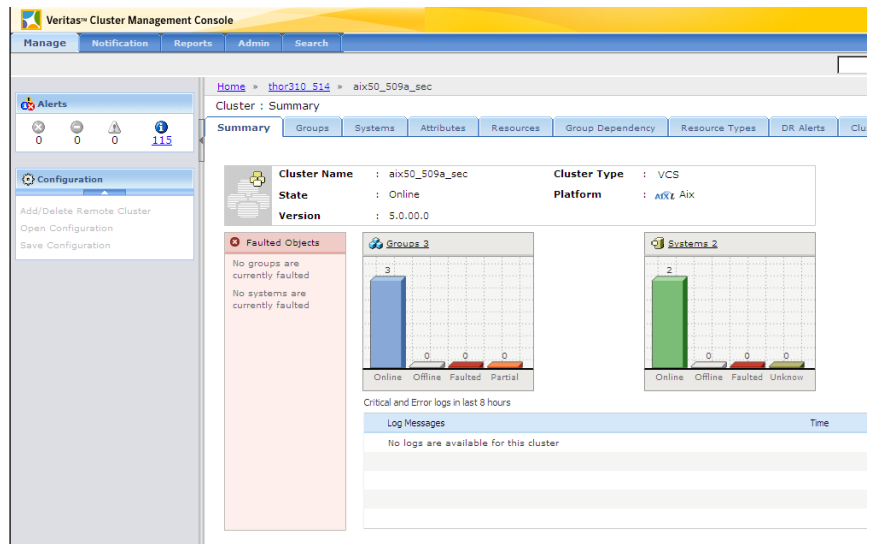
The Cluster:Summary view is the first view at the cluster level and contains the following panels and tables:

- **Faulted Objects panel**
Contains the linked name of each group or system configured in the currently selected cluster and which are in a faulted state; can also contain a message stating that no service groups or systems are faulted.
- **Groups panel**
Contains a bar graph and numeric totals that indicate service groups in each available state: online, offline, faulted and partial. The table title is followed by a total indicating the total number of service groups configured under all management servers. Click the table title “Groups” to navigate to the Cluster:Groups view.
- **Systems panel**
Contains a bar graph and numeric totals that indicate systems in each available state: running, offline, and faulted. The table title is followed by a numeric total indicating the total number of systems configured under all

management servers. Click the table title “Systems” to navigate to the Cluster:Systems view.

- Remote Clusters Status table (applies to global clusters only)
 Contains the cluster name, IP address, state, and heartbeat state of the global cluster configured as the remote cluster for the selected cluster. VCS global clusters are cluster configurations that enable wide-area failover and disaster recovery. See your *Veritas Cluster Server 5.0 User’s Guide* for more information on global clusters.
- Critical logs in last 8 hours table
 Lists messages from events that have occurred in the last eight hours and that generated an alert with a severity of “critical”.

Figure 7-3 Cluster:Summary view



Group:Summary view

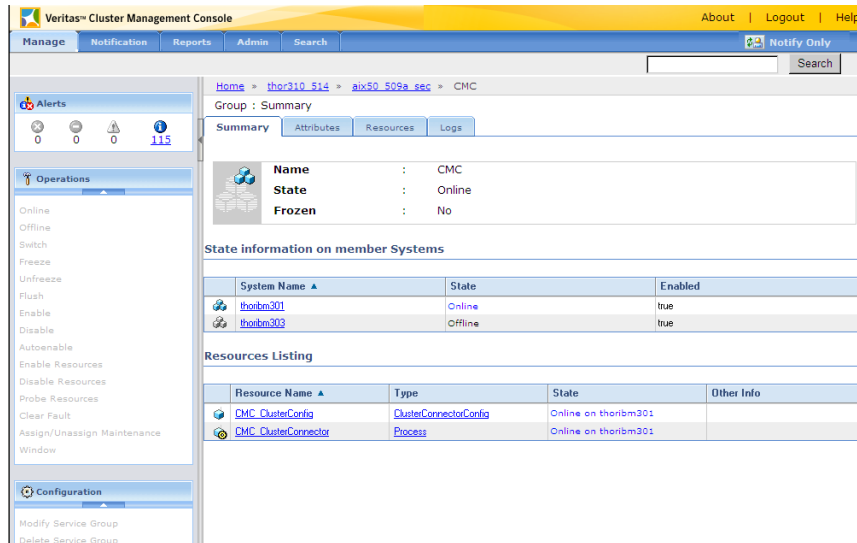
The Group:Summary view is the first view at the service group level and contains the following panels and tables:

- Name-State-Frozen table
 Indicates the name and current state of the selected service group, and whether or not the service group is frozen.
- Status information on member Systems table

Lists the system name, state, and enabled status (true or false) for all systems in the parent cluster that currently host the selected service group. Click a system name to navigate to the System:Summary view.

- **Service groups linked to this Group table**
 Lists service groups which share a dependency with the selected service group.
- **Resources Listing table**
 Lists the resource name, type, and state of all resources that are members of the selected service group. Click a resource name to navigate to the Resource:Summary view; click a resource type name to navigate to the Resource Type:Attributes view.
- **Group status on remote Clusters table (applies to global clusters only)**
 Indicates the status of any remote service groups configured for the selected global service group.
 VCS global clusters are cluster configurations that enable wide-area failover and disaster recovery. See your *Veritas Cluster Server 5.0 User's Guide* for more information on global clusters.
- **Replication Status for Resource table (applies to global clusters only)**
 Indicates the current state of replication of the selected global service group on any remote clusters (failover targets) configured for it.

Figure 7-4 Group:Summary view

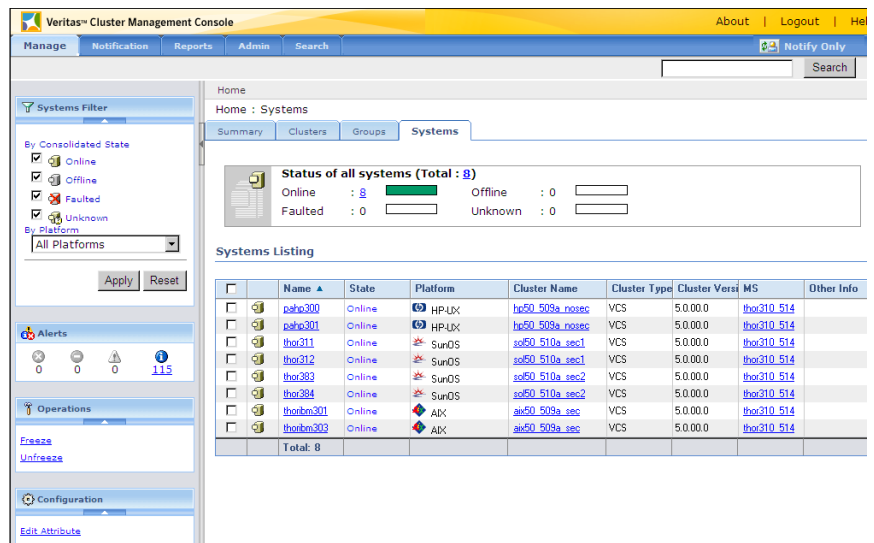


System:Summary view

The System:Summary view is the first view at the system level and contains the following panels and tables:

- **Name-Status-OS table**
 Indicates the name, current state, and operating system of the selected system.
- **Details of Groups configured on this System table**
 Lists the service group name and current state for all service groups configured on the selected system. Click a service group name to navigate to the Group:Summary view.

Figure 7-5 System:Summary view



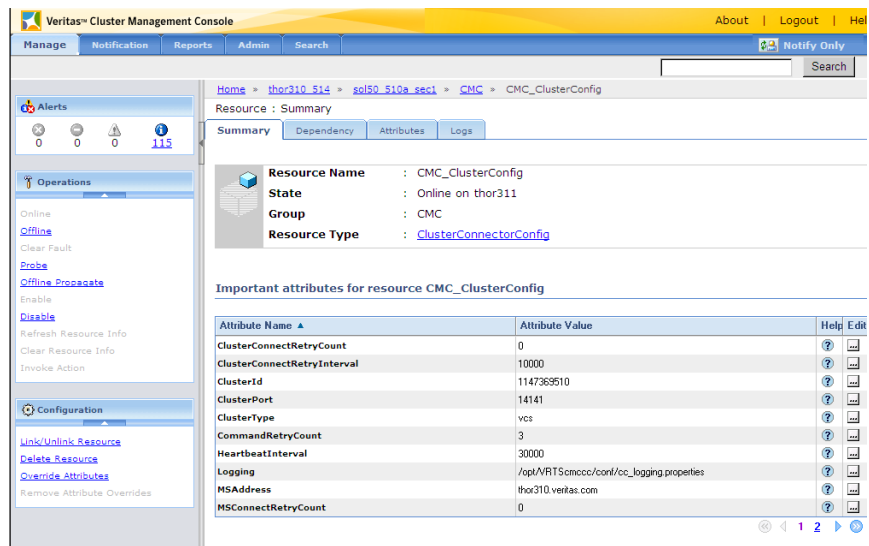
Resource:Summary view

The Resource:Summary view is the first view at the resource level and contains the following panels and tables:

- **Name-Status-Group-Type table**
 Indicates the name, current state, parent or containing group (group of which the resource is a member), and the resource type of the selected resource. Click the Resources Type link to navigate to the Resource Type:Attributes view.

- **Important attributes for Resource table**
 Lists the name and the value of attributes applied to the selected resource. Click the ... (edit) button to launch the Edit Attribute wizard and modify attribute parameters.
- **Status information on member Systems table**
 Lists the name and current state of systems that host the selected resource. Click a system name to navigate to the System:Summary view.
- **Parent Resources of this Resource**
 Lists the name, resource type, and current state for any parent (containing) resources of the selected resource. Click a resource name to navigate to the Resource:Summary view for a parent resource. Click a resource type name to navigate to the Resource Type:Summary view for the parent resource.
- **Child Resources of this Resource**
 Lists the name, resource type, and current state for any child resources of the selected resource. Click a resource name to navigate to the Resource:Summary view for a child resource. Click a resource type name to navigate to the Resource Type:Summary view for the child resource.

Figure 7-6 Resource:Summary view

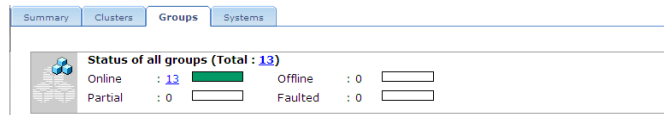


Summary information in state-wise distribution tables

State-wise distribution tables contain summary information about cluster objects, but they are not available on a summary view. Rather, they usually appear on one or more views available through the other tabs (other than Summary) on the secondary tab bar, which typically contain information about objects that are children of (contained by, members of) the object detailed in the Summary tab.

For example, at the cluster level of views, the secondary tab bar contains a Groups tab, which takes you to the Cluster:Groups view. This view contains the Status of all Groups table, which displays information about service groups that are members of the cluster detailed on the Summary tab.

Figure 7-7 A state-wise distribution table for service groups in a cluster



Each numeric total is labelled with one of four possible consolidated states for an object. Each numeric total is also a linked “hotspot” that filters the table to show only the objects in that state. Click TOTAL to filter the table to show the totals of all objects in all consolidated states.

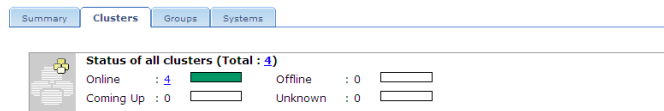
All state-wise distribution tables behave identically, and the information they report is similar.

To quickly see a state-wise distribution table

- ◆ On the navigation bar, click **Home** and then click **Clusters**.

This action takes you to the **Home:Clusters** view. The **Status of all clusters** table appears at the top of the view.

Figure 7-8 A state-wise distribution table for clusters



The table shows a numeric total (TOTAL) of all clusters that are configured under this management server. It also shows a numeric total of clusters in each of four consolidated states. Click TOTAL to filter the table to show the number of

clusters in all states. Click a linked numeric total next to a consolidated state name to filter the table to show the number of clusters in a single state.

Administering users and user privileges

The Cluster Management Console uses existing operating system user accounts. It is not necessary to create a new, separate set of accounts for the Cluster Management Console. The operating system user accounts must be valid on the system where the management server is installed.

Note: The user account that is active at the time the Cluster Management Console management server is installed is automatically assigned the role of management server administrator.

When the management server is installed on a Windows system, software that enables you to use the operating system accounts that exist on the local server is automatically loaded. If the management server is installed on a system that is a member of an NT or ActiveDirectory domain, domain accounts on any NT or ActiveDirectory domain that the system recognizes may also be used.

When the management server is installed on a Solaris system, software that enables you to use the operating system accounts that exist on the local server is automatically loaded. If the system where the management server is installed is a member of an NIS or NIS+ domain, domain accounts on that domain can also be used.

The Administration:Management Server Users view contains a list of management server users. This is a home-level view of all management server users configured across all management servers.

The Cluster:Users view contains a list of cluster users. This is a cluster-level view of the users configured on one specific cluster.

The Management Server:Clusters view contains a list of all clusters configured under one management server. This view enables you to:

- Add a new cluster user to many clusters
- Add an existing management server user to a cluster

The Management Server:Groups view contains a list of all service groups configured under one management server. This view enables you to add existing management server and cluster users to a service group

To navigate to the list of users in the Administration:Management Server Users view

- 1 On the navigation bar, click **Home**.
- 2 On the main tab bar, click **Admin**.
- 3 On the secondary tab bar, click **Users**.

In the **Administration:Management Server Users** view, the **Management Server Users Listing** table lists all management server users across all management servers.

To navigate to the list of users in the Cluster:Users view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Clusters**.
- 3 In the **Home:Clusters** view, in the **Clusters Listing** table, click the linked name of a cluster.
- 4 In the **Cluster:Summary** view, on the secondary tab bar, click **Users**.
In the **Cluster:Users** view, the **Users** table lists the cluster users configured for the selected cluster.

To navigate to the list of clusters in the Management Server:Clusters view

- 1 On the navigation bar, click **Home**.
- 2 In the **Home:Summary** view, in the **Management Servers** panel, click the linked name of a management server.
- 3 In the **Management Server:Summary** view, on the secondary tab bar, click **Clusters**.
In the **Management Server:Clusters** view, the **Clusters Listing** table lists the clusters configured under the selected management server.

To navigate to the list of service groups in the Management Server:Groups view

- 1 On the navigation bar, click **Home**.
- 2 In the **Home:Summary** view, in the **Management Servers** panel, click the linked name of a management server.
- 3 In the **Management Server:Summary** view, on the secondary tab bar, click **Groups**.
In the **Management Server:Groups** view, the **Groups Listing** table lists the service groups configured under the selected management server.

About user listing tables

The following is a list of the columns and data in tables that list user information.

- Name - the user name string
- Domain name - the domain to which the user belongs

- Domain type - the type of domain to which the user belongs
- Management Server Roles - the roles the user has on the management server and for management server objects. Assigned using the Set MS User Roles dialog box.
See “[Adding and deleting a management server user](#)” on page 68.
- Privileges - the roles assigned to a cluster user
- Assign Privileges - a button that takes you to the role assignment part of the Add User wizard.
See “[Adding and deleting a cluster user](#)” on page 69.
- Delete - a button that prompts you to delete a cluster user
- Report Privileges - Whether or not a management server user has privileges to view and create report jobs and report outputs.
- Date Created - user creation date
- Date Modified - most recent date that user information was changed

Sorting the list

You can sort a user listing table according to your needs:

To sort users

- 1 In the either the **Administration:Management Server Users** view or the **Cluster:Users** view, in the **Users** table, locate the column by which you want to sort the list.
- 2 Click the column heading.
The list is sorted by the values in the selected column in ascending order. A triangle (pointing up) displays in that column heading. Click the column heading again to reverse the sort; this action also reverses the triangle.

Command line tips

You can view cluster information using the command line.

To view a list of users at the home level using the command line

◆ # gauser -list

To view users at the cluster level using the command line

◆ # gauser -display *cluster-name*

Adding and deleting a management server user

A management server user is a user that has been assigned a role on a specific management server. Management server users must be assigned a role on each management server that they are intended to administer.

To add a management server user

- 1 In the **Administration:Management Server Users** view, in the **Configuration** task panel, click **Add a user**.
- 2 In the **Add a user** dialog box, specify the following user details and then click **OK**:
 - The user name
In the **User Name** text box, enter the name for the user account that you want to add to the management server.
 - The name of the operating system domain in which the user name is valid.
In the **Domain Name** text box, enter the name of the domain to which the user account belongs. (The domain name is either be the name of an operating system domain or the name of the local system where the management server is installed.)
 - The domain type
In the **Domain Type** drop-down list box, select the type of operating system domain for the specified domain name. Valid domain types are Windows, UNIX NIS, UNIX NIS+, UNIX Password (the Unix system password), Veritas (VCS security services), Lightweight Directory Access Protocol (LDAP), VCS (VCS user identifiers for clusters not configured in secure mode)

Note: This procedure does not validate the user account. The account is assumed to exist either on the specified domain or on the local system where the management server is installed.

To delete a management server user

- 1 In the **Administration:Management Server Users** view, in the **Management server users listing** table, select the users you want to delete by checking the check box preceding the line item for each user. Select *all* users by checking the check box at the top.
- 2 On the **Configuration** task panel, click **Delete selected users**.
- 3 In **The following users will be deleted** dialog box, click **OK** to confirm that you want to delete the selected users.

To add a management server user using the command line

```
◆ # gauser -add name domain domainType
```

Note: The actual user account remains at the operating system level.

To delete a management server user using the command line

```
◆ # gauser -delete name domain domainType
```

Adding and deleting a cluster user

A cluster user is a user that has been assigned a role on a specific cluster. Cluster users must have a role assigned on each cluster that they are intended to manage.

To add a cluster user to a single cluster

- 1 In the **Cluster:Users** view, in the **Configuration** task panel, click **Add a user**.
- 2 In the **New User** wizard, specify the following new user details and then click **Next**:
 - The new user name.
 - If the target cluster is not configured in secure mode, you must also specify a password for the new user and confirm it.
- 3 In the **Assign Privileges** dialog box, specify the following options and then click **OK**:
 - The role
The available roles for a cluster user are **Cluster Administrator**, **Cluster Operator**, **Group Administrator**, or **Group Operator**. You can select more than one, but be aware that some option combinations are redundant.
See “[User roles](#)” on page 24.
 - The objects to which the role grants authority
To begin this procedure, you selected a single cluster from a **Clusters Listing** table. If you select a role of **Cluster Administrator** or **Cluster Operator**, you have already specified the object to which the user’s role applies. You are not required to specify anything more, so the service group selection boxes are unavailable.
If you select **Group Administrator** or **Group Operator**, you must select at least one service group. To select a service group, click a service group name under **Available Groups** and then click the right-arrow

button. To reject a service group, click a name under **Selected Groups** and then click the left-arrow button to return it to **Available Groups**.

Note: This procedure does not validate the user account. For a cluster that is configured in secure mode, the account is assumed to exist on the domain. For a cluster that is not configured in secure mode, the account is assumed to exist on the cluster.

To add a cluster user to multiple clusters

- 1 In the **Management Server:Clusters** view, in the **Clusters Listing** table, select the clusters to which you want to add a user. Check the check box preceding the line item for each cluster, or select *all* clusters by checking the check box at the top.
You can select clusters that are configured in secure mode and clusters that are not. (Secure mode means that a cluster is configured to use an authentication broker instead of a local configuration file to authenticate users.) If your selection does include both types of clusters, parts of the wizard repeat so that you can add users to clusters of each type.
- 2 In the **Configuration** task panel, click **Add User**.
- 3 In the **Add User to VxSS enabled clusters** wizard (for secure clusters) or the **Add User to Non-VxSS enabled clusters** wizard, specify the following user details and then click **Next**:
 - The user name.
 - If the target clusters are not configured in secure mode, you must also specify a password for the user and confirm it.
 - Domain (optional)
 - Domain Type (optional)
- 4 In the subsequent dialog box, click **Next** to confirm that you want to add the user to the listed clusters.
- 5 In the **Select Privilege** dialog box, specify the cluster role that you want to assign and then click **Finish**.
Two of the possible roles for a cluster user are available, **Cluster Administrator** and **Cluster Operator**.
See “[User roles](#)” on page 24.
- 6 In the **Results** dialog box, review the user addition information and then click **Close**.

Note: This procedure does not validate the user account. For a cluster that is configured in secure mode, the account is assumed to exist on the domain. For a cluster that is not configured in secure mode, the account is assumed to exist on the cluster.

To delete a cluster user

- 1 In the **Cluster:Users** view, in the **Delete** column of the **Users** table, click the **X** button at the end of the line item corresponding to the user that you want to delete.
- 2 In the **Delete User** dialog box, click **OK** to confirm that you want to delete the selected user.

Adding management server users to clusters

This task enables you to:

- Add one or more existing management server users to one or more clusters.
- Add one or more existing cluster users to one or more additional clusters

You may select a combination of management server users and cluster users for this task.

To add management server users to clusters

- 1 In the **Management Server:Clusters** view, in the **Configuration** task panel, click **Assign User Privileges**.
- 2 In **Management Server Users** dialog box, select one or more management server users that you want to add to one or more clusters and then click **Next**.
- 3 In the **Select Privilege** dialog box, specify the cluster role that you want to assign and then click **Finish**.
Two of the possible roles for a cluster user are available, **Cluster Administrator** and **Cluster Operator**.
See “[User roles](#)” on page 24.
- 4 In the **Results** dialog box, review the user addition information and then click **Close**.

Note: This procedure does not validate the user account. For a cluster that is configured in secure mode, the account is assumed to exist on the domain. For a cluster that is not configured in secure mode, the account is assumed to exist on the cluster.

Adding management server users and cluster users to service groups

This task is almost identical to the Assign User Privileges task for clusters. The differences are:

- You select service groups from the table instead of clusters
- An additional step enables you to specify cluster users.

This task is available in the Management Server:Groups view.

To navigate to the Assign User Privileges task for service groups

- 1 On the navigation bar, click **Home**.
- 2 In the **Home:Summary** view, in the **Management Servers** panel, click the linked name of a management server.
- 3 In the **Management Server:Summary** view, on the secondary tab bar, click **Groups**.
In the **Management Server:Groups** view, in the **Configuration** task panel, click **Assign User Privileges**.

See “[Adding management server users to clusters](#)” on page 71.

Granting and revoking the reporting privileges

Reporting privileges are exclusive to a management server user. Reporting privileges include creating, deleting, and editing report jobs, running existing report jobs, and viewing existing report outputs.

Reporting privileges are automatically granted to a management server admin. They may also be explicitly granted to a management server guest. By default, management server users are created in the role of guest, with no reporting privileges.

Note: Reporting privileges cannot be revoked from a management server administrator.

To grant or revoke reporting privileges

- 1 In the **Administration:Management Server Users** view, check the check box preceding the line item for the user to whom you want to grant reporting privileges. Select all users by checking the check box at the top.
- 2 In the **Configuration** task panel, click **Set Reporting Privileges**.
- 3 In the **Grant/revoke the reporting privileges to/from the users** dialog box, in the **Reporting Privileges** column of the table, check a check box to grant privileges to the corresponding user. Clear a check box to revoke privileges from the corresponding user. The check box for a management server administrator who has previously been granted reporting privileges is checked, grayed-out, and unavailable.
- 4 Click **OK**.

Administering management servers

The Home:Summary and the Management Server:Summary views enable you to perform tasks on management servers. Bringing sites online, taking sites offline, and migrating sites are important operations in disaster recovery.

The Management Servers panel appears in both the Home:Summary and Management Server:Summary views. In Home:Summary, it contains information about all management servers configured throughout your enterprise. In Management Server:Summary, it contains information about just one configured management server.

To navigate to the Home:Summary view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Summary**.

To navigate to the Management Server:Summary view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Summary**.
- 3 In the **Home:Summary** view, in the **Management Servers** panel, click a linked management server name.

VCS global clusters

Some of the tasks at the management server level involve disaster recovery. VCS disaster recovery makes use of objects called *global clusters* and *global service groups*. Global clusters and global service groups have corresponding *remote clusters* and *remote service groups*.

A global cluster is a cluster that contains at least one global service group. A global service group is a service group that has been replicated and configured on one or more remote clusters. A remote cluster is a cluster that is specifically configured as a failover target for a global service group. A remote cluster contains a remote service group, which is the replicated global service group.

The global service group fails over to the preconfigured remote cluster if failover within the local cluster is not possible. See “Connecting clusters—creating global clusters” in your *Veritas Cluster Server 5.0 User’s Guide* for information about creating, configuring, and maintaining global clusters and service groups.

Note: Remote clusters are usually configured at a physically separate location that is a significant distance away from the global clusters. Once configured, the designation of “global” and “remote” depends on perspective. In the disaster recovery tasks available in the Cluster Management Console, “global” indicates the local clusters and service groups, and “remote” indicates the preconfigured failover targets. The local and global cluster and service group setup is called a *global cluster configuration* or *global cluster environment*.

Migrating a site (local site disaster recovery)

Use the Migrate Site task to bring global service groups in one site online on the preconfigured failover target clusters at another site. You must select which site is the source site. The Migrate Site task is an extension of the global cluster operations features in VCS 5.0, and is part of the Cluster Management Console disaster recovery (DR) solution.

Note: Although this task is designed to enable local site disaster recovery, you can also use it to migrate healthy, online service groups.

When to use site migration for DR

Use the Migrate Site task for DR when the following conditions apply:

- A site containing global clusters is faulting.
- The service groups in those clusters cannot be failed over normally within the local site (because of widespread faulting or inadequate resources).
- The faulting clusters are still communicating.

Under these conditions, you can attempt to fail the local service groups over to preconfigured remote clusters. Only those service groups that are ONLINE, FAULTED, or PARTIAL. PARTIAL indicates that a service group is online on at least one system and is FAULTED on none. The service group attribute ClusterList lists, in order of preference, the remote clusters that can bring a global service group online.

