Veritas™ High Availability Agent for Siebel CRM Installation and Configuration Guide

AIX, Solaris

5.1

September 2009

symantec™

Veritas High Availability Agent for Siebel CRM Installation and Configuration Guide

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

Agent version: 5.1.2.0

Document version: 5.1.2

Legal Notice

Copyright © 2009 Symantec Corporation. All rights reserved.

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

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's maintenance offerings include the following:

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

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

www.symantec.com/techsupp/

Contacting Technical Support

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

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

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

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

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

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

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

Documentation feedback

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions to clustering_docs@symantec.com. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting.

Maintenance agreement resources

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

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

Additional enterprise services

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

Enterprise services that are available include the following:

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

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

www.symantec.com

Select your country or language from the site index.

Contents

Technical Support 4

Chapter 1 Introducing the Veritas High Availability Agent for Siebel CRM 11

About the Veritas agent for Siebel CRM 11
What's new in this agent 12
Supported software 12
How the agent makes Siebel CRM highly available 13
High availability for Siebel CRM instances running in Solaris zones 13
Siebel CRM agent functions 14
Online 14
Offline 15
Monitor 15
Clean 17
Identifying IPC resources pertaining to Siebel CRM 17
Setting up Siebel CRM in a VCS cluster 18

Chapter 2 Installing and configuring Siebel CRM for high availability 19

About Siebel CRM 19
About Siebel Gateway Server 20
About Siebel Name Server 20
Installing the Siebel Server instance 20
Recommended directory structure 21
Specifying virtual Siebel Server names during installation 22
Installing the database client 22
Using the Siebel installation properties file 23
Setting Siebel Server parameters after installation 23
Setting the host address parameter for a Siebel Server 23
Setting the host parameter for a Siebel Server 24
Configuring the Siebel Server File System 24
Setting environment variables for Siebel CRM 24
Disabling the autostart option 26
Configuring unique port numbers for Siebel Remote Servers 26

Chapter 3 Installing, upgrading, and removing the agent for Siebel CRM 27

Before you install the Veritas agent for Siebel CRM 27
Prerequisites for installing the agent to support Solaris zones 28
About ACC Library 28
Installing the ACC library 29
Installing the agent in a VCS environment 29
Installing the agent in VCS One environment 30
Installing the agent packages using the installer 30
Installing the agent package using the CLI 31
Adding the agent resource type definitions 32
Removing the agent in a VCS environment 33
Removing the agent in VCS One environment 34
Removing the agent packages using the installer 35
Removing the agent package using CLI 36
Removing the agent type definition from the Policy Master system 36
Removing the ACC library 37
Upgrading the agent in a VCS environment 37
Upgrading the agent in a VCS One environment 39

Chapter 4 Configuring the agent for Siebel CRM 41

About configuring the Veritas agent for Siebel CRM 41
Importing the agent types files in a VCS environment 41
Siebel CRM agent attributes 43
Executing a customized monitoring program 48

Chapter 5 Configuring the service groups for Siebel CRM 51

About configuring service groups for Siebel CRM 51
Before configuring the service groups for Siebel CRM 51
Siebel CRM entities in a clustered environment 52
Configuring Siebel Server resources for Solaris zones support 53

Chapter 6 Troubleshooting the agent for Siebel CRM 55

Using the correct software and operating system versions 55
Meeting prerequisites 55
Configuring Siebel CRM resources 56
Starting the Siebel CRM instance outside a cluster 56
Reviewing error log files 60

Using Siebel CRM log files 60
Reviewing cluster log files 61
Using trace level logging 61
Configuration checks for Solaris zones support 62

Appendix A Sample Configurations 63

About sample configurations for the agent for Siebel CRM 63
Sample agent type definition for Siebel CRM 63
For VCS 4.x 63
For VCS 5.0 64
For VCS 5.0 with Solaris zone support 65
Sample configuration files 65
Sample service group configurations for Siebel CRM 69
Sample service group configurations for Solaris zone support 70

Appendix B Changes introduced in previous releases 73

Changes introduced in previous releases 73

Index 75

Chapter 1

Introducing the Veritas High Availability Agent for Siebel CRM

This chapter includes the following topics:

- About the Veritas agent for Siebel CRM
- What's new in this agent
- Supported software
- How the agent makes Siebel CRM highly available
- Siebel CRM agent functions
- Setting up Siebel CRM in a VCS cluster

About the Veritas agent for Siebel CRM

The Veritas High Availability agents monitor specific resources within an enterprise application. They determine the status of resources and start or stop them according to external events.

The Veritas agent for Siebel CRM provides high availability for all Siebel Servers in a cluster. This agent manages the Siebel Servers in a clustered environment. The agent can bring a specific Siebel Server instance online and monitor the state of the Siebel Server. The agent can also detect failures and shut down the instance in case of a failure.

See the following Technical Support TechNote for the latest updates or software issues for this agent:

http://seer.entsupport.symantec.com/docs/282004.htm

What's new in this agent

The enhancements in this release of Veritas High Availability agent for Siebel CRM are as follows:

- Added support for VCS 5.1 on AIX, Linux, and Solaris.
- Added support for VCS One 5.0

For information on the changes introduced in the previous releases,

See "Changes introduced in previous releases" on page 73.

Supported software

The Veritas agent for Siebel CRM supports the following software versions in a VCS environment:

Veritas Cluster Server	■ AIX—VCS 4.0, 5.0, 5.1 ■ Solaris—VCS 4.0, 4.1, 5.0, 5.1 and all intermediate Maintenance Packs of these major releases. **Note:** In the software disc, no separate agent is provided for VCS 4.0 and 5.1 on Solaris. To use the agent for VCS 4.0 and 5.1 on Solaris, use the agent provided for VCS 4.1 and 5.0 respectively. Similarly, on AIX, to use the agent for VCS 5.1, use the agent provided for VCS 5.0
ACC Library	5.1.5.0 and later
Operating Systems	■ AIX 5.1, 5.2, 5.3 on pSeries ■ Solaris 8, 9, 10 including zones and logical domains.
Siebel CRM	7.7, 7.8, 8.0, 8.1 and all intermediate minor versions of these releases.

The Veritas agent for Siebel CRM supports the following software versions in a VCS One environment:

Veritas Cluster Server One	VCS One 2.0, 5.0 on AIX and Solaris
Operating Systems	■ AIX 5.3 on pSeries ■ Solaris 9, 10 including zones.
Siebel CRM	7.7, 7.8, 8.0, 8.1 and all intermediate minor versions of these releases.

How the agent makes Siebel CRM highly available

The agent provides the following levels of application monitoring:

- Primary or Basic monitoring
  This mode has Process check and Health check monitoring options. With the default Process check option, the agent verifies that the Siebel CRM instance processes are present in the process table. Process check cannot detect whether processes are in a hung or stopped states.
- Secondary or Detail monitoring
  In this mode, the agent runs a utility to verify the status of Siebel CRM instance. The agent detects application failure if the monitoring routine reports an improper function of the Siebel CRM instance processes. When this application failure occurs, the Siebel CRM instance service group fails over to another node in the cluster. Thus, the agent ensures high availability for Siebel CRM instance.

High availability for Siebel CRM instances running in Solaris zones

Solaris provides a means of virtualizing operating system services, allowing one or more processes to run in isolation from other activity on the system. Such a "sandbox" is called a "non-global zone." Each zone can provide a rich and customized set of services. The processes that run in a “global zone” have the same set of privileges that are available on a Solaris system today.

VCS provides high availability to applications running in non-global zones by extending the failover capability to zones. VCS is installed in a global zone, and all the agents and the engine components run in the global zone. For applications running within non-global zones, agents run script entry points inside the zones. If a zone configured under VCS control faults, VCS fails over the entire service group containing the zone.

For more details refer to, *Veritas Cluster Server User's Guide.*

The Veritas agent for Siebel CRM is zone-aware and can monitor Siebel CRM instances running in non-global zones.

Siebel CRM agent functions

The agent consists of resource type declarations and agent executables. The agent executables implement the online, offline, monitor, and clean operations.

Online

The online operation performs the following tasks:

- Verifies that the required attributes are set correctly.
- Verifies whether the Siebel Server instance is not already online. If the instance is online, the online operation exits immediately.
- Kills Siebel Server processes that remain online using the login specified by the SiebelUser attribute along with a filter. This ensures that processes belonging to this login, not pertaining to this instance of Siebel Server, are not affected.
- Removes any existing IPC resources that the user specified in the SiebelUser attribute owns, if not registered with the agent as a shared login.
- Performs the following tasks depending on the ServerType attribute:

SRVR	Checks whether a stale .shm file is present. If the file exists, the operation deletes it. Removes the .osdf file, if it is an empty file. Checks if the service file is present. If the service file is an empty file or if the file does not exist, the online operation re-creates the service file. Executes the start_server script as the user specified in the SiebelUser attribute.
GTWY	Executes the start_ns script as the user specified in the SiebelUser attribute.

The online operation ensures that the siebsvc process for the Siebel Server instance starts successfully.

For Siebel Enterprise Server, the operation ensures that the percentage CPU utilization falls below 5 for the siebsvc process. This fall in the percentage ensures that the Siebel Enterprise Server instantiates completely.

Offline

The offline operation performs the following tasks:

- Verifies that the required attributes are set correctly.
- Verifies that the Siebel Server instance is not offline. If found, the operation kills any existing processes that belong to this instance of Siebel being clustered, and exits.
- Executes the stop_ns script as the user specified in the SiebelUser attribute if the ServerType attribute is GTWY.
- Executes the stop_server script as the user specified in the SiebelUser attribute if the ServerType attribute is SRVR.
- Kills any existing processes that belong to this instance of Siebel Server after the offline script is executed.
- Removes any existing IPC resources that the user specified in the SiebelUser attribute owns, if not registered with the agent as a shared login.
- Backs up the siebns.dat file to the /var/tmp/.VRTSSiebel/ResourceName/BACKUP directory if the ServerType attribute is GTWY.

The offline operation exits either after all the processes stop successfully, or after the timeout period specified in the OfflineTimeout attribute expires.

Monitor

The monitor operation monitors the states of the Siebel Servers on all nodes within the cluster.

The operation performs the following tasks:

- Conducts a first level check to determine that the Siebel Server processes that the user specified in the SiebelUser attribute owns, are running on the system in the cluster.
  Depending on the ServerType attribute, the following tasks are performed.

SRVR	Determines whether the siebsvc process is running for the Siebel Server instance.
GTWY	Determines whether the siebsvc process that is configured for the SiebelRoot/sys/siebns.dat file is running for the Siebel Gateway Server instance.

  If the first level check does not find these processes running on the node, the check exits immediately, and reports the instance as offline.

