Oracle® Solaris Cluster Data Service for Siebel Guide

SPARC Platform Edition
Preface

Oracle Solaris Cluster Data Service for Siebel Guide explains how to install and configure Oracle Solaris Cluster data services.

Note – This Oracle Solaris Cluster release supports systems that use the SPARC and x86 families of processor architectures: UltraSPARC, SPARC64, AMD64, and Intel 64. In this document, x86 refers to the larger family of 64-bit x86 compatible products. Information in this document pertains to all platforms unless otherwise specified.

This document is intended for system administrators with extensive knowledge of Oracle software and hardware. Do not use this document as a planning or presales guide. Before reading this document, you should have already determined your system requirements and purchased the appropriate equipment and software.

The instructions in this book assume knowledge of the Oracle Solaris operating system and expertise with the volume-manager software that is used with Oracle Solaris Cluster software.

Using UNIX Commands

This document contains information about commands that are specific to installing and configuring Oracle Solaris Cluster data services. The document does not contain comprehensive information about basic UNIX commands and procedures, such as shutting down the system, booting the system, and configuring devices. Information about basic UNIX commands and procedures is available from the following sources:

- Online documentation for the Oracle Solaris operating system
- Oracle Solaris operating system man pages
- Other software documentation that you received with your system
Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1   Typographic Conventions

<table>
<thead>
<tr>
<th>Typeface</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>AaBbCc123</td>
<td>The names of commands, files, and directories, and onscreen computer output</td>
<td>Edit your \login file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use \ls -a to list all files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>machine_name% you have mail.</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>What you type, contrasted with onscreen computer output</td>
<td>machine_name% su</td>
</tr>
<tr>
<td>aabbcc123</td>
<td>Placeholder: replace with a real name or value</td>
<td>Password:</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>Book titles, new terms, and terms to be emphasized</td>
<td>The command to remove a file is rm filename.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Read Chapter 6 in the User's Guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A cache is a copy that is stored locally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not save the file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Some emphasized items appear bold online.</td>
</tr>
</tbody>
</table>

Shell Prompts in Command Examples

The following table shows UNIX system prompts and superuser prompts for shells that are included in the Oracle Solaris OS. In command examples, the shell prompt indicates whether the command should be executed by a regular user or a user with privileges.

TABLE P–2   Shell Prompts

<table>
<thead>
<tr>
<th>Shell</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bash shell, Korn shell, and Bourne shell</td>
<td>$</td>
</tr>
<tr>
<td>Bash shell, Korn shell, and Bourne shell for superuser</td>
<td>#</td>
</tr>
<tr>
<td>C shell</td>
<td>machine_name%</td>
</tr>
<tr>
<td>C shell for superuser</td>
<td>machine_name#</td>
</tr>
</tbody>
</table>
Related Documentation

Information about related Oracle Solaris Cluster topics is available in the documentation that is listed in the following table. All Oracle Solaris Cluster documentation is available at http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concepts</td>
<td>Oracle Solaris Cluster Concepts Guide</td>
</tr>
<tr>
<td>Hardware installation and administration</td>
<td>Oracle Solaris Cluster 3.3 3/13 Hardware Administration Manual and individual hardware administration guides</td>
</tr>
<tr>
<td>Software installation</td>
<td>Oracle Solaris Cluster Software Installation Guide</td>
</tr>
<tr>
<td>Data service installation and administration</td>
<td>Oracle Solaris Cluster Data Services Planning and Administration Guide and individual data service guides</td>
</tr>
<tr>
<td>Data service development</td>
<td>Oracle Solaris Cluster Data Services Developer's Guide</td>
</tr>
<tr>
<td>System administration</td>
<td>Oracle Solaris Cluster System Administration Guide</td>
</tr>
<tr>
<td></td>
<td>Oracle Solaris Cluster Quick Reference</td>
</tr>
<tr>
<td>Software upgrade</td>
<td>Oracle Solaris Cluster Upgrade Guide</td>
</tr>
<tr>
<td>Error messages</td>
<td>Oracle Solaris Cluster Error Messages Guide</td>
</tr>
<tr>
<td>Command and function references</td>
<td>Oracle Solaris Cluster Reference Manual</td>
</tr>
<tr>
<td></td>
<td>Oracle Solaris Cluster Data Services Reference Manual</td>
</tr>
</tbody>
</table>

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Getting Help

If you have problems installing or using Oracle Solaris Cluster, contact your service provider and provide the following information.