The Migrate Site task is most effectively used when global clusters in a site experience serious problems, but are still communicating. This is the best point at which to move critical service groups to the target failover clusters designated for them.

The site tag

To identify a “site” for use in the Migrate Failed Site task, the Cluster Management Console offers the user-definable tag Site. This tag is merely a label and can be applied arbitrarily. However, it is recommended that, for the purpose of disaster recovery, it be applied to indicate geographic location.

The Site tag identifies only those clusters that contain global service groups available for failover. The Site tag alone has no role in determining the target (remote) clusters. The remote clusters available for each global service group are determined by the overall configuration of the global cluster environment.

See “[VCS global clusters](#)” on page 74.

Migrating the site

The Migrate Failed Site feature enables you to select global service groups that are: (1) in the selected site, and (2) online or faulted on a global cluster.

Note: You must define one or more values for the Site tag, and then assign a Site tag value to the appropriate clusters before attempting to use the Migrate Site wizard.

See “[Managing tags](#)” on page 78 for information on defining tag values.

See “[Modifying tags of selected clusters](#)” on page 86 for information on assigning tags.

To migrate a site

- 1 In the **Home:Summary** or **Management Server:Summary** view, in the **Operations** task panel, click **Migrate site**.
- 2 In the **Migrate Site Wizard** dialog box, click **Next**.
- 3 In the **Site Selection** dialog box, select the site you want to migrate from the **Site** drop-down menu and then click **Next**.
- 4 In the **Global Application Group Selection** dialog box, select the service groups you want to failover to a remote cluster and then click **Next**.
- 5 In the **Completion of Migrate Site Wizard** dialog box, review the information and then click **Finish** to fail over the selected groups.

Recovering a failed site (remote site disaster recovery)

You can use the Recover Failed Site task to bring failed service groups at a remote site online at the local site.

The Recover Failed Site feature is an extension of the global cluster operations features in VCS 5.0, and is part of the Cluster Management Console disaster recovery (DR) solution.

See “[VCS global clusters](#)” on page 74.

When to use failed site recovery

Use failed site recovery only when the following conditions apply:

- A remote site containing global clusters fails unexpectedly
- Communications with the remote site have been lost

Under these conditions, you can attempt to bring the failed remote service groups online on preconfigured global (local) clusters. The service group attribute ClusterList lists, in order of preference, the local clusters that can bring a failed remote service group online.

Recover Failed Site should be used only when remote clusters at another site experience total sudden failure and are no longer communicating. “Sudden failure” is defined as a failure that occurs faster than normal failover can occur within the remote site, indicating a possible site-wide disaster. In this case, the clusters at the remote site still show an authority value of “1”. This is the last transmitted status, indicating that the remote clusters did not relinquish authority; normal failover did not have a chance to begin.

Recovering the site

The Recover Failed Site feature enables you to select global service groups that: (1) are in the selected site, (2) were last online on a remote global cluster that still has the authority but is now failed, and (3) are offline on the local global cluster.

Note: You must define one or more values for the Site tag, and then assign a Site tag value to the appropriate clusters before attempting to use the Migrate Site wizard.

See “[Managing tags](#)” on page 78 for information on defining tag values.

See “[Modifying tags of selected clusters](#)” on page 86 for information on assigning tags.

To recover a failed site

- 1 In either the or **Home:Summary** or **Management Server:Summary** view, in the **Operations** task panel, click **Online site**.
- 2 In the **Online Site Wizard** dialog box, click **Next**.

- 3 In the **Site Selection** dialog box, select the site you want to online from the **Site** drop-down menu and click **Next**.
- 4 In the **Global Application Group Selection** dialog box, select the service groups you want to online at the selected site and then click **Next**.
- 5 In the **Completion of Online Site Wizard** dialog box, review the information and then click **Finish** to bring the selected service groups online.

Managing tags

Tags are user-defined labels that you can apply to clusters and service groups. Tags are a convenient way to identify these objects easily for filtering, searching, and batch operations.

While the values of tags are user-definable, the types of tags are predefined. The following are the available tag types:

- Cluster Regions
- Cluster Sites
- Group Departments
- Group Lines of Business

In the Cluster Management Console, tag names are usually truncated to Region, Site, Department, and LOB.

Tags have a scope of one management server. When you create a tag, you can apply it to clusters and service groups configured under the current management server.

Use the Administration:Tags view to manage tags. To apply tags to objects, navigate to a view that contains a list of the desired objects and then click the Edit Tags task on the Configuration task panel.

To create or modify a tag

- 1 On the main tab bar, click **Administration**.
- 2 On the secondary tab bar, click **Tags**.
- 3 In the Administration:Tags view, in the **Configuration** task panel, click one of the following:
 - **Edit Cluster Regions**
 - **Edit Cluster Sites**
 - **Edit Group Departments**
 - **Edit Group Lines of Business**

- 4 In the **Update Tag** dialog box, to create a new value, enter a value and then click **Add**. To delete a value, check a checkbox beside one or more values and then click **Remove**.
- 5 When finished editing tag values, click **OK**.

Creating and deleting maintenance windows

Creating a maintenance window enables you to designate an interval of planned downtime. The downtime interval is not applied to uptime calculations in reports. Maintenance windows are assigned in the Administration:Management Server view.

To create a maintenance window

- 1 On the main tab bar, click **Admin**.
- 2 On the secondary tab bar, click **Management Server**.
- 3 In the **Administration:Management Server** view, in the **Configuration** task panel, click **Create a maintenance window**.
- 4 In the **Create Maintenance Window** wizard, click **Next**.
- 5 Specify the desired start date, time, and interval duration using the appropriate controls.
To choose a start date from a calendar, click the calendar icon to the right of the **Effective date:** text box.
- 6 Check a check box for each type of recurrence you want to set:
 - **Day interval** - specify a number of days between each maintenance window occurrence.
 - **Week days of the month** - specify the days of the month by order and name, such as every first Tuesday or every 3rd Friday.
 - **Days of the month** - specify the days of the month by date, such as the first and 15th of every month.
 - **Specific dates** - specify dates by entering month, day, and year.
 - **Excluded dates** - specify dates by entering month, day, and year.
- 7 Click **Next**.
The wizard then cycles through a screen for each type of recurrence you checked. Each screen contains instructions at the top.
Any time you see a calendar icon to the right of a text box, you can click it to choose a date instead of typing one. Click **Next** after specifying all the options in each recurrence screen.

- 8 When you reach the **Name and Description** screen, enter a name and optional description for the maintenance window and then click **Next**.
- 9 In the **Completion of Create Maintenance Window Wizard** screen, review the summary information about the maintenance window you just specified. If needed, use the **Back** button to cycle back through the wizard windows and make changes.
- 10 Click **Finish**.

Note: You can also create a maintenance window at the service group level of views. Navigate to the Groups:Summary view and click Assign/Unassign Maintenance Window in the Operations task panel. Click the Create new maintenance window option and then click OK to start the Create Maintenance Window wizard.

To delete a maintenance window

- 1 On the main tab bar, click **Admin**.
- 2 On the secondary tab bar, click **Management Server**.
- 3 In the **Administration:Management Server** view, in the **Maintenance Windows** table, select the maintenance windows you want to delete by checking the check box preceding the line item for each maintenance window. Select *all* maintenance windows by checking the check box at the top.
- 4 In the **Configuration** task panel, click **Delete selected maintenance windows**.
- 5 When prompted if you want to delete the one or more maintenance windows listed, click **OK**.

Configuring a peer management server

Configuring a peer management server enables you to expand the scope of the Cluster Management Console to include remote physical locations. Remote locations usually have a management server that is local to them. The management server at the remote location is the one that you configure as a *peer* to your local management server.

After configuration, both management servers are considered to be peers of the other. Users logging in to either management server are able to administer objects at both sites from a single console, using a single login. The views and tasks available at the peer location are determined by the user's role, just as they are on the local management server.

Symantec recommends that you configure only one management server per physical location.

To configure a peer management server

- 1 Configure a trust relationship between the local authentication broker and the peer authentication broker.

- 2 Run the `gaserver -add` command on each management server.

See the *Veritas Cluster Server 5.0 Installation Guide* for information about configuring a trust relationship between two authentication brokers.

See “[gaserver](#)” on page 188 for the proper parameters to use for the `gaserver` command.

Both management servers appear in the Management Servers panel in the Home:Summary view. The name of the remote management server appears in the middle of the Management Servers panel. After the first peer-to-peer updates occur, you can click this link to navigate to the peer management server. The file `Managmentserver.conf` contains the URL of the local management server. This value is sent to the peer management server during the peer-to-peer update process.

Adding a cluster to the management server using direct connection

When using direct connection to manage a cluster, the management server initiates the connection. If you want the management server to use direct connection to administer a cluster, you must specify some of the connection parameters.

If you add a *secure* cluster using direct connection, you must first configure a trust relationship between the management server authentication broker and the cluster authentication broker.

See the *Veritas Cluster Server 5.0 Installation Guide* for information about configuring a trust relationship between two authentication brokers.

To configure the management server to use direct connection for a cluster

- 1 On the navigation bar, click **Home**.

- 2 On the main tab bar, click **Admin**.

- 3 On the secondary tab bar, click **Configured Clusters**.

- 4 In the **Configuration** task panel, click **Configure Cluster**.

- 5 When prompted, specify the system name or the IP address of any running system in the cluster.

- 6 When prompted to provide a user name and password, do one of the following and then click **OK**:
 - If the cluster is configured in secure mode, provide a cluster user account that is known to the authentication broker used by the cluster. The user account must have the role of cluster administrator on the cluster.
 - If the cluster is not configured in secure mode, provide a cluster user account that is known to the cluster. The user account must have the role of cluster administrator on the cluster.

If authentication is successful, the cluster is added to the management server.

Note: No configuration is required on the cluster to configure direct connection.

Removing a direct connection cluster from the management server

This task removes a cluster that is using direct connection from the management server. You can remove only clusters that are in an **OFFLINE** or **UNKNOWN** state. If you remove a direct connection cluster, all data related to that cluster is also removed from the management server database.

To remove a direct connection cluster

- 1 On the navigation bar, click **Home**.
- 2 On the main tab bar, click **Admin**.
- 3 On the secondary tab bar, click **Configured Clusters**.
- 4 In the **Configuration** task panel, click **Remove Cluster**.
When prompted to confirm that you want to remove the direct connection cluster from the management server, click **OK**.

Administering clusters

The following views contain a list of clusters:

- **Home:Clusters**
This is a home-level view of all clusters configured under all management servers.
- **Management Server:Clusters**
This is a management-server-level view of clusters configured under one specific management server.

To navigate to the list in the Home:Clusters view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Clusters**.
In the **Home:Clusters** view, the **Clusters Listing** table contains the list of clusters across all management servers.

To navigate to the list in the Management Server:Clusters view

- 1 On the navigation bar, click **Home**.
- 2 In the **Home:Summary** view, in the **Management Servers** panel, click a linked management server name.
- 3 In the **Management Server:Summary** view, on the secondary tab bar, click **Clusters**.
In the **Management Server:Clusters** view, the **Clusters Listing** table contains the list of clusters configured under the selected management server.

About cluster listing tables

The following is a list of the columns and data in tables that list service group information; these tables are usually labeled Clusters Listing, but may have more detailed labels at lower view levels.

Note: A table with a specific label can appear on more than one view, but some columns may be omitted if the data they contain is made implicit by your having navigated to a particular view.

For example, to reach a particular view, you may have already navigated, or “drilled down,” through one or more view levels by selecting objects such as a management server, cluster, or service group. In such a case, columns that might have indicated these higher-level (parent) objects that you have visited are not included. However, the navigation bar always contains this information.

- Cluster- name of the cluster and a link to the Cluster:Summary view for the cluster.
- Consolidated State - provides information on whether or not the cluster is online, partially online, or unknown.
- # Groups - the number of groups in the cluster.
- # Systems - the number of systems in the cluster.
- Management Server - the name of the management server to which the cluster belongs.
- Platform - the operating system platform of the cluster.
- Region - region or area that cluster services resides. (The region is a user-definable tag.
- Site - site or location where cluster resides. (The site is a user-definable tag)

See “[Modifying tags of selected clusters](#)” on page 86 for more information.

Using filtering, sorting, and navigation path to tailor the list

You can tailor a cluster listing table according to your needs by doing one or more of the following:

- Filter – filter the list of clusters to reduce it to those of current interest to you.
- Sort – sort the list by the values in a column.

- Move up the navigation bar - see more clusters from a higher perspective, or position, within the view hierarchy by moving up the navigation bar from the management server level to the home level.

To filter clusters

- 1 In the either the **Home:Clusters** or **Management Server:Clusters** view, under the **Cluster Filter** panel in the task pane, do any of the following:
 - To view *only* the clusters that are in certain states, under **By Status**, select the states you want (one or more) by checking the check boxes next to **Online**, **Partial**, or **Unknown**.
 - To view *only* the clusters of one platform, select the platform you want from the **By Platform** drop-down menu.
 - If you want to view *only* the clusters of one site, select the site you want from the **By Site** drop-down menu (this filter uses the Site tag).
- 2 Click **Apply**.

To sort clusters

- 1 In the **Clusters Listing** table, locate the column by which you want to sort the list.
- 2 Click the column heading.
The list is sorted by the values in the selected column in ascending order. A triangle (pointing up) displays in that column heading. Click the column heading again to reverse the sort; this action also reverses the triangle.

Command line tips

You can view cluster information using the command line.

To view a list of clusters at the home level using the command line

```
◆ # gaclus -list
```

To view cluster attributes at the cluster level using the command line

```
◆ # gaclus -display cluster-name
```

Cluster tasks at the home and management server level

The following tasks are available for all clusters across all management servers and for clusters configured under one management server.

- Edit attributes
- Edit tags

The Home:Clusters view enables you to see a list of all clusters configured under all management servers. This view contains specific information about your clusters.

Modifying attributes of selected clusters

The Edit Attributes task in either the Home:Clusters or Management Server:Clusters view enables you to edit attributes on selected clusters in a one-to-many fashion (one action modifies many clusters).

To edit attributes

- 1 In either the **Home:Clusters** or **Management Server:Clusters** view, in the **Clusters Listing** table, select the clusters you want to modify by checking the check box preceding the line item for each cluster. Select *all* clusters by checking the check box at the top.
- 2 In the **Configuration** task panel, click **Edit Attribute**.
- 3 In the **Edit Attribute** dialog box, specify the following attribute details and then click **OK**:
 - The attribute name
Select the attribute you want to edit from the **Attribute Name** drop-down menu.
 - The attribute value
In the **Values** box, either click a value to change the it, or click the **+** (plus) button to add a value. Click a value and then click the **-** (minus) button to remove a value.
You can enter more than one value for some attributes. Use the up- and down-arrow buttons to scroll among multiple values.
 - The systems on which to change the attribute
Specify a setting for the **Apply value to** option. **Apply to all nodes** applies the changes to all systems listed the **System List**, which lists all systems on which the attribute is configured. **Apply to selected nodes** enables you to select nodes from the **System List**.

Modifying tags of selected clusters

The **Edit Tags** task enables you to edit tags on selected clusters in a one-to-many fashion (one command modifies many clusters).

Note: You must be a management server administrator on the current management server to modify tags.

To edit tags

- 1 In either the **Home:Clusters** or **Management Server:Clusters** view, in the **Clusters Listing** table, select the clusters you want to modify by checking the check box preceding the line item for each cluster. Select *all* clusters by checking the check box at the top.
- 2 In the **Configuration** task panel, click **Edit Tags**.
- 3 In the **Edit Tags** dialog box, select the tag you want to modify from the **Tag name** drop-down menu.
- 4 Enter the new value for the tag into the **Values** box. You can also enter an optional description into the **Description** box.
- 5 Click **OK**.

Cluster tasks at the cluster level

Some of the views available when using the Cluster Management Console to manage multiple clusters are the same as when using it to manage only a single cluster. Specifically, on the Management tab, any views or tasks at the cluster level are also available when managing a single VCS 5.0 cluster. The views that are common to both environments are shown in the following table:

Table 7-2 Availability of views and tasks changes for different uses

For these view hierarchy levels	The corresponding views and tasks are in
Home (all management servers)	Cluster Management Console managing multiple clusters only
Management server	Cluster Management Console managing multiple clusters only
Cluster	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Service group	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
System	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)

For these view hierarchy levels	The corresponding views and tasks are in
Resource	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Resource type	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)

Refer to the Administering Clusters section of your *Veritas Cluster Server 5.0 User's Guide* for procedures describing cluster tasks at the cluster level.

Note: When used to manage a single cluster, the Cluster Management Console does not share the Reporting, Notification, or Admin tabs, or any of their respective views. These tabs and views are exclusive to centralized cluster management.

Administering service groups

The following views contain a list of service groups:

- **Home:Groups**
This is a home-level (all-management-servers-level) view of all service groups configured under all management servers.
- **Management Server:Groups**
This is a management-server-level view of the service groups configured under one specific management server.
- **Cluster:Groups**
This is a cluster-level view of service groups that are members of one specific cluster.

To navigate to the list in the Home:Groups view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Groups**.
In the **Home:Groups** view, the **Groups Listing** table contains the list of service groups across all management servers.

To navigate to the list in the Management Server:Groups view

- 1 On the navigation bar, click **Home**.
- 2 In the **Home:Summary** view, in the **Management Servers** panel, click a linked management server name.
- 3 In the **Management Server:Summary** view, on the secondary tab bar, click **Groups**.
In the **Management Server:Groups** view, the **Groups Listing** table contains the list of service groups configured under the selected management server.

To navigate to the list in the Cluster:Groups view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Clusters**.
- 3 In the **Home:Clusters** view, in the **Clusters Listing** table, click a linked cluster name.
In the **Cluster:Summary** view, the **Groups Listing** table contains the list of service groups that are members of the selected cluster.

About service group listing tables

The following is a list of the columns and data in tables that list service group information; these tables are usually labeled Groups Listing, but may have more detailed labels at lower view levels.

Note: A table with a specific label can appear on more than one view, but some columns may be omitted if the data they contain is made implicit by your having navigated to a particular view.

For example, to reach a particular view, you may have already navigated, or “drilled down,” through one or more view levels by selecting objects such as a management server, cluster, or service group. In such a case, columns that might have indicated these higher-level (parent) objects that you have visited are not included. However, the navigation bar always contains this information.

- Name - name of the service group and a link to the Group:Summary view for the service group.
- State - the consolidated state of the service group: online, partially online, or unknown.
- Cluster Name - name of the parent, or containing, cluster.
- Site - the site under which the service group is configured. The site is user-definable.
See “[Creating and deleting maintenance windows](#)” on page 79.
- Line of Business - the user-defined line of business of the group. (The line of business is user-definable.
See “[Creating and deleting maintenance windows](#)” on page 79.
- Department - the user-defined department of the group. (The department is user-definable.
See “[Creating and deleting maintenance windows](#)” on page 79.
- Priority - Currently unused, possibly not displayed.
- Cluster Type - the product or technology used to implement the cluster. A cluster implemented using Veritas Cluster Server has a Cluster Type value of VCS.
- Cluster Version - the version number of the product used to implement the cluster.
- Other info - various logged status information.

Using filtering, sorting, and navigation path to tailor the list

You can tailor a groups listing table according to your needs by doing one or more of the following:

- Filter - filter the list of service groups to reduce it to those of current interest to you.
- Sort - sort the list by the values in a column.
- Move up the navigation bar - see more service groups from different perspectives, or positions, within the view hierarchy. Move up the navigation bar from the cluster level to the management server or home level.

To filter service groups

- 1 In the **Home:Groups**, **Management Server:Groups**, or **Cluster:Groups** view, in the **Groups Filter** task panel, do any of the following:
 - To view *only* the clusters that are in certain states, under **By Status**, select the states you want (one or more) by checking the **Online**, **Offline**, **Partial**, **Faulted**, or **Unknown** options.
 - To view *only* the clusters of one platform, select the platform you want from the **By Platform** drop-down menu.
 - To view *only* the clusters of one site, select the site you want from the **By Site** drop-down menu.
 - To include global service groups in the list, check the **Global groups** option.
See your *Veritas Cluster Server 5.0 User's Guide* for information on global service groups and global clusters.
- 2 Click **Apply**.

To sort service groups

- 1 In the **Groups Listing** table, locate the column by which you want to sort the list.
- 2 Click the column heading.
The list is sorted by the values in the selected column in ascending order. A triangle (pointing up) displays in that column heading. Click the column heading again to reverse the sort; this action also reverses the triangle.

Command line tips

You can view service group information using the command line.

To view a list of service groups at the home level using the command line

◆ # `gagrp -list`

To view a list of service group attributes at the group level using the command line

◆ # `gagrp -display grp-name`

Service group tasks at the home and management server level

The following tasks are available for all service groups across all management servers and for service groups configured under one management server.

- Modify attributes
- Modify tags
- Online anywhere
- Offline anywhere
- Clear fault
- Freeze
- Unfreeze
- Assign maintenance windows
- Clear all maintenance windows

Note: Service group icons change in appearance when the states of the objects that they represent are manipulated. For example, if you freeze a service group, the corresponding icon changes to reflect the new state.

See “[Icon conventions](#)” on page 47 for information on Cluster Management Console icon conventions.

Modifying attributes of selected service groups

The Edit attributes task in either the Home:Groups or the Management Server:Groups view enables you to edit attributes on selected service groups in a one-to-many fashion (one command modifies many service groups).

To edit attributes

- 1 In either the **Home:Groups** or **Management Server:Groups** view, select the service groups you want to modify by checking the check box preceding the line item for each service group. Select *all* service groups by checking the check box at the top.

- 2 In the **Configuration** task panel, click **Edit Attributes**.
- 3 In the **Edit Attribute** dialog box, specify the following attribute details and then click **OK**:
 - The attribute name
Select the attribute you want to edit from the **Attribute Name** drop-down menu.
 - The attribute value
In the **Values** box, either click a value to change the it, or click the **+** (plus) button to add a value. Click a value and then click the **-** (minus) button to remove a value.
You can enter more than one value for some attributes. Use the up- and down-arrow buttons to scroll among multiple values.
 - The systems on which to change the attribute
Specify a setting for the **Apply value to** option. **Apply to all nodes** applies the changes to all systems listed the **System List**, which lists all systems on which the attribute is configured. **Apply to selected nodes** enables you to select nodes from the **System List**.

Modifying tags of selected service groups

The Edit Tags task in either the Home:Groups or the Management Server:Groups view enables you to edit tags on selected service groups in a one-to-many fashion (one command modifies many service groups).

Note: You must be a management server administrator on the current management server to modify tags.

To edit tags

- 1 In either the **Home:Groups** or the **Management Server:Groups** view, select the service groups you want to modify by checking the check box preceding the line item for each group. Select *all* service groups by checking the check box at the top.
- 2 In the **Configuration** task panel, click **Edit Tags**.
- 3 In the **Edit Tags** dialog box, select the tag you want to modify from the **Tag name** drop-down menu.
- 4 Enter the new value for the tag into the **Values** box. You can also enter an optional description into the **Description** box.
- 5 Click **OK**.

Freezing and unfreezing service groups (persistent and temporary freezing)

The Freeze task in either the Home:Groups or the Management Server:Groups view enables you to place a service group into a state in which it is active, but not monitored, not able to change state, and not able to fail over to another system. Freezing is useful for performing maintenance tasks on a service group.

For example, you may want to freeze a service group if you want to stop VCS (specifically, HAD), but do not want the service group and the corresponding applications to fail over to another cluster node.

During the time that a service group is frozen, it is running, but not highly available. Do not unfreeze a service group until VCS has been restarted.

To freeze or unfreeze selected groups

- 1 In either the **Home:Groups** or the **Management Server:Groups** view, select the service groups you want to freeze or unfreeze by checking the check box preceding the line item for each group. Select *all* service groups by checking the check box at the top.
- 2 In the **Operations** task panel, click **Freeze** or **Unfreeze**.

Note: When you freeze the selected service groups, a red padlock is added to the status icon for each service group. When you subsequently unfreeze them, the padlock is removed.

To freeze or unfreeze a group using the command line

- # gagrp -freeze *grp* -persistent
- # gagrp -unfreeze *grp* -temporary

Assigning and unassigning maintenance windows

You can schedule intervals of time to perform maintenance on service groups. These intervals are called *maintenance windows*. During a maintenance window, the service group is failed over to another system; the service group is switched back to the original system after the window expires.

You can assign maintenance windows only to service groups. You must first create a maintenance window before you can assign it to a service group.

See “[Creating and deleting maintenance windows](#)” on page 79.

To assign a maintenance window to a service group

- 1 In the **Home:Groups**, **Management Server:Groups**, or **Cluster:Groups** view, in the **Clusters Listing** table, click a linked service group name.
- 2 In the **Group:Summary** view, in the **Operations** task panel, click **Assign/Unassign Maintenance Window**.
- 3 In the **Add or Remove Maintenance Windows** dialog box, click **Select an existing maintenance window**.
- 4 In the **Available** list, check the check box next to the maintenance window that you want to assign to the currently selected service group. You may select more than one available maintenance window.
- 5 Click the right-arrow button.
This action moves the selected maintenance window to the **Assigned** list.
- 6 Click **OK**.

To unassign a maintenance window from a service group

- 1 In the **Home:Groups**, **Management Server:Groups**, or **Cluster:Groups** view, in the **Clusters Listing** table, click a linked service group name.
- 2 In the **Group:Summary** view, in the **Operations** task panel, click **Assign/Unassign Maintenance Window**.
- 3 In the **Add or Remove Maintenance Windows** dialog box, click **Select an existing maintenance window**.
- 4 In the **Assigned** list, check the check box next to the maintenance window that you want to delete from the currently selected service group. You may select more than one assigned maintenance window.
- 5 Click the left-arrow button.
This action moves the selected maintenance window to the **Available** list.
- 6 Click **OK**.