- Conducts a second level check if the SecondLevelMonitor attribute is set to a value greater than 0.
  Depending on the ServerType attribute, the following tasks are performed.

SRVR	Attempts an ODBC connection using the `odbcsql` command. The `odbcsql` command uses the Sadmin and SadminCrPasswd attribute values to determine if the database can be queried. If the ODBC connection is successful, the monitor operation executes the Siebel supplied utility, siebctl, to connect to the Siebel Server instance. If the operation is unable to connect to the instance, the instance is flagged as offline. If the optional attributes, CompGrps, Sadmin, and SadminCrPasswd are defined, the monitor operation executes the Siebel supplied utility, srvrmgr, to connect to the Siebel Server instance. The operation uses this utility to query all the components in the component groups that are listed in attribute CompGrps. If any of the components in the component groups are not in either Running or Online states, the operation flags the state of the Siebel Server instance as unknown. Such a check ensures that the agent for Siebel Server does not fault the resource and the administrator is sufficiently warned to attempt to correct the issue.
GTWY	Executes the `srvredit` command to verify the state of the Siebel Server instance. The `srvredit` command uses the values of the SiebelRoot, SiebelGWHost, and SiebelGWPort attributes for execution. If the Siebel Gateway Name Server needs authentication, it also makes use of the Sadmin and SadminCrPasswd agent attribute values. If the command returns 0, the Siebel Server instance is reported as online.

Note: For Siebel CRM 8.1 and later, any utility that connects to the Siebel Gateway Name Server needs to specify the Gateway Name Server authentication user name and password.

- Depending upon the MonitorProgram attribute, the monitor operation can perform a customized check using a user-supplied monitoring utility.

More information about executing a custom monitor program are available.

See "Executing a customized monitoring program" on page 48.

Clean

The clean operation performs the following tasks in the event of a failure or an unsuccessful attempt to bring a Siebel Server instance online or take it offline:

- Attempts to gracefully shut down the Siebel Server instance.
- Kills the remaining processes pertaining to this Siebel Server if the instance does not shut down normally.
- Removes any existing IPC resources that the user specified in the SiebelUser attribute owns, if not registered with the agent as a shared login.
- Checks whether the .shm file is present if the ServerType attribute is SRVR. If the file is present, the operation deletes it.
  Backs up a copy of the SiebelRoot/sys/siebns.dat file if the ServerType attribute is GTWY. The backup copy is stored as /var/tmp/.VRTSSiebel/ResourceName/BACKUP/siebns.dat.

Identifying IPC resources pertaining to Siebel CRM

Symantec highly recommends installing each Siebel CRM instance to run as a unique UNIX login in the cluster.

This ensures maximum high availability to the Siebel CRM enterprise.

The agent uses the following approach when identifying IPC resources pertaining to a particular Siebel CRM:

- If the UNIX login declared through the SiebelUser attribute is unique within the cluster then the agent removes all IPC resources that this login owns. This ensures that stale IPC resources do not exist, which could prevent the online function of the resource on this cluster node.
- If the UNIX login declared through the SiebelUser attribute is not unique within the cluster, then the following holds true:
  - The value of the SiebelUser attribute indicates that the UNIX login has not been dedicated to this VCS resource alone.
  - The agent has no way to identify IPC resources pertaining to this instance of Siebel Server. The IPC resources are not removed.
    In such an event, the onus of identifying and clearing such IPC resources pertaining to a particular Siebel Server instance lies with the system administrator. Failure to do so can prevent the Siebel Server instance from restarting on this cluster node.

Setting up Siebel CRM in a VCS cluster

Follow the steps below to set up Siebel CRM in a cluster:

- Set up a VCS cluster.
  Refer to *Veritas Cluster Server Installation Guide* for more information on installing and configuring VCS.
- Install and configure Siebel CRM for High Availability.
- Install the Veritas High Availability agent for Siebel CRM.
  See "Installing the agent in a VCS environment" on page 29.
  See "Installing the agent in VCS One environment" on page 30.
- Configure the service groups for Siebel CRM.
  See "About configuring service groups for Siebel CRM" on page 51.

Chapter 2

Installing and configuring Siebel CRM for high availability

This chapter includes the following topics:

- About Siebel CRM
- Installing the Siebel Server instance
- Setting Siebel Server parameters after installation
- Configuring unique port numbers for Siebel Remote Servers

About Siebel CRM

Siebel CRM is a middle-tier platform application that provides back end processes and interactive processes for all Siebel CRM clients.

These processes are present with the Siebel CRM architecture and provide the following functions:

- Mobile Web client synchronization
- Operation of business logic for Siebel Web clients, as well as connectivity and access to the Siebel Database server and Siebel File System
- Integration with legacy or third-party data
- Automatic assignment of new accounts, opportunities, service requests, and other records
- Workflow management

Siebel CRM supports both multi-process and multi-threaded components. The server can operate components in background, batch, and interactive modes. Many of Siebel CRM components can operate on multiple Siebel Servers simultaneously to support an increased number of users or larger batch workloads.

About Siebel Gateway Server

Siebel Gateway Server is a logical entity that consists of a Siebel Name Server. The Siebel Name Server is the primary service of the Siebel Gateway Name Server. The Name Server coordinates the Siebel Enterprise Servers and the Siebel Servers. A single Siebel Gateway Name Server can support Siebel Enterprise Servers.

About Siebel Name Server

The Siebel Name Server provides support for the following Siebel Enterprise Server configuration information:

- Operational parameters
- Connectivity information
- Definition and assignment of component groups and components

This configuration information is dynamic and may change during Siebel CRM installation or configuration. These changes are logged in the siebns.dat file on the Name Server. At startup, the Siebel Server obtains the configuration information from the siebns.dat file.

The Siebel Name Server also serves as the dynamic registry for the Siebel Server and for keeping information about component availability. At startup, a Siebel Server within the Siebel Enterprise Server notifies the Name Server of its availability. The Siebel Server stores the connectivity information such as network addresses in the non-persistent store of the Name Server.

Periodically, the Name Server also flushes its current state to the siebns.dat file. Enterprise components, such as the Server Manager query the Name Server for the Siebel Server availability and connectivity information. When a Siebel Server shuts down, the relevant information is cleared from the Name Server.

Installing the Siebel Server instance

Review the following sections while installing a Siebel Server instance.

- Recommended directory structure
- Specifying virtual Siebel Server names during installation

- Installing the database client
- Using the Siebel installation properties file

Recommended directory structure

A Siebel Enterprise consists of the following core application services:

- A Siebel Gateway Server
- One or more Siebel Enterprise Servers
- A Siebel File System
- A database server
- One or more Web servers

Symantec recommends a directory structure for these services for a simplified cluster configuration.

The following example shows directory structure for two Siebel Servers and two Web servers. But the naming structure supports an unlimited number of each type of servers.

A well designed directory structure also creates a storage environment that is more intuitive and easier to manage.

Table 2-1 shows the Symantec recommended directory structure.

Table 2-1 Recommended directory structure

Recommended directory structure	Description
/siebel/v81/gtw	Mount point of the Siebel Gateway Server.
/siebel/v81/gtw/ora11g	Location for the database client for the Siebel Gateway Server, if it requires database authentication.
/siebel/v81/srv1	Mount point of the first Siebel Server.
/siebel/v81/srv1/ora11g	Location for the database client for the first Siebel Server.
/siebel/v81/srv2	Mount point of the second Siebel Server.
/siebel/v81/srv2/ora11g	Location for the database client for the second Siebel Server.
/siebel/v81/web1	Mount point of the first Web server that is required for SWSE (Siebel Web Extension).

Table 2-1 Recommended directory structure *(continued)*

Recommended directory structure	Description
/siebel/v81/web2	Mount point of the second Web server that is required for SWSE (if needed).

If all the Siebel Servers use a common enterprise level Siebel File System, you can create the /siebel/v81/sfs81 directory on all the configured nodes in the cluster.

This directory is the mount point for the Siebel File System. This file system can be NFS mounted on all nodes in the cluster, that are configured for the Siebel Enterprise Servers. This file system can be configured as a parallel service group using the Mount resource.

If the Siebel Servers use dedicated file systems, then create dedicated mount points for each Siebel File System. For example, /siebel/v81/sfs81_srv1, /siebel/v81/sfs81_srv2.

Ensure that you create Mount resources for each file system. These resources can be a part of the failover service group that is configured for the respective Siebel Server.

Specifying virtual Siebel Server names during installation

While installing a Siebel Server instance, the program prompts you for a logical name to assign to the Siebel Server. Symantec recommends assigning a name that does not include the host name of the system in the cluster. Therefore, the name of a Siebel Server must not imply the system in the cluster on which the instance is allowed to run.

Installing the database client

While installing the Siebel Server, you must also install the appropriate database client software, for example, Oracle client. Symantec recommends installing the database client on the file system that is dedicated to the program and data files of the Siebel Server. This ensures that the Siebel Server instance can access the client, even when the service group switches among the nodes in the cluster.

For Siebel CRM 8.1 and later, the Siebel Gateway Server also needs the database client to be installed for authentication with the database.

Using the Siebel installation properties file

The Siebel e-Business Applications, version 7.5, introduces the use of InstallShield and a Configuration GUI for installation and configuration of the Siebel application on UNIX platforms. During the server installation, the installer creates a vpd.properties file that records installation information. This file is located in /var/adm/siebel directory on the system in which the server is installed.

Note: This is an internal system directory, and not the SiebelRoot directory that is located on shared disk.

This file is not referenced for normal server operations such as startup or shutdown. But the installer may use data from this file to perform other tasks, such as checking versions, applying patches, and adding language packs.

Therefore, when you perform software upgrades to a Siebel Server, ensure that you switch the Siebel service group to the system on which the Group was originally installed, so that the installer is able to access the vpd.properties file. Refer to the Siebel product documentation for more information about this file.

Setting Siebel Server parameters after installation

After installing a Siebel Server, you must set some parameters so that you can cluster the instance.

Perform the following steps to configure the parameters.

- Setting the host address parameter for a Siebel Server
- Setting the host parameter for a Siebel Server
- Configuring the Siebel Server File System
- Setting environment variables for Siebel CRM
- Disabling the autostart option

Setting the host address parameter for a Siebel Server

Siebel versions 7.5 and later introduce a new parameter, ServerHostAddress. This parameter specifies the virtual host name of a Siebel Server instance.

After installing each Siebel Server, perform the following steps to set the ServerHostAddress parameter:

To set the host address parameter for a Siebel Server

1. Log in to the Siebel Server Manager utility, srvrmgr.
2. Change the value of the ServerHostAddress parameter.

```
srvrmgr> change param ServerHostAddress=HostName for server
ServerName
```

Setting the host parameter for a Siebel Server

For Siebel versions 7.5 and later, you must set the Host parameter to enable a Siebel Server instance to run on any system in the cluster. You must set the parameter as equal to the virtual IP host name assigned to the instance.