- Your name and email address (if available)
- Your company name, address, and phone number
- The model number and serial number of your systems
- The release number of the operating environment (for example, Oracle Solaris 10)
The release number of Oracle Solaris Cluster (for example, Oracle Solaris Cluster 3.3)

Use the following commands to gather information about your system for your service provider.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>prtconf (-v)</td>
<td>Displays the size of the system memory and reports information about peripheral devices</td>
</tr>
<tr>
<td>psrinfo (-v)</td>
<td>Displays information about processors</td>
</tr>
<tr>
<td>showrev (-p)</td>
<td>Reports which patches are installed</td>
</tr>
<tr>
<td>prtdiag (-v)</td>
<td>Displays system diagnostic information</td>
</tr>
<tr>
<td>/usr/cluster/bin/clnode show-rev (-v)</td>
<td>Displays Oracle Solaris Cluster release and package version information for each node</td>
</tr>
</tbody>
</table>

Also have available the contents of the \(/var/adm/messages\) file.
Installing and Configuring HA for Siebel

This chapter explains how to install and configure HA for Siebel.

This chapter contains the following sections.

- “HA for Siebel Overview” on page 9
- “Installing and Configuring HA for Siebel” on page 10
- “Planning the HA for Siebel Installation and Configuration” on page 11
- “Preparing the Nodes and Disks” on page 14
- “Installing and Configuring the Siebel Application” on page 16
- “Verifying the Siebel Installation and Configuration” on page 21
- “Installing the HA for Siebel Packages” on page 22
- “Registering and Configuring HA for Siebel” on page 24
- “Verifying the HA for Siebel Installation and Configuration” on page 31
- “Maintaining HA for Siebel” on page 32
- “Tuning the HA for Siebel Fault Monitors” on page 32
- “Upgrading the HA for Siebel Resource Types” on page 34

**HA for Siebel Overview**

HA for Siebel provides fault monitoring and automatic failover for the Siebel application. High availability is provided for the Siebel gateway and Siebel server. With a Siebel implementation, any physical node running the Oracle Solaris Cluster agent cannot be running the Resonate agent as well. Resonate and Oracle Solaris Cluster can coexist within the same Siebel enterprise, but not on the same physical server.

**Note** – Install and configure this data service to run in the global zone, non-global zone, or zone cluster. For updated information about supported configurations of this data service, contact your Oracle service representative.
For conceptual information about failover services, see the *Oracle Solaris Cluster Concepts Guide*.

**TABLE 1** Protection of Siebel Components

<table>
<thead>
<tr>
<th>Siebel Component</th>
<th>Protected by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siebel gateway</td>
<td>HA for Siebel</td>
</tr>
<tr>
<td></td>
<td>The resource type is SUNW.sblgtwy.</td>
</tr>
<tr>
<td>Siebel server</td>
<td>HA for Siebel</td>
</tr>
<tr>
<td></td>
<td>The resource type is SUNW.sblsrvr.</td>
</tr>
</tbody>
</table>

**Installing and Configuring HA for Siebel**

*Table 2* lists the tasks for installing and configuring HA for Siebel. Perform these tasks in the order that they are listed.

**TABLE 2** Task Map: Installing and Configuring HA for Siebel

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan the Siebel installation</td>
<td>“Planning the HA for Siebel Installation and Configuration” on page 11</td>
</tr>
<tr>
<td>Prepare the nodes and disks</td>
<td>“How to Prepare the Nodes” on page 14</td>
</tr>
<tr>
<td>Install and configure Siebel</td>
<td>“How to Install the Siebel Gateway on the Global File System” on page 16</td>
</tr>
<tr>
<td></td>
<td>“How to Install the Siebel Gateway on Local Disks of Physical Hosts” on page 17</td>
</tr>
<tr>
<td></td>
<td>“How to Install the Siebel Server and Siebel Database on the Global File System” on page 19</td>
</tr>
<tr>
<td></td>
<td>“How to Install the Siebel Server and Siebel Database on Local Disks of Physical Hosts” on page 20</td>
</tr>
<tr>
<td>Verify Siebel installation and configuration</td>
<td>“How to Verify the Siebel Installation and Configuration” on page 21</td>
</tr>
<tr>
<td>Install HA for Siebel packages</td>
<td>“Installing the HA for Siebel Packages” on page 22</td>
</tr>
<tr>
<td>Register and configure HA for Siebel as a failover data service</td>
<td>“How to Register and Configure HA for Siebel as a Failover Data Service” on page 25</td>
</tr>
<tr>
<td></td>
<td>“How to Register and Configure the Siebel Server” on page 27</td>
</tr>
</tbody>
</table>
Planning the HA for Siebel Installation and Configuration

This section contains the information you need to plan your HA for Siebel installation and configuration.