Bringing service groups online or taking them offline anywhere

Manually put a service group into a responsive, functioning state, or into an unresponsive, non-functioning state. You must have the role of cluster administrator or service group administrator to bring a service group online or to take one offline.

You can bring a service group online on a specific system, or you can bring the service group online “anywhere.” If you select the Anywhere option, the service group is brought online on the first available system in the cluster.

Likewise, you can take a service group offline on a specific system, or you can take the service group offline “anywhere”. If you select the Anywhere option, the service group is taken offline on the first system in the cluster on which it is found.

To bring a service group online or take it offline anywhere

- 1 In either the **Home:Groups** or **Management Server:Groups** view, select the service groups that you want to bring online or take offline anywhere. Check the check box preceding the line item for each service group. Select *all* service groups by checking the check box at the top.
- 2 In the **Operations** task panel, select **Online anywhere** or **Offline anywhere**. The candidate systems are members of the system list for each service group. Both of these tasks try each system in a system list until every service group is successfully brought online or taken offline.
- 3 When prompted to confirm that you want to continue, click **OK**.

Service group tasks at or below the cluster level

Some of the views available when using the Cluster Management Console to manage multiple clusters are the same as when using it to manage only a single cluster. Specifically, on the Management tab, any views or tasks at or below the cluster level are also available when managing a single VCS 5.0 cluster. The views that are common to both environments are shown in the following table:

Table 7-3 Availability of views and tasks changes for different uses

For these view hierarchy levels	The corresponding views and tasks are in
Home (all management servers)	Cluster Management Console managing multiple clusters only
Management server	Cluster Management Console managing multiple clusters only
Cluster	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Service group	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)

For these view hierarchy levels	The corresponding views and tasks are in
System	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Resource	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Resource type	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)

Refer to the Administering Service Groups section of your *Veritas Cluster Server 5.0 User's Guide* for procedures describing service group tasks at or below the cluster level.

Note: When used to manage a single cluster, the Cluster Management Console does not share the Reporting, Notification, or Admin tabs, or any of their respective views. These tabs and views are exclusive to centralized cluster management.

Administering systems

The following views contain a list of systems:

- **Home:Systems**
This is a home-level (all-management-servers-level) view of all systems configured under all management servers.
- **Management Server:Systems**
This is a management-server-level view of the systems configured under one specific management server.
- **Cluster:Systems**
This is a cluster-level view of systems that are members of one specific cluster.
- **Groups:Summary**
This is a service-group-level view that contains a list of systems on which one specific service group is configured.
- **Resource:Summary**
This is a resource-level view that contains a list of systems on which one specific resource is installed.

To navigate to the list in the Home:Systems view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Systems**.
In the **Home:Systems** view, the **Systems Listing** table contains the list of systems across all management servers.

To navigate to the list in the Management Server:Systems view

- 1 On the navigation bar, click **Home**.
- 2 In the **Home:Summary** view, in the **Management Servers** panel, click a linked management server name.
- 3 In the **Management Server:Summary** view, on the secondary tab bar, click **Systems**.
In the **Management Server:Systems** view, the **Systems Listing** table contains the list of systems configured under the selected management server.

To navigate to the list in the Cluster:Systems view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Clusters**.

- 3 In the **Home:Clusters** view, in the **Clusters Listing** table, click a linked cluster name.
- 4 In the **Cluster:Summary** view, on the secondary tab bar, click **Systems**. In the **Cluster:Systems** view, in the **Systems Listing** table contains the list of systems that are members of the selected cluster.

To navigate to the list in the Group:Summary view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Groups**.
- 3 In the **Home:Groups** view, in the **Groups Listing** table, click a linked service group name.
In the **Group:Summary** view, the **Systems Listing** table contains a list of system on which the selected service group is configured.

To navigate to the list in the Resource:Summary view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Clusters**.
- 3 In the **Home:Clusters** view, on the secondary tab bar, click **Resources**.
- 4 In the **Cluster:Resources** view, in the **Resources Listing** table, click a linked resource name.
In the **Resource:Summary** view, the **Systems Listing** table contains a list of systems on which the selected resource is configured.

About system listing tables

The following is a list of the columns and data in tables that list system information; these tables are usually labeled Systems Listing, but may have more detailed labels at lower view levels.

Note: A table with a specific label can appear on more than one view, but some columns may be omitted if the data they contain is made implicit by your having navigated to a particular view.

For example, to reach a particular view, you may have already navigated, or “drilled down,” through one or more view levels by selecting objects such as a management server, cluster, or service group. In such a case, columns that might have indicated these higher-level (parent) objects that you have visited are not included. However, the navigation bar always contains this information.

- System- name of the system and a link to the System:Summary view for that system.
- Consolidated State - provides real-time state of the system; whether it is online, offline, partially online, or unknown.
- VCS Version - the version of VCS used on the system.
- Platform - the operating system installed on the system.
- Parent Cluster - the cluster to which the system belongs.

Using filtering, sorting, and navigation path to tailor the list

You can tailor a systems listing table according to your needs by doing one or more of the following:

- Filter - filter the list of systems to reduce it to those of current interest to you.
- Sort - sort the list by the values in a column.
- Move up the navigation bar - see more systems from different perspectives, or positions, within the view hierarchy by moving up the navigation bar from the system level to the group, cluster, management server, or home level.

To filter systems

- 1 In the **Home:Systems**, **Management Server:Systems**, or **Cluster:Systems** view, in the **Systems Filter** task panel, do any of the following:
 - To view *only* the systems that are in certain states, under **By Status**, select the states you want (one or more) by checking the **Online**, **Offline**, **Partial**, **Faulted**, or **Unknown** options.
 - To view *only* the systems of one platform, select the platform you want from the **By Platform** drop-down menu.
 - To view *only* the systems of one site, select the site you want from the **By Site** drop-down menu.
- 2 Click **Apply**.

To sort service groups

- 1 In the **Systems Listing** table, locate the column by which you want to sort the list.
- 2 Click the column heading.

The list is sorted by the values in the selected column in ascending order. A triangle (pointing up) displays in that column heading. Click the column heading again to reverse the sort; this action also reverses the triangle.

Command line tips

You can view system information using the command line.

To view a list of systems in the enterprise using the command line

```
◆ # gasys -list
```

To view a list of system attributes using the command line

```
# gasys -display sys-name
```

System tasks at the home and management server level

The following tasks are available for all systems across all management servers and for systems configured under one specific management server.

- Modify Attributes
- Freeze System
- Unfreeze System

Modifying attributes of selected systems

The Edit Attributes task in either the Home:Systems or Management Server:Systems view enables you to edit attributes on selected systems in a one-to-many fashion (one action modifies many systems).

To edit attributes

- 1 In either the **Home:Systems** or **Management Server:Systems** view, select the systems you want to modify.
Check the check box preceding the line item for each system. Select *all* systems by checking the check box at the top.
- 2 In the **Configuration** task panel, click **Edit attributes**.
- 3 In the **Edit Attribute** dialog box, specify the following attribute details and then click **OK**:
 - The attribute name
Select the attribute you want to edit from the **Attribute Name** drop-down menu.
 - The attribute value
In the **Values** box, either click a value to change the it, or click the + (plus) button to add a value. Click a value and then click the - (minus) button to remove a value.
You can enter more than one value for some attributes. Use the up- and down-arrow buttons to scroll among multiple values.

- The systems on which to change the attribute
Specify a setting for the **Apply value to** option. **Apply to all nodes** applies the changes to all systems listed the **System List**, which lists all systems on which the attribute is configured. **Apply to selected nodes** enables you to select nodes from the **System List**.

Freezing and unfreezing systems (persistent and temporary freezing)

The Freeze task in either the Home:Systems or the Management Server:Systems view enables you to place a system into a state in which it is active, but not monitored, not able to change state, and not able to fail over any of the service groups it contains to another system. Freezing is useful for performing maintenance tasks.

For example, you may want to freeze a system if you want to stop VCS (specifically, HAD), but do not want the service groups it contains and the corresponding applications to fail over to another cluster node.

During the time that a system is frozen, it is running, but not the applications that is hosts are not highly available. Do not unfreeze a service group until VCS has been restarted.

To freeze or unfreeze selected systems

- 1 In either the **Home:Systems** or **Management Server:Systems** view, select the systems you want to freeze or unfreeze by checking the check box preceding the line item for each system. Select *all* systems by checking the check box at the top.
- 2 In the **Operations** task panel, click either **Freeze** or **Unfreeze**.

Note: When you freeze the selected systems, a red padlock is added to the status icon for each system. When you subsequently unfreeze them, the padlock is removed.

System tasks at or below the cluster level

Some of the views available when using the Cluster Management Console to manage multiple clusters are the same as when using it to manage only a single cluster. Specifically, on the Management tab, any views or tasks at or below the cluster level are also available when managing a single VCS 5.0 cluster. The views that are common to both environments are shown in the following table:

Table 7-4 Availability of views and tasks changes for different uses

For these view hierarchy levels	The corresponding views and tasks are in
Home (all management servers)	Cluster Management Console managing multiple clusters only
Management server	Cluster Management Console managing multiple clusters only
Cluster	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Service group	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
System	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Resource	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Resource type	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)

Refer to the Administering Systems section of your *Veritas Cluster Server 5.0 User's Guide* for procedures describing system tasks at or below the cluster level.

Note: When used to manage a single cluster, the Cluster Management Console does not share the Reporting, Notification, or Admin tabs, or any of their respective views. These tabs and views are exclusive to centralized cluster management.

Administering resources

The following views contain a list of resources:

- **Cluster:Resources**
This is a cluster-level view of all resources that are members of one specific cluster.
- **Group:Summary**
This is a service-group-level view of all resources that are members of one specific service group.
- **Group:Resources**
This is a service-group-level view that, instead of a list, contains a graphical representation of the resources that are members of one specific service group and any relationships (parent-child dependencies) that exist among them.
- **Resource:Summary**
This is a resource-level view that contains lists of both parent and child resources, if any, of one specific resource. This information is shown graphically in the Group:Resources view.

To navigate to the list in the Cluster:Resources view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Clusters**.
- 3 In the **Home:Clusters** view, on the secondary tab bar, click **Resources**.
In the **Cluster:Resources** view, the **Systems Listing** table contains the list of all resources that are members of the selected cluster.

To navigate to the list in the Group:Summary view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Groups**.
- 3 In the **Home:Groups** view, in the **Groups Listing** table, click a linked service group name.
In the **Group:Summary** view, the **Resource List** table contains all resources that are members of the selected service group.

To navigate to the list in the Group:Resources view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Groups**.

- 3 In the **Home:Groups** view, in the **Groups Listing** table, click a linked service group name.
- 4 In the **Group:Summary** view, on the secondary tab bar, click **Resources**. In the **Group:Resources** view, a diagram shows the resources that are members of the selected service group and any relationships (parent-child dependencies) that exist among them.

To navigate to the list in the Resource:Summary view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Clusters**.
- 3 In the **Home:Clusters** view, in the **Clusters Listing** table, click a linked cluster name.
- 4 In the **Cluster:Summary** view, on the secondary tab bar, click **Resources**.
- 5 In the **Cluster:Resources** view, in the **Resources Listing** table, click a linked resource name.

In the **Resource:Summary** view, the **Parent resources of this resource** table and the **Child resources of this resource** table list any resources that have dependency relationships with the selected resource.

About resource listing tables

The following is a list of the columns and data in tables that list resource information; these tables are usually labeled Resources Listing, but may have more detailed labels at lower view levels.

Note: A table with a specific label can appear on more than one view, but some columns may be omitted if the data they contain is made implicit by your having navigated to a particular view.

For example, to reach a particular view, you may have already navigated, or “drilled down,” through one or more view levels by selecting objects such as a management server, cluster, or service group. In such a case, columns that might have indicated these higher-level (parent) objects that you have visited are not included. However, the navigation bar always contains this information.

- Name - name of the resource and a link to the Resource:Summary view for the resource.
- State - the state of the resource - online, offline, partial, or faulted.
- Type - type of resource and a link to the resource type attribute.

- Parent group - name of the group to which the resource belongs.

Using filtering, sorting, and navigation path to tailor the list

You can tailor a resource listing table according to your needs by doing one or more of the following:

- Sort - sort the list by the values in a column.
- Move up the navigation bar - see more resources from different perspectives, or positions, within the view hierarchy by moving up the navigation bar from the resource level to the service group or cluster level.

To sort resources

- 1 In any system listing table, locate the column by which you want to sort the list.
- 2 Click the column heading.
The list is sorted by the values in the selected column in ascending order. A triangle (pointing up) displays in that column heading. Click the column heading again to reverse the sort; this action also reverses the triangle.

Command line tips

You can view resource information using the command line.

To view a list of resources across all management servers using the command line

```
◆ # gares -list
```

To view a list of resource attributes using the command line

```
◆ # gares -display res-name
```

Resource tasks at or below the cluster level

Note: No resource tasks are available at the home or management server level. All resource tasks are performed in the context of a single parent, or containing, object, such as a cluster, service group, or dependant resource.

Some of the views available when using the Cluster Management Console to manage multiple clusters are the same as when using it to manage only a single cluster. Specifically, on the Management tab, any views or tasks at or below the cluster level are also available when managing a single VCS 5.0 cluster. The views that are common to both environments are shown in the following table:

Table 7-5 Availability of views and tasks changes for different uses

For these view hierarchy levels	The corresponding views and tasks are in
Home (all management servers)	Cluster Management Console managing multiple clusters only
Management server	Cluster Management Console managing multiple clusters only
Cluster	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Service group	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
System	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Resource	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Resource type	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)

Refer to the Administering Resources section of your *Veritas Cluster Server 5.0 User's Guide* for procedures describing tasks for resources at or below the cluster level.

Note: When used to manage a single cluster, the Cluster Management Console does not share the Reporting, Notification, or Admin tabs, or any of their respective views. These tabs and views are exclusive to centralized cluster management.

Administering resource types

The following views contain a list of resource types:

- **Cluster:Resource Types**
This is a cluster-level view that lists the resource types of all resources that are members of one specific cluster.
- **Group:Summary**
This is a service-group-level view that lists the resource types of all resources that are members of one specific service group.
- **Resource:Summary**
This is a resource-level view that lists the resource types of any parent or child resources of one specific resource. This view also contains the linked name of the resource type of the one specific resource that the view details.

To navigate to the list in the Cluster:Resource Types view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Clusters**.
- 1 In the **Home:Clusters** view, in the **Clusters Listing** table, click a linked cluster name.
- 2 In the **Cluster:Summary** view, on the secondary tab bar, click **Resource Types**.
In the **Cluster:Resource Types** view, the **Resource Types Listing** table lists the resource types of all resources that are members of the selected cluster.

To navigate to the list in the Group:Summary view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Groups**.
- 3 In the **Home:Groups** view, in the **Groups Listing** table, click a linked service group name.
In the **Group:Summary** view, the **Resource List** table lists all resources that are members of the selected service group. The **Type** column in this table lists the resource type of each resource.

To navigate to the list in the Resource:Summary view

- 1 On the navigation bar, click **Home**.
- 2 On the secondary tab bar, click **Clusters**.
- 3 In the **Home:Clusters** view, in the **Clusters Listing** table, click a linked cluster name.

- 4 In the **Cluster:Summary** view, on the secondary tab bar, click **Resources**.
- 5 In the **Cluster:Resources** view, in the **Resources Listing** table, click a linked resource name.
- 6 In the **Resource:Summary** view, the **Parent resources of this resource** table and the **Child resources of this resource** table list any resources that have a dependency relationship with the selected resource. The **Type** column in these tables lists the resource type of each resource.

About resource type listing tables

Only one resource types listing table exists; it is located in the Cluster:Resource Types view, and has only one column, Resource Type, which lists the resource type name. Click a linked resource type name from here to view the attributes associated with the resource type.

Using filtering, sorting, and navigation path to tailor the list

You can tailor a table with a resource types column by doing one or more of the following:

- Sort - sort the Resource Types column by the values in another column.
- Move up the navigation bar - see more resource types from different perspectives, or positions, within the view hierarchy by moving up the navigation bar from the resource type level to the resource, group, or cluster level.

To sort resource types

- 1 In any table that lists resource types, locate the column by which you want to sort the list.
- 2 Click the column heading.
The list is sorted by the values in the selected column in ascending order. A triangle (pointing up) displays in that column heading. Click the column heading again to reverse the sort; this action also reverses the triangle.

Command line tips

To view a list of resource types using the command line

◆ # `gatype -list`

To view a list of resource type attributes using the command line

◆ # `gatype -display type-name`

Resource type tasks at or below the cluster level

Note: No resource type tasks are available at the home or management server level. All resource type tasks are performed in the context of a single parent, or containing, object, such as a cluster, service group, or resource.

Some of the views available when using the Cluster Management Console to manage multiple clusters are the same as when using it to manage only a single cluster. Specifically, on the Management tab, any views or tasks at or below the cluster level are also available when managing a single VCS 5.0 cluster. The views that are common to both environments are shown in the following table:

Table 7-6 Availability of views and tasks changes for different uses

For these view hierarchy levels	The corresponding views and tasks are in
Home (all management servers)	Cluster Management Console managing multiple clusters only
Management server	Cluster Management Console managing multiple clusters only
Cluster	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Service group	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
System	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Resource	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)
Resource type	Cluster Management Console managing multiple clusters or a single cluster (views shared in both environments)

Refer to the Administering Resource Types section of your *Veritas Cluster Server 5.0 User's Guide* for procedures describing tasks for resource types at or below the cluster level.

Note: When used to manage a single cluster, the Cluster Management Console does not share the Reporting, Notification, or Admin tabs, or any of their respective views. These tabs and views are exclusive to centralized cluster management.

Viewing logs

In the Manage tab view hierarchy, the following levels of views each have a logs tab on the secondary tab bar.

- Management server
- Cluster
- Group
- System
- Resource

See “[Main tabs, secondary tabs, and view hierarchies](#)” on page 42.

The Logs tab takes you to a view of log entries about the individual object that you select.

To navigate to the logs view for an object

- 1 On the navigation bar, click **Home**.
- 2 Navigate to one of the following views for a particular object:
 - **Management server:Summary**
 - **Cluster:Summary**
 - **Group:Summary**
 - **System:Summary**
 - **Resource:Summary**
- 3 In the *Object:Summary* view, on the secondary tab bar, click **Logs**.
Object is the type of the object that you selected. Each logs tab contains a search box and **Search** button so that you can quickly find the log entries that you want.

See “[Overview of the Cluster Management Console](#)” on page 35 for information about navigating among views.

See “[Conducting a search](#)” on page 152.

Note: Logs for clusters and service groups contain entries about only the object that you select. Entries for descendant objects are not included.

Reporting historical data

The following topics are included in this chapter:

- [About reporting](#)
- [Administering report jobs](#)
- [Administering report outputs](#)
- [Understanding report types by functionality](#)

About reporting

The Reporting function allows you to report cluster performance and management history from the Cluster Management Console database. *Report jobs* specify how and when to run a report, and *report outputs* are the results of running a report. You can save report jobs and outputs in the database.

The types of reports you can generate are predefined, yet comprehensive. The predefined report types are described in the following table:

Table 8-1 Types of reports

Report type	Description
Agent Inventory	An inventory of installed enterprise (third party) VCS agents, and optionally, bundled VCS agents on each selected cluster, <i>by cluster</i> . For each agent, displays information from the agent information file. The agent information includes version, minimum VCS version, agent type, vendor, files installed with agent, and nodes where the agent is installed.
Agent Usage	A summary of all agents that are installed on the selected clusters, <i>by agent</i> . For each agent, this summary includes the clusters where the agent is installed, and groups containing resources of that type.
Cluster Activity	A listing of all event information, representing changes that are made to the selected clusters over a specified time period.
Cluster Attribute	A tabular report that displays the current value of selected attributes for each of the selected clusters. Each cluster is represented as a single row in the resulting attributes table.
Cluster Inventory	A summary of configuration information about the selected clusters. May be used in a manner similar to a “run book”.
Configuration Analysis	A detailed analysis of configuration aspects of the selected clusters and their groups, with reported results of possible configuration problems. A summary chart displays the configured clusters and groups with the number of errors and warnings generated. Individual tests and results are provided, and may include supporting subtest results.
Current Schedules	A summary of the schedules that are defined for the management server, including maintenance windows and scheduled reports. Information includes all objects that are associated with each schedule.

Table 8-1 Types of reports

Report type	Description
Failure Summary	Statistics about resource failures, gathered for each of the selected clusters over the specified date range. A "failure" refers to any offline or faulted status. The report shows failures by resource type, node, and group, plus time to recovery.
Failure Summary by Group	Statistics about resource failures, gathered for each of the selected groups over the specified date range. A "failure" refers to any offline or faulted status. The report shows failures by resource type, node, and resource, plus time to recovery.
Fault Trending	Fault statistics for each resource type, including faults per week and faults per resource. Purpose is to help locate possible fault trends.
Group Activity	A listing of all event information, representing changes that are made to the selected groups over a specified time period.
Group Attribute	A tabular report that displays the current value of selected attributes for each of the selected groups. Each group is represented as a single row in the resulting attributes table.
Resource Activity	A listing of all event information, representing changes that are made to the selected resources over a specified time period.
Resource Attribute	A tabular report that displays the current value of selected attributes for each of the selected resources. Each resource is represented as a single row in the resulting attributes table.
Uptime Analysis	Analysis of "uptime," the amount of time the selected groups were accessible to the user over a time period. You can specify time periods, called "maintenance windows," to exclude from the overall uptime calculation. You can also exclude individual resources from the calculation.
Virtual IP Usage	A table of all virtual IP addresses that are <i>in use</i> for resources in the selected clusters. Information on each IP address includes the associated group, resource, node, subnet mask, and MAC address.

Administering report jobs

Report jobs are stored specifications for generating report outputs. You can run a report job at arbitrary times or on a schedule. One report job can produce many report outputs. Report job specifications include:

- Report Type - brief descriptor of one of several reports that are provided with the product; specifies data to be reported.
- Job Name - report job name, supplied by the user.
- Description - report job description, supplied by the user.
- Time Range (some report types) - the time period of the report's data; only used by some report types.
- Selected Objects - cluster objects on which to base the report; the object type depends on the report type.
- Schedule - optional specification of dates for the report job to run automatically; several recurrence patterns are available.
- Owner - the user that created the report job
- Enabled - whether or not the report job is set to run at the intervals that are specified for it.

You can create, delete, run, enable, disable, and clone report jobs.

Viewing a list of report jobs

The Report:Jobs view displays a list of stored report jobs along with the following information about each job:

- job name
- report type
- date last run
- report outputs
- whether or not the maximum number of outputs have been stored
- report schedule
- owner of the report
- whether or not the report schedule is enabled.

To navigate to the list in the Report:Jobs view

- 1 On the main tab bar, click **Reporting**.
- 2 On the secondary tab bar, click **Jobs**.

In the **Last Available Output** column, icons next to the date and time indicate whether the report job is running, complete, or failed.

Table 8-2 Report job status Icons



Report job is running.



Report job is complete.



Report job has failed.

Viewing and modifying details of a report job

Report jobs are lists of attributes and values that define report content and scheduling. Running a report job gathers data from *target* objects that you specify. These target objects are stored as values of the Selected Objects attribute, which is one of the attributes that define a report job. The Report Job Details view lists all of the attributes and values for a report job.

To navigate to the attribute list in the Report Job Details view

- 1 On the main tab bar, click **Reporting**.
- 2 On the secondary tab bar, click **Jobs**.
- 3 In the **Report:Jobs** view, in the **Report Jobs** table, click a linked job name. The **Report Job Details** view displays the report job attributes and values in a table. Editable attributes have a ...(edit) button in the **Edit** column of the table, as well as a link in the **Configuration** task panel. If any target objects previously selected for a report job are no longer in the database, a **Remove Missing Target Objects** link appears in the **Configuration** task panel. Click this link to remove one or more missing target objects from the report job. Missing target objects are excluded from the list of candidate target objects when you create subsequent report jobs.

Creating a new report job

The Cluster Management Console provides a wizard that guides you through the steps for creating a new report job. You can create report jobs from sixteen predefined report types (see “[About reporting](#)” on page 114). After you choose a predefined report type, you can provide the job specifics, such as scheduling and which objects serve as the subject of the report.

Report job scheduling options

The wizard you use to create report jobs offers many options for specifying a report job schedule. It is important to know exactly what information these options require and how to enter them using the wizard controls. Gaining familiarity with scheduling options enables you to fully exploit the flexibility of the scheduling feature. You may want to refer to these option descriptions during the first few times you use the wizard.

Schedule the report option

The Schedule the report option specifies whether or not you want to create a schedule for running the report job. In the Start Date and Time dialog box, if you want to set up a schedule, check the check box next to the Schedule the report option. This action activates additional scheduling options. If you want to run this report only when desired and do not want to schedule it, leave the check box clear.

Start time option

The Start Time option specifies the time at which you want the report to start running. Use the two drop-down menus to select the hour and minutes of the start time. On all dates that it runs, the report runs at this start time.

Effective date option

The Effective date option specifies the date you want the report schedule to become active. In the Effective date: box, click the calendar icon to display a calendar and then select an effective date. Depending on your selections, the starting date for the report schedule can be different, but the report will not run until after the effective date.

Time range options

The Time Range option specifies the reporting time period. The resulting report includes the data (stored in the database) that was collected over that period of time. In the Time range dialog box, you can specify any of the following options

- Last
Enter a number and then select hour, day, week, month, or year. This number and amount of time specify a time range, starting that amount of time ago, and ending now.
For example, the last 1 day is a time range starting 24 hours ago.
- Current
Select hour, day, week, month, or year to report on the current hour, day (today), week, month, or year.
- Specific period

Specify the From: and To: information for the specific period. You can choose to report on the events that take place on a certain day, at a certain time, or you can choose to report the events that take place on a certain day.