After installing each Siebel Server, perform these steps to set the ServerHostAddress parameter:

To set the host parameter for a Siebel Server

1. Log in to the Siebel Server Manager utility, srvrmgr.
2. Change the value of the Host parameter:

```
srvrmgr> change param Host=HostName for server ServerName
```

Configuring the Siebel Server File System

Each Siebel Server can either have a dedicated file system, or all Siebel Servers can use a single file system created in the Siebel Enterprise.

For details about this configuration, refer to the Siebel documentation or contact your Siebel administrator.

Setting environment variables for Siebel CRM

The Siebel Server installation program generates two Unix scripts. The Siebel administrators use one of the two scripts to set the environment prior to starting or stopping a Siebel Server instance.

The siebenv.sh script sets the environment for a Bourne or Korn shell. The siebenv.csh script sets the environment for a C shell. In both scripts, ensure that the SIEBEL_GATEWAY environment variable is set to the virtual host name of the Siebel Gateway Server. This variable should not be set to the IP address or the host name of the system.

To ensure database connectivity with the database, environment variables needed by the database client that is used by the Siebel server need to be correctly exported.

Symantec recommends creating a separate environment file (at *SiebelRoot*/envfile) using the default scripts provided by Siebel CRM, so that these environment variables get exported.

Following is an excerpt from a typical environment file that can be used with the agent for Bourne shell on Solaris:

```
#ident "@(#) Environment File for Siebel Enterprise Server 1"
USER=sbl81sv1
HOME=/lhome/sbl81sv1
ORACLE_HOME=/siebel/v81/sv1/ora11g
ORACLE_SID=sbl81sol
LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:
PATH=/bin:/sbin:/opt/VRTSvcs/bin:$ORACLE_HOME/bin:/usr/openwin/bin:
/usr/xpg4/bin:/siebel/v81/sv1/siebsrvr/bin:.
export USER HOME ORACLE_HOME ORACLE_SID LD_LIBRARY_PATH PATH
#
# Copied from siebenv.sh
#
if [ ! -d "$HOME" ]; then
  echo "ERROR: HOME must be set prior to starting the Siebel server!"
  exit 1
fi
```

To create an environment file

1. As user *SiebelUser*, using your favourite editor create a file *SiebelRoot*/envfile and manually add the environment variables as per the excerpt above.

   Creating this file as *SiebelUser* ensures that the new environment file has read permissions for the *SiebelUser*, when this file is sourced by the agent.

2. If you are using Oracle as your database software, and the installation is a 64 bit installation, ensure that "$ORACLE_HOME/lib32" preceeds "$ORACLE_HOME/lib", when setting the value of LD_LIBRARY_PATH (Solaris) or LIBPATH (AIX).

3 Save this file and append the contents of the default environment file provided by Siebel CRM using the following command.

```
$ cat SiebelRoot/siebenv.sh >> SiebelRoot/envfile
```

This creates a complete environment file that needs to be specified as the value of the agent attribute *EnvFile*.

4 Verify that you can start the Siebel Server outside the cluster using this environment file.

See "Starting the Siebel CRM instance outside a cluster" on page 56.

Disabling the autostart option

Ensure that you disable the autostart option while configuring the Siebel Server instance for clustering.

For details about the autostart option, refer to the Siebel documentation or contact your Siebel administrator.

Configuring unique port numbers for Siebel Remote Servers

The Siebel Remote component group provides data synchronization support between Siebel Mobile Web Clients and the Siebel Database server. To perform synchronization, Siebel Mobile Web Client users must be able to connect to a Siebel Remote Server using TCP/IP.

By default, Remote Servers listen for client requests on the 40400 port. If multiple Remote Servers are deployed, and if these Servers are configured within the cluster such that two or more servers may run simultaneously on the same system, ensure that you configure each Remote Server to listen on a unique port.

Such an arrangement is necessary to avoid port number conflicts, since a Remote Server listens on its configured port on all IP addresses active on the system. Therefore the server listens promiscuously on its port for all active IP addresses.

Refer to the Siebel documentation for instructions to configure a port number for a Remote Server.

Chapter 3

Installing, upgrading, and removing the agent for Siebel CRM

This chapter includes the following topics:

- Before you install the Veritas agent for Siebel CRM
- Installing the ACC library
- Installing the agent in a VCS environment
- Installing the agent in VCS One environment
- Removing the agent in a VCS environment
- Removing the agent in VCS One environment
- Removing the ACC library
- Upgrading the agent in a VCS environment
- Upgrading the agent in a VCS One environment

Before you install the Veritas agent for Siebel CRM

You must install the Veritas agent for Siebel CRM on all the systems that will host a Siebel CRM service group.

Ensure that you meet the following prerequisites to install the agent for Siebel CRM.

For VCS, do the following:

- Install and configure Veritas Cluster Server.
  For more information on installing and configuring Veritas Cluster Server, refer to the *Veritas Cluster Server Installation Guide*.
- Remove any previous version of this agent.
  To remove the agent,
  See "Removing the agent in a VCS environment" on page 33.
- Install the latest version of ACC Library.
  To install or update the ACC Library package, locate the library and related documentation on the agentpack disc.
  See "Installing the ACC library" on page 29.

For VCS One, do the following:

- Install and configure Veritas Cluster Server One.
  For more information on installing and configuring Veritas Cluster Server One, refer to the *Veritas Cluster Server One Installation Guide*.
- Remove any previous version of this agent.
  To remove the agent,
  See "Removing the agent in VCS One environment" on page 34.

Prerequisites for installing the agent to support Solaris zones

Ensure that you meet the following prerequisites to install the agent for Siebel CRM:

- Install Siebel CRM to support Solaris zones.
- Install and configure the VCS 5.0 or 5.1 environment to support Solaris zones. Refer to the VCS user documentation for details.
- Install the required version of ACC Library.
- Remove any previous version of this agent.

About ACC Library

The operations of a VCS agent depend on a set of Perl modules known as the ACC library. The library must be installed on each system in the cluster that runs the agent. The ACC library contains common, reusable functions that perform tasks, such as process identification, logging, and system calls.

The ACC library installation package is included within each agent's software distribution media (tar file or CD). Instructions to install or remove the ACC library on a single system in the cluster are given in the following sections. The

instructions assume that the agent's tar file has already been extracted or that you are working from the agent's installation CD.

Installing the ACC library

Install the ACC library on each system in the cluster that runs an agent that depends on the ACC library.

To install the ACC library

1. Log in as superuser.
2. Navigate to the directory containing the package for the platform running in your environment.

AIX	*cd1*/aix/vcs/application/acc_library/*version*_library/pkgs
Solaris	*cd1*/solaris/*dist_arch*/vcs/application/acc_library/*version*_library/pkgs where *dist_arch* is sol_sparc or sol_x64.

3. Install the package. Enter **Yes** if asked to confirm overwriting of files in the existing package.

AIX	`# installp -ac -d VRTSacclib.bff VRTSacclib`
Solaris	`# pkgadd -d VRTSacclib.pkg`

Installing the agent in a VCS environment

Install the agent for Siebel CRM on each node in the cluster.

To install the agent in a VCS environment

1. Log in as superuser.
2. Navigate to the directory containing the package for the platform running in your environment.

AIX	`cd1/aix/vcs/application/siebel_agent/` `vcs_version/version_agent/pkgs`

Solaris	`cd1/solaris/dist_arch/vcs/application/siebel_agent/`
	`vcs_version/version_agent/pkgs`
	where, *dist_arch* is sol_x64 or sol_sparc

3 Install the package.

AIX `# installp -ac -d VRTSsiebel.rte.bff VRTSsiebel.rte`

Solaris `# pkgadd -d . VRTSsiebel`

Installing the agent in VCS One environment

You must install the agent for Siebel CRM on all the client systems of the VCS One cluster that will host the Siebel CRM service group. You can install the agent for Siebel CRM using the installagpack program or using the command line interface (CLI).

The installation of the agent packs involves the following phases:

Installing the agent packages	See "Installing the agent packages using the installer" on page 30.
Adding the agent resource type definitions	See "Adding the agent resource type definitions" on page 32.

Note: The installagpack program supports only the -addtypes, -rmtypes, -responsefile, and -rsh options. Symantec recommends that you do not use any of the other options from the `installagpack` command help output.

Installing the agent packages using the installer

You can install the agent packages on one or more client systems of a specific platform type.

Perform the following steps to install the agent packages using the installer

1 Mount the VCS One Agent Pack software disc on the client system where you plan to run the installation.

2 Depending on the platform type, navigate to the directory containing the agent installer:

AIX `cd1/aix/vcsone/`*`vcsone_version`*

Solaris `cd1/solaris/`*`dist_arch`*`/vcsone/`*`vcsone_version`*

Where, *dist_arch* is 'sol_sparc' or 'sol_x64'.

3 Enter the following command to start the agent pack installation:

```
# ./installagpack [-rsh]
```

You can use the `-rsh` option if rsh and rcp are used for communication between systems instead of the default ssh and scp. This option requires that systems be preconfigured such that the `rsh` commands between systems execute without prompting for passwords or confirmations.

4 Enter the name of the client systems where you want to install the agents.

5 Choose whether to install all the agents or any specific agent. Follow the installer prompt to specify your option.

6 Review the output as the installation program installs the agent packages.

You can view installation logs in the /var/VRTS/install/logs directory.

Installing the agent package using the CLI

You can install the desired agent package using the CLI, on one or more client systems of a specific platform type.

Perform the following steps to install the agent packages using CLI

1. Mount the VCS One Agent Pack software disc on the client system where you plan to run the installation.
2. Depending on the platform type, navigate to the directory containing the agent installer:

   AIX: `# cd1/aix/vcsone/vcsone_version/pkgs`

   Solaris: `# cd1/solaris/dist_arch/vcsone/vcsone_version/pkgs`

   Where *dist_arch* is 'sol_sparc' or 'sol_x64'

3. Type the following command on each client system to install the agent. Answer the prompt accordingly:

   AIX: `# installp -ac -d . VRTSsiebel.rte`

   HP-UX: `# swinstall -s `pwd` VRTSsiebel`

   Linux: `# rpm -ivh VRTSsiebel_rpm_filename`

   Solaris: `# pkgadd -d . VRTSsiebel`

Adding the agent resource type definitions

You must add the agent resource type definitions to the Policy Master database configuration. You can perform this task from any client system in the VCS One cluster.

Note: You must add the agent resource type definitions only one time per platform type.