Configuration Restrictions

**Caution** – Your data service configuration might not be supported if you do not observe these restrictions.

Use the restrictions in this section to plan the installation and configuration of HA for Siebel. This section provides a list of software and hardware configuration restrictions that apply to HA for Siebel.

For restrictions that apply to all data services, see the release notes for your release of Oracle Solaris Cluster.

- High availability is provided for the Siebel gateway and Siebel server.
- With a Siebel implementation, any physical node running the Oracle Solaris Cluster agent cannot be running the Resonate agent as well. Resonate and Oracle Solaris Cluster can coexist within the same Siebel enterprise, but not on the same physical server.
- If you are using HA for Siebel with HA for Oracle iPlanet Web Server, you **must** configure HA for Oracle iPlanet Web Server as a failover data service. Scalable HA for Oracle iPlanet Web Server **cannot** be used with HA for Siebel.
Configuration Requirements

Caution – Your data service configuration might not be supported if you do not adhere to these requirements.

Use the requirements in this section to plan the installation and configuration of HA for Siebel. These requirements apply to HA for Siebel only. You must meet these requirements before you proceed with your HA for Siebel installation and configuration.

For requirements that apply to all data services, see “Configuration Guidelines for Oracle Solaris Cluster Data Services” in Oracle Solaris Cluster Data Services Planning and Administration Guide.

- Install each Siebel gateway and each Siebel server in its own Siebel root environment (each instance has its own siebenv.sh file). This allows each instance to be independent of others, making failovers and problem diagnosis easier.
- If more than one Siebel server will use the Siebel file system, install the Siebel file system on a global file system. This will ensure that all Siebel server resources have access to the same Filesystem from any node in the cluster.
- Do not use the Autostart feature. When prompted to configure this parameter during the Siebel gateway or Siebel server installation, configure Autostart=NO.

Standard Data Service Configurations

Use the standard configuration in this section to plan the installation and configuration of HA for Siebel. HA for Siebel supports the standard configuration in this section. HA for Siebel might support additional configurations. However, you must contact your Oracle service provider for information on additional configurations.

Figure 1 illustrates a possible configuration using HA for Siebel. The Siebel server and the Siebel gateway are configured as failover data services.
Configuration Planning Questions

Use the questions in this section to plan the installation and configuration of HA for Siebel.

- What is the logical hostname for the following resources: Siebel gateway and Siebel server?
- Where will the system configuration files reside?

See "Configuration Guidelines for Oracle Solaris Cluster Data Services" in Oracle Solaris Cluster Data Services Planning and Administration Guide for the advantages and disadvantages of placing the Siebel binaries on the local file system as opposed to the cluster file system.
Preparing the Nodes and Disks

This section contains the procedures you need to prepare the nodes and disks.

▼ How to Prepare the Nodes

Use this procedure to prepare for the installation and configuration of Siebel.

1 Become super user on all of the nodes.

2 Configure the /etc/nsswitch.conf file so that HA for Siebel starts and stops correctly if a
switchover or a failover occurs.

On each node that can master the logical host that runs HA for Siebel, include the following
entries in the /etc/nsswitch.conf file.

```
passwd: files [NOTFOUND=return] nis [TRYAGAIN=0]
publickey: files [NOTFOUND=return] nis [TRYAGAIN=0]
project: files [NOTFOUND=return] nis [TRYAGAIN=0]
group: files [NOTFOUND=return] nis [TRYAGAIN=0]
```

HA for Siebel uses the su - user command to start, stop, and probe the service.

The network information name service might become unavailable when a cluster node's public
network fails. Adding the preceding entries ensures that the su(1M) command does not refer to
the NIS/NIS+ name services if the network information name service is unavailable.

3 Prevent the Siebel gateway probe from timing out while trying to open a file on /home.

When the node running the Siebel gateway has a path beginning with /home, which depends on
network resources such as NFS and NIS, and the public network fails, the Siebel gateway probe
times out and causes the Siebel gateway resource to go offline. Without the public network,
Siebel gateway probe hangs while trying to open a file on /home, causing the probe to time out.