- Include Maintenance Windows (this option is checked by default)
Uncheck this option if you do not want to include maintenance windows in the time range. Refer to “[Creating and deleting maintenance windows](#)” on page 79 for more information.

Recurrence pattern options

The Recurrence Pattern dialog box, you can select one or all of the available options. The report job runs on all dates specified by all options (except for dates specified by the Excluded dates option). On all dates that the report runs, it runs at the start time specified by the recurrence pattern. In the Recurrence pattern dialog box, you can specify the following options:

- Day Interval
Enter the number of days (for example, every 2 days or every 15 days) between runs of the report. Click the calendar icon next to the Calculated From: box to display a calendar, and then select a date to start the report.
- Week Days of the Month
Select the days of each week in a month for the report to run. For example, if you select Monday and Saturday in the first week, the report will run the first Monday and first Saturday of each month.
Click Select All to select all the week days of a month, or click Deselect All to remove all selected days of each week in a month
- Days of the Month
Select specific days of the month for the report to run. For example, if you select 2 and 15, the report will run on the second and fifteenth of each month.
Click Select All to select all the days of a month, or click Deselect All to remove all selected days in a month. You can also select the Last option, which will enable this option to run on the last day of each month, regardless of the month or how many days are in a month.
- Specific dates
Select specific dates throughout a month or a year for the report to run. For example, you can specify that the report run specifically on June 17, 2004 and August 12, 2004.
Click the calendar icon next to the Select Date box to display a calendar, select a date to start the maintenance window, and then click Add to add it to the Specific Dates box. You can continue adding specific dates in this manner.

If you need to delete a particular date, highlight the date in the Specific Dates box and then click Remove. You can select multiple dates by holding down the Shift key and clicking on the desired dates.

- Excluded dates - select specific dates to exclude. For example, you can specify January 1, 2004 and July 4, 2004 as days that the report will not run, even if specified in another option.

Click the calendar icon next to the Select Date box to display a calendar, select a date to exclude from the schedule, and then click Add to add it to the Excluded Dates box. You can continue adding specific dates in this manner.

If you need to delete a particular date, highlight the date in the Excluded Dates box and then click Remove. You can select multiple dates by holding down the Shift key and clicking on the desired dates.

How to use the report target object chooser

For some report types, the job creation wizard requires you to select the cluster objects (which include attributes) from which the report retrieves data. To facilitate your selection, the wizard offers a control called a *chooser*. A chooser looks like two boxes with large left- and right-arrow buttons between them. The boxes contain expandable “trees” of cluster objects that work like the graphical file system (folder) trees used in many graphical operating systems.

To use the object chooser

- 1 In the **Available Objects** (or **Available Attributes**) box, locate and select the target objects to use for the report.
Click the + (plus) sign next to an object to expand it into the lower-level objects that it contains. Select an object by checking the check box next to it. Checking an object with a + sign selects all objects that are within the checked object.
You do not have to decide which objects can be correctly or justifiably selected for the report. The wizard displays *only* those objects that are appropriate and relevant for the selected report type.
- 2 After locating and selecting target objects for the report, click the right-arrow button to add it to the **Selected Objects** (or **Selected Attributes**) box. To deselect an object, check the checkbox next to it in the **Selected Objects** box and then click the left-arrow button to move it back under **Available Objects**.

Create the job

After you understand how to specify target objects and scheduling information, you are ready to create the report job.

To create a new report job

- 1 In the **Report Jobs** view, in the **Configuration** task panel, click **Create a new report job**.
- 2 In the **Welcome to the Report Job Creation Wizard**, read the introduction and then click **Next**.
- 3 In the **Report Type** dialog box, select one of the predefined report types from the drop-down menu, and click **Next**.
See “[About reporting](#)” on page 114 for a description of each report type.
- 4 In the **Name and Description** dialog box, enter a name and description for the report job.
- 5 If you want to set a maximum number of outputs to be stored for the job, perform the following step; otherwise, click **Next**.
Check the **Limit outputs stored for this job** check box, enter the maximum number of outputs into the **Limit to** box, and then click **Next**. You may enter numbers in the range of one to 999.
- 6 At each subsequent step in the wizard, follow the instructions in each dialog box and enter the requested information *exactly as described*. At each step, you can click **Next** to continue to the next step, click **Back** to revisit a previous step, or click **Cancel** to cancel the task wizard.

Modifying a report job

You can modify some of the attributes of a report job. Editable attributes have an ... (edit) button in the Edit column of the table in the Report Job Details view. The Report Outputs view displays report outputs that were created before the report job was most recently modified. The names for these report jobs are unlinked.

To modify a report job

- 1 In the **Report Job Details** view, locate the attribute you want to modify.
- 2 Click the ... (edit) button.
- 3 In the **Name and Description** dialog box, change the attribute information as desired.
- 4 Click **Apply**.

Deleting a report job

The Delete Selected Jobs task enables you to delete one or more report jobs. This task does not delete report outputs previously generated by a job. However, in the Report Outputs view, the deleted report job name no longer links to any job details (attributes and values).

To delete selected report jobs

- 1 In the **Report Jobs** view, select the report jobs you want to delete by checking the check box next to each job name, or select *all* report jobs by checking the check box at the top.
- 2 In the **Configuration** task panel, click **Delete Selected Jobs**.
- 3 In the dialog box with the message, “The following jobs will be deleted. Do you want to continue?” click **OK** to delete the jobs.

Note: This task is also available as **Delete Job** for deleting one job at a time in the Report Job Details view.

Running a report job to generate a report output

You can use the Run Selected Jobs task to immediately run a report job and generate a report output. Running a report in this way does not affect any scheduled runs of any job. When a job run is complete, a new report output is available.

To run selected report jobs

- 1 In the **Report Jobs** view, select the report jobs you want to run by clicking the check box next to each job name or select *all* report jobs by clicking the check box at the top.
- 2 In the **Operations** task panel, click **Run Selected Jobs**.
- 3 In the dialog box with the message, “The following report jobs will be run. Do you want to continue?” click **OK**.
The report job starts and runs “in the background”. Click the **Outputs** tab to go to the **Report Outputs** view. This view contains a new entry in the table with the current date, time, and the name of the job you ran.
You may see a status of **Running**; the status changes to **Completed** when the job is finished. In the **Report Jobs** view, the **Last Available Output** value for the job is also updated.
- 4 If you want to view the generated report output, do one of the following:

- In the **Report Outputs** view, click the **Date Generated** column for the recent output of the job you ran. (You can sort by this column to find it.)
- In the **Report Jobs** view, click the **Date Last Run** column for the job you ran.

Note: This task is also available as **Run Job** for running one job at a time in the Report Job Details view.

Enabling and disabling a report job

You can use the **Disable Selected Jobs** task to disable a report job schedule. If a schedule has been specified for a job, it remains in place, but the job does not run.

Disabling a job does not prevent manual runs of the job. You can use the **Run** command at any time to generate output from a disabled job. Use the **Enable Selected Jobs** task to re-enable a disabled job.

To disable selected report jobs

- 1 In the **Report Jobs** view, select the report jobs you want to disable by checking the check box next to each job name, or select *all* report jobs by checking the check box at the top.
- 2 In the **Operations** task panel, click **Disable Selected Jobs**.
- 3 In the dialog box with the message, “The following jobs will be disabled. Do you want to continue?” click **OK** to disable the jobs.

To enable selected report jobs

- 1 In the **Report Jobs** view, select the report jobs you want to enable by checking the check box next to each job name, or select *all* report jobs by checking the check box at the top.
- 2 In the **Operations** task panel, click **Enable Selected Jobs**.
- 3 If the selected jobs are scheduled, a dialog box appears with the message, “The following jobs will be enabled. Do you want to continue?” Click **OK** to enable the jobs. Otherwise, the message is “None of the selected report jobs can be enabled. They are either not scheduled or already enabled.”

Cloning a report job

The **Clone Selected Jobs** task enables you to create a copy of a report job. You can then modify the cloned job as desired. Cloning report jobs is useful if you

have job specifications, such as a selected objects list, that need to be the same for multiple report jobs.

Note: Schedule information is not cloned. If you want a cloned job to be scheduled, edit its Schedule attribute in the Report Job Details view and create the desired schedule.

To clone selected jobs

- 1 In the **Report Jobs** view, select the report jobs you want to clone by clicking the check box next to each job name, or select *all* report jobs by clicking the check box at the top.
- 2 In the **Operations** task panel, click **Clone**.
- 3 In the dialog box with the message, “The following jobs will be cloned. Do you want to continue?” click **OK** to clone the jobs.
The **Report Jobs** view displays a new entry in the table, with a **Job Name** like the one you cloned, but prefixed with “Copy of “. The **Last Available Output** value for the new job is **None**. You can modify job attributes, such as the job name or the target objects in the **Report Job Details** view.

Note: This task is also available as **Clone Job** for cloning one job at a time in the Report Job Details view.

Filtering the report jobs table

You can filter the table in the Report Jobs view by report type or by job owner.

To filter report jobs

- 1 In the **Report Jobs** view, in the **Reports Job Filter** task panel, do one of the following:
 - a If you want to view only the report jobs with a specified report type, select the report type you want from the **By Report Type** drop-down menu.
 - b If you want to view only the report jobs created by a specified user, select the owner you want from the **By Owner** drop-down menu.
- 2 Click **Apply**.

Granting and revoking reporting privileges

Reporting privileges may be granted by management server administrators only, and may be revoked by only the same. See “[Administering clusters](#)” on page 83 for information about this task.

Administering report outputs

Report outputs are the retrieved, formatted cluster data that result from running a report job on its target objects. One report job, when run several times, can create many report outputs. After creation, report outputs are stored in the database and can be viewed at any time. New report outputs can be generated from any job at any time. Some report types report data over a time range (for example, Cluster Activity) and other types provide a current snapshot of data (for example, Agent Inventory). All report types require you to choose cluster objects on which to report (target objects), and give you the option to schedule the report.

Viewing a list of report outputs

The Report Outputs view contains a table of outputs. The table provides information on each output, including:

- Date Generated - the date the report output was generated; also a link to the output itself.
- Job Name - name of the report job that generated the output.
- Run By - the user who ran the report.
- Report Type - the type of report
- Status - the status of the report output.

Creating a report output

You create a report output by running a report job. Refer to “[Running a report job to generate a report output](#)” on page 122 for instructions.

Viewing a report output

In the Report Outputs view, click a linked date in the Date Generated column to view the report output in a new window. All report output windows include the following information:

- Description.
- Run time.
- A list of the target objects, which are also links to the corresponding sections of the report output.
- The report output data, which usually includes one or more tables.

Deleting a report output

The Delete command lets you delete one or more report outputs.

Note: Deleting a report output does not delete the report job that generated the outputs.

If you are deleting several outputs at one time, you may want to use the Filter task. This task enables you to reduce the list to only those that you want to delete. Using the prune command on the Database view, you can also delete all report outputs of a certain age.

See “[Pruning the database](#)” on page 157.

To delete selected report outputs

- 1 In the **Report Outputs** view, select the report outputs you want to delete by clicking the check box next to each report (left-most column), or select *all* reports by clicking the check box at the top.
- 2 In the **Configuration** task panel, click **Delete**.
- 3 In the **Delete Selected Outputs** dialog box, click **OK**.

Linking a reinstalled cluster back to its historical data

No historical data is available for a cluster after reinstalling cluster connector. This situation can occur if cluster connector is uninstalled and then reinstalled on a cluster.

When cluster connector is reinstalled, a new identifier is assigned to the cluster. All historical data is unlinked from the cluster because the management server identifies the cluster as new. Perform the following steps to link the cluster back to the appropriate historical data.

Note: This procedure assumes that cluster connector has already been uninstalled and then reinstalled on the same cluster.

To link a cluster back to the appropriate historical data

- 1 Verify that the **Home:Clusters** view displays two clusters, one in an UNKNOWN state and one in an ONLINE state.
- 2 Change the value of the **ClusterID** attribute of the new **CMC_ClusterConfig** resource (**CMC** service group) to the original **Cluster ID** value.
- 3 Restart the **CMC** service group.

- 4 Delete the old cluster, using **Remove this cluster** on the Cluster:Summary view.
Reports for this cluster should now include its historical data.

Filtering report outputs

You can filter the Report Outputs view by report output status, time generated, type, or report job.

To filter report outputs

- 1 In the **Report Outputs** view, in the **Report Output Filter** task panel, specify any of the following:
 - a To filter by status, click the check boxes under **By State** to select one or more choices from **Running**, **Completed**, or **Failed**.
 - b To filter by when the output was generated, select a time window from the **By Time** drop-down menu, such as the **Last Day** or **Last Week**.
 - c To filter by a report type, select a report type from the **By Report Type** drop-down menu.
 - d To filter by a report job (view only the outputs generated by one job), select a report job name from the **By Report Job** drop-down menu.
- 2 Click **Apply**.

Understanding report types by functionality

The remaining sections are grouped into functional areas, and describe the contents and purpose of each report type.

- [“Tracking VCS agents across the enterprise with reports”](#) on page 129
- [“Managing cluster configurations with reports”](#) on page 130
- [“Analyzing failures for trends, patterns, and problem areas”](#) on page 133
- [“Managing and reporting uptime of service groups”](#) on page 135
- [“Managing cluster storage with reports”](#) on page 136
- [“Tracking activity using reports”](#) on page 136

Tracking VCS agents across the enterprise with reports

Tracking VCS agents across the enterprise can be done through the following reports:

- [“Tracking agents by cluster using the Agent Inventory report”](#)
- [“Tracking agents by name using the Agent Usage report”](#)

Tracking agents by cluster using the Agent Inventory report

The Agent Inventory report contains information about installed VCS agents on each selected cluster. This information is acquired by reading the agent information file transmitted to the management server during the cluster snapshot operation. If the cluster does not contain any agent information files (typically any VCS version other than 4.0 on Solaris. All others require a special information file generation utility), the report states that no information is available. Agent information includes: name, version, minimum VCS version, agent type (script or DLL), vendor, files installed with the agent, and nodes on which the agent is installed.

- Objects of Interest: Clusters
- Uses Historical Data: No
- Uses Maintenance Windows: No

Tracking agents by name using the Agent Usage report

The Agent Usage report displays a summary of all agents installed on the selected clusters.

- Objects of Interest: Clusters
- Uses Historical Data: No

- Uses Maintenance Windows: No

The top of the report shows summary of all the installed agents on the cluster. Clicking on the navigation link of an agent takes you to summary area for that agent.

For each agent, you can view the cluster name, platform, VCS version number, and the groups containing resources of that type.

Managing cluster configurations with reports

Managing cluster configurations can be done through the following reports:

- [“Reporting cluster basics using the Cluster Inventory report”](#)
- [“Finding cluster configuration problems using the Configuration Analysis report”](#)
- [“Reviewing cluster attributes using the Cluster Attribute report”](#)
- [“Reviewing group attributes using the Group Attribute report”](#)
- [“Reviewing resource attributes using the Resource Attribute report”](#)
- [“Tracking cluster IP’s using the Virtual IP Usage report”](#)

Reporting cluster basics using the Cluster Inventory report

The Cluster Inventory report shows a variety of configuration information about the selected clusters. Ideally, this report will be used in a fashion similar to a run book. Information displayed about the selected clusters includes: operating system, VCS version number, cluster IP address, cluster UUID, cluster notification list, wide area connection information, enabled feature options, and the VCS mode of the cluster. The table describes additional information about each cluster, including: systems in the cluster, nodes ID of each system, license type, processor type, operating system, and system information string.

- Objects of Interest: Clusters
- Uses Historical Data: No
- Uses Maintenance Windows: No

Finding cluster configuration problems using the Configuration Analysis report

The Configuration Analysis report analyzes configuration aspects of the selected cluster and its groups, and reports on a number of possible configuration problems. For each configured cluster and group within the cluster, the report displays the state of the object at the time the report is run.

- Objects of Interest: Clusters
- Uses Historical Data: No
- Uses Maintenance Windows: No

The top of the report is a summary chart displaying all the configured clusters and groups along with the number of errors and warnings generated.

The report performs a series of tests on the configuration. Each test results in one of four possible verdicts:

- PASSED - The configuration is within the realm of normalcy.
- FAILED - There is something wrong with the configuration.
- WARNING - An aspect of the configuration is suspect, but not necessarily wrong.
- UNKNOWN - Configuration information pertaining to the test is unavailable.

Underneath the results for each test, the report will, when possible, display a chart of information detailing results of subtests used to reach the verdict of the test.

Tests performed on a cluster:

- Ensures that OS versions are consistent across nodes, local and remote.
- Ensures that ClusterService group has its Tag attribute set to "CSG" if it contains the connector resource (wac).
- Ensures that notifier and VRTSWebApp resources (if part of ClusterService) are set to non-critical, and have OnlineRetryLimit set to some non-zero value.
- Ensures that there are at least two private heartbeats configured and operational.
- Ensures that heartbeats are defined for each remote cluster.

Tests performed on a group:

- Ensures that resources that are "Persistent" or "OnOnly" do not have child resources.
- Validates resource dependencies (IP above NIC, etc.).
- Verifies the system list. Checks that each system in the system list exists, is online, and is not faulted. Displays the results in a chart.
- Verifies remote system list. Checks that each system in the remote system list exists, is online, and is not faulted. Displays the results in a chart.

- Verifies that auto-start is set for the group. If auto-start is not set, this is not a failure but is a warning.
- Verifies that the group is not frozen on any of the nodes.
- Verifies that the MAC address is consistent with the NIC resource.
- Verifies that MountV resources refer to an actual VMDg resource.
- Verifies that a global cluster group ClusterList is a subset of the cluster's ClusterList.
- Verifies that a global cluster group has the same name as its remote counterpart.
- Verifies that only one group in a global cluster (local or remote) has the “authority” attribute set. (Both groups with authority is evidence of a takeover.)
- Verifies that systems in a group's remote system list are configured in clusters listed in the ClusterList.

Reviewing cluster attributes using the Cluster Attribute report

The Cluster Attribute report requires the user to select clusters and cluster attributes on which to report. The report output displays the current value of these attributes for each of the selected clusters. Each cluster is represented as a single row in the resulting table of attributes, which includes the cluster name and the values of the selected attributes. Clusters have attributes such as configuration, major and minor versions, and VCS mode.

- Objects of Interest: Clusters
- Uses Historical Data: No
- Uses Maintenance Windows: No

Reviewing group attributes using the Group Attribute report

The Group Attribute report requires the user to select groups and group attributes on which to report. The report output displays the current value of these attributes for each of the selected groups. Each group is represented as a single row in the resulting table of attributes, which includes the group name and the values of the selected attributes. Groups have attributes such as system list, state, whether or not the systems in the group are enabled, and number of retries.

- Objects of Interest: Groups
- Uses Historical Data: No

- Uses Maintenance Windows: No

Reviewing resource attributes using the Resource Attribute report

The Resource Attribute report requires the user to select resources and resource attributes on which to report. The report output displays the current value of these attributes for each of the selected resources. Each resource is represented as a single row in the resulting table of attributes, which includes the resource name and the values of the selected attributes. Resources have attributes such as state, critical/non-critical, last resource online, and resource flags.

- Objects of Interest: Resources
- Uses Historical Data: No
- Uses Maintenance Windows: No

Tracking cluster IP's using the Virtual IP Usage report

The Virtual IP Usage report displays all virtual IP addresses that are in use for resources in the selected clusters. For each IP address, a table provides the associated group, resource, node, subnet mask, and MAC address.

- Objects of Interest: Cluster
- Uses Historical Data: No
- Uses Maintenance Windows: No

Analyzing failures for trends, patterns, and problem areas

Analyzing failures for trends, patterns, and problematic can be done through the following reports:

- [“Reviewing cluster failures using the Failure Summary report”](#)
- [“Reviewing cluster failures using the Failure Summary by Group report”](#)
- [“Reviewing faults using the Fault Trending Report”](#)

Reviewing cluster failures using the Failure Summary report

The Failure Summary report contains statistical information about resource failures. These statistics are gathered for each of the selected objects over the specified date range. A "failure" in this report refers to any offline status, either because of a fault or manual command. The report shows failures by resource type, failures by node, failures by group, plus min/max/average time to recover.

- Objects of Interest: Clusters

- Uses Historical Data: Yes
- Uses Maintenance Windows: No

Reviewing cluster failures using the Failure Summary by Group report

The Failure Summary by Group report contains statistics about resource failures. These statistics are gathered for each of the selected objects over the specified date range. A "failure" in this report refers to any offline status, either because of a fault or manual command. The report shows failures by resource type, failures by node, failures by specific resource, plus min/max/average time to recover.

- Objects of Interest: Group
- Uses Historical Data: Yes
- Uses Maintenance Windows: No

Reviewing faults using the *Fault Trending Report*

The Fault Trending report displays fault statistics for each resource type. A "fault" in this report refers to faulted resource types. For a given resource type, the faults per week and faults per resource numbers can help you locate possible fault trends.

- Objects of Interest: Resource Type
- Uses Historical Data: Yes
- Uses Maintenance Windows: No

The top of the chart shows a pie chart, which accounts for the percent of resource types that faulted over the specified time.

The histochart shows the resource type faults over the course of time.

When you hover your mouse over any given area in the pie chart or any of the graphs, you will get additional information. For example, if you hover your mouse over an area in the pie chart, fault percentages are presented. For example, if an area shows 40 percent, that means the resource type has faulted 40 percent of the time. If you hover your mouse over an area of a graph, the total number of faults for a given day are presented. In the graph, if more than one color is represented in a day, those colors represent the number of resource type faults for that day.

Managing and reporting uptime of service groups

Managing and report uptime of service groups can be done through the following reports:

- [“Reviewing uptime statistics using the Uptime Analysis report”](#)
- [“Reviewing Schedule Information using the Current Schedules report”](#)

Reviewing uptime statistics using the Uptime Analysis report

The Uptime Analysis report provides information on the amount of time an object is accessible to a user. You can report down to the group level, and you have the option to specify which resources within a group affect the overall uptime calculation. You can exclude non-critical resources from uptime calculations.

- Objects of Interest: management servers
- Uses Historical Data: No
- Uses Maintenance Windows: Yes

The top of the report shows the group name and uptime percentage. If you click a linked group name, you are taken to the uptime information for that group.

The first graph includes the overall uptime information for the service group and maintenance window information. The next graph shows uptime information for each resource in the group. When you hover your mouse over any given area in a graph, you see additional information. For example, if you hover your mouse over a green area, you see information about how long that particular group or resource is online.

If you have scheduled maintenance windows, they are not calculated as downtime, because they have been defined.

See [“Creating and deleting maintenance windows”](#) on page 79.

See [“Assigning and unassigning maintenance windows”](#) on page 94.

A legend follows each graph so you can determine the various states of each group and its resources. The following describes the various states:

- green - online
- light grey - offline
- red - faulted
- light yellow - partial
- light blue - coming up
- dark yellow - faulting
- unknown - dark blue

- dark grey - maintenance

Following the graph is a chart, which represents the same information, plus online totals and total time for each group.

Note: All calculations are rounded to the next highest number. Anything less than 1% will not show in the chart. It is considered in the overall calculation, but it will not show as faulted.

Reviewing Schedule Information using the Current Schedules report

The Current Schedules report displays information about the schedules defined on the management server. All objects associated with these schedules are displayed. Schedules include: name, description, start date, type of schedule, whether or not it is enabled, whether or not it is periodic, the duration, repeat parameters, specific dates, and assigned objects.

- Objects of Interest: management servers
- Uses Historical Data: No
- Uses Maintenance Windows: No

Managing cluster storage with reports

Cluster storage can be managed using the Storage report. The Storage report displays information on the DiskRes, Mount, VMDg, and MountV resources for each selected cluster. The information gathered includes disk signatures, mount paths, VM disk group names, volume names, mount points, and cluster platforms.

- Objects of Interest: Clusters
- Uses Historical Data: No
- Uses Maintenance Windows: No

Tracking activity using reports

Tracking activity can be done through the following reports:

- [“Reviewing cluster activity using the Cluster Activity report”](#)
- [“Reviewing group activity using the Group Activity report”](#)
- [“Reviewing resource activity using the Resource Activity report”](#)

Reviewing cluster activity using the Cluster Activity report

The Cluster Activity report collects the list of all event information (if events are configured to be transmitted to the management server) that define changes made to selected clusters over a specified period of time.

Note: By default, only error-level event messages are sent to the management server; this report output may have a small number of event entries.

- Objects of Interest: Clusters
- Uses Historical Data: Yes
- Uses Maintenance Windows: No

Reviewing group activity using the Group Activity report

The Group Activity report collects the list of all event information (if events are configured to be transmitted to the management server) that define changes made to selected groups over a specified period of time.

Note: By default, only error-level event messages are sent to the management server; this report output may have a small number of event entries.

- Objects of Interest: Groups
- Uses Historical Data: Yes
- Uses Maintenance Windows: No

Reviewing resource activity using the Resource Activity report

The Resource Activity report collects the list of all event information (if events are configured to be transmitted to the management server) that define changes made to selected resources over a specified period of time.

Note: By default, only error-level event messages are sent to the management server; this report output may have a small number of event entries.

- Objects of Interest: Resources
- Uses Historical Data: Yes
- Uses Maintenance Windows: No

Understanding report types by functionality

Administering notification

This chapter includes the following topics:

- [Events, policies, and notifications](#)
- [Notification settings](#)
- [Configuring SNMP consoles to receive traps](#)
- [Viewing a list of policies](#)
- [Viewing policy details](#)
- [Creating a policy](#)
- [Editing a policy](#)
- [Deleting a policy](#)
- [Disabling a policy](#)
- [Enabling a policy](#)
- [Exporting policies](#)
- [Importing policies](#)

Events, policies, and notifications

The Cluster Management Console monitors clusters, generates events, and responds to events by sending notifications or performing an action. Cluster problems or changes in cluster configuration or state can cause the notifier to generate an event and initiate a response.