To add the agent resource types to the PM database configuration

1. Set up rsh or SSH communications between the client system and the PM system.

   For information on configuring SSH for remote communication, refer to the *Veritas Cluster Server One Installation Guide*.

2. Make sure that the PM daemon is running.

   ```
   # /opt/VRTSvcsone/bin/haclus -display
   ```

   The output should show ClusterState is RUNNING.

3. If you have just installed the agents on VCS One client systems and still have the VCS One Agent Pack software disc mounted, skip to step 6.

4. Mount the VCS One Agent Pack software disc.

5. Depending on the platform type, navigate to the directory containing the agent installer:

AIX	`cd1/aix/vcsone/`*`vcsone_version`*
Solaris	`cd1/solaris/`*`dist_arch`*`/vcsone/`*`vcsone_version`* Where *dist_arch* is the sol_sparc or sol_x64.

6. Enter the command to start the agent pack installer for adding resource types to the Policy Master configuration database. Use the `-addtypes` option:

   ```
   # ./installagpack -addtypes
   ```

7. When the installer prompts, enter the virtual IP address of the Policy Master.

8. Review the output as the installer verifies communication with the Policy Master system.

9. Choose whether to add the type definitions for all the agents or for specific agents. Follow the installer prompts to add the type definitions.

10. Review the output as the installer adds the agent types to the PM database configuration and copies the appropriates types.xml files to the PM system.

    You can view installation logs in the /var/VRTS/install/logs directory.

Removing the agent in a VCS environment

You must uninstall the agent for Siebel CRM from a cluster while the cluster is active.

To uninstall the agent in a VCS environment

1. Log in as a superuser.
2. Set the cluster configuration mode to read/write by typing the following command from any node in the cluster:

   ```
   # haconf -makerw
   ```

3. Remove all Siebel CRM resources from the cluster. Use the following command to verify that all resources have been removed:

   ```
   # hares -list Type=Siebel
   ```

4. Remove the agent type from the cluster configuration by typing the following command from any node in the cluster:

   ```
   # hatype -delete Siebel
   ```

   Removing the agent's type file from the cluster removes the include statement for the agent from the main.cf file, but the agent's type file is not removed from the cluster configuration directory. You can remove the agent's type file later from the cluster configuration directory.

5. Save these changes. Then set the cluster configuration mode to read-only by typing the following command from any node in the cluster:

   ```
   # haconf -dump -makero
   ```

6. Use the platform's native software management program to remove the agent for Siebel CRM from each node in the cluster.

   Execute the following command to uninstall the agent:

AIX	`# installp -u VRTSsiebel.rte`
Solaris	`# pkgrm VRTSsiebel`

Removing the agent in VCS One environment

Make sure you stop the agent on all client systems before you remove the service group, the resource type, or both from the VCS One configuration.

You can remove all the VCS One agent packages that the installagpack program installed, or can remove only a particularly desired agent package. Removing the

agent package involves removing the agent files from each client system where it was installed.

Note: Before you attempt to remove the agent package, make sure its application service group is not ONLINE.

See "Removing the agent packages using the installer" on page 35.

See "Removing the agent package using CLI" on page 36.

After removing the agent packages you can remove the agent type definition from the Policy Master system.

See "Removing the agent type definition from the Policy Master system" on page 36.

Removing the agent packages using the installer

You can remove all the agent packages or the desired agent package using the uninstallagpack program.

Note: The uninstallagpack program supports only the -responsefile and -rsh options. Symantec recommends that you do not use any of the other options from the `uninstallagpack` command help output.

To remove the agent packages from the client systems

1. Mount the VCS One Agent Pack software disc on the client system where you plan to run the uninstallagpack program.
2. Depending on the platform type, navigate to the directory containing the agent uninstaller:

   AIX — **`cd1/aix/vcsone/vcsone_version`**

   Solaris — **`cd1/solaris/dist_arch/vcsone/vcsone_version`**

   Where *dist_arch* is the sol_sparc or sol_x64.

3. Start the uninstallagpack program.

   ```
   # ./uninstallagpack [-rsh]
   ```

4 Enter the name of the client systems on which you want to uninstall the agent pack. The names must be separated by spaces.

5 Choose whether to remove all the agent packages or a specific agent package. Follow the installer prompt to remove the agent package.

6 Review the output as the program verifies the agent pack that you installed and removes the agent packages.

You can view logs in the /var/VRTS/install/logs directory.

Removing the agent package using CLI

You can remove a desired agent package using the CLI.

Note: You must remove this agent package from each client system in the cluster.

To remove the agent for Siebel CRM from a client system

- Type the following command on each client system to remove the agent. Answer prompts accordingly:

AIX `# installp -u VRTSsiebel`

Solaris `# pkgrm VRTSsiebel`

Removing the agent type definition from the Policy Master system

After you remove the agent packages, you can remove the agent type definitions for all the agents for specific agents from the Policy Master system.

To remove the agent type definition from the Policy Master system

1 Navigate to the following directory on the client system.

```
# cd /opt/VRTS/install
```

2 Run the following command to remove the agent type definition from the Policy Master system:

```
# ./installagpack -rmtypes
```

3 When the installer prompts, enter the virtual IP address of the Policy Master.

4 Choose whether to remove the type definitions for all the agents or for specific agents. Follow the installer prompts to remove the type definitions.

You can view logs in the /var/VRTS/install/logs directory.

Removing the ACC library

Perform the following steps to remove the ACC library.

To remove the ACC library

1 Ensure that all agents that use ACC library are removed.

2 Run the following command to remove the ACC library package.

AIX	`# installp -u VRTSacclib`
Solaris	`# pkgrm VRTSacclib`

Upgrading the agent in a VCS environment

Perform the following steps to upgrade the agent with minimal disruption, in a VCS environment.

To upgrade the agent in a VCS environment

1 Persistently freeze the service groups that host the application.

```
# hagrp -freeze GroupName -persistent
```

2 Stop the cluster services forcibly.

```
# hastop -all -force
```

3 Ensure that the agent operations are stopped on all the nodes.

```
# ps -ef | grep Siebel
```

4 Uninstall the agent package from all the nodes.

Refer to step 6 from,

Removing the agent in a VCS environment

5 Install the new agent on all the nodes.

See "Installing the agent in a VCS environment" on page 29.

6 Copy the new SiebelTypes.cf file from the agent's sample conf directory,

VCS version	Operating system	Agent types file
VCS 4.x	■ AIX ■ Solaris	/etc/VRTSvcs/conf/sample_Siebel/SiebelTypes.cf
VCS 5.x	■ AIX	/etc/VRTSagents/ha/conf/Siebel/SiebelTypes.cf
VCS 5.0	■ Solaris SPARC and x64	/etc/VRTSagents/ha/conf/Siebel/SiebelTypes50.cf
VCS 5.1	■ Solaris SPARC and x64	/etc/VRTSagents/ha/conf/Siebel/SiebelTypes51.cf

to the VCS conf directory /etc/VRTSvcs/conf/config.

Note: If you are using Solaris SPARC or Solaris x64, copy the SiebelTypes50.cf file for VCS 5.0 (and its intermediate Maintenance Packs) and SiebelTypes51.cf file for VCS 5.1

7 Check for the changes in the resource values required, if any, due to the new agent types file.

Note: To note the list of changed attributes, compare the new type definition file with the old type definition file.

8 Start the cluster services.

```
# hastart
```

9 Start the agent on all nodes, if not started.

```
# haagent -start Siebel -sys SystemName
```

10 Unfreeze the service groups once all the resources come to an online steady state.

```
# hagrp -unfreeze GroupName -persistent
```

Upgrading the agent in a VCS One environment

Perform the following steps to upgrade the agent with minimal disruption, in a VCS One environment.

To upgrade the agent with minimal disruption, in a VCS One environment

1. Freeze service groups that hosts the application.

   `# hagrp -freeze -propagate GroupName`

2. Stop the clients forcibly. Execute the following command from the Policy Master.

   `# hastop -client -sys SystemName -force`

3. Ensure that the agent operations are stopped on all the nodes.

   `# ps -ef | grep Siebel`

4. Uninstall the agent package from all the nodes.

   Refer to step 6 from,

   Removing the agent in VCS One environment

5. Install the new agent on all the nodes in the cluster.

   See "Installing the agent in VCS One environment" on page 30.

6. Add the agent types, using the installagpack program.

   See "Adding the agent resource type definitions" on page 32.

7. Check for the changes in the resource values required, if any, due to the new agent types file.

8. Start the clients.

   `# hastart -client`

9. Start the agent on all nodes, if not started.

   `# haagent -start Siebel -sys SystemName`

10. Unfreeze the service groups.

    `# hagrp -unfreeze -propagate GroupName`

Chapter 4

Configuring the agent for Siebel CRM

This chapter includes the following topics:

- About configuring the Veritas agent for Siebel CRM
- Importing the agent types files in a VCS environment
- Siebel CRM agent attributes
- Executing a customized monitoring program

About configuring the Veritas agent for Siebel CRM

After installing the Veritas agent for Siebel CRM, you must import the agent type configuration file. After importing this file, you can create and configure a Siebel CRM resource. Before you configure a resource, review the attributes table that describes the resource type and its attributes.

To view the sample agent type definition and service groups configuration.

See "About sample configurations for the agent for Siebel CRM" on page 63.

Importing the agent types files in a VCS environment

To use the agent for Siebel CRM, you must import the agent types file into the cluster.

To import the agent types file using the Veritas Cluster Server graphical user interface

1. Start the Veritas Cluster Manager and connect to the cluster on which the agent is installed.
2. Click **File > Import Types**.
3. In the Import Types dialog box, select the following file:

VCS version	Operating System	Agent types file
VCS 4.x	■ AIX ■ Solaris	`/etc/VRTSvcs/conf/sample_Siebel/SiebelTypes.cf`
VCS 5.x	■ AIX	`/etc/VRTSagents/ha/conf/Siebel/SiebelTypes.cf`
VCS 5.0	■ Solaris SPARC and x64	`/etc/VRTSagents/ha/conf/Siebel/SiebelTypes50.cf`
VCS 5.1	■ Solaris SPARC and x64	`/etc/VRTSagents/ha/conf/Siebel/SiebelTypes51.cf`

4. Click **Import**.
5. Save the VCS configuration.

   The Siebel Server agent type is now imported to the VCS engine.

   You can now create Siebel CRM resources. For additional information about using the VCS GUI, refer to the *Veritas Cluster Server User's Guide*.

To import the agent types file using the Veritas Cluster Server command line interface (CLI), perform the following steps.