To prevent the Siebel gateway probe from timing out while trying to open a file on /home,
configure all nodes of the cluster that can be the Siebel gateway as follows:

a. Eliminate all NFS or NIS dependencies for any path starting with /home.

You may either have a locally mounted /home path or rename the /home mount point to
/export/home or another name which does not start with /home.

b. Comment out the line containing +auto_master in the /etc/auto_master file, and change
any /home entries to auto_home.

c. Comment out the line containing +auto_home in the /etc/auto_home file.

4 Prepare the Siebel administrator's home directory.
Preparing the Nodes and Disks

5 On each node, create an entry for the Siebel administrator group in the `/etc/group` file, and add potential users to the group.

   **Tip** – In the following example, the Siebel administrator group is named `siebel`.

   Ensure that group IDs are the same on all of the nodes that run HA for Siebel.

   ```
   siebel:*:521:
   ```

   You can create group entries in a network name service. If you do so, also add your entries to the local `/etc/inet/hosts` file to eliminate dependency on the network name service.

6 On each node, create an entry for the Siebel administrator.

   **Tip** – In the following example, the Siebel administrator is named `siebel`.

   The following command updates the `/etc/passwd` and `/etc/shadow` files with an entry for the Siebel administrator.

   ```
   # useradd -u 121 -g siebel -s /bin/ksh -d /Siebel-home siebel
   ```

   Ensure that the Siebel user entry is the same on all of the nodes that run HA for Siebel.

7 Ensure that the Siebel administrator's default environment contains settings for accessing the Siebel database. For example, if the Siebel database is on Oracle, the following entries may be included in the `.profile` file.

   ```
   export ORACLE_HOME=/global/oracle/OraHome
   export PATH=$PATH:$ORACLE_HOME/bin
   export LD_LIBRARY_PATH=$ORACLE_HOME/lib:/usr/lib
   export TNS_ADMIN=$ORACLE_HOME/network/admin
   export ORACLE_SID=siebeldb
   ```

8 Create a failover resource group to hold the logical hostname and the Siebel gateway resources.

   ```
   # clresourcegroup create [-n node] failover-rg
   ```

   `-n node` Specifies the node name that can master this resource group.

   `failover-rg` Specifies your choice of the name of the failover resource group to add. This name must begin with an ASCII character.

9 Add the logical hostname resource.

   Ensure that logical hostname matches the value of the SIEBEL_GATEWAY environment variable that is set in the `siebenv.sh` file of the Siebel gateway, and also the Siebel server installations.

   ```
   # clreslogicalhostname create -g failover-rg logical_host
   ```

   `logical_host` Specifies an optional resource name of your choice.
Installing and Configuring the Siebel Application

This section contains the procedures you need to install and configure the Siebel application. To install the Siebel application, you must install the Siebel gateway, the Siebel server, and the Siebel database.

To install the Siebel application, you need the following information about your configuration.

- The gateway and server root directories (installation locations).
- The logical host names for the Siebel gateway and Siebel server (one logical hostname per Siebel server instance, if they are to failover independently).
  
  You must configure these addresses and they must be online.

To install the Siebel application, see the following sections.

- “Installing the Siebel Gateway” on page 16
- “Installing the Siebel Server and Siebel Database” on page 18

Installing the Siebel Gateway

You can install the Siebel gateway either on the global file system or on local disks of physical hosts. To install the Siebel gateway, see one of the following procedures.

- “How to Install the Siebel Gateway on the Global File System” on page 16
- “How to Install the Siebel Gateway on Local Disks of Physical Hosts” on page 17

How to Install the Siebel Gateway on the Global File System

Use this procedure to install the Siebel gateway on the global file system. To install the Siebel gateway on local disks of physical hosts, see “How to Install the Siebel Gateway on Local Disks of Physical Hosts” on page 17.

To install the Siebel gateway on the global file system, install the Siebel software only once from any node of the cluster.

Install the Siebel gateway by following the instructions in the Siebel installation documentation and the latest release notes.

Do not use the Autostart feature. When prompted, configure Autostart=NO.
Verifying the $suitev.sh file is under gateway_root, and is owned by the user who will launch the Siebel gateway.

In the home directory of the user who will launch the Siebel gateway, create an empty file that is named .hushlogin.

The .hushlogin file prevents failure of a cluster node’s public network from causing an attempt to start, stop, or probe the service to time out.

Change the SIEBEL_GATEWAY to the logical hostname that is selected for the Siebel gateway in siebenv.sh and siebenv.csh files under gateway_root.