The Cluster Management Console enables you to create and configure notification *policies*. The notifier uses policies to determine how it responds to an event. The process occurs in three steps:

- The notifier generates events when it receives cluster status updates that indicate problems or issues of sufficient severity.
- The notifier evaluates the events against the conditions specified in all policies.
- For each policy condition that is met, the notifier performs the response specified in the policy.

The notifier can respond to events by sending SNMP traps, by sending e-mails or by running custom scripts.

You must be a user with the role of management server administrator to create notification policies. Management server administrators can also view, edit, or delete their own policies or those created by other administrators. All configured policies are in effect at all times regardless of the administrator that created them.

You must specify the following conditions in a policy configuration:

- Object type condition
Specifies the type of cluster objects to which the policy applies. The available object types are:
 - cluster
 - service group
 - system
 - resource and associated resources and systems.
- Filter condition
Specifies the object filters. It is based on the object type you have selected. The available filter conditions are:
 - All objects
 - A list of objects that you specify
 - A list of operating systems that you specify, if the object type is service group
 - A list of resource types that you specify, if the object type is resource

- **Event condition**

Specifies the events to which the policy applies. The possible events vary by cluster object. If you do not specify an event condition, the policy applies to all events. The following is a list of all events that the notifier can monitor:

 - Cluster events**
 - Cluster faulted
 - Cluster exited
 - Cluster joined
 - System events**
 - System exited
 - System joined
 - System faulted
 - System in jeopardy
 - Resource events**
 - Resource Faulted
 - Resource Monitor timed out
 - Resource Offline ineffective
 - Resource in admin wait
 - Resource restarting
 - Resource Offline
 - Resource state unknown
 - Service group events**
 - Group Offline
 - Group concurrency violation
 - Group Partial Online
 - Initiated Group Offline
 - Group Online
 - Group Fault
 - Initiated Group Online
- **Severity condition**

Specifies the event severities to which the policy applies. The available severities of an SNMP event are:

 - Critical
 - Error
 - Warning
 - Information.

If you do not specify an event severity, the policy applies to events of all severities.

Notifications are recorded in a log, which is stored in the management server database. You can view a table of log entries for notifier events. Each log entry is a response to a notifier-generated event.

To navigate to the notifier log entries

- 1 On the main tab bar, click **Notification**.
- 2 On the secondary tab bar, click **Logs**.

The **Notification Logs** table contains the log entries.

You can configure a policy to send SMTP e-mails or SNMP traps to specified recipients, such as your personal e-mail account or an SNMP console. You can also configure a policy to run a custom NTH script each time a qualifying event occurs.

Note: The notifier monitors only events generated by cluster objects configured under the local management server. You cannot write policies for remote management servers.

Configuring SNMP consoles to receive traps

The Cluster Management Console includes two SNMP-specific files: `cmc.mib` and `cmc_trapd`, which are created in `$MS_HOME/conf/snmp`.

The file `cmc.mib` is the textual MIB for built-in traps supported by the Cluster Management Console. Load this MIB into your SNMP console to add it to the list of recognized traps.

The file `vad_trapd` is specific to the HP OpenView Network Node Manager (NNM) SNMP console, and includes sample events configured for the built-in SNMP traps supported by the Cluster Management Console. To merge these events with those configured for SNMP traps, type the following on the system running the HP OpenView Network Node Manager:

```
xnmevents -merge cmc_trapd
```

When you merge events, the SNMP traps sent by the Cluster Management Console notifier are displayed in the HP OpenView NNM SNMP console.

Note: For more information on `xnmevents`, see the HP OpenView documentation.

Notification settings

The notification system enables you to receive the notifications that are important to you even when you are not using the Cluster Management Console. You can set the notifier to send SMTP e-mails and SNMP traps to both an SMTP and SNMP recipient. The SMTP recipient is e-mail account, and the SNMP recipient is usually an SNMP systems management console, most likely at a remote location. You must provide valid settings for both recipients.

To specify settings for the SMTP recipient

- 1 On the main tab bar, click **Notification**.
- 2 On the secondary tab bar, click **Settings**.
- 3 In the **Notification Settings** view, in the **Configuration** task panel, click **Edit SMTP Settings**.
- 4 In the **Edit SMTP Settings** dialog box, specify the following information:
 - **SMTP Server** - Specify the fully-qualified SMTP server name to use for outgoing e-mail notifications.
 - **Secondary SMTP Server** - Specify an alternate SMTP server to use if the main server specified in **SMTP Server** is not available.
 - **SMTP From Path** - Specify the text to use for the from path of e-mail headers.
 - **SMTP Return Path** - Specify the text to use for the return path of the e-mail header. Failure e-mail is sent to this path.
 - **SMTP Server Timeout** - Specify the connection time-out for both the main and secondary SMTP servers.
 - **Default Email Address** - Specify a recipient e-mail address to configure by default when creating a policy. You can specify one or more other addresses when creating a policy.
If no email addresses are specified in a policy, the default e-mail address is not used.
 - **Send VRFY command to validate users** - Check this option to attempt to validate the default e-mail address or the addresses specified in policy configurations.
- 5 Click **OK**.

To test the SMTP settings

- 1 On the main tab bar, click **Notification**.
- 2 On the secondary tab bar, click **Settings**.

- 3 In the **Notification Settings** view, in the **Configuration** task panel, click **Test SMTP Settings**.
- 4 In the **Test SMTP Settings** dialog box, choose to send an e-mail or to activate a notification policy.
- 5 Depending upon your selection in step 4, do one of the following:
 - Specify a recipient e-mail address for the test notification.
 - Select a notification policy from the list.
- 6 Click **OK**.

To specify settings for the SNMP recipient

- 1 On the main tab bar, click **Notification**.
- 2 On the secondary tab bar, click **Settings**.
- 3 In the **Notification Settings** view, in the **Configuration** task panel, click **Edit SNMP Settings**.
- 4 In the **Edit SNMP Settings** dialog box, specify the following information:
 - **SNMP Community** - Specify the community property for SNMP traps. The default community is **public**.
 - **SNMP trap port** - Specify the UDP port of the SNMP manager that you intend to receive the SNMP traps. The default port is **162**.
 - **Default SNMP Console** - Specify a system name or IP address of a system that hosts an SNMP management console. You can select one or more other consoles when creating a policy.
If no consoles are specified in a policy, the default SNMP console is not used.
- 5 Click **OK**.

Viewing a list of policies

The Notification Policies view (default view under the Notification tab) contains a list of all policies defined in the management server database.

In the Notification Policies table, each row represents one policy. Each column contains the following specific policy information:

- Name- name of the policy.
- Clusters - the clusters that contain objects to which the policy applies
- Scope - the objects to which the policy applies; either all objects, or one object type

- State - status of the policy, either enabled or disabled
- Description - user-authored description text

To view the list of policies

- ◆ On the main tab bar, click the **Notification**, and then click **Policies**.
This action takes you to the **Notification Policies** view, which contains the **Notification Policies** table.

Viewing policy details

Policy details are a record of the selections made during the most recent run of the Notification Policy Configuration wizard. This wizard is used in creating and editing a policy. You can view policy details in the Notification Policy Details view.

To navigate to the Notification Policy Details view

- 1 On the main tab bar, click the **Notification**, and then click **Policies**.
- 2 In the **Notification Policies** view, click a linked policy name in the **Notification Policies** table.

The **Notification Policy Details** view shows the settings for name, enabled or disabled status, description, cluster selection, object selection, event selection, recipients, and the code for the custom script, if any.

Creating a policy

Policies are created using a single wizard. You can create new policies in the Notification Policies view.

To create a policy

- 1 On the main tab bar, click the **Notification**, and then click **Policies**.
- 2 In the **Notification Policies** view, in the **Configuration** task panel, click **Add Notification Policy**.
- 3 In the **Notification Policy Configuration** wizard, click **Next**.
- 4 At the **Enter a Name and Description** step, do the following and then click **Next**:
 - Type a name and a description for the policy into the appropriate boxes.

For names, the character limit is 50 and it should start with a letter. The name box does not accept special characters, except for '_' (underscore) and '-' (em-dash).

For descriptions, the character limit is 250, and special characters are allowed.

- In the **Create Policy For** list box, select the object type to which the policy applies.
You can make only one selection from the **Create Policy For** list box. If you want the policy to apply to more than one object type, you can select **Service Groups and associated Resources and Systems**.
- 5 At the **Cluster Selection** step, click either **All Clusters** or **Selected Clusters**. If you click **Selected Clusters**, the wizard presents a list of clusters; check the clusters you want. Click **Next**.
- 6 At the **Object Selection** step, click either **All <objects>** or **Selected <objects>**, where *<Object>* and *<objects>* are the object type you selected in step 3. If you click **Selected <objects>**, the wizard presents a list of those objects; check the objects you want. Click **Next**.
- 7 At the **Event Selection** step, click **All Events**, **Selected Events**, or **Events with Selected Severities**. If you click **Selected Events** or **Events with Selected Severities**, the wizard presents a list of events or severities; check the events or severities you want. Click **Next**.
- 8 At the **Notification Recipients** step, specify the e-mail addresses and SNMP consoles (console host name or IP address) that you want to receive notifications. Click a + (plus) button to add a recipient; click a recipient and then click a - (minus) button to remove a recipient. If you want the policy to run a custom script upon notification, specify the fully qualified path name and script name. Click **Next**.
- 9 At the **Override Default Settings** step, you may click **Next** to continue and modify the default settings specified in the **Notification Settings** view, or click **Finish**. See “[Notification settings](#)” on page 143 for information on default settings.

Editing a policy

Editing a policy involves using the same wizard that creates a policy. You can edit a policy in the Notification Policy Details view.

To edit a policy

- 1 On the main tab bar, click the **Notification**, and then click **Policies**.
- 2 In the **Notification Policies** view, click a linked policy name in the **Notification Policies** table.
- 3 In the **Notification Policy Details** view, in the **Configuration** task panel, click **Edit Notification Policy**.
- 4 In the **Notification Policy Configuration** wizard, follow each step exactly as described in “[Creating a policy](#)” on page 145.

Deleting a policy

You can delete policies in the Notification Policy Details view.

To delete a policy

- 1 On the main tab bar, click the **Notification**, and then click **Policies**.
- 2 In the **Notification Policies** view, click a linked policy name in the **Notification Policies** table.
- 3 In the **Notification Policy Details** view, in the **Configuration** task panel, click **Delete Notification Policy**.
- 4 In the **Delete Notification Policy** dialog box, click **OK**.

Disabling a policy

If the notifier is currently evaluating all events against the conditions in a policy, the notifier is *enforcing* that policy, and that policy is *enabled*. Policies are enabled by default after creation.

If you don't want the notifier to enforce a policy but also do not want to delete the policy configuration, you can disable the policy. The configuration for a disabled policy exists, but the notifier does not enforce the policy. You can disable a policy in the Notification Policy Details view.

To disable a policy

- 1 On the main tab bar, click the **Notification**, and then click **Policies**.

- 2 In the **Notification Policies** view, click a linked policy name in the **Notification Policies** table.
- 3 In the **Notification Policy Details** view, in the **Operations** task panel, click **Disable Notification Policy**.
- 4 In the **Disable Notification Policy** dialog box, click **OK**.

Enabling a policy

Policies are initially enabled after creation, and can be manually disabled. You can re-enable a disabled policy in the Notification Policy Details view.

To enable selected policies

- 1 On the main tab bar, click the **Notification**, and then click **Policies**.
- 2 In the **Notification Policies** view, click a linked policy name in the **Notification Policies** table.
- 3 In the **Notification Policy Details** view, in the **Operations** task panel, click **Enable Notification Policy**.
- 4 In the **Enable Notification Policy** dialog box, click **OK**.

Exporting policies

Policies can be exported to an .xml file on the management server. These files can be viewed or downloaded to other locations. They can also be imported to any other Cluster Management Console management server. You can export all currently configured policies in the Notification Policies view.

You cannot export single policies or selected policies. If you want to export only one or selected policies to another management server, you can import all policies from the .xml file and then delete unwanted policies individually on the destination management server.

To export policies

- 1 On the main tab bar, click the **Notification**, and then click **Policies**.
- 2 In the **Notification Policies** view, in the **Configuration** task panel, click **Export Notification Policies**.
The console presents the standard file download or file save dialog box that is native to your operating system.
- 3 In the dialog box, specify destination path in which to create the exported .xml file and click **OK**.

Importing policies

Policies that were previously exported to an .xml file can be imported into a management server. Use the export and import tasks to quickly create the same policies on several management servers. You can import policies in the Notification Policies view.

To import policies

- 1 On the main tab bar, click **Notification**.
- 2 On the secondary tab bar, click **Policies**.
- 3 In the **Notifications:Policies** view, in the **Configuration** task panel, click Import **Notification Policies**.
- 4 In the **Import Notification Policies** dialog box, specify a file to import. Enter a path and file name for the .xml file into the **Select File** box, or search for the file by clicking the **Browse** button.
- 5 Check the **Discard Duplicate Policies** option if you want to avoid creating redundant policies in the database, and then click **OK**.

Note: You cannot import Global-type policies originally created in CommandCentral Availability because the Cluster Management Console does not support this policy type.

Searches

This chapter includes the following topics:

- [About the search feature](#)
- [Conducting a search](#)

About the search feature

The Cluster Management Console offers a search feature that enables you to find every item and object that can be presented in the Cluster Management Console. The search feature retrieves data from the management server database. Search results are restricted by user roles; the search feature returns only those results that your user role permits you to view. See [“User accounts and user authentication”](#) on page 23 for more information.

Conducting a search

The search feature uses text-based comparison. You can perform a search using either the search bar or the Search tab.

The search bar is located immediately below the main tab bar, and contains a text entry box and a Search button. (You may need to scroll right to see these controls on some systems.) The search bar is available for all views except those under the Search tab.

The Search tab is located on the main tab bar. Views under the Search tab contain a text entry box and a Search button and offer some filtering options that the search bar does not.

The search feature displays results in one or more of the search views, which you navigate to using secondary tabs under Search. These tabs are labeled Clusters, Groups, Systems, Resources, Resource Types, and Logs. Each tab contains a table that lists the search results, or *hits*, in the corresponding object category. By default, the console takes you to the search views after each search. The destination view is whichever view was most recently visited.

Searches are limited to text strings. Separate two or more strings using a space character. The search feature supports a form of Boolean AND and OR operations, as well as “wildcard” searches, with the Exact Match and Match All Terms options. The search feature does not currently support:

- Direct textual entry of Boolean operators
- Direct textual entry of wildcards
- Query expressions

To perform a search using the search bar

- 1 In the text entry box, type one or more text strings that you want to find. Use a space character to separate text strings.
- 2 Click **Search**.
- 3 Visit each search view to see the hits in each object category.

Your particular destination view depends on which search view was most recently visited. Click the other secondary tabs (**Clusters, Groups**, and so on) to visit the other search views.

To perform a search using the Search tab

- 1 On the main tab bar, click **Search**.
- 2 On the secondary tab bar, click the object category (**Clusters, Groups**, and so on) in which you want to begin your search.
- 3 In the text entry box, type one or more text strings that you want to find. Use a space character to separate text strings.
- 4 Check one or more of the following options and then click **Search**:

- **Exact Match**

Requires each search result to match at least one whole search string. This option excludes occurrences in which a search string is part of a longer string.

- **Match All Terms**

Requires each search result to match all search terms (strings). The behavior of this option depends on the setting of the **Exact Match** option according to the following example: Consider object1 with attribute path = /tmp/f3 and object2 with attribute path = /tmp/f4:

Search String	Exact Match Option Setting	Match All Terms Option Setting	Search results
path f3	checked	checked	none
path f3	checked	cleared	none
path f3	cleared	checked	object1
path f3	cleared	cleared	object1, object2

- **Highlight**

Highlights the string occurrences in the search result tables. Combine **Exact Match** and **Match All Terms** to minimize the number of candidate occurrences.

- 5 Visit each search view to see the hits in each object category. Your first results are displayed in the same view in which you started the search. Click the other secondary tabs (**Clusters, Groups**, and so on) to see any hits the other search views.

Note: After you perform a search, changing the Exact Match, Match All Terms, and Highlight option settings automatically updates the results.

Administering the database

This chapter includes the following topics:

- [Viewing information about the database](#)
- [Pruning the database](#)
- [Backing up the database](#)
- [Restoring the database from a backup](#)
- [Modifying guest access to the database](#)

Viewing information about the database

The Administration: Management Server Database view contains information about the Cluster Management Console management server database. The management server database is a repository of data for all cluster objects (such as clusters, service groups, and resources) and all management server objects (such as users, tags, and report jobs).

Information in the Administration: Management Server Database view includes:

- Database Status
 - Creation date - Date the database was first created.
 - Database name - Name of the database.
 - Database path - Physical location (full directory path) of the database on disk.
 - Date of last successful backup - Date of the most recent successful backup of the database.
 - Last backup file - Name of the most recent backup file.
 - Oldest log - Date of the oldest event entry in the database.
 - Oldest report output - Date of the oldest report output in the database.
 - Server name - Name of the database server process.
 - Size, allocated - Physical space reserved for the database (in MB).
 - Size, used (approximate) - Actual size of the database (in MB).
 - Space on volume, available - Space remaining on the volume on which the database file was installed.
 - Status of current backup - Outcome of most recent backup of the database.
 - Status of current prune - Outcome of most recent prune of the database, including the number of records deleted if successful.
- Database Guest Access
 - Guest access - Indicates whether guest access is enabled or disabled.
 - Guest account name - User name of an account with guest database access.
- Database Server Information
 - IP Address: Port - IP address and port number of the database server process.
 - Server name - Name of the database server process.
 - Server version - Version of the database server process.

Pruning the database

You can prune or remove historical information from the database and reduce the database size. The pruning task allows you to remove all object types, report outputs only, or event entries only, created within a certain time period, from the database. The time period can be either the life of the database, or from the beginning through some number of years, months, weeks, or days ago.

To prune the database

- 1 In the **Administration: Management Server Database** view, in the **Operations** task panel, click **Prune the database**.
- 2 In the **Select the historical data to be removed** dialog box, use the **Type of Data** drop-down menu to select the type of data you want to remove. The following types are available:
 - **Cluster data**
This option specifies historical cluster data. Historical cluster data includes: (1) cluster and management server objects that have been deleted by the user, and (2) historical attribute and tag values. The current values of attributes and tags are *not* removed.
 - **Report outputs only**
This option specifies report outputs, *not* the associated report jobs.
 - **Log entries only**
This option specifies log entries only, but includes all entries and does not discriminate based upon the object or event that generated the entry.
- 3 Specify a time interval by selecting one of the two options under **Starting with oldest data, remove** and then click **OK**.
To clear all historical cluster data, select the first option, which is labeled **all data through today**. To select a specific time interval, select the second option, which is set to **1 year** by default. If desired, enter a different number in place of **1** and then select **year, month, week, or day** from the drop-down menu.
Time intervals begin at the date when the oldest data was stored and end at a later date that is specified by the length of the interval. For example, assume that you enter the number **2** and select **month**. The database is pruned beginning with the *oldest* data and ending with data stored two months after the oldest data. If the oldest data was stored on January 1, and the most recent data was stored on May 1, the data stored between January 1 to March 1 is pruned.
- 4 When asked to confirm that you want to prune the database, click **OK**.

When the pruning operation is finished, the management server updates the **Status of current prune** value in the **Database Status** table. This value also indicates whether the prune was successful and the number of records deleted.

Backing up the database

Backing up the database is necessary so that crucial configuration and historical information can be recovered in the event of a failure. You can back up the database using the Cluster Management Console or the CLI. During the backup task, an archived copy of the database file and the associated transaction log file are backed up to a physically separate location. This location can be a tape drive or a disk drive.

To backup the database to a file

- 1 In the **Administration: Management Server Database** view, in the **Operations** task panel, click **Backup database to a file**.
- 2 In the **Enter a valid directory or tape drive on the server** dialog box, enter a file name and an *existing* directory path on the management server. If the directory path you specify does not exist, the database backup command does not create it.
- 3 Click **OK**.

To backup the database to a file using the command line

- ◆ `# gadb -backup -to archive`
This command saves a backup copy of the database file and the transaction log file. The database is backed up to the directory path and archive file name specified by *archive*. The transaction log is saved to the \Log directory in the installation directory.

Restoring the database from a backup

Restoring the database from a backup returns the database to the state it was in when the backup was performed. The restoration task restores the database file and the associated transaction log file from an archive tape backup or archive disk backup.

Note: This feature can only be used from the command line.

To restore the database from a backup

```
◆ # gadbrestore -archive ArchiveFile -data DatabaseDataDir -log  
   DatabaseLogDir
```

This command restores the database from an archive previously saved using `gadb -backup -to archive`.

Modifying guest access to the database

The management server is preconfigured with a guest user account that can be used for external database access only. A management server administrator can enable this account. The guest user account name is CCAVAILGUEST and the password is set by the management server administrator when the account is enabled.

To modify guest access

- 1 In the **Administration: Management Server Database** view, in the **Configuration** task panel, click **Modify guest access**.
- 2 In the **Database Access for Guests** dialog box, select an action from the following options and then click **OK**.
 - **Enable database access**
Enables the guest user account for the database.
 - **Disable database access**
Disables the guest user account for the database.
 - **Change password**
Enables you to change the password for the guest user account for the database. If you select **Change password**, you must enter a valid database password and then confirm it.

Section



Appendixes

Command line interface

This chapter includes the following topics:

- [Introduction to the command line interface](#)
- [Notations for object names in the CLI](#)
- [Output options summary](#)
- [gaclus](#)
- [gaconf](#)
- [gadbd](#)
- [gadbrestart](#)
- [gagrpd](#)
- [galogin](#)
- [galogout](#)
- [gares](#)
- [gaserver](#)
- [gasys](#)
- [gatypd](#)
- [gauser](#)

Introduction to the command line interface

The command line interface (CLI) is a non-graphical user interface to the Cluster Management Console. You perform tasks in the CLI by entering commands, arguments, and options at your operating system command prompt. You must run CLI commands on a system running a management server.

You can use the CLI commands to obtain information and perform tasks on both management server objects and cluster objects. This chapter contains a reference of CLI commands and usage.

Both Unix and Windows platforms support the CLI. The following is a list of both management server and cluster objects and the CLI commands used to perform tasks upon them:

- Management servers -- gaserver, galogin, galogout
- Clusters -- gaclus
- Systems -- gasys
- Groups -- gagrp
- Resources -- gares
- Resource Types -- gatype
- Management server database -- gadb, gadbrestore
- Management server users -- gauser
- Cluster configurations -- gaconf

Note: You must log in to the management server before you can use the CLI. See “[galogin](#)” on page 182.

Notations for object names in the CLI

The following object notations are used in the -help options of CLI commands. The following table contains distinct notations that differentiate qualified object names from unqualified object names.

Table A-1 Generic object notations

Generic CLI Notations	Definition
[item]	Optional item
item...	A list of one or more items, separated by spaces.
<object-name>	Unqualified name of object. No parent specifications. For example, <clus-name> is a cluster name such as ClusNW43..
<object>	Qualified name of object. Includes parent specifications. For example, <clus> might be PersonnelMS:ClusNW43.
<qualified-name>	<server> <clus> <grp> <type> <sys> <res>

Table A-2 Generic object notations

Specific object CLI Notations	Doc Notation	Definition	Expansion
<server>	<i>server</i>	Management server name	server
<clus>	<i>cluster</i>	Cluster name	[server:]clus-name
<grp>	<i>grp</i>	Group name	[[server:]clus-name:] grp
<type>	<i>type</i>	Resource type name	[[server:]clus-name:] type
<sys>	<i>sys</i>	System name	[[server:]clus-name:] sys
<res>	<i>res</i>	Resource name	[[server:]clus-name:]res- name
<attr>	<i>attr</i>	Attribute name	attr-name

Use of qualified and unqualified names

You can refer to the `-help` option on any command for the exact options and object specifications required for that command. However, here are several rules for object specification that are true across commands and can be helpful to know.

- `<qualified-name> ::= <server> | <cluster> | <grp> | <type> | <sys> | <res>`
If the name is not *fully* qualified, the first object that matches the name is used.
- Limit the use of qualified names (such as `server:cluster:group`) to those command elements that require only one object. These elements include options such as `-value` and `-state`.
- For the `-list` and `-display` options, specify unqualified names only.
- For the `-display` option, you can specify a list of unqualified names. If specified, objects that have any one of the names are displayed. If you do not specify any names, all objects are displayed (subject to limits imposed by other options).

Output options summary

Commands that provide cluster object information as output usually offer the four output options described below. When available, the output options, `-list`, `-display`, `-value`, and `-state`, are the first options in the `-help` output for the command. Other command options are affect command operation and take action on cluster objects.

Table A-3 Output options

Option	What is displayed	What objects are chosen
<code>-list</code>	Lists all objects of the type, limited by the other options. Displays ancestors' names. For example, for groups, the group name, cluster name and management server names are displayed.	Objects may be filtered. If <code>-server <server></code> is given, only objects in that server are selected. If <code>-clus <cluster></code> is given, only objects in that cluster are selected, etc. A list table may be empty if the filter object name (server or cluster) does not exist.
<code>-display</code>	Displays all attributes of all the objects of the type, limited by the other options. For local attributes, values for all contexts are shown.	Objects may be filtered. If <code>-server <server></code> is given only these objects in that server is selected. If <code>-clus <clus-name></code> is given, only those objects in a cluster with the given name is selected, etc.
<code>-value</code>	Displays a single attribute value for a single object. If the attribute is local, the <code>-sys</code> option is required.	You specify exactly one object by giving a qualified name.
<code>-state</code>	Displays a single state value. If the attribute is local, the <code>-sys</code> option is required.	You specify exactly one object by giving a qualified name.

gaclus

NAME

gaclus - provides managed cluster information and operations

SYNOPSIS

```
gaclus -list [-server server]  
gaclus -display [cluster...] [-server server]  
gaclus -state [cluster...] [-server server]  
gaclus -value cluster attr  
gaclus [-help]
```

DESCRIPTION

The `gaclus` command provides various cluster information as requested, including parent information and attribute values. One administration option, `synchuser`, is available.