1. Log on to any one of the systems in the cluster as the superuser.
2. Create a temporary directory.

   ```
   # mkdir ./temp

   # cd ./temp
   ```

3. Copy the sample file Types.cf from the following location:

VCS Version	Operating System	Agent types file
VCS 4.x	■ AIX ■ Solaris	`/etc/VRTSvcs/conf/sample_Siebel/SiebelTypes.cf`

VCS 5.x	■ AIX	/etc/VRTSagents/ha/conf/Siebel/SiebelTypes.cf
VCS 5.0	■ Solaris SPARC and x64	/etc/VRTSagents/ha/conf/Siebel/SiebelTypes50.cf
VCS 5.1	■ Solaris SPARC	/etc/VRTSagents/ha/conf/Siebel/SiebelTypes51.cf

The following example assumes VCS 5.0 is installed on AIX:

```
# cp /etc/VRTSagents/ha/conf/Siebel/SiebelTypes.cf .
```

4 Create a dummy main.cf file:

```
# echo 'include "SiebelTypes.cf"' > main.cf
```

5 Create the Siebel CRM resource type as follows:

```
# hacf -verify .

# haconf -makerw

# sh main.cmd

# haconf -dump
```

The Siebel Server agent type is now imported to the VCS engine.

You can now create Siebel CRM resources. For additional information about using the VCS CLI, refer to the *Veritas Cluster Server User's Guide*.

Siebel CRM agent attributes

Refer to the required and optional attributes while configuring the agent for Siebel CRM.

Table 4-1 lists the required attributes for the Siebel CRM agent.

Table 4-1 Required attributes

Required attributes	Description
EnvFile	Full path to the file that the agent sources to set the environment before executing any Siebel programs. This file is the Siebel supplied shell script, $SIEBEL_ROOT/siebenv.sh. Symantec recommends storing this file on a shared disk. The supported shell environments are: ksh, sh, and csh. Type and dimension: string-scalar Default: "" Example: /siebel/v81/srv1/siebsrvr/envfile
HostName	IP address or host name of the virtual host which is configured for the Siebel Server instance. Type and dimension: string-scalar Default: "" Example 1: sbl81sv1sol Example 2: 10.212.98.240
ResLogLevel	Logging detail performed by the agent for the resource. The valid values are as follows: ■ ERROR: Only logs error messages. ■ WARN: Logs above plus warning messages. ■ INFO: Logs above plus informational messages. ■ TRACE: Logs above plus trace messages. TRACE is very verbose and should only be used during initial configuration or for troubleshooting and diagnostic operations. Type and dimension: string-scalar Default: INFO Example: TRACE
ServerName	Name of the Siebel Server in the Siebel Enterprise. This attribute is not required for a Siebel Gateway Server. Type and dimension: string-scalar Default: "" Example: siebsrv1

Table 4-1 Required attributes *(continued)*

Required attributes	Description
ServerType	Type of Siebel Server that the agent must support. The valid values are as follows: ■ SRVR—for a Siebel Enterprise Server instance ■ GTWY—for a Siebel Gateway Server instance **Note:** In a Siebel Enterprise, you can configure one Siebel Gateway Server instance only. Type and dimension: string-scalar Default: SRVR Example: GTWY
SiebelEnterprise	Name of the Enterprise to which the Siebel Server instance belongs. Type and dimension: string-scalar Default: "" Example: sbl81sol
SiebelGWHost	The virtual host name of the machine that hosts the Siebel Gateway Server instance. You must cluster this instance on one of the nodes in the cluster. For a Siebel Gateway Server instance, the values of the HostName and SiebelGWHost attributes must be the same. Type and dimension: string-scalar Default: "" Example: sbl81gtwsol
SiebelGWPort	The port number on which the Siebel Gateway Server listens. Type and dimension: integer-scalar Default: 2320
SiebelRoot	Full path to the installation or root directory of the Siebel Server. Symantec recommends storing this directory on the shared storage device. Type and dimension: string-scalar Default: "" Example: /siebel/v81/srv1/siebsrvr

Table 4-1 Required attributes *(continued)*

Required attributes	Description
SiebelUser	User name that the agent for Siebel Server uses to execute the programs for managing a Siebel Server instance. Sharing of a UNIX login name across Siebel Servers could also compromise the high availability of the Siebel setup. In case the UNIX login name is not dedicated to the Siebel Server, it has to be registered with the agent by adding a + at the start of the acutal login name. More information about behavior of the agent when a shared login is registered is available. See "Identifying IPC resources pertaining to Siebel CRM" on page 17. The user name must also be synchronized across the systems in the cluster. In other words, the user name must resolve to the same UID and have the same default shell on each system in the cluster. Agent entry points use the getpwnam(3c) function call to obtain UNIX user attributes. As a result, the user can be defined locally or can be defined in a common repository (that is, NIS, NIS+, or LDAP). In the latter case, the agent will fail if the access to this repository fails. With this user, the agent entry points executes Siebel administrative programs such as, start_server, stop_server, startns, stopns, siebctl, and srvrmgr. The user's login shell must be Bourne, Korn, or C shell. Type and dimension: string-scalar Default: "" Example 1 (dedicated UNIX login): sbl81adm Example 2 (shared UNIX login): +sbl81adm

Table 4-2 lists the optional attributes for the Siebel CRM agent.

Table 4-2 Optional attributes

Optional attribute	Description
CompGrps	A comma separated list of the name aliases (CG_ALIAS) for Siebel component groups that the agent for Siebel CRM must monitor. These components must be enabled in the Siebel Enterprise Server. Type and dimension: string-scalar Default: "" Example 1: CallCenter, Sales, SiebAnywhere, Remote Example 2: EAI,System

Table 4-2 Optional attributes *(continued)*

Optional attribute	Description
MonitorProgram	Absolute path name of an external, user-supplied monitor executable. For information about setting this attribute: See "Executing a customized monitoring program" on page 48. Type and dimension: string-scalar Default: "" Example 1: /siebel/v81/srv1/siebsrvr/chk_gendb.sh Example 2: /siebel/v81/srv1/siebsrvr/comm_inbound.pl arg1 arg2
Sadmin	The administrative login that is defined for the Siebel Enterprise. You must use this login if you want to perform a second level check for the Siebel Enterprise Server and the Siebel Gateway Name Server, if the Siebel Gateway Name Server needs authentication. **Note:** Define this attribute for the Siebel Gateway Name Server, only if it requires authentication. Type and dimension: string-scalar Default: sadmin
SadminCrPasswd	Password for the administrator specified in the Sadmin attribute. The password is encrypted using the VCS encrypt utility, vcsencrypt(1m) for VCS cluster and the VCS One encrypt utility, haencrypt(1m) for VCS One Server Farm. **Note:** You need not encrypt the password if you are using the VCS GUI to enter the same. VCS GUI automatically encrypts the password. You must specify this attribute if you have specified the Sadmin, and SecondLevelMonitor attributes. Type and dimension: string-scalar Default: "" Example: EshQfqIqrQnqS

Table 4-2 Optional attributes *(continued)*

Optional attribute	Description
SecondLevelMonitor	Used to enable second-level monitoring. Second-level monitoring is a deeper, more thorough state check of the Siebel Server. The numeric value specifies how often the monitoring routines must run. 0 means never run the second-level monitoring routines, 1 means run routines every monitor interval, 2 means run routines every second monitor interval. This interpretation may be extended to other values. **Note:** Exercise caution while setting SecondLevelMonitor to large numbers. For example, if the MonitorInterval is set to 60 seconds and the SecondLevelMonitor is set to 100, then the second level check is executed every 100 minutes, which may not be as often as intended. For maximum flexibility, no upper limit is defined for SecondLevelMonitor. Type and dimension: integer-scalar Default: 0 Example: 5

Executing a customized monitoring program

You can configure the monitor function to execute a custom monitor utility to perform a user-defined Siebel Server state check. The utility is executed in the context of the UNIX user that is defined in the SiebelUser attribute. The environment is set by sourcing the file specified in the EnvFile attribute.

The monitor function executes the utility specified in the MonitorProgram attribute if the following conditions are satisfied:

- The MonitorProgram attribute value is set to a valid executable utility.
- The first level process check indicates that the Siebel CRM instance is online.
- The SecondLevelMonitor attribute is set to 1 and the second level check returns the server state as "online" or the SecondLevelMonitor attribute is set to a value greater than 1, but the second level check is deferred for this monitoring cycle.

The monitor function interprets the utility exit code as follows:

110 or 0	Siebel Server instance is online
100 or 1	Siebel Server instance is offline
99	Siebel Server instance is unknown
Any other value	Siebel Server instance is unknown

To ensure that the custom monitor utility is always available to the agent application, Symantec recommends storing the file in the directory that the SiebelRoot attribute specifies on the shared storage device.

Chapter 5

Configuring the service groups for Siebel CRM

This chapter includes the following topics:

- About configuring service groups for Siebel CRM
- Before configuring the service groups for Siebel CRM
- Siebel CRM entities in a clustered environment
- Configuring Siebel Server resources for Solaris zones support

About configuring service groups for Siebel CRM

Configuring the Siebel CRM service group involves creating the Siebel Server service group, its resources, and defining attribute values for the configured resources. You must have administrator privileges to create and configure a service group.

You can configure the service groups using one of the following:

- The Cluster Manager (Java console)
- The command-line

Before configuring the service groups for Siebel CRM

Before you configure the Siebel CRM service group, you must:

- Verify that VCS is installed and configured on all nodes in the cluster where you will configure the service group.
  Refer to the *Veritas Cluster Server Installation Guide* for more information.

- Verify that the Veritas agent for Siebel CRM is installed on all nodes in the cluster.
  See "Installing the agent in a VCS environment" on page 29.
  See "Installing the agent in VCS One environment" on page 30.

Siebel CRM entities in a clustered environment

A service group is a logical setup containing all resources that can support a Siebel Server instance in a clustered environment.

The required resources are as follows.

Disk group	Contains a volume and a file system, which is a mount resource containing the Siebel Server installation files. Use the DiskGroup resource type to create this resource. Create the disk group from the shared disk so that you can import the group into any system in the cluster.
Mount	Mounts, monitors, and unmounts the file system that is dedicated to the Siebel Server installation files. Use the Mount resource type to create this resource.
Network interface	Monitors the network interface card through which the Siebel Server instance communicates with other services. Use the NIC resource type to create this resource.
Virtual IP	Configures the virtual IP address dedicated to the Siebel Server instance. The external services, programs, and clients use this address to communicate with this instance. Use the IP resource type to create this resource.
NFS mount	If the Siebel File System is shared among all the Siebel Server instances using NFS services, the file system must be NFS mounted on each node in the cluster. The file system must also be configured for the Siebel Enterprise Server. Placing the remote mount under cluster control ensures effective communication among the resources that are required to bring the Siebel Server instance online. Configuring an NFS Mount resource is optional. Use the Mount resource type to create this resource.
Siebel Server	Starts, stops, and monitors the Siebel Server instance. Use the Siebel resource type to create this resource.