Stop and restart the Siebel gateway to ensure that the gateway is using the logical hostname.

How to Install the Siebel Gateway on Local Disks of Physical Hosts

Use this procedure to install the Siebel gateway on local disks of physical hosts. To install the Siebel gateway on the global file system, see “How to Install the Siebel Gateway on the Global File System” on page 16.

Note – To install the Siebel gateway on local disks of physical hosts, the directory gateway_root/sys must be highly available (it must be installed on a global file system).

Verify that the $suitev.sh file is under gateway_root, and is owned by the user who will launch the Siebel gateway.

In the home directory of the user who will launch the Siebel gateway, create an empty file that is named .hushlogin.

The .hushlogin file prevents failure of a cluster node’s public network from causing an attempt to start, stop, or probe the service to time out.

Change the SIEBEL_GATEWAY to the logical hostname that is selected for the gateway in siebenv.sh and siebenv.csh files under gateway_root.

Stop and restart the Siebel gateway to ensure that the gateway is using the logical hostname.
6 Move gateway_root/sys to /global/siebel/sys and create a link to the global file system from the local file system.

   # mv gateway_root/sys /global/siebel/sys
   # ln -s /global/siebel/sys gateway_root/sys

7 Replicate the installation on all remaining nodes of the cluster.

   # rdist -c gateway_root hostname:gateway_root

8 Verify that the ownerships and permissions of the files and directories in the Siebel gateway installation are identical on all nodes of the cluster.

9 For each node on the cluster, change the ownership of the link to the appropriate Siebel user.

   # chown -h siebel:siebel gateway_root/sys

10 As Siebel user, verify that the gateway is properly installed and configured.

    Ensure the command below returns a version string.

    $ srvredit -q -g SIEBEL_GATEWAY -e none -z -c '$Gateway.VersionString'

11 If you are using Siebel 8.1 or later version, use the following command to verify the status of the gateway server:

    $ srvredit -q -u gateway_user -p gateway_pwd -g Siebel_gateway -e none -z -c \  
    '$Gateway.VersionString'

    Where:

    ■ gateway_user - user name for gateway authentication
    ■ gateway_pwd - password for gateway authentication

## Installing the Siebel Server and Siebel Database

You can install the Siebel server either on the global file system or on local disks of physical hosts.

**Note** – If more than one Siebel server will use the Siebel Filesystem, you must install the Siebel Filesystem on a global file system.

To install the Siebel server and configure the Siebel server and Siebel database, see one of the following procedures

- “How to Install the Siebel Server and Siebel Database on the Global File System” on page 19
- “How to Install the Siebel Server and Siebel Database on Local Disks of Physical Hosts” on page 20
How to Install the Siebel Server and Siebel Database on the Global File System

Use this procedure to install the Siebel server and configure the Siebel server and Siebel database on the global file system. To install the Siebel server on local disks of physical hosts, see “How to Install the Siebel Server and Siebel Database on Local Disks of Physical Hosts” on page 20.

To install the Siebel server on the global file system, install the software only once from any node of the cluster.

1 Install the Siebel server by following the instructions in the Siebel installation documentation and the latest release notes.
   Do not use the Autostart feature. When prompted, configure Autostart=No.
   When prompted to enter the gateway hostname, enter the logical hostname for the Siebel gateway.

2 Verify that the siebenv.sh file is under server_root and is owned by the user who will launch the Siebel server.

3 In the home directory of the user who will launch the Siebel server, create an empty file that is named .hushlogin.
   The .hushlogin file prevents failure of a cluster node's public network from causing an attempt to start, stop, or probe the service to time out.

4 Ensure that a database such as HA Oracle is configured for Siebel and that the database is online.

5 Use the Siebel documentation to configure and populate the Siebel database.

6 Create a database user (for example, dbuser/dbpassword) with permission to connect to the Siebel database for use by the HA for Siebel Fault Monitor.

7 Log in as the user who will launch the Siebel server and manually start the Siebel server.

8 Run srvrmgr to change the configuration of Siebel server to enable Siebel server to run in a cluster.

   - If you are using Siebel 7.7 or a later version, change the ServerHostAddress parameter to the IP address of the Siebel server's logical host name resource.
     $ srvrmgr:hasiebel> change param ServerHostAddress=lhaddr for server hasiebel

   - If you are using a version of Siebel earlier than 7.7, change the HOST parameter to the logical hostname for the Siebel server.
     $ srvrmgr:hasiebel> change param Host=lhname for server hasiebel
Note – These changes take effect when the Siebel server is started under Oracle Solaris Cluster control.