OPTIONS

```
-list [-server server]  
    Lists all clusters or only those clusters managed by the specified  
    management server.  
    No argument indicates all clusters managed by all management  
    servers.  
    [-server server] indicates clusters managed by management  
    server server.  
    The output includes a header row and one row for each cluster.  
    Each row contains the cluster name and its parent management  
    server name. The header looks like:  
    #Cluster  Server  
-display [cluster...] [-server server]  
    Displays all cluster attribute values for the specified clusters. You  
    can specify individual cluster names, clusters managed by a  
    particular management server, or all managed clusters.  
    No argument indicates clusters managed by all management  
    servers.  
    [cluster ...] is a list of one or more clusters.
```


`[-server server]` indicates all clusters managed by the management server *server*.

The output includes a header row and one row for each cluster. Each row contains the cluster name, parent management server name, attribute name, attribute scope, and attribute value. The header looks like:

```
#Cluster  Server      Attribute      Scope      Value
```

```
-state [cluster...] [-server server]
```

Displays the state of the specified clusters. You can specify individual cluster names, clusters managed by a particular a management server, or all managed clusters.

No argument indicates clusters managed by all management servers. The output lists the state values requested.

`[cluster ...]` is a list of one or more clusters.

`[-server server]` indicates all clusters managed by the management server *server*.

```
-value cluster attr
```

Displays the value of attribute *attr* on cluster *cluster*. The output is the single attribute value requested.

```
-help
```

Provides basic command usage information.

NOTES

EXAMPLES

List the clusters in the management server *qasite171*.

```
gaclus -list -server qasite171
```

```
#Cluster      Server
VCSCluster01  qasite171
Clus163_164   qasite171
```

Display the cluster attribute values for the cluster *Clus401_402*.

```
gaclus -display Clus401_402
```

```
#Cluster Server Attribute Scope Value
Clus401_402 MSHOU Administrators global admin
Clus401_402 MSHOU AllowNativeCliUsers global 0
Clus401_402 MSHOU ClusterLocation global
Clus401_402 MSHOU ClusterName global Clus401_402
Clus401_402 MSHOU ClusterOwner global
Clus401_402 MSHOU CompareRSM global 0
Clus401_402 MSHOU CounterInterval global 5
Clus401_402 MSHOU DumpingMembership global 0
Clus401_402 MSHOU EngineClass global RT
Clus401_402 MSHOU EnginePriority global
```

```
Clus401_402 MSHOU GUIAddress global none
Clus401_402 MSHOU GroupLimit global 200
Clus401_402 MSHOU HAConnectInterval global 5
Clus401_402 MSHOU HacliUserLevel global NONE
Clus401_402 MSHOU LastIAA global 0
Clus401_402 MSHOU LockMemory global ALL
Clus401_402 MSHOU LogSize global 33554432
Clus401_402 MSHOU MajorVersion global 2
Clus401_402 MSHOU MSConnectInterval global 5
Clus401_402 MSHOU MinorVersion global 0
Clus401_402 MSHOU Notifier global Host: none Queue: 30 Severity:
Information State: none
Clus401_402 MSHOU PanicOnNoMem global 0
Clus401_402 MSHOU PrintMsg global 0
Clus401_402 MSHOU ProcessClass global TS
Clus401_402 MSHOU ProcessPriority global
Clus401_402 MSHOU ReadOnly global 1
Clus401_402 MSHOU ResourceLimit global 5000
Clus401_402 MSHOU SourceFile global .\main.cf
Clus401_402 MSHOU State global 4
Clus401_402 MSHOU SysName global
Clus401_402 MSHOU SystemList global
Clus401_402 MSHOU TimeoutIAA global 180
Clus401_402 MSHOU TypeLimit global 100
Clus401_402 MSHOU UserNames global admin
Clus401_402 MSHOU VCSMode global VCS
Clus401_402 MSHOU VCSNotifierState global none
Clus401_402 MSHOU lastVCSLog global 1970-01-01T00:00:00.0Z
```

Display the value of the attribute ResourceLimit for the cluster VCSCluster01.

```
gaclus -value VCSCluster01 ResourceLimit
5000
```

SEE ALSO

gaconf

NAME

gaconf - provides configuration file operations.

SYNOPSIS

```
gaconf -makerw [cluster]  
gaconf -dump [-makero] [cluster]  
gaconf [-help]
```

DESCRIPTION

This command allows (1) change of configuration on the target cluster to read-write (-makerw), save of configuration changes to cluster main.cf file (-dump), and change of configuration to read-only (-dump -makero).

OPTIONS

-makerw
Makes the target cluster configuration read/write.

-makero
This option will make the configuration file read only.

-dump [-makero]
Saves and makes read-only.

-help
Provides basic command usage information.

NOTES

EXAMPLES

SEE ALSO

gadb

NAME

gadb - provides database information and operations

SYNOPSIS

```
gadb -grant CCAVAILGUEST [pwd]  
gadb -modify CCAVAILGUEST [pwd]  
gadb -revoke CCAVAILGUEST  
gadb -backup -to archive  
gadb -info  
gadb -prune DataType -oldest [Integer TimeUnit | -  
all]
```

DESCRIPTION

The `gadb` command provides pertinent information on the Cluster Server database. Operational commands, such as `backup` and `prune`, provide standard database administration. You can also grant, modify, or revoke access from an external guest account.

OPTIONS

```
-grant CCAVAILGUEST [pwd]  
    Gives the guest account (CCAVAILGUEST) access to the  
    database. pwd is the password you can specify for the account.  
-modify CCAVAILGUEST [pwd]  
    Modifies the guest account's password to the one specified.  
-revoke CCAVAILGUEST  
    Removes the guest account access to the database.  
-backup -to archive  
    Saves a backup copy of the database and the transaction log. The  
    database is backed up to the archive file archive, which includes  
    the file directory path. The transaction log is saved to  
    \CCAvailDb\Log\CCAvailDb.log under the installation  
    directory.  
-info
```

Provides detailed information on the database including name, size, location, backup status, prune status, and oldest record dates.

`-prune DataType -oldest [Integer TimeUnit | -all]`

Removes specified data from the database. You specify the type and age of data to remove. Data is always removed starting from the oldest data through the indicated time period.

DataType is either `Clusters`, `Log`, or `Rptout` and specifies the type of data to remove:

`Clusters` indicates to remove cluster historical data only. Log entries and report outputs (except for those associated with deleted report jobs) are not removed. Specifically, cluster historical data includes:

- Objects that have been deleted by the user including deleted cluster objects, deleted report jobs and their associated outputs.
- Historical values in the time period. This means that the latest values of attributes are not removed, even if in the specified time period.

`Log` indicates to remove log entries only.

`Rptout` indicates to remove report outputs only.

`-oldest [Integer TimeUnit | -all]`

Starting from the oldest data, remove data through the indicated time period, or specify all data.

Integer is the number of years, months, weeks, or days to remove.

TimeUnit is year, month, week, or day, corresponding to the *Integer* specified.

`-all` indicates to remove all data (over time) of the specified type.

NOTES

EXAMPLES

Display general information about the local Cluster Server database.

```
gadb -info
```

```
#Database Information
```

```
Database Status
```

Attribute	Value
Creation date	May 21, 2004 3:53:11 PM
Database name	CCAvailDb
Database path	C:\PROGRA~1\VERITAS\COMMAN~1\AVAILA~1\CCAVAI~1\Data

Date of last successful backup	Not available
Oldest log	May 21, 2004 3:45:40 PM
Oldest report output	May 22, 2004 6:00:03 PM
Server name	VERITAS_DBMS_HOUWIN407
Size, allocated	8.461MB
Size, used (approximate)	6.656MB
Space on volume, available	13,423.035MB
Status of current backup	Undefined
Status of current prune	Undefined

Database Guest Access	
Attribute	Value
Guest access	Disabled
Guest account name	CCAVALLGUEST

Database Server information	
Attribute	Value
IP Address:Port	10.141.11.107:2993
Server name	VERITAS_DBMS_HOUWIN407
Server version	2.00.028

SEE ALSO

[“gadbrestore”](#) on page 175

gadbrestore

NAME

gadbrestore - restores the database from an archive

SYNOPSIS

```
gadbrestore -archive archive file -data  
             DatabaseDataDir -log Database log dir
```

DESCRIPTION

The `gadbrestore` command restores the Cluster Server database from a previously saved archive.

OPTIONS

`-archive ArchiveFile`
ArchiveFile specifies the full path and file name of an existing database archive. This path and file name includes a .1 extension. If the database backup resulted in more than one archive file, other archive files with extensions .2, .3, and so on are in the same directory.

`-data DatabaseDataDir`
Specifies the directory of the CCAvailDb.db database that is to be restored from the archive.

`-log DatabaseLogDir`
Specifies the directory of an existing database transaction log.

NOTES

EXAMPLES

SEE ALSO

[“gadb”](#) on page 172

gagr

NAME

gagr - provides cluster group information and operations

SYNOPSIS

```
gagr -list [-clus cluster] [-server server]  
gagr -display [grp...] [-clus cluster] [-server  
    server]  
gagr -state [grp...] [-clus cluster] [-server  
    server]  
gagr -value grp attr [-sys sys]  
gagr -clearadminwait [-fault] grp -sys sysname  
gagr -clear grp [-sys sys]  
gagr -clear grp [-sys sys]  
    [-rclus cluster | -localclus]  
gagr -online grp -sys sys [-propogate]  
    [-ejectlowpri] [-force] [-nopre]  
    [-checkpartial sys]  
    [-rclus cluster]  
gagr -online grp -any [-force] [-ejectlowpri]  
    [-checkpartial sys] [-rclus cluster]  
gagr -online grp -sys sys [-force] [-nopre] [-  
    checkpartial sys] [-rclus cluster]  
gagr -online grp -any [-force] [-checkpartial sys]  
    [-rclus cluster]  
gagr -offline grp -sys sys [-ifprobed] [-force]  
gagr -offline grp -any [-ifprobed] [-force]  
gagr -switch grp [-to sys] [-torclus cluster]  
gagr -switch grp -any [-clus cluster]  
gagr -switch grp [-ejectlowpri] [-to sys]  
    [-torclus <cluster>]
```



```
gagrp -switch grp [-ejectlowpri] -any  
      [-torclus cluster]  
gagrp -freeze grp [-persistent]  
gagrp -freeze grp [-rclus cluster | -localclus]  
gagrp -unfreeze grp [-persistent]  
gagrp -enable grp [-sys sys]  
gagrp -disable grp [-sys sys]  
gagrp -enableresources grp  
gagrp -disableresources grp  
gagrp -flush grp -sys sys  
gagrp -autoenable grp -sys sys  
gagrp [-help]
```

DESCRIPTION

The `gagrp` command provides various group information as requested, including parent information and attribute values. Operational commands, such as `online`, `offline`, `switch`, `freeze`, and `enable`, take the same actions they do in VCS. These commands are forwarded to the VCS engine, and any limitations and errors returned are from VCS.

OPTIONS

```
-list [-clus cluster] [-server server]  
    Lists all groups, groups in a specific cluster, or groups managed by  
    a specific management server.  
    No argument indicates all groups managed by all management  
    servers.  
    [-clus cluster] indicates all groups in the cluster cluster.  
    [-server server] indicates all groups managed by the  
    management server server.  
    The output includes a header row and one row for each group. Each  
    row contains the group, parent cluster, and parent management  
    server names. The header looks like:  
    #Group Cluster Server  
-display [grp...] [-clus cluster] [-server server]
```

Displays all group attribute values for the specified groups. You can specify individual group names, groups in a specific cluster, or groups managed by a specific management server.

No argument indicates all groups managed by all management servers.

`[grp ...]` is a list of one or more groups.

`[-clus cluster]` indicates all groups in the cluster `cluster`.

`[-server server]` indicates all groups in the management server `server`.

The output includes a header row and one row for each group. Each row contains the group name, parent cluster name, parent management server name, attribute name, attribute scope, and attribute value. The header looks like:

```
#Group Cluster Server Attribute Scope Value
-state [grp...] [-clus cluster] [-server server]
```

Displays the state of the specified groups in all contexts (on all systems). You can specify group names, groups in a specific cluster, or groups managed by a specific management server.

No argument indicates all groups managed by all management servers.

`[grp ...]` is a list of one or more groups.

`[-clus cluster]` indicates all groups in the cluster `cluster`.

`[-server server]` indicates all groups managed by the management server `server`.

The output is the state values for all specified groups on all systems. The header looks like:

```
#Group Cluster Server Attribute System Value
The value under the Attribute header is always state.
-value grp attr [-sys sys]
```

Displays the value of attribute `attr` on the group `grp`. The output is the single attribute value requested.

`[-sys sys]` indicates a specific system `sys`; it is required for local attributes (which vary per system.) and not required for global attributes.

```
-clear grp [-sys sys]
```

Clears all faulted, non-persistent resources in the group `grp` on the system `sys`, or on all systems if no system is specified. Initiates a state change from `FAULTED` to `OFFLINE`, and automatically initiates an online process if one was previously blocked.

```
-online grp -sys sys [-force] [-nopre] [-checkpartial sys] [-
rclus cluster]
```

Starts the group *grp* and brings its resources online on the system *sys*.

- sys *sys* indicates the system where you want to bring the group online. Use either the -any or the -sys argument, not both.
- [-force] indicates to bring the group online for the first time or to override cluster authority.
- [-nopre] indicates that the group can be brought online (normally determined by the PreOnline event trigger).
- [-checkpartial *sys*] indicates to bring online only those resources already online on the system *sys*.
- [-rclus *cluster*] applies to global groups only; indicates to bring the group online on a system in the remote cluster *cluster*.

-online *grp* [-any [-force] [-checkpartial *sys*] [-rclus *cluster*]]
Starts the group *grp* and brings its resources online on any system in the cluster.

- any indicates to bring the group online on any system in the cluster. Use either the -any or the -sys argument, not both.
- [-force] indicates to bring the group online for the first time or to override cluster authority.
- [-checkpartial *sys*] indicates to bring online only those resources already online on the system *sys*.
- [-rclus *cluster*] applies to global groups only; indicates to bring the group online on a system in the remote cluster *cluster*.

-offline *grp* [-sys *sys*] [-ifprobed] [-force]
Takes the group *grp* offline on the system *sys*. Use either the -any or the -sys argument, not both.

- [-ifprobed] indicates to take the group offline only if all resources are probed (monitored to determine status) on the system.

-offline *grp* [-any [-ifprobed] [-force]]
Takes the group *grp* offline on any system. Use either the -any or the -sys argument, not both.

-switch *grp* [-to *sys*] [-torclus *cluster*]
Switches the group *grp* to the system *sys*, or, in the case of a global group, to the remote cluster *cluster*.

-switch *grp* [-any [-clus *cluster*]]
Switches the group *grp* to any system in cluster *cluster*.

-freeze *grp* [-persistent]
Freezes the group *grp* using the VCS freeze command.

- [-persistent] indicates to remember the frozen state when the cluster is rebooted.

-unfreeze *grp* [-persistent]

- Unfreezes the group `grp` using the VCS unfreeze command.
- `-enable grp [-sys sys]`
Enables the group `grp` on the system `sys` or on all systems. A group can be brought online only if it is enabled.
- `-disable grp [-sys sys]`
Disables the group `grp` on the system `sys` or on all systems. A group cannot be brought online or switched if it is disabled.
- `-enableresources grp`
Enables all resources of the group `grp`. A resource can be monitored only if it is enabled.
- `-disableresources grp`
Disables all resources of the group `grp`. A resource cannot be monitored if it is disabled.
- `-flush grp -sys sys`
Clears the internal state of VCS for the group `grp` on the system `sys`. Used when a group is waiting for a resource to come online.
- `-autoenable grp -sys sys`
Autoenables a group `grp` that is autodisabled on system `sys`. Groups are autodisabled until VCS probes all of the resources and determines if they are ready to bring online. You may need to autoenable a group in certain situations where VCS does not.
- `-help`
Provides basic command usage information.

NOTES

EXAMPLES

List all groups.

```
gagr -list
#Group      Cluster      Server
ClusterService Clus163_164  QaSite407
FSGRP1      Clus163_164  QaSite407
SQL_GRP     Clus163_164  QaSite407
SQL_GRP2    Clus163_164  QaSite407
CCAvail     Clus163_164  QaSite407
```

Display the state of all groups.

```
gagr -state
#GroupClusterServerAttributeSystemValue
AGroupSunClus1DiamondStateglobalOFFLINE
CCAvailSunClus1DiamondStatehousun7ONLINE
CCAvailSunClus1DiamondState housun9OFFLINE
ClusterServiceSunClus1DiamondState housun7 ONLINE
ClusterServiceSunClus1DiamondState housun9 OFFLINE
LfileSunClus1DiamondState housun7 ONLINE
```

```
LfileSunClus1DiamondState housun9 OFFLINE  
NBU_2SunClus1DiamondState housun7 PARTIAL  
NBU_2SunClus1DiamondState housun9 PARTIAL|STOPPING  
Oracle_1SunClus1DiamondState housun7 OFFLINE  
Oracle_1SunClus1DiamondState housun9 OFFLINE  
TestGrpSunClus1DiamondState housun7 OFFLINE  
TestGrpSunClus1DiamondState housun9 OFFLINE  
WfileSunClus1DiamondState housun7 OFFLINE  
WfileSunClus1DiamondState housun9 OFFLINE  
db2_GRPSunClus1DiamondState housun7 OFFLINE  
db2_GRPSunClus1DiamondState housun9 OFFLINE
```

SEE ALSO

galogin

NAME

galogin - provides a connection to the local management server

SYNOPSIS

```
galogin username domain domainType
        [-passfile "path to password file"]

galogin -help
```

DESCRIPTION

The galogin command provides a connection to the local management server, which includes user authentication. This command takes no options or arguments. The galogin command prompts the user for a user name, password, domain name, and domain type. If the responses are correct, the user is authenticated and connected to the management server.

OPTIONS

-help
Provides basic command usage information. Version and copyright information only for this command.

NOTES

EXAMPLES

Login to the local management server as the user “Administrator”.

```
galogin
Enter user name: root
Enter domain name: thor310.veritas.com
Enter domain type [ Windows | nis | nisplus | unixpwd | ldap ]:
unixpwd
Enter password:
Connecting to Management Server...
Login successful.
```

SEE ALSO

[“galogout”](#) on page 183

galogout

NAME

galogout - removes a connection to the local management server

SYNOPSIS

```
galogout [-help]
```

DESCRIPTION

The galogout command removes an existing connection and authentication on the local management server. This command takes no options or arguments.

OPTIONS

-help

Provides basic command usage information. Version and copyright information only for this command.

NOTES

EXAMPLES

Logout from the local management server.

```
galogout
```

```
Logout successful.
```

SEE ALSO

[“galogin”](#) on page 182

gares

NAME

gares - provides resource information and operations

SYNOPSIS

```
gares -list [-grp grp] [-clus cluster] [-server  
            server]  
gares -display [res-name...] [-grp grp] [-clus  
            cluster] [-server server]  
gares -state [res-name...] [-grp grp] [-clus  
            cluster] [-server server]  
gares -value res attr [-sys sys]  
gares -clear res [-sys sys]  
gares -online [-force] res -sys sys  
gares -offline [-ignoreparent] res -sys sys  
gares -refreshinfo res [-sys sys] [-rclus cluster]  
gares -flushinfo res [-sys sys] [-rclus cluster]  
gares -offprop [-ignoreparent] res -sys sys  
gares -probe res -sys sys  
gares -override res staticattribute  
gares -undo_override res staticattribute  
gares [-help]
```

DESCRIPTION

The `gares` command provides various resource information as requested, including parent information and attribute values. Operational commands, such as `online`, `offline`, and `probe`, take the same actions that they do in VCS. The commands are forwarded to the VCS engine, and any limitations and errors returned are from VCS.

OPTIONS

`-list [-grp grp] [-clus cluster] [-server server]`

Lists all resources, resources in a specific group, resources in a specific cluster, or resources managed by a specific management server.

No argument indicates all resources managed by all management servers.

`[-grp grp]` indicates all resources within the group *grp*.

`[-clus cluster]` indicates all resources within the cluster *cluster*.

`[-server server]` indicates all resources managed by the management server *server*.

The output includes a header row and one row for each resource. Each row contains the resource name, parent group, parent cluster, and parent management server names. The header looks like:

```
#Resource Group Cluster Server
```

`-display [res-name...] [-grp grp] [-clus cluster] [-server server]`

Displays all resource attribute values for the specified resources. You can specify individual resource names, resources in a specific group, resources in a specific cluster, or resources managed by a specific management server.

No argument indicates all resources managed by all management servers.

`[res-name ...]` is a list of one or more resources.

`[-grp grp]` indicates all resources in the group *grp*.

`[-clus cluster]` indicates all resources in this cluster *cluster*.

`[-server server]` indicates all resources managed by the management server *server*.

The output includes a header row and one row for each resource. Each row contains the resource name, parent group name, parent cluster name, parent management server name, attribute name, attribute scope, and attribute value. The header looks like:

```
#Resource Group Cluster Server Attribute Scope Value
```

`-state [res-name...] [-grp grp] [-clus cluster] [-server server]`

Displays the state of the specified resources in all contexts (on all systems). You can specify resource names, resources in a specific group, resources in a specific cluster, or resources managed by a specific management server.

No argument indicates all resources managed by all management servers.

[*res-name ...*] is a list of one or more resources.

[-*grp grp*] indicates all resources in the group *grp*.

[-*clus cluster*] indicates all resources in the cluster *cluster*.

[-*server server*] indicates all resources managed by the management server *server*.

The output is the state values for all specified resources on all systems. The header looks like:

```
#Resource Group Cluster Server Attribute System Value
```

The value under the **Attribute** header is always **state**.

-value *res attr* [-*sys sys*]

Displays the value of attribute *attr* on a resource *res*. The output is the single attribute value requested.

[-*sys sys*] indicates a specific system *sys*; it is required for local attributes (which vary per system) and not required for global attributes.

-clear *res* [-*sys sys*]

Clears the resource *res* on the system *sys*, or on all systems if no system is specified. Initiates a state change from `FAULTED` to `OFFLINE`, and automatically initiates an online process if one was previously blocked.

-online [-*force*] *res* -*sys sys*

Brings the resource *res* online on the system *sys*.

[-*force*] indicates to bring the resource online for the first time or to override cluster authority.

-offline [-*ignoreparent*] *res* -*sys sys*

Takes the resource *res* offline on the system *sys*.

[-*ignoreparent*] indicates to take the resource offline even if its parent resources in the group are online. This option does not work if taking the resources offline violates the group dependency.

-refreshinfo *res* [-*sys sys*] [-*rclus cluster*]

Updates the value of the ResourceInfo attribute for the resource *res* if the resource is online.

[-*sys sys*] indicates a system name other than local system(s).

[-*rclus cluster*] indicates a remote cluster.

If no system or remote cluster is specified, this occurs on local system(s) where the resource is online.

-flushinfo *res* [-*sys sys*] [-*rclus cluster*]

-offprop [-*ignoreparent*] *res* -*sys sys*

Takes the resource *res* offline and propagates the command to its children on the system *sys*.

`-probe res -sys sys`

Monitors the resource *res* on the system *sys* to determine its status.

`-help`

Provides basic command usage information.

NOTES

EXAMPLES

List all resources.

```
gares -list
```

#Resource	Group	Cluster	Server
webip	ClusterService	W2KClus121_122	QaSite181
VRTSweb	ClusterService	W2KClus121_122	QaSite181
FS_DISKRES	FS_TEST	W2KClus121_122	QaSite181
FS_FILESHARE	FS_TEST	W2KClus121_122	QaSite181
FS_IP	FS_TEST	W2KClus121_122	QaSite181
FS_LANMAN	FS_TEST	W2KClus121_122	QaSite181
FS_MOUNT	FS_TEST	W2KClus121_122	QaSite181
FS_NIC	FS_TEST	W2KClus121_122	QaSite181
CCAvail_ClusterConfig	CCAvail	W2KClus121_122	QaSite181
CCAvail_ClusterMonitor	CCAvail	W2KClus121_122	QaSite181

SEE ALSO

gaserver

NAME

gaserver - provides management server information and operations

SYNOPSIS

```
gaserver -list [-local]
gaserver -display [server...]
gaserver -state [server...]
gaserver -value server attr
gaserver -modify [-port portnumber]
gaserver -modify [-address ipaddress]
gaserver -rename name [-nocheck]
gaserver -add id name ipaddress [portnumber]
gaserver -delete server
gaserver -delete -id id
gaserver -delete [-local]
gaserver -listab
gaserver -addab address [port]
gaserver -deleteab address
gaserver [-help]
```

DESCRIPTION

The gaserver command provides various management server information, including attribute values. A modify option is provided to change the port number and IP address of the management server. Options are also available to add and remove peer management servers.

OPTIONS

```
-list [-local]
    Lists all peer management servers.
```

The output includes a header row and one row for each management server with server name, IP address, Port number (always 14145), and ID. The header looks like:

```
#Name Address Port ID
```

`-display [server...]`

Displays all management server attribute values for the specified servers. No argument indicates all management servers.

`[server...]` is a list of one or more management servers.

The output includes a header row and one row for each cluster. Each row contains the cluster name, parent management server name, attribute name, attribute scope, and attribute value. The header looks like:

```
#Server[home] Attribute Scope Value
```

`-state [server...]`

Displays the state of the specified management servers.

`[server...]` is a list of one or more management servers.

The output is the single state value requested.