Configuring Siebel Server resources for Solaris zones support

To enable the agent for Siebel CRM to support Solaris zones, ensure that you perform the following configuration steps:

- Install Siebel CRM on dedicated Solaris zones.
- Preferrably, follow the Symantec recommendation of installing zones on a shared disk for convenient configuration, failover, and maintenance.
- Make sure that the name of the Solaris zone is the same as the virtual host name that you use to install and configure the Siebel CRM.
  For sample service groups that depict Solaris zone support:
  See "Sample service group configurations for Solaris zone support" on page 70.
- In a VCS environment, ensure that you have set the value of ContainerName attribute to the name of the Solaris zone.
  By default the agent function executes in the Global zone.

Chapter 6

Troubleshooting the agent for Siebel CRM

This chapter includes the following topics:

- Using the correct software and operating system versions
- Meeting prerequisites
- Configuring Siebel CRM resources
- Starting the Siebel CRM instance outside a cluster
- Reviewing error log files
- Configuration checks for Solaris zones support

Using the correct software and operating system versions

Ensure that no issues arise due to incorrect software and operating system versions. For the correct versions of operating system and software to be installed on the resource systems:

See "Supported software" on page 12.

Meeting prerequisites

Before installing the agent for Siebel CRM, double check that you meet the prerequisites.

For example, you must install the ACC library on VCS before installing the agent for Siebel CRM.

See "Before you install the Veritas agent for Siebel CRM" on page 27.

Configuring Siebel CRM resources

Before using a Siebel CRM resource, ensure that you configure the resource properly. For a list of attributes used to configure all Siebel CRM resources, refer to the agent attributes.

Starting the Siebel CRM instance outside a cluster

If you face problems while working with a resource, you must disable the resource within the cluster framework. A disabled resource is not under the control of the cluster framework, and so you can test the Siebel CRM instance independent of the cluster framework. Refer to the cluster documentation for information about disabling a resource.

You can then restart the Siebel CRM instance outside the cluster framework.

Note: Use the same parameters that the resource attributes define within the cluster framework while restarting the resource outside the cluster framework.

A sample procedure to start a Siebel CRM instance outside the cluster framework, is illustrated as follows.

To start the Siebel Gateway Server instance outside the framework

1 Start the Siebel Gateway Server instance using these commands:

```
# su SiebelUser
$ . EnvFile
$ SiebelRoot/bin/start_ns -p SiebelGWPort
```

2 Execute this command to check whether the siebsvc process of the Siebel Gateway Server instance is present in the processes table of the system:

```
$ /bin/ps -ef | grep siebsvc | grep -v grep
```

For example:

```
SiebelUser 23804 25691   0 12:03:36 ?           1:37 siebsvc -
s gtwyns -a /f SiebelRoot/sys/siebns.dat /t SiebelGWPort /t
SiebelGWPort
```

If this line appears in the processes table, the siebsvc process has started. The user specified in the SiebelUser attribute owns this process, and the repository file is the *SiebelRoot*/sys/siebns.dat file.

3 Execute the following command to query the Siebel Gateway Server instance to verify its version.

For example,

For Siebel CRM 7.7, 7.8 and 8.0

```
$ SiebelRoot/bin/srvredit -q -g SiebelGWHost:SiebelGWPort \
-e none -z -c '$Gateway.VersionString'
```

For Siebel CRM 8.1

```
$ SiebelRoot/bin/srvredit -u Sadmin -p Password -q -g \
SiebelGWHost:SiebelGWPort -e none -z -c '$Gateway.VersionString'
```

Note: For Siebel CRM 8.1 when using any of the Siebel utilities that connect to the Gateway Name Server, you must specify the Gateway Name Server authentication user name and password.

To stop the Siebel Gateway Server instance outside the framework

- If the Siebel Gateway Server instance starts successfully, attempt to shut down the instance using these commands:

```
# su SiebelUser
$ . EnvFile
$ SiebelRoot/bin/stop_ns
```

If you are able to successfully stop a Siebel Gateway Server instance outside the cluster framework, attempt to use the instance inside the framework.

To start the Siebel Enterprise Server outside the framework

1. Execute these commands to start the Siebel Enterprise Server:

```
# su SiebelUser
% source EnvFile
% SiebelRoot/bin/start_server -e SiebelEnterprise \
-g SiebelGWHost:SiebelGWPort ServerName
```

2. Execute this command to check whether the siebsvc process of the Siebel Enterprise Server instance is present in the processes table of the system:

```
$ /bin/ps -ef | grep siebsvc | grep -v grep
```

For example:

```
SiebelUser 20783 20497   0 11:55:22 ?           0:21 siebsvc -
s siebsrvr -a /g SiebelGWHost /e SiebelEnterprise /s
ServerName /g SiebelGWHost:SiebelGWPort
```

If this line appears in the proc table, the siebsvc process of the Siebel Enterprise Server instance has started properly. This process is for the *ServerName* Siebel Server and belongs to the *SiebelEnterprise* Siebel Enterprise. It is configured with the Siebel Gateway Server that is running on the *SiebelGWHost* virtual host, which is listening on the *SiebelGWPort* port.

3. Attempt to query the database to ensure that the Siebel Enterprise Server is able to reach the data stored in the database.

For example, you can execute the following command as the table owner querying the database:

For Siebel 7.7 and 7.8:

```
% SiebelRoot/bin/odbcsql /s siebsrvr_SiebelEnterprise << !
login Sadmin/Password
```

```
quit
!
```

For Siebel 8.0 and 8.1:

```
% SiebelRoot/bin/odbcsql /s SiebelEnterprise_DSN << !
login Sadmin/Password
quit
!
```

If you receive the following message, the Siebel Enterprise Server is able to reach the database:

```
Outstanding transaction committed.
```

You can also consider the following options:

- Ensure that you are able to connect to the database using the database supplied client utilities. For example, for an Oracle database, you can use the tnsping utility to connect to the listener of the database.
- Ensure that the environment variables required for connecting to the database are set correctly. Contact the database administrator for more information.

4 Attempt to check if the component groups specified in the CompGrps attribute are up and running.

For example, consider the following:

- Run the following command to connect to the Siebel Server and enter the authentication password when prompted:

```
% SiebelRoot/bin/srvrmgr \
/e SiebelEnterprise /g SiebelGWHost /q \
/s ServerName \
Password: Password
```

- Check the status of the component groups for *ServerName* server:

```
srvrmgr:ServerName> list compgrp show CG_ALIAS,
CA_RUN_STATE
CG_ALIAS      CA_RUN_STATE
  ------------  ------------
SiebAnywhere  Online
CallCenter    Online
Remote        Running
Sales         Online
```

```
System        Running
5 rows returned.
```

- Check the status of the components in the CallCenter component group.

```
srvrmgr:ServerName> list comp for compgrp CallCenter show
CC_ALIAS, CG_ALIAS, CP_DISP_RUN_STATE

  CC_ALIAS             CG_ALIAS    CP_DISP_RUN_STATE
  -------------------  ----------  -----------------
  SCCObjMgr_enu        CallCenter  Online
  eServiceObjMgr_enu   CallCenter  Online

  2 rows returned.
```

  For the agent to report the cluster resource as ONLINE, the component groups and the components must either be in Running or Online state.

- Quit the connection:

```
srvrmgr:ServerName> quit
```

5 Check if the value of the SadminCrPasswd attribute is set correctly.

To stop the Siebel Enterprise Server outside the framework

- Stop the Siebel Enterprise Server using these commands:

```
# su SiebelUser
% source EnvFile
% SiebelRoot/bin/stop_server -e SiebelEnterprise \
-M ServerName
```

  If you are able to successfully start and stop the Siebel Enterprise Server outside the framework, attempt to use the Server inside the cluster framework.

Reviewing error log files

If you face problems while using Siebel CRM or the agent for Siebel CRM, use the log files described in this section to investigate the problems.

Using Siebel CRM log files

If a Siebel Server is facing problems, you can access the server log files to further diagnose the problem.

- For a Siebel Enterprise Server, the log files are located in the following directories:
  SiebelRoot/log
  SiebelRoot/enterprises/*SiebelEnterprise*/*ServerName*/log
- For a Siebel Gateway Server, the log files are located in the *SiebelRoot*/sys/log directory. You can look for the NameSrvr.log and siebel.log files.

Reviewing cluster log files

In case of problems while using the agent for Siebel CRM, you can also access the engine log file for more information about a particular resource. The engine log files are located at the following location:

- The VCS engine log file is /var/VRTSvcs/log/engine_A.log.
- The VCS One engine log file is /var/VRTSvcsone/log/engine_A.log.
- The VCS One client log file is /var/VRTSvcsone/log/vcsoneclientd_A.log.

Using trace level logging

The ResLogLevel attribute controls the level of logging that is written in a cluster log file for each Siebel CRM resource. You can set this attribute to TRACE, which enables very detailed and verbose logging.

If you set ResLogLevel to TRACE, a very high volume of messages are produced. Symantec recommends that you localize the ResLogLevel attribute for a particular resource.

Note: Starting with version 5.1.1.0 of the ACC library, the TRACE level logs for any ACCLib based agent are generated locally at the location /var/VRTSvcs/log/*Agent*_A.log.

To localize ResLogLevel attribute for a resource

1. Identify the resource for which you want to enable detailed logging.
2. Localize the ResLogLevel attribute for the identified resource:

   ```
   # hares -local Resource_Name ResLogLevel
   ```

3. Set the ResLogLevel attribute to TRACE for the identified resource:

   ```
   # hares -modify Resource_Name ResLogLevel TRACE -sys SysA
   ```

4 Test the identified resource. The function reproduces the problem that you are attempting to diagnose.

5 Set the ResLogLevel attribute back to INFO for the identified resource:

```
# hares -modify Resource_Name ResLogLevel INFO -sys SysA
```

6 Review the contents of the log file. Use the time noted in Step 4 and Step 6 to diagnose the problem.

You can also contact Symantec support for more help.

Configuration checks for Solaris zones support

If you have configured the agent for Siebel CRM to support Solaris zones, ensure that you have followed all the configuration steps described in the following sections:

- Prerequisites for enabling Solaris zone support
  See "Before you install the Veritas agent for Siebel CRM" on page 27.
- Importing the types.cf file for Solaris zone support
  See "Importing the agent types files in a VCS environment" on page 41.
- Configuring the Siebel Server resources for Solaris zone support
  See "Configuring Siebel Server resources for Solaris zones support" on page 53.