How to Install the Siebel Server and Siebel Database on Local Disks of Physical Hosts

Use this procedure to install the Siebel server and configure the Siebel server and Siebel database on local disks of physical hosts. To install the Siebel server on the global file system, see “How to Install the Siebel Server and Siebel Database on the Global File System” on page 19.

To install the Siebel server on the local disks of the physical hosts, install the software on any one node of the cluster.

1 Install the Siebel server by following the instructions in the Siebel installation documentation and the latest release notes.
   Do not use the Autostart feature. When prompted, configure Autostart=No.
   When prompted to enter the gateway hostname, enter the logical hostname for the Siebel gateway.

2 Verify that the siebenv.sh file is under server_root and is owned by the user who will launch the Siebel server.

3 In the home directory of the user who will launch the Siebel server, create an empty file that is named .hushlogin.
   The .hushlogin file prevents failure of a cluster node’s public network from causing an attempt to start, stop, or probe the service to time out.

4 Ensure that a database such as HA Oracle is configured for Siebel and that the database is online.

5 Use the Siebel documentation to configure and populate the Siebel database.

6 Create a database user (for example, dbuser/dbpassword) with permission to connect to the Siebel database for use by the HA for Siebel Fault Monitor.

7 Log in as the user who will launch the Siebel server and manually start the Siebel server.
Run `srvrmgr` to change the configuration of Siebel server to enable Siebel server to run in a cluster.

- If you are using Siebel 7.7 or later version, change the `ServerHostAddress` parameter to the IP address of the Siebel server’s logical host name resource.
  ```
  $ srvrmgr:hasiebel> change param ServerHostAddress=lhaddr for server hasiebel
  ```

- If you are using a version of Siebel earlier than 7.7, change the `HOST` parameter to the logical hostname for the Siebel server.
  ```
  $ srvrmgr:hasiebel> change param Host=lhname for server hasiebel
  ```

Note – These changes take effect when the Siebel server is started under Oracle Solaris Cluster control.

Replicate the installation on all of the remaining nodes of the cluster.

# `rdist -c server_root hostname:server_root`

Verify that the ownerships and permissions of files and directories in the Siebel gateway installation are identical on all nodes of the cluster.

---

### Verifying the Siebel Installation and Configuration

This section contains the procedure you need to verify the Siebel installation and configuration.

#### How to Verify the Siebel Installation and Configuration

Use this procedure to verify the Siebel gateway, Siebel server, and Siebel database installation and configuration. This procedure does not verify that your application is highly available because you have not installed your data service yet.

1. Verify that the logical hostname is online on the node on which the resource will be brought online.
2. Manually start the Siebel gateway as the user who will launch the Siebel gateway.
3. Manually start the Siebel server as the user who will launch the Siebel server.
4 **Use odbcsql to verify connectivity to the Siebel database.**

```
# odbcsql /s siebsrvr_siebel_enterprise /u dbuser /p dbpassword
```

**Note**—For Siebel 8.0, the data source name is DSN. Use the following command for Siebel 8.0.

```
# odbcsql /s siebel Enterprise DSN /u dbuser /p dbpassword
```

5 **Run list servers subcommand under srvrmgr.**

Before the Siebel server is configured to be highly available, the HOST_NAME parameter for the Siebel server shows the physical host name.

After the Siebel server is configured to be highly available, the output from this command depends on the version of Siebel that you are using.

- If you are using Siebel 7.7 or later, the HOST_NAME parameter for the Siebel server shows the physical host name of the node where Siebel server is running. Therefore, running this command at different times might show different names, depending on whether the Siebel server resource has failed over or has been switched over.

- If you are using a version of Siebel earlier than 7.7, the HOST_NAME parameter for the Siebel server shows the logical host name.

6 **If you are using Siebel 7.7 or later, confirm that the serverhostaddress parameter is set to the IP address of the Siebel server’s logical host name resource.**

```
$ srvrmgr:hasiebel> list advanced param serverhostaddress
```

7 **Test various Siebel user sessions, such as sales and call center using a Siebel dedicated client and supported thin client (browser).**

8 **Manually stop the Siebel server as the user who started the Siebel server.**

9 **Manually stop the Siebel gateway as the user who started the Siebel gateway.**

### Installing the HA for Siebel Packages

If you did not install the HA for Siebel packages during your initial Oracle Solaris Cluster installation, perform this procedure to install the packages. To install the packages, use the installer program.