`-value server attr`

Displays the value of attribute `attr` on the management server `server`. The output is the single attribute value requested.

`-modify port portnumber`

Modifies the port number used to connect to the local management server. You must restart your local management server to make the new setting effective.

`-modify address ipaddress`

Modifies the IP address of the local management server. You must restart your local management server to make the new setting effective.

`-rename name [-nocheck]`

Modifies the name of the local management server. You must restart your local management server to make the new setting effective.

`name` is the new management server name; valid characters include upper- and lowercase letters (A-Z, a-z), digits (0-9), underscore (`_`), and hyphen (`-`).

`[-nocheck]` indicates to skip validation of the name and allow all characters.

`-add id name ipaddress [portnumber]`

Adds the specified management server `name` to the enterprise.

`id` is the management server id.

`-delete server`

Removes the management server *server* from the enterprise. The named management server will not be re-connected once it is disconnected.

`-delete -id id`

Removes a peer management server by id rather than by name. This command is especially useful for removing a peer management server with the same name as another.

`-delete [-local]`

Removes the local management server from the enterprise. The management server will form an enterprise consisting of one management server (itself).

`-listab`

Lists all existing Symantec Product Authentication Service authentication brokers in a table.

The output includes a header row and one row for each authentication broker. Each row contains an IP address and port number. The header looks like:

```
#Address Port
```

`-addab address [port]`

Adds a new Symantec Product Authentication Service authentication broker. No validation is performed.

`-deleteab address`

Deletes an existing Symantec Product Authentication Service authentication broker. The address specified must match one displayed in `-listab` output.

`-help`

Provides basic command usage information.

NOTES

EXAMPLES

List all management servers and attributes.

```
gaserver -list
```

```
#Name          Address          Port  ID
QaSite407      10.141.11.107   14145 be2b0098-d9b9-4bd8-b00e-
27b9f53db080
```

SEE ALSO

gasys

NAME

gasys - provides cluster system information and operations

SYNOPSIS

```
gasys -list [-clus cluster] [-server server]  
gasys -display [sys...] [-clus cluster] [-server  
    server]  
gasys -state [sys...] [-clus cluster] [-server  
    server]  
gasys -value sys attr  
gasys -freeze sys [-persistent] [-evacuate]  
gasys -unfreeze sys [-persistent]  
gasys [-help]
```

DESCRIPTION

The `gasys` command provides various system information as requested, including parent information and attribute values. Operational commands, such as `freeze`, take the same actions they do in VCS. The commands are forwarded to the VCS engine, and any limitations and errors returned are from VCS.

OPTIONS

```
-list [-clus cluster] [-server server]  
    Lists all systems, systems in a specific cluster, or systems managed  
    by a specific management server.  
    No argument indicates all systems managed by all management  
    servers.  
    [-clus cluster] indicates all systems in the cluster cluster.  
    [-server server] indicates all systems in the management  
    server server.  
    The output includes a header row and one row for each system.  
    Each row contains the system , parent cluster, and parent  
    management server names. The header looks like:
```

#System Cluster Server

Note: This list may be empty if you supply a cluster or management server name that does not exist in the enterprise.

`-display [sys...] [-clus cluster] [-server server]`

Displays all system attribute values for the specified systems. You can specify system names, systems in a specific cluster, or systems managed by a specific management server.

No argument indicates all systems managed by all management servers.

[*sys ...*] is a list of one or more systems.

[*-clus cluster*] indicates all systems in the cluster *cluster*.

[*-server server*] indicates all systems managed by the management server *server*.

The output includes a header row and one row for each system.

Each row contains the system name, parent cluster name, parent management server name, attribute name, attribute scope, and attribute value. The header looks like:

```
#System Cluster Server Attribute Scope Value
```

`-state [sys...] [-clus cluster] [-server server]`

Displays the state of the specified systems. You must specify *sys* if state is a local attribute; *sys* is optional if state is a global attribute.

You can specify individual system names, systems in a specific cluster, or systems managed by a specific management server.

No argument indicates all systems managed by all management servers.

[*sys ...*] is a list of one or more systems.

[*-clus cluster*] indicates all systems in the cluster *cluster*.

[*-server server*] indicates all systems managed by the management server *server*.

The output includes a header row and one row for each system.

Each row contains the system name, parent cluster name, parent management server name, attribute name, attribute scope, and attribute value . The header looks like:

```
#System Cluster Server Attribute Scope Value
```

The value under the **Attribute** header is always **state**.

`-value sys attr`

Displays the value of attribute *attr* on the system *sys*. The output is the single attribute value requested.

`-freeze sys [-persistent] [-evacuate]`

Freezes the system *sys* using the VCS freeze command. Groups are then prevented from being brought online on this system.

`[-persistent]` indicates to remember the frozen state when the cluster is rebooted.

`[-evacuate]` fails over any active groups to another system in the cluster before freezing the system.

`-unfreeze sys [-persistent]`

Unfreezes the system `sys` using the VCS unfreeze command.

`-help`

Provides basic command usage information.

NOTES

EXAMPLES

List all systems and their parents.

```
gasys -list
```

#System	Cluster	Server
HOUWIN163	Clus163_164	QaSite407
HOUWIN164	Clus163_164	QaSite407

Freeze the system HOUWIN163.

```
gasys -freeze HOUWIN163
```

```
Success
```

SEE ALSO

gatype

NAME

gatype - provides resource type information and operations

SYNOPSIS

```
gatype -list [-clus cluster] [-server server]  
gatype -display [type...] [-clus cluster] [-server server]  
gatype -value type attr [-sys sys]  
gatype [-help]
```

DESCRIPTION

The gatype command provides various resource type information as requested, including parent information and attribute values.

OPTIONS

`-list [-clus cluster] [-server server]`
Lists all resource types, types in a specific group, types in a specific cluster, or types managed by a specific management server. No argument indicates all resource types managed by all management servers.
`[-clus cluster]` indicates all resource types in the cluster *cluster*.
`[-server server]` indicates all resource types managed by the management server *server*.
The output includes a header row and one row for each resource type. Each row contains the resource type, parent cluster, and parent management server names. The header looks like:
#Type Cluster Server

`-display [type...] [-clus cluster] [-server server]`
Displays all resource type attribute values for the specified type. You can specify individual resource type names, types in a specific group, types in a specific cluster, or types managed by a specific management server.
No argument indicates all resource types in all clusters.
`[type ...]` is a list of one or more resource types.
`[-clus cluster]` indicates all resource types in the cluster *cluster*.

`[-server server]` indicates all resource types managed by the management server *server*.

The output includes a header row and one row for each resource type. Each row contains the resource type name, parent cluster name, parent management server name, attribute name, attribute scope, and attribute value. The header looks like:

```
#Type Cluster Server Attribute Scope Value
```

`-value type attr [-sys sys]`

Displays the value of attribute *attr* on the resource type *type*.

The output is the single attribute value requested.

`[-sys sys]` indicates a specific system *sys*; it is required for local attributes (which vary per system.) and not required for global attributes.

`-help`

Provides basic command usage information.

NOTES

EXAMPLES

List all resource types and parents.

```
gatype -list
```

#Type	Cluster	Server
CompositeFileShare	Clus163_164	QaSite407
DiskRes	Clus163_164	QaSite407
E2KProtocol	Clus163_164	QaSite407
E2KService	Clus163_164	QaSite407
ElifNone	Clus163_164	QaSite407
Exchange	Clus163_164	QaSite407
FileNone	Clus163_164	QaSite407
FileOnOff	Clus163_164	QaSite407
FileOnOnly	Clus163_164	QaSite407
FileShare	Clus163_164	QaSite407
GenericService	Clus163_164	QaSite407
IP	Clus163_164	QaSite407
IPMultiNicPlus	Clus163_164	QaSite407
Lanman	Clus163_164	QaSite407
Mount	Clus163_164	QaSite407
MountV	Clus163_164	QaSite407
NIC	Clus163_164	QaSite407
NotifierMngr	Clus163_164	QaSite407
Oracle	Clus163_164	QaSite407
Phantom	Clus163_164	QaSite407
PrintShare	Clus163_164	QaSite407
PrintSpool	Clus163_164	QaSite407
Process	Clus163_164	QaSite407

Proxy	Clus163_164	QaSite407
RegRep	Clus163_164	QaSite407
SQLServer2000	Clus163_164	QaSite407
ServiceMonitor	Clus163_164	QaSite407
Sqlnet	Clus163_164	QaSite407
VMDg	Clus163_164	QaSite407
ClusterMonitorConfig	Clus163_164	QaSite407

SEE ALSO

gauser

NAME

gauser - provides user information and operations

SYNOPSIS

```
gauser -list
gauser -add name domain domainType
gauser -delete name domain domainType
gauser -admin name domain domainType
gauser [-help]
```

DESCRIPTION

The `gauser` command provides a listing of the management server user accounts with their domain information. These are domain user accounts that have been added (made known) to the management server. You can add and delete users with the `gauser` command.

OPTIONS

`-list`

Lists users in this management server.

The output includes a header row and one row for each user. Each row contains the user name, domain, and domain type. The header looks like:

```
#Name Domain Type
```

`-add user-name domain domainType`

Adds the user *user-name* to this management server with guest access rights.

name is the domain user name you want to add.

domain is the name of the domain for this user

domainType is the domain type (nt, nis, nisplus, vx, or unixpwd) of the specified domain

`-delete name domain domainType`

Removes the specified user from this management server

name is the user name you want to remove.

domain is the name of the domain for this user

`domainType` is the domain type (nt, nis, nisplus, vx, or unixpwd) of the specified domain

`-admin name domain domainType`

Adds the specified user with *Admin* access rights to this management server. You do *not* need to login (using galogin) to the management server before using this command, but you *must* be logged in on the system as a member of the Administrators group (Windows) or with an uid of 0 (Unix). If the user account already exists, then its access rights are set to Admin for this Cluster Server management server.

Note: Use the `-admin` option of `gauser` if you have lost your admin account name or password. It allows you to add an admin account without logging in.

Note: You *must* be logged in on the system as a member of the Administrators group (Windows) or with an uid of 0 (Unix) to use this command.

`name` is the Admin user name you want to add.

`domain` is the name of the domain for this user

`domainType` is the domain type (nt, nis, nisplus, vx, or unixpwd) of the specified domain

`-help`

Provides basic command usage information.

NOTES

EXAMPLES

List all users in the local management server.

```
gauser -list
```

#Name	Domain	Type
Administrator	HOULAB	nt

SEE ALSO

Creating custom reports

The following topics are covered in this appendix:

- [Accessing the database information](#)
- [Database schema objects](#)
- [Published database schema objects](#)
- [Example statements](#)

Accessing the database information

Depending on which third-party application or tool you use to connect to the Cluster Management Console database, you must configure an ODBC data source to enable custom reporting. You must also consult the third-party application documentation to learn how to set up a connection to an external database.

Use the following procedure to create an ODBC data source for the Cluster Management Console management server database. The data source is not required for the management server to operate correctly. It is intended to be used with third-party software to generate custom reports created from data in the guest table views.

To create an ODBC data source

- 1 Open the ODBC Data Source Administrator tool by selecting **Start->Programs->Administrative Tools->Data Sources**.
- 2 Click the **System DSN** or **User DSN** tab, and then click **Add**.
- 3 Select the **Veritas CCAvailDb Adaptive Server Anywhere 9.0** driver.
- 4 In the **ODBC Adaptive Server Anywhere Configuration** dialog box, enter a name for the data source, such as CMC Guest DSN.
- 5 Click the **Login** tab to configure login information.
The User ID is CCAVAILGUEST. The password must be the same as the one used to configure guest database access. You can not connect to the management server database using the DSN unless the account is enabled. See "[Modifying guest access to the database](#)" on page 159.
- 6 Click the **Database** tab to configure database information.
The database server name is of the form VERITAS_DBMS3_ \$ms_host, where \$ms_host is the host name of the management server system. The database name is CCAvailDb
Ensure that the **Stop database after last disconnect** check box is not checked.
- 7 Click the **Network** tab to configure network information.
Check the TCP/IP check box only. No other protocols should be checked. The TCP/IP options are:
 - host=\$ms_host
 - port=2994where \$ms_host is the host name of the management server.
- 8 Click the ODBC tab and test the connection.
A pop-up message appears. Click **Yes** to continue the test.

If a pop-up message does not appear, ensure that the **Stop database after last disconnect** check box is not checked before you continue.

If all is configured correctly, you receive the message, "Connection successful"

Database schema objects

The following includes the published objects in the database:

- Enterprise - Only one enterprise object exists per database. This object is replicated and made the same for all connected management servers.
- MServer - Only one management server object exists per database. This object contains information about the local management server.
- Schedule - More than one schedule object can exist in the database. This object contains schedule information on objects that are managed by the local management server.
- Cluster - More than one cluster object can exist in the database. This object contains information about clusters that are managed by the local management server.
- Node - More than one node object can exist in the database. This object contains information on clustered nodes that are managed by the local management server.
- Resource type - More than one resource type object can exist in the database. This object contains information on clustered resource types that are managed by the local management server.
- Group - More than one group object can exist in the database. This object contains information on clustered groups that are managed by the local management server.
- Resource - More than one resource object can exist in the database. This object contains information on group resources that are managed by the local management server.
- Log - This object contains information about an event on a managed object or a about a user command on the local management server. Events on enterprise objects are not available.

Published database schema objects

Information in the database is presented in views that contain historical, as well as current information on managed objects. The information is stored in an attribute-based format (for example, information on an object is stored as an attribute of the object). The database is case sensitive. The user name, password, and data are case sensitive, however, the names of the schema objects are not. All database dates are stored in Greenwich Mean Time.

Information in the database can be read externally from the following list of published database schema objects.

Note: Use only the published list of database schema objects to retrieve information from the database. Only the published database schema objects are maintained and compatible from release to release of the Cluster Management Console. Other objects are subject to change without notice.

The following describes each database view, providing descriptions of the views, attribute information, and descriptions of the views and their columns.

K2VW_ENTERPRISE

The following attribute information is available on this object type:

Table B-1 K2VW_ENTERPRISE Attribute Information

Attribute	Description
ConsolidatedState	Not available.
Site	Possible site extended attribute values.
Region	Possible region extended attribute values.
LOB	Possible line of business (LOB) extended attribute values.
Department	Possible department extended attribute values.
ExtendedAttributes	Map of names of all extended attributes (name=object type, for example, LOB=4).
fqn	Fully qualified object name.
RemoteSites	Map of remote site IDs to connection information.
Applications	Map of application name to string representation of description and list of groups.

Table B-1 K2VW_ENTERPRISE Attribute Information

Attribute	Description
ApplicationType	Set of all application types.

The K2VW_ENTERPRISE table provides the following data:

Table B-2 K2VW_ENTERPRISE Table Information

Column	Data Type	Description
ObjectID	Integer	Unique database ID that identifies each object in the view.
ObjectName	Varchar (256)	Name of the object.
DateCreated	Timestamp	Date the object was created.
AttributeName	Varchar (256)	Name of an attribute on the object.
AttributeDimension	Varchar (50)	Dimension of the attribute. Can be any of the following values: Scalar attribute, Association attribute, Key List attribute, or Vector attribute.
AttributeType	Varchar (50)	Actual data type of the attribute values.
AttributeScope	Varchar (50)	Specifies the scope of the attribute. An attribute can be either locally scoped or globally scoped.
AttributeDateModified	Timestamp	Date the attribute was modified.
AttributeState	Varchar (3)	Specifies if the attribute is an historical record ('OLD') or if it is a current record ('NEW').
AttributeContext	Varchar (512)	The context for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeKey	Varchar (512)	The key for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeValue	Varchar (512)	The attribute values. Depending on the attribute dimension, this may contain a NULL value.

K2VW_MServers

The following attribute information is available on this object type:

Table B-3 K2VW_MServer Attribute Information

Attribute	Description
explicitUserAccessRight	Map of user IDs to users right on this object. Explicit may be empty.
effectiveUserAccessRight	Map of user IDs to users right on this object. Effective=explicit or is inherited from parents effective.
fqn	Fully qualified object name.
SysName	Name of system where local management server is installed and running.
Port	Port for local management server.
DowntimeWindows	Array of time windows when the management server is down.
Platform	Platform name for management server.
Version	Version of the management server.
State	State of management server.
ConsolidatedState	State of management server.
PreviousConsolidatedState	State of management server before last transition.
UptimeTick	Last time the management server recorded its online state (in milliseconds).

The K2VW_MServer table provides the following data:

Table B-4 K2VW_MServer Table Information

Column	Data Type	Description
ObjectID	Integer	Unique database ID that identifies each object of this type in the database.
ObjectUuid	Varchar (256)	Universal unique identifier of the object.

Table B-4 K2VW_MServer Table Information

Column	Data Type	Description
ObjectName	Varchar (256)	Name of the object.
DateCreated	Timestamp	Date the object was created.
DateDeleted	Timestamp	Date the object was deleted. If NULL, the object is not deleted.
AttributeName	Varchar (256)	Name of an attribute on the object.
AttributeDimension	Varchar (50)	Dimension of the attribute. Can be any of the following values: Scalar attribute, Association attribute, Key List attribute, or Vector attribute.
AttributeType	Varchar (50)	Actual data type of the attribute values.
AttributeScope	Varchar (50)	Specifies the scope of the attribute. An attribute can be either locally scoped or globally scoped.
AttributeDateModified	Timestamp	Date the attribute was modified.
AttributeState	Varchar (3)	Specifies if the attribute is an historical record ('OLD') or if it is a current record ('NEW').
AttributeContext	Varchar (512)	The context for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeKey	Varchar (512)	The key for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeValue	Varchar (512)	The attribute values. Depending on the attribute dimension, this may contain a NULL value.

K2VW_Clusters

The following attribute information is available on this object type:

Table B-5 K2VW_Cluster Attribute Information

Attribute	Description
All VCS attributes on the cluster except for the following: GlobalCounter, ClusterTime.	Note: Refer to the <i>VERITAS Cluster Server User's Guide</i> for a complete list of VCS attributes.
Site	Cluster extended attribute "Site."
effectiveUserAccessRight	Map of user IDs to users right on this object. Effective=explicit or is inherited from parents effective.
MaintenanceWindow	Periods of time when there is a configured maintenance window.
ConsolidatedState	State of management server.
fqn	Fully qualified object name.
RClusterNameList	Map of remote cluster names to remote cluster states. Global clusters only.
PreviousConsolidatedState	State of management server before last transition.
ClusterType	Type of cluster. Value is 'VCS' for VCS clusters.
Region	Cluster extended attribute "Region."
explicitUserAccessRight	Map of user IDs to users right on this object. Explicit may be empty.
Platform	Platform name for the cluster.
RClusterList	Map of remote cluster IDs to remote cluster states. Global clusters only.

The K2VW_Cluster table provides the following data:

Table B-6 K2VW_Cluster Table Information

Column	Data Type	Description
ObjectID	Integer	Unique database ID that identifies each object of this type in the database.
ObjectUuid	Varchar (256)	Universal unique identifier of the object.
ObjectName	Varchar (256)	Name of the object.
ParentID	Integer	The parent of a cluster object is a management server object. This column contains the unique database ID for the parent of this object.
DateCreated	Timestamp	Date the object was created.
DateDeleted	Timestamp	Date the object was deleted. If NULL, the object is not deleted.
AttributeName	Varchar (256)	Name of an attribute on the object.
AttributeDimension	Varchar (50)	Dimension of the attribute. Can be any of the following values: Scalar attribute, Association attribute, Key List attribute, or Vector attribute.
AttributeType	Varchar (50)	Actual data type of the attribute values.
AttributeScope	Varchar (50)	Specifies the scope of the attribute. An attribute can be either locally scoped or globally scoped.
AttributeDateModified	Timestamp	Date the attribute was modified.
AttributeState	Varchar (3)	Specifies if the attribute is an historical record ('OLD') or if it is a current record ('NEW').
AttributeContext	Varchar (512)	The context for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
Attributekey	Varchar (512)	The key for an attribute value. Depending on the attribute dimension, this may contain a NULL value.

Table B-6 K2VW_Cluster Table Information

Column	Data Type	Description
AttributeValue	Varchar (512)	The attribute values. Depending on the attribute dimension, this may contain a NULL value.

K2VW_Groups

The following attribute information is available on this object type:

Table B-7 K2VW_Group Attribute Information

Attribute	Description
All VCS attributes on the group.	Note: Refer to the <i>VERITAS Cluster Server User's Guide</i> for a complete list of VCS attributes.
Department	Group extended attribute "Department."
LOB	Group extended attribute "LOB."
explicitUserAccessRight	Map of user IDs to users right on this object. Explicit may be empty.
effectiveUserAccessRight	Map of user IDs to users right on this object. Effective=explicit or is inherited from parents effective.
fqn	Fully qualified object name.
MaintenanceWindow	Configured maintenance window for this group.
ConsolidatedState	State of management server.
PreviousConsolidatedState	State of management server before last transition.

The K2VW_Group table provides the following data:

Table B-8 K2VW_Group Table Information

Column	Data Type	Description
ObjectID	Integer	Unique database ID that identifies each object of this type in the database.
ObjectName	Varchar (256)	Name of the object.

Table B-8 K2VW_Group Table Information

Column	Data Type	Description
ParentID	Integer	The parent of a group object is a Cluster object. This column contains the unique database ID for the parent of this object.
DateCreated	Timestamp	Date the object was created.
DateDeleted	Timestamp	Date the object was deleted. If NULL, the object is not deleted.
AttributeName	Varchar (256)	Name of an attribute on the object.
AttributeDimension	Varchar (50)	Dimension of the attribute. Can be any of the following values: Scalar attribute, Association attribute, Key List attribute, or Vector attribute.
AttributeType	Varchar (50)	Actual data type of the attribute values.
AttributeScope	Varchar (50)	Specifies the scope of the attribute. An attribute can be either locally scoped or globally scoped.
AttributeDateModified	Timestamp	Date the attribute was modified.
AttributeState	Varchar (3)	Specifies if the attribute is an historical record ('OLD') or if it is a current record ('NEW').
AttributeContext	Varchar (512)	The context for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
Attributekey	Varchar (512)	The key for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeValue	Varchar (512)	The attribute values. Depending on the attribute dimension, this may contain a NULL value.

K2VW_Nodes

The following attribute information is available on this object type:

Table B-9 K2VW_Node Attribute Information

Attribute	Description
All VCS attributes on the node except for the following: LoadTimeCounter.	Note: Refer to the <i>VERITAS Cluster Server User's Guide</i> for a complete list of VCS attributes.
explicitUserAccessRight	Map of user IDs to users right on this object. Explicit may be empty.
effectiveUserAccessRight	Map of user IDs to users right on this object. Effective=explicit or is inherited from parents effective.
fqn	Fully qualified object name.
Platform	Platform name of the node.
ConsolidatedState	State of management server.
PreviousConsolidatedState	State of management server before last transition.

The K2VW_Node table provides the following data:

Table B-10 K2VW_Node Table Information

Column	Data Type	Description
ObjectID	Integer	Unique database ID that identifies each object of this type in the database.
ObjectName	Varchar (256)	Name of the object.
ParentID	Integer	The parent of a node object is a Cluster object. This column contains the unique database ID for the parent of this object.
DateCreated	Timestamp	Date the object was created.
DateDeleted	Timestamp	Date the object was deleted. If NULL, the object is not deleted.

Table B-10 K2VW_Node Table Information

Column	Data Type	Description
AttributeName	Varchar (256)	Name of an attribute on the object.
AttributeDimension	Varchar (50)	Dimension of the attribute. Can be any of the following values: Scalar attribute, Association attribute, Key List attribute, or Vector attribute.
AttributeType	Varchar (50)	Actual data type of the attribute values.
AttributeScope	Varchar (50)	Specifies the scope of the attribute. An attribute can be either locally scoped or globally scoped.
AttributeDateModified	Timestamp	Date the attribute was modified.
AttributeState	Varchar (3)	Specifies if the attribute is an historical record ('OLD') or if it is a current record ('NEW').
AttributeContext	Varchar (512)	The context for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeKey	Varchar (512)	The key for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeValue	Varchar (512)	The attribute values. Depending on the attribute dimension, this may contain a NULL value.

K2VW_ResourceTypes

The following attribute information is available on this object type:

Table B-11 K2VW_ResourceType Attribute Information

Attribute	Description
All VCS attributes on the resource type.	Note: Refer to the <i>VERITAS Cluster Server User's Guide</i> for a complete list of VCS attributes.
effectiveUserAccessRight	Map of user IDs to users right on this object. Effective=explicit or is inherited from parents effective.
explicitUserAccessRight	Map of user IDs to users right on this object. Explicit may be empty.

Table B-11 K2VW_ResourceType Attribute Information

Attribute	Description
fqn	Fully qualified object name.

The K2VW_ResourceType table provides the following data:

Table B-12 K2VW_ResourceType Table Information

Column	Data Type	Description
ObjectID	Integer	Unique database ID that identifies each object of this type in the database.
ObjectName	Varchar (256)	Name of the object.
ParentID	Integer	The parent of a resource type object is a Cluster object. This column contains the unique database ID for the parent of this object.
DateCreated	Timestamp	Date the object was created.
DateDeleted	Timestamp	Date the object was deleted. If NULL, the object is not deleted.
AttributeName	Varchar (256)	Name of an attribute on the object.
AttributeDimension	Varchar (50)	Dimension of the attribute. Can be any of the following values: Scalar attribute, Association attribute, Key List attribute, or Vector attribute.
AttributeType	Varchar (50)	Actual data type of the attribute values.
AttributeScope	Varchar (50)	Specifies the scope of the attribute. An attribute can be either locally scoped or globally scoped.
AttributeDateModified	Timestamp	Date the attribute was modified.
AttributeState	Varchar (3)	Specifies if the attribute is an historical record ('OLD') or if it is a current record ('NEW').
AttributeContext	Varchar (512)	The context for an attribute value. Depending on the attribute dimension, this may contain a NULL value.