Appendix A

Sample Configurations

This appendix includes the following topics:

- About sample configurations for the agent for Siebel CRM
- Sample agent type definition for Siebel CRM
- Sample configuration files
- Sample service group configurations for Siebel CRM
- Sample service group configurations for Solaris zone support

About sample configurations for the agent for Siebel CRM

The sample configuration graphically depicts the resource types, resources, and resource dependencies within the service group. Review these dependencies carefully before configuring the agent for Siebel CRM. For more information about these resource types, see the *Veritas Cluster Server Bundled Agents Reference Guide*.

Sample agent type definition for Siebel CRM

This section lists sample agent type definition for Siebel CRM agent on different versions of VCS.

For VCS 4.x

```
type Siebel (
        static str ArgList[] = { ResLogLevel, State, IState, EnvFile,
```

```
        HostName, SiebelRoot, SiebelUser, Sadmin, SadminCrPasswd,
        SiebelGWHost, SiebelGWPort, ServerName, ServerType,
        SiebelEnterprise, CompGrps, MonitorProgram, SecondLevelMonitor }
        str ResLogLevel = INFO
        str EnvFile
        str HostName
        str SiebelRoot
        str SiebelUser
        str Sadmin = sadmin
        str SadminCrPasswd
        str SiebelGWHost
        int SiebelGWPort = 2320
        str ServerName
        str ServerType = SRVR
        str SiebelEnterprise
        str CompGrps
        str MonitorProgram
        int SecondLevelMonitor = 0
)
```

For VCS 5.0

```
type Siebel (
    static str AgentFile = "/opt/VRTSvcs/bin/Script50Agent"
    static str AgentDirectory = "/opt/VRTSagents/ha/bin/Siebel"
    static str ArgList[] = { ResLogLevel, State, IState, EnvFile,
    HostName, SiebelRoot, SiebelUser, Sadmin, SadminCrPasswd,
    SiebelGWHost, SiebelGWPort, ServerName, ServerType,
    SiebelEnterprise, CompGrps, MonitorProgram, SecondLevelMonitor }
    str ResLogLevel = INFO
    str EnvFile
    str HostName
    str SiebelRoot
    str SiebelUser
    str Sadmin = sadmin
    str SadminCrPasswd
    str SiebelGWHost
    int SiebelGWPort = 2320
    str ServerName
    str ServerType = SRVR
    str SiebelEnterprise
    str CompGrps
```

```
    str MonitorProgram
    int SecondLevelMonitor = 0
)
```

For VCS 5.0 with Solaris zone support

```
type Siebel (
    static str ContainerType = Zone
    static str AgentFile = "/opt/VRTSvcs/bin/Script50Agent"
    static str AgentDirectory = "/opt/VRTSagents/ha/bin/Siebel"
    static str ArgList[] = { ResLogLevel, State, IState, EnvFile,
    HostName, SiebelRoot, SiebelUser, Sadmin, SadminCrPasswd,
    SiebelGWHost, SiebelGWPort, ServerName, ServerType,
    SiebelEnterprise, CompGrps, MonitorProgram, SecondLevelMonitor }
    str ResLogLevel = INFO
    str EnvFile
    str HostName
    str SiebelRoot
    str SiebelUser
    str Sadmin = sadmin
    str SadminCrPasswd
    str SiebelGWHost
    int SiebelGWPort = 2320
    str ServerName
    str ServerType = SRVR
    str SiebelEnterprise
    str CompGrps
    str MonitorProgram
    int SecondLevelMonitor = 0
    str ContainerName
)
```

Sample configuration files

This section lists sample configuration files for Siebel CRM agent on different versions of VCS.

A sample main.cf file is as follows.

```
include "types.cf"
include "SiebelTypes.cf"
```

```
cluster siebel80sol (
    UserNames = { admin = aHIaHChEIdIIgQIcHF }
    Administrators = { admin }
    CredRenewFrequency = 0
    CounterInterval = 5
    )

system nodeA (
    )

system nodeB (
    )

group sbl80gtw (
    SystemList = { nodeA = 0, nodeB = 1 }
    AutoStartList = { nodeA }
    )

    DiskGroup sbl80gtw_dg (
        Critical = 0
        DiskGroup = sbl80gtwsol
        )

    IP sbl80gtw_ip (
        Critical = 0
        Device = bge0
        Address = "10.212.98.244"
        NetMask = "255.255.254.0"
        )

    Mount sbl80gtw_mnt (
        Critical = 0
        MountPoint = "/siebel/v80/gtw"
        BlockDevice = "/dev/vx/dsk/sbl80gtwsol/siebel"
        FSType = vxfs
        FsckOpt = "-y"
        )

    NIC sbl80gtw_nic (
        Critical = 0
        Device = bge1
        NetworkType = ether
        )
```

```
    Siebel sbl80gtw_srvr (
        EnvFile = "/siebel/v80/gtw/gtwysrvr/envfile.csh"
        HostName = sbl80gtwsol
        SiebelRoot = "/siebel/v80/gtw/gtwysrvr"
        SiebelUser = sbl80gtw
        SiebelGWHost = sbl80gtwsol
        ServerType = GTWY
        SiebelEnterprise = sbl80sol
        SecondLevelMonitor = 1
        )

    sbl80gtw_mnt requires sbl80gtw_dg
    sbl80gtw_ip requires sbl80gtw_nic
    sbl80gtw_srvr requires sbl80gtw_ip
    sbl80gtw_srvr requires sbl80gtw_mnt


    // resource dependency tree
    //
    //  group sbl80gtw
    //  {
    //  Siebel sbl80gtw_srvr
    //      {
    //      Mount sbl80gtw_mnt
    //          {
    //          DiskGroup sbl80gtw_dg
    //          }
    //      IP sbl80gtw_ip
    //      }
    //  }


group sbl80srv1 (
    SystemList = { nodeA = 0, nodeB = 1 }
    AutoStartList = { nodeB }
    )

    DiskGroup sbl80srv1_dg (
        Critical = 0
        DiskGroup = sbl80srv1sol
        )
```

```
IP sbl80srv1_ip (
    Critical = 0
    Device = bge0
    Address = "10.212.98.240"
    NetMask = "255.255.254.0"
    )

Mount sbl80srv1_mnt (
    Critical = 0
    MountPoint = "/siebel/v80/srv1"
    BlockDevice = "/dev/vx/dsk/sbl80srv1sol/siebel"
    FSType = vxfs
    FsckOpt = "-y"
    )

NIC sbl80srv1_nic (
    Critical = 0
    Device = bge2
    NetworkType = ether
)

Siebel sbl80srv1_srvr (
    EnvFile = "/siebel/v80/srv1/siebsrvr/envfile.csh"
    HostName = sbl80sv1sol
    SiebelRoot = "/siebel/v80/srv1/siebsrvr"
    SiebelUser = sbl80sv1
    SadminCrPasswd = ftiRgrJrsRorT
    SiebelGWHost = sbl80gtwsol
    ServerName = siebsrv1
    SiebelEnterprise = sbl80sol
    CompGrps = "CallCenter, Remote, Sales, SiebAnywhere, System"
    SecondLevelMonitor = 1
    )

requires group sbl80gtw online global soft
sbl80srv1_mnt requires sbl80srv1_dg
sbl80srv1_ip requires sbl80srv1_nic
sbl80srv1_srvr requires sbl80srv1_ip
sbl80srv1_srvr requires sbl80srv1_mnt


// resource dependency tree
//
```

```
//  group sbl80srv1
//  {
//  Siebel sbl80srv1_srvr
//      {
//      IP sbl80srv1_ip
//      Mount sbl80srv1_mnt
//          {
//          DiskGroup sbl80srv1_dg
//          }
//      }
//  }
```

Sample service group configurations for Siebel CRM

This section includes sample service groups configurations in a VCS environment.

Figure A-1 shows a service group with a Siebel Enterprise Server instance running in a VCS environment.

The service group also includes a DiskGroup resource, a NIC resource, and a Mount resource.

Figure A-1 Sample service group for a Siebel Enterprise Server instance

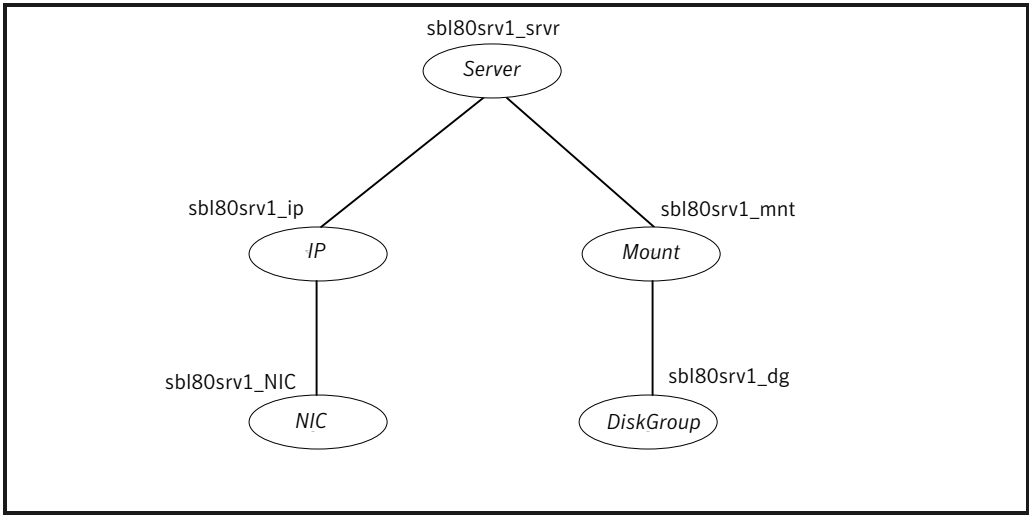
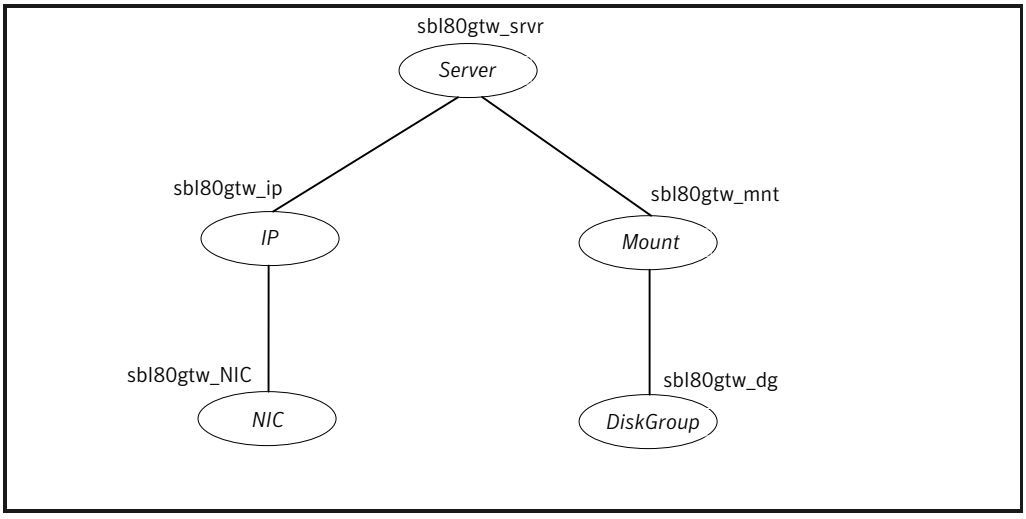


Figure A-2 shows a service group with a Siebel Gateway Server instance running in a VCS environment.