**Note**—You need to install the HA for Siebel packages in the global cluster and not in the zone cluster.
How to Install the HA for Siebel Packages

Perform this procedure on each cluster node where you want the HA for Siebel software to run.

You can run the installer program with a command-line interface (CLI) or with a graphical user interface (GUI). The content and sequence of instructions in the CLI and the GUI are similar.

Note – Even if you plan to configure this data service to run in non-global zones, install the packages for this data service in the global zone. The packages are propagated to any existing non-global zones and to any non-global zones that are created after you install the packages.

Before You Begin

Ensure that you have the Oracle Solaris Cluster installation media.

If you intend to run the installer program with a GUI, ensure that your DISPLAY environment variable is set.

1 On the cluster node where you are installing the data service packages, become superuser.

2 Load the Oracle Solaris Cluster installation media into the DVD-ROM drive.

If the Volume Management daemon vold(1M) is running and configured to manage DVD-ROM devices, the daemon automatically mounts the DVD-ROM on the /cdrom directory.

3 Change to the installation wizard directory of the DVD-ROM.

- If you are installing the data service packages on the SPARC platform, type the following command:
  
  ```
  # cd /cdrom/cdrom0/Solaris_sparc
  ```

- If you are installing the data service packages on the x86 platform, type the following command:
  
  ```
  # cd /cdrom/cdrom0/Solaris_x86
  ```

4 Start the installation wizard.

  ```
  # ./installer
  ```

5 When you are prompted, accept the license agreement.

6 From the list of Oracle Solaris Cluster agents under Availability Services, select the data service for Siebel.
If you require support for languages other than English, select the option to install multilingual packages. English language support is always installed.

When prompted whether to configure the data service now or later, choose Configure Later. Choose Configure Later to perform the configuration after the installation.

Follow the instructions on the screen to install the data service packages on the node. The installation wizard displays the status of the installation. When the installation is complete, the wizard displays an installation summary and the installation logs.

(GUI only) If you do not want to register the product and receive product updates, deselect the Product Registration option. The Product Registration option is not available with the CLI. If you are running the installation wizard with the CLI, omit this step.

Exit the installation wizard.

Unload the installation media from the DVD-ROM drive.

a. To ensure that the DVD-ROM is not being used, change to a directory that does not reside on the DVD-ROM.

b. Eject the DVD-ROM.

# eject cdrom

Registering and Configuring HA for Siebel

This section contains the procedures you need to configure HA for Siebel.

Setting HA for Siebel Extension Properties

The sections that follow contain instructions for registering and configuring resources. These instructions explain how to set only extension properties that HA for Siebel requires you to set. For information about all HA for Siebel extension properties, see HA for Siebel Extension Properties. You can update some extension properties dynamically. You can update other properties, however, only when you create or disable a resource. The Tunable entry indicates when you can update a property.
To set an extension property of a resource, include the following option in the `clresource(1CL)` command that creates or modifies the resource:

```
-p property=value
```

- `property` Identifies the extension property that you are setting
- `value` Specifies the value to which you are setting the extension property

You can also use the procedures in Chapter 2, “Administering Data Service Resources,” in Oracle Solaris Cluster Data Services Planning and Administration Guide to configure resources after the resources are created.

▼ **How to Register and Configure HA for Siebel as a Failover Data Service**

Use this procedure to configure HA for Siebel as a failover data service. This procedure assumes that the data service packages are already installed. If the HA for Siebel packages are not already installed, see “Installing the HA for Siebel Packages” on page 22 to install the packages. Otherwise, use this procedure to configure the HA for Siebel.

1. **On one of the nodes in the cluster that hosts the application server become superuser or assume a role that provides `solaris.cluster.modify` and `solaris.cluster.admin` RBAC authorizations.**

2. **Register the resource type for the Siebel gateway.**

   ```
   # clresourcetype register SUNW.sblgtwy
   ```

3. **Create a failover resource group to hold the logical hostname and the Siebel gateway resources.**

   ```
   # clresourcegroup create [-n node] gateway-rg
   
   -n node Specifies the node name that can master this resource group.
   
   gateway-rg Specifies your choice of the name of the failover resource group to add. This name must begin with an ASCII character.
   ```

   Note – If you have already created a resource group, added the logical hostname resource, and brought the resource group online when you completed the “How to Prepare the Nodes” on page 14 procedure, you may skip to Step 6.
4 Add the logical hostname resource.