Table B-12 K2VW_ResourceType Table Information

Column	Data Type	Description
Attributekey	Varchar (512)	The key for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeValue	Varchar (512)	The attribute values. Depending on the attribute dimension, this may contain a NULL value.

K2VW_Resources

The following attribute information is available on this object type:

Table B-13 K2VW_Resources Attribute Information

Attribute	Description
All VCS attributes on the resource except for the following: Signaled, MonitorTimeStats.	Note: Refer to the <i>VERITAS Cluster Server User's Guide</i> for a complete list of VCS attributes.
explicitUserAccessRight	Map of user IDs to users right on this object. Explicit may be empty.
effectiveUserAccessRight	Map of user IDs to users right on this object. Effective=explicit or is inherited from parents effective.
fqn	Fully qualified object name.
ExcludeFromUptimeReport	Don't include resource in uptime calculations.
ChildDependencies	IDs of children.
ParentDependencies	IDs of parents.
ConsolidatedState	State of management server.
PreviousConsolidatedState	State of management server before last transition.
resourceType	ID of resource type for this resource.

The K2VW_Resource table provides the following data:

Table B-14 K2VW_Resource Table Information

Column	Data Type	Description
ObjectID	Integer	Unique database ID that identifies each object of this type in the database.
ObjectName	Varchar (256)	Name of the object.
ParentID	Integer	The parent of a resource object is a Group object. This column contains the unique database ID for the parent of this object.
DateCreated	Timestamp	Date the object was created.
DateDeleted	Timestamp	Date the object was deleted. If NULL, the object is not deleted.
AttributeName	Varchar (256)	Name of an attribute on the object.
AttributeDimension	Varchar (50)	Dimension of the attribute. Can be any of the following values: Scalar attribute, Association attribute, Key List attribute, or Vector attribute.
AttributeType	Varchar (50)	Actual data type of the attribute values.
AttributeScope	Varchar (50)	Specifies the scope of the attribute. An attribute can be either locally scoped or globally scoped.
AttributeDateModified	Timestamp	Date the attribute was modified.
AttributeState	Varchar (3)	Specifies if the attribute is an historical record ('OLD') or if it is a current record ('NEW').
AttributeContext	Varchar (512)	The context for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeKey	Varchar (512)	The key for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeValue	Varchar (512)	The attribute values. Depending on the attribute dimension, this may contain a NULL value.

K2VW_Schedules

The following attribute information is available on this object type:

Table B-15 K2VW_Schedules Attribute Information

Attribute	Description
explicitUserAccessRight	Map of user IDs to users right on this object. Explicit may be empty.
effectiveUserAccessRight	Map of user IDs to users right on this object. Effective=explicit or is inherited from parents effective.
fqn	Fully qualified object name.
Description	Description of the schedule object
EffectiveDate	The date on which the schedule object takes effect
StartTime	Starting time for the schedule object
RepeatInterval	Repeat interval in days for the schedule object
DayOfWeek	Day of the week for the schedule object (Sunday = 1, ..., Saturday = 7)
DayOfMonth	Day of the month for the schedule object (1 - 31)
SpecificDate	Specific date for the schedule object
IsPeriodic	Boolean flag which determines if the schedule periodically repeats
IsEnabled	Boolean flag which determines if the schedule is enabled
Event	Event to fire.

The K2VW_Schedule table provides the following data:

Table B-16 K2VW_Schedule Table Information

Column	Data Type	Description
ObjectID	Integer	Unique database ID that identifies each object of this type in the database.

Table B-16 K2VW_Schedule Table Information

Column	Data Type	Description
ObjectUuid	Varchar (256)	Unique database ID that identifies each object of this type in the database.
ObjectName	Varchar (256)	Name of the object.
ParentID	Integer	The parent of a schedule object is a Cluster object. This column contains the unique database ID for the parent of this object.
DateCreated	Timestamp	Date the object was created.
DateDeleted	Timestamp	Date the object was deleted. If NULL, the object is not deleted.
AttributeName	Varchar (256)	Name of an attribute on the object.
AttributeDimension	Varchar (50)	Dimension of the attribute. Can be any of the following values: Scalar attribute, Association attribute, Key List attribute, or Vector attribute.
AttributeType	Varchar (50)	Actual data type of the attribute values.
AttributeScope	Varchar (50)	Specifies the scope of the attribute. An attribute can be either locally scoped or globally scoped.
AttributeDateModified	Timestamp	Date the attribute was modified.
AttributeState	Varchar (3)	Specifies if the attribute is an historical record ('OLD') or if it is a current record ('NEW').
AttributeContext	Varchar (512)	The context for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
Attributekey	Varchar (512)	The key for an attribute value. Depending on the attribute dimension, this may contain a NULL value.
AttributeValue	Varchar (512)	The attribute values. Depending on the attribute dimension, this may contain a NULL value.

K2VW_Logs

The K2VW_Logs table provides the following data:

Note: There is no attribute information for logs.

Table B-17 K2VW_Logs Table Information

Column	Data Type	Description
ObjectType	Varchar (15)	Object type for which the log was generated.
ObjectID	Integer	Unique database ID that identifies the object for which the log was generated.
EntryDate	Timestamp	Date the log was generated.
UserName	Long Varchar	Name of the user whose action generated the log.
LogID	Varchar (50)	Application-specific ID for the log message.
LogSource	Varch (15)	Source of the log/event for CommandCentral Availability or VCS.
LogLevel	Long Varchar	The log message text.
LogArgs	Long Varchar	Arguments on the log messages text stored in .xml format.

Example statements

The following section includes examples of Structured Query Language (SQL) statements to retrieve information using the published database schema objects.

Example 1

To retrieve a list of currently managed clusters:

```
SELECT distinct a.ObjectName, a.ObjectUuid, a.DateCreated, b.ObjectName  
'Parent(Site)'  
FROM K2VW_Clusters a  
JOIN K2VW_MServers b ON a.ParentID = b.ObjectID  
WHERE a.DateDeleted IS NULL  
ORDER BY a.ObjectUuid
```

Example 2

To retrieve a list of current cluster users on managed clusters:

```
SELECT distinct a.ObjectName, a.ObjectUuid, b.ObjectName 'Parent(Site)',  
a.attributeKey Users FROM K2VW_Clusters a  
JOIN K2VW_MServers b ON a.ParentID = b.ObjectID  
WHERE a.DateDeleted IS NULL  
AND a.attributename = 'UserNames'  
AND a.attributeState = 'NEW'  
ORDER BY a.ObjectUuid
```

Example 3

To retrieve basic uptime information on a specific managed cluster:

```
SELECT distinct a.ObjectName, a.ObjectUuid, b.ObjectName 'Parent(Site)',  
(CASE a.attributeValue  
WHEN '0' then 'STATE_CLUSTER_INIT'  
WHEN '1' then 'STATE_CLUSTER_LOCAL_VCS_BUILD'  
WHEN '2' then 'STATE_CLUSTER_MASTER_CONNECT'  
WHEN '3' then 'STATE_CLUSTER_SLAVE_BUILD'  
WHEN '4' then 'STATE_CLUSTER_RUNNING'  
WHEN '5' then 'STATE_CLUSTER_EXITING'  
WHEN '6' then 'STATE_CLUSTER_EXITED'  
WHEN '7' then 'STATE_CLUSTER_FAULTED'  
WHEN '8' then 'STATE_CLUSTER_DEAD'  
ELSE 'Unknown'  
END) State, a.AttributedateModified timestamp
```

```
FROM K2VW_Clusters a  
JOIN K2VW_MServers b ON a.ParentID = b.ObjectID
```

Example statements

Accessibility

The following topics are covered in this appendix:

- [Navigating the Cluster Management Console](#)
- [Accessibility features in GUI controls](#)

Navigating the Cluster Management Console

You can use your keyboard to view information and perform operations by selecting a variety of different controls in the Cluster Management Console. Examples of selectable controls include:

- Tabs and subtabs
- Navigational links at the top of the content pane
- Column headings in tables
- Hyperlinked objects in tables
- Areas, such as bars in a graph, in graphical reports
- Navigation arrows and zoom buttons in the Topology Map
- Alert categories in the Alerts Summary list
- Controls in the header such as **Logout**, **About**, and **Help**
- Refresh icon

The current active control is enclosed with a rectangle formed by dotted lines. This area has *focus*. Use the **Tab** key to move focus from one control to another. Following are general rules for navigating the Console and performing operations:

- Pressing **Tab** moves the focus to the next active area or control.
- Pressing **Shift+Tab** moves the focus to the previous active area. In effect, **Shift+Tab** is the reverse of **Tab**.
- Pressing **Ctrl+Tab** moves the focus to the top of the browser window.
- Pressing **Enter** activates the item that has focus. For example, after pressing **Tab** to select a host in the Hosts summary pane, press **Enter** to display the object view for that host.
- In a drop-down list, press the arrow keys to move up and down the list.
- When a checkbox has focus, press the Spacebar to select (check) or deselect the box.
- Normal accessibility features for your Web browser apply. In many browsers, for example, pressing **Shift+F10** displays a context menu with which you can move back to the previous page, print the current page, and perform other operations.

Accessibility features in GUI controls

In the Cluster Management Console Console GUI, the current active control has focus. You can use the Tab key to move focus from one control to another.

When a radio button has focus, use the up and down arrow keys to move focus to a different radio button. When a button has focus, pressing **Enter** activates or selects the button.

When a drop-down menu has focus, use the up and down arrow keys to move among the selections and then press **Enter** to make your selection.

When a check box has focus, press the Spacebar to select (check) or deselect (uncheck) the box.

When a text box has focus, use your keyboard to type text in the box.

Troubleshooting

The following topics are covered in this appendix:

- [Installation issues and recommendations](#)
- [Configuration issues and recommendations](#)
- [Operational issues and recommendations](#)
- [Log file locations](#)
- [Status icon reference](#)

Installation issues and recommendations

This topic contains information that can help to address common installation issues. Use this section to supplement information in your *Veritas Cluster Server 5.0 Installation Guide*.

Avoid concurrent installations

Under no circumstances should you attempt to install the Cluster Management Console while other installation programs for any other products are running. Such attempts can result in installations that appear to be successful, but are not.

Authentication broker installer location

Cluster connector installation on Windows requires the Symantec Product Authentication Broker installer VxAutht 4.3 or higher on the system from which you are installing. The following path shows the location of this installer (the AT installer) on the distribution DVD:

```
/windows/SymantecProductAuthentication/VxSSVRTSatSetup.exe
```

VCS 4.3 upgrade

If you install VCS 4.3 on Windows platforms, the Cluster Management Console requires that you must upgrade VSS. If you subsequently perform an uninstallation of VCS, you receive the message that the uninstall operation can only be performed on "installed" products. The uninstallation program is looking for an older version of VSS. This message can be ignored.

Installation user account role

The installer assigns the role of management server administrator to the local root user if you choose root as the initial user during install. If you choose a domain-level user, then you must explicitly assign root the role of management server administrator in the Cluster Management Console.

Configuration issues and recommendations

This topic contains information that can help to address common configuration issues.

Resetting the CMC_CC@CMC_SERVICES user account

During management server installation, you must provide a password for a newly-created operating system user account, CMC_CC@CMC_SERVICES. Cluster connector uses this account to connect to the management server. As with all accounts that attempt to log in, the management server authenticates this account against the local authentication broker. The following scenarios could result in the need to reset the password for the cluster connector user account.

Scenario 1:

The user forgets the password. No additional clusters can be deployed.

Scenario 2:

Company policy requires that all passwords be changed every 90 days or when an IT administrator leaves the company. The password for the cluster connector user account must be changed as well.

For both scenarios, reinstalling the management server creates another opportunity to set the cluster connector password, but this resolution is impractical and undesirable in almost all situations.

The recommended resolution is to use Symantec Product Authentication Service to reset the password for the user account CMC_CC@CMC_SERVICES. The following is the command to reset this password:

```
vssat resetpasswd
```

Type a space after “resetpasswd” and add the following parameters and values on the same line:

```
--pdrtype ab --domain CMC_SERVICES --prplname CMC_CC
```

No action is necessary for currently-configured managed clusters. All such clusters have a valid authentication credential. When deploying new clusters, the new password must be used during the cluster connector installation.

Cluster configuration state after cluster user addition

If you are a management server administrator and add yourself as a cluster user, the cluster configuration is left in a read-write state. To return the configuration to a read-only state, use the Save Configuration task in the Cluster:Summary view and specify the read-only option.

Cluster connector, direct connection, and DNS configuration

Your network and DNS configuration must provide proper name resolution. Otherwise, one of the following occurs:

- If using cluster connector, cluster connector is not able to properly resolve the management server host name when attempting to connect to the management server. The initial handshake for the connection fails.
- If using direct connection with secure clusters, the management server is not able to resolve cluster host names when attempting to connect to the clusters. The initial handshake for connections to secure clusters fail.

Improperly configured network and name resolution services can create similar issues in the Cluster Management Console and other Storage Foundation and High Availability Solutions 5.0 products.

Using direct connection to manage a VCS 5.0 secure cluster

If you want to add a secure cluster to the management server using direct connection, you must first configure a trust relationship between the local authentication broker and the peer authentication broker.

See the *Veritas Cluster Server 5.0 Installation Guide* for information about configuring a trust relationship between two authentication brokers

Next, use the Configure Cluster task on the Admin tab to add the cluster.

See “[Adding a cluster to the management server using direct connection](#)” on page 81.

Operational issues and recommendations

This topic contains information that can help to address common operational issues.

Cluster Management Console controls not immediately active

In some versions of Internet Explorer, you may need to click GUI controls (buttons, drop-down menus, radio buttons, and so on) once before the control becomes active. Controls that require this activating click show the following message when you roll over them with your mouse pointer:

`Press SpaceBar or Click to activate this Control`

Cluster status during snapshot

The Cluster Management Console receives updates of cluster data called *snapshots*. It uses these snapshots to refresh the many cluster administration views. For direct connection clusters, the management server initiates the snapshot. If cluster connector is used for communications between a cluster and the management server, cluster connector initiates the snapshot.

In both cases, if a cluster is initiating or coming up during a snapshot, neither the management server nor cluster connector can connect to it. Consequently, the Cluster Management Console shows the cluster in an OFFLINE state.

Log file locations



















The following are the locations of the various log files that can help to resolve issues:























- Management server log files
 - UNIX
`/var/VRTScmc/log`
 - Windows
`CMC_HOME\log`
Replace `CMC_HOME` with the path where CMC is installed.
- Cluster connector log files
 - UNIX
`/var/VRTScmccc/log`
 - Windows
`CMC_HOME\log`
Replace `CMC_HOME` with the path where CMC is installed.
- Installation log files
 - UNIX
`/opt/VRTS/install/logs/NAME_OF_SCRIPT UNIQUE_HASH`
Replace `NAME_OF_SCRIPT` with an appropriate script file name, such as `installcmc`, `uninstallcmc`, `installer`, `installvcs`, or `uninstallvcs`.
Replace `UNIQUE_HASH` with the hash of the root broker used by the management server.
 - Windows
`C:\Documents and Settings\All Users\Application Data\VERITAS\Cluster Management Console`
- User authentication (VxAT) log files:
 - UNIX
`VxAT_HOME/bin`
Replace `VxAT_HOME` with the path where VxAT is installed.
 - Windows
`VxAT_HOME\bin`
Replace `VxAT_HOME` with the path where VxAT is installed.























Status icon reference

Knowing the possible states of an object can be helpful when resolving issues. The following is a list of the status icons used in the Cluster Management Console.

Table D-1 Status icons

	Cluster - FAULTED		Cluster - OFFLINE
	Cluster - ONLINE		Cluster - PARTIAL
	Cluster - UNKNOWN		Global Service Group - FAULTED
	Global Service Group - OFFLINE		Global Service Group - ONLINE
	Global Service Group - PARTIAL		Service Group - FAULTED
	Service Group - FAULTED and AUTODISABLED		Service Group - FAULTED and FROZEN
	Service Group - OFFLINE		Service Group - OFFLINE and AUTODISABLED
	Service Group - OFFLINE and FROZEN		Service Group - ONLINE
	Service Group - ONLINE and AUTODISABLED		Service Group - ONLINE and CONCURRENCY VIOLATION

	Service Group - ONLINE and FROZEN		Service Group - PARTIAL
	Service Group - PARTIAL and AUTODISABLED		Service Group - PARTIAL and CONCURRENCY VIOLATION
	Service Group - PARTIAL and FROZEN		Service Group - UNKNOWN
	Policy - DISABLED		Policy - ENABLED
	Remote Cluster - FAULTED		Remote Cluster - OFFLINE
	Remote Cluster - ONLINE		Remote Cluster - UNKNOWN
	Resource - FAULTED		Resource - FAULTED and UNKNOWN
	Resource - UNKNOWN		Resource - OFFLINE
	Resource - OFFLINE and UNKNOWN		Resource - GOING OFFLINE
	Resource - ONLINE		Resource - ONLINE and UNKNOWN
	Resource - COMING ONLINE		RemoteGroup Resource - FAULTED

	RemoteGroup Resource - OFFLINE		RemoteGroup Resource - ONLINE
	RemoteGroup Resource - PARTIAL		Remote Service Group - FAULTED
	Remote Service Group - FAULTED and AUTODISABLED		Remote Service Group - FAULTED and FROZEN
	Remote Service Group - OFFLINE		Remote Service Group - OFFLINE and AUTODISABLED
	Remote Service Group - OFFLINE and FROZEN		Remote Service Group - ONLINE
	Remote Service Group - ONLINE and AUTODISABLED		Remote Service Group - ONLINE and FROZEN
	Remote Service Group - PARTIAL		Remote Service Group - PARTIAL and AUTODISABLED
	Remote Service Group - PARTIAL and FROZEN		Remote Service Group - UNKNOWN
	Site - FAULTED		Site - FAULTED and FROZEN
	Site - OFFLINE		Site - OFFLINE and FROZEN
	Site - ONLINE		Site - ONLINE and FROZEN



Site - PARTIAL



Site - PARTIAL and FROZEN



Site - UNKNOWN



System - EXITED



System - FAULTED



System - FAULTED and FROZEN



System - OFFLINE



System - OFFLINE and FROZEN



System - ONLINE



System - ONLINE and FROZEN



System - ONLINE and IN
JEOPARDY



System - PARTIAL



System - PARTIAL and FROZEN



System - UNKNOWN



Resource Type - STATELESS

Index

A

- accessibility
 - Cluster Management Console 222
 - dialog windows 223
 - tools 223
- accessing
 - multiple pages of data tables 49
 - online help 51
- adding
 - users 68, 69
- Agent Inventory report 129
- Agent Usage report 129
- agents
 - tracking with reports 129
- alerts
 - critical 40
 - errors 40
 - information 40
 - viewing 40
 - warning 40
- attributes
 - modifying 101
 - modifying Cluster Management Console 86
 - modifying groups 92
- Auto Refresh mode 49

B

- backing up
 - database to a file 158

C

- clearing
 - maintenance windows from groups 94
- cloning
 - report job 123
- Cluster Activity report 137
- Cluster Attribute report 132
- Cluster Inventory report 130
- Cluster Management Console
 - Availability

- understanding the console 35
 - connecting to management server 32
 - definition 14
 - icon conventions 47
 - logging out 34
 - modifying attributes 86, 101
 - tracking agents with reports 129
- clusters
 - configuring 83
 - summary 54, 58
 - viewing 83
- collapsing
 - panels 41
- commands
 - gaclus 168
 - gaconf 171
 - gadb 172
 - gadbrestore 175
 - gagrp 176
 - galogin 182
 - galogout 183
 - gares 184
 - gaserver 188
 - gasys 191
 - gatype 194
 - gauser 197
 - notations for object names 165
- Configuration Analysis report 130
- configuring
 - clusters 83
- connecting
 - management server 32
- console
 - accessibility 222
 - Cluster Management Console 32
 - understanding 35
- conventions
 - Cluster Management Console icons 47
- creating
 - maintenance windows 79
 - notification policy 145
 - report job 117

- report output 126
- critical
 - alerts 40
- Current Schedules report 136

D

- data
 - tables 49
- database
 - backing up to a file 158
 - modifying guest access 159
 - pruning 157
 - restoring 158
- deleting
 - maintenance windows 79
 - policy 147
 - report job 122
 - report output 127
- details
 - policy 145
 - report jobs 117
 - report output 126
- dialog windows
 - accessibility 223
- Disabled mode 49
- disabling
 - policy 147
 - report job 123

E

- enabling
 - policy 147
 - report job 123
- errors
 - alerts 40
- expanding
 - panels 41
- exporting
 - policy 148

F

- Failure Summary by Group report 134
- Failure Summary report 133
- Fault Trending report 134
- files
 - backing up database 158
- filter

- lists 39
- panel 39
- filtering 39
 - lists 67, 84, 91, 100, 106, 109
 - report jobs 124
 - report output 128
- freezing
 - groups 94
 - systems 102

G

- gaclus
 - command 168
- gaconf
 - command 171
- gadb
 - command 172
- gadbrestore
 - command 175
- gagrp
 - command 176
- galogin
 - command 182
- galogout
 - command 183
- gares
 - command 184
- gaserver
 - command 188
- gasys
 - command 191
- gatype
 - command 194
- gauser
 - command 197
- granting
 - report permissions 72, 125
- Group Activity report 137
- Group Attribute report 132
- group data 54
- groups
 - clearing maintenance windows 94
 - freezing 94
 - modifying attributes 92
 - summary 59
 - unfreezing 94
- guests
 - modifying access to database 159

H

- help
 - accessing online 51
 - locating topics 51
 - navigating online 51

I

- icons
 - Cluster Management Console conventions 47
 - refresh 49
- importing
 - policy 149
- information
 - alerts 40

J

- jobs
 - cloning report 123
 - creating report 117
 - deleting report 122
 - disabling report 123
 - enabling report 123
 - filtering report 124
 - modifying report 121
 - reports 116
 - running report 122

L

- lists
 - filtering 39, 67, 84, 91, 100, 106, 109
 - navigation path 84, 91, 100, 106, 109
 - sorting 67, 84, 91, 100, 106, 109
 - viewing policies 144
 - viewing report jobs 116
 - viewing report outputs 126
- logging
 - out 34
- logs 112
 - viewing 112

M

- maintenance windows
 - clearing from groups 94
 - creating 79
 - deleting 79
- management server

- connecting to 32
- managing
 - user privileges 65
- managing user privileges 65
- modes
 - Auto Refresh 49
 - Disabled 49
 - Notify Only 49
 - setting 49
 - update 49
- modifying
 - attributes 86, 101
 - group attributes 92
 - guest access to database 159
 - report job 121
 - tags 93

N

- name
 - qualified 166
 - unqualified 166
 - user 32
- navigation
 - online help 51
 - path 84, 91, 100, 106, 109
- notification policy
 - creating 145
- Notify Only mode 49

O

- object names
 - command notations 165
- online help
 - accessing 51
 - locating topics 51
 - navigating 51
- output
 - creating report 126
 - deleting report 127
 - filtering report 128
- outputs
 - options summary 167
 - reports 126

P

- panels
 - collapsing and expanding 41

- filter 39
- tasks 38
- viewing alerts 40
- password 32
- performing
 - tasks 38
- permissions
 - granting report 72, 125
- policies
 - deleting 147
 - disabling 147
 - enabling 147
 - exporting 148
 - importing 149
 - list 144
 - viewing details 145
- pruning
 - database 157

Q

- qualified
 - name 166

R

- recovery
 - site 76
- removing
 - report permissions 72, 125
- reports
 - Agent Inventory 129
 - Agent Usage 129
 - cloning jobs 123
 - Cluster Activity 137
 - Cluster Attribute 132
 - Cluster Inventory 130
 - Configuration Analysis 130
 - creating jobs 117
 - creating output 126
 - Current Schedules 136
 - deleting jobs 122
 - deleting output 127
 - disabling jobs 123
 - enabling jobs 123
 - Failure Summary 133
 - Failure Summary by Group 134
 - Fault Trending 134
 - filtering jobs 124
 - filtering output 128

- granting permissions 72, 125
- Group Activity 137
- Group Attribute 132
- job list 116
- jobs 116
- modifying jobs 121
- output list 126
- outputs 126
- Resource Activity 137
- Resource Attribute 133
- revoking permissions 72, 125
- running jobs 122
- tracking VCS agents 129
- understanding by functionality 129
- understanding jobs 116
- understanding outputs 126
- Uptime Analysis 135
- viewing job details 117
- viewing output 126
- Virtual IP Usage 133
- Resource Activity report 137
- Resource Attribute report 133
- restoring
 - database 158
- running
 - report job 122

S

- search 151
 - conducting 152
 - definition 152
- searches 151
- searching 151
- server
 - logging out of the Cluster Management Console 34
- settings
 - refresh 49
 - update mode 49
- site
 - recovery 76
- sorting
 - data tables 48
 - lists 67, 84, 91, 100, 106, 109
- summary
 - cluster 54
 - clusters 58
 - group data 54
 - groups 59

- output options 167
- views 55

systems

- freezing 102
- unfreezing 102

T

tables

- accessing multiple pages 49
- sorting data 48

tags

- modifying 93

tasks

- panel 38
- performing 38

tools

- accessibility 223

tracking

- VCS agents with reports 129

U

unfreezing

- groups 94
- systems 102

unqualified

- name 166

updates

- controlling view 49
- mode 49

Uptime Analysis report 135

user

- adding 68, 69
- managing user privileges 65
- name 32

V

Veritas 3

Veritas Cluster Management Console

- modifying attributes 86, 101

viewing 112

- alerts 40
- clusters 83
- policy details 145
- policy list 144
- report job details 117
- report jobs list 116
- report output 126

- report output list 126

views

- controlling updates 49
- summary 55
- summary of cluster 54
- summary of group data 54

Virtual IP Usage report 133

W

warning

- alerts 40