The service group also includes a DiskGroup resource, a NIC resource, and a Mount resource.

Figure A-2 Sample service group for a Siebel Gateway Server instance



Sample service group configurations for Solaris zone support

This section includes sample service groups with Solaris zone support.

Figure A-3 shows a service group with a Siebel Enterprise Server instance running in a local zone, if the zone binaries are present on the shared disk.

The service group also includes a DiskGroup resource, a NIC resource, and a Mount resource.

Figure A-3 Sample service group with a Siebel Enterprise Server instance

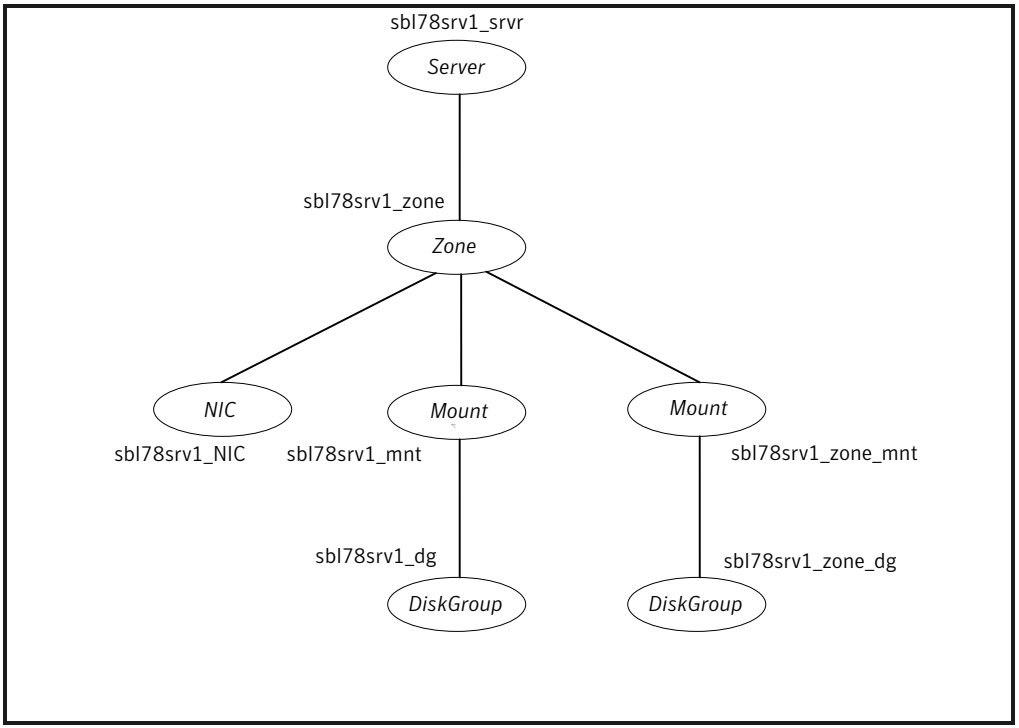
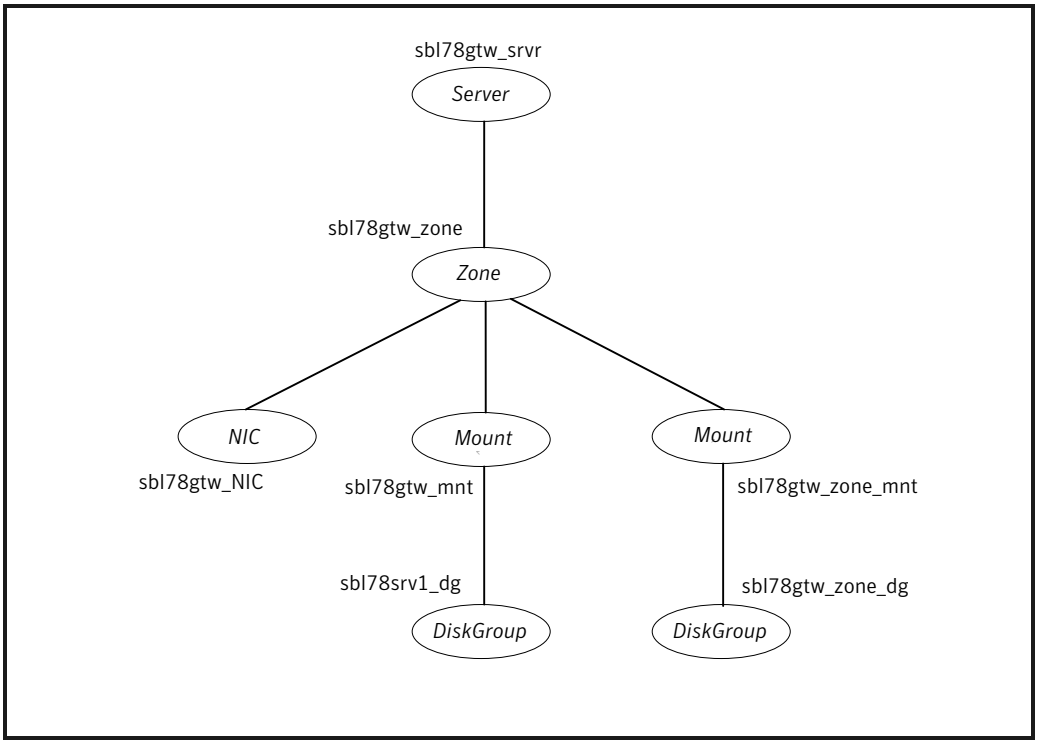


Figure A-4 shows a service group with a Siebel Gateway Server instance running in a local zone, if the zone binaries are present on the shared disk.

The service group also includes a DiskGroup resource, an NIC resource, and a Mount resource.

Figure A-4 Sample service group with a Siebel Gateway Server instance



Appendix B

Changes introduced in previous releases

This appendix includes the following topics:

- Changes introduced in previous releases

Changes introduced in previous releases

The enhancements in the previous releases of Veritas agent for Siebel CRM are as follows:

- Added support for LDOM v1.1 on Solaris
- Added support for Siebel CRM 8.1
- Mandate to specify the values for Sadmin and SadminCrPasswd agent attributes for performing in-depth monitoring on the Siebel Gateway Server, if it requires authentication.
- Mandate to specify the values for Sadmin and SadminCrPasswd agent attributes for performing in-depth monitoring on the Siebel Enterprise Server.
- Added support for VCS One 2.0
- Added support for recovering an empty or missing service file for the Siebel Gateway, in addition to the Siebel Enterprise Server.
- VCS GUI automatically encrypts the values needed for SadminCrPasswd attribute.
- Fix for Siebel administrator's password being visible for srvrmgr check during in depth monitoring of a Siebel Enterprise Server.

Index

A

about
  configuring service groups 51
about ACC library 28
ACC library
  installing 29
  removing 37
agent
  importing agent types files 41
  installing, VCS environment 29
  optional attributes 46
  overview 11
  required attributes 43
  supported software 12
  uninstalling, VCS environment 33
  upgrading 37
  what's new 12
agent attributes
  CompGrps 46
  EnvFile 44
  HostName 44
  MonitorProgram 47
  ResLogLevel 44
  Sadmin 47
  SadminCrPasswd 47
  SecondLevelMonitor 48
  ServerName 44
  ServerType 45
  SiebelEnterprise 45
  SiebelGWHost 45
  SiebelGWPort 45
  SiebelRoot 45
  SiebelUser 46
agent configuration file
  importing 41
agent functions
  configuring monitor function. *See* executing custom monitor program
agent installation
  general requirements 27
  requirements for Solaris zones 28
agent installation *(continued)*
  steps to install 29
agent operations
  clean 17
  monitor 15
  offline 15
  online 14

B

before
  configuring the service groups 51

C

configuring monitor function 48
configuring Siebel Server File System 24

D

disabling autostart option 26

E

executing custom monitor program 48

I

installing Siebel Server instance 20

L

logs
  reviewing cluster log files 61
  reviewing error log files 60
  using Siebel CRM logs 60
  using trace level logging 61

P

post-installation tasks. *See* setting Siebel Server parameters
  configuring Siebel Server File System 24
  disabling autostart option 26
  setting host address parameter 23
  setting host parameter 24

post-installation tasks *(continued)*
setting SIEBEL_GATEWAY environment variable 24

R

removing agent, VCS environment 33

S

sample
configuration file 65
sample agent type definition
VCS 4.x 63
VCS 5.0 64
VCS 5.0, Solaris zone support 65
service group
sample configurations 69
sample configurations, Solaris zone support 70
setting
Siebel CRM in a cluster 18
setting host address parameter 23
setting host parameter 24
setting Siebel Server parameters 23
setting SIEBEL_GATEWAY environment variable 24
Siebel CRM
about Siebel Gateway Server 20
about Siebel Name Server 20
agent attributes 43
agent functions 14
configuring port numbers for Siebel Remote Servers 26
configuring resources 56
configuring resources for Solaris zones 53
entities in clustered environment 52
overview 19
sample agent type definition 63
sample service group configurations 69
sample service group configurations, Solaris zone support 70
starting instance outside cluster 56
Siebel entities, clustered environment 52
Siebel Server installation
installing database client 22
recommended directory structure 21
specifying virtual Siebel Server names 22
using installation properties file 23
Solaris zone support
configuring Siebel Serverresources 53
installation requirements 28
Solaris zone support *(continued)*
Siebel CRM, sample service group configurations 70
troubleshooting 62
starting the Siebel CRM instance outside a cluster 56
supported software 12

T

troubleshooting
configuration checks for Solaris zones support 62
meeting prerequisites 55
reviewing error log files 60
reviewing cluster log files 61
using Siebel CRM log files 60
using trace level logging 61
using correct software 55

U

uninstalling agent, VCS environment 33
upgrading agent 37
VCS One environment 39