Ensure that logical hostname matches the value of the SIEBEL_GATEWAY environment variable that is set in the siebenv.sh file of the Siebel gateway, and also the Siebel server installations.

```bash
# cGRESlogicalhostname create -g gateway-rg logical_host
logical_host Specifies an optional resource name of your choice.
```

5 Bring the resource group online.

```bash
# cGRESresourcegroup online -M gateway-rg
```

6 Verify that siebenv.sh file exists under gateway_root.

The owner of this file launches the Siebel gateway server when the Siebel gateway resource is brought online.

7 If you are using Siebel 8.1 or later version, create a file called scgtwyconfig under gateway_root, owned by the owner of siebenv.sh.

If the Siebel gateway is installed locally, create the file scgtwyconfig under gateway_root on all nodes. For security reasons, make this file readable only by the owner.

```bash
# cd gateway_root
# touch scgtwyconfig
# chown siebel:siebel scgtwyconfig
# chmod 400 scgtwyconfig
```

8 If you are using Siebel 8.1 or later version, in the scgtwyconfig file, enter the gateway user name and password that was given while configuring the gateway server enterprise.

For example: gtwyuser gtwypassword

This user name and password combination must have permission to connect to the database and also to the gateway server for use by the Sun Cluster HA for Siebel Gateway Fault Monitor.

```bash
export GTWYUSR=gtwyuser
export GTWYPWD=gtwyuserpassword
```

9 Optional: If you want to encrypt the scgtwyconfig file, perform the following steps.

   a. As root user, encrypt the password file scgtwyconfig for the gateway server and place the password file and the key file in the /var/cluster directory.

In the example below, the password file scgtwyconfig is being encrypted and gtwy-rg reflects the gateway server resource name. The key file name must be in the format /var/cluster/.gateway_resource_name_key. The password file name must be in the format /var/cluster/.gateway_resource_name_gtwy_pdata. The PATH_TO_CONFIGFILE is the location of the scgtwyconfig file.

```bash
node1# dd if=/dev/urandom of=/var/cluster/.sblgtwy-rg_key bs=16 count=1
node1# chmod 400 /var/cluster/.sblgtwy-rg_key
node1# usr/sfw/bin/openssl enc -aes128 -e -in \$PATH_TO_CONFIGFILE/scgtwyconfig -k 
```
b. Verify that the encrypted password can be decrypted.

```bash
node1# /usr/sfw/bin/openssl enc -aes128 -d -in /var/cluster/.sblgtwy-rs_gtwy_pdata -k /var/cluster/.sblgtwy-rs_key -out /var/cluster/tmpfile
```

c. Repeat steps a and b on all other Oracle Solaris Cluster nodes that will host the gateway server resource.

10 Create the Siebel gateway resource.

```bash
# clresource create -g gateway-rg \\
-t SUNW.sblgtwy \\
-p Confdir_list=gateway_root -p siebel_version=version number sblgtwy-rs \\
-p Confdir_list=gateway_root -p siebel_version=version number sblgtwy-rs
```

- **Specifiesthe name of the resource type for the resource.**
- **Specifiesthe path name to the Siebel server root directory.**
- **Specifiesthe Siebel server version.**

---

**Caution** – If you enter an incorrect value for `siebel_version`, you might not see errors during validation but the resource startup will fail. If `siebel_version` is incorrect, the probe method is not able to verify database connectivity.

**sblgtwy-rs** Specifies your choice of the name of the resource to add.

The resource is created in the enabled state.

11 Verify that the Siebel resource group and the Siebel gateway resource are online by using `cluster status -t resourcegroup,resource` and `ps -ef`.

▼ **How to Register and Configure the Siebel Server**

1 Add the resource type for the Siebel server.

```bash
# clresource create SUNW.sblsrvr
```

2 Create the failover resource group to hold the logical hostname and the Siebel server resources.

---

**Note** – If you have already created a resource group, added the logical hostname resource, and brought the resource group online when you completed the "How to Prepare the Nodes" on page 14 procedure, you may skip to Step 5.
# clresourcegroup create [-n node] siebel-rg

- **node**  Specifies the node name that can master this resource group.

- **siebel-rg**  Specifies your choice of the name of the failover resource group to add. This name must begin with an ASCII character.

3 **Add the logical hostname resource.**

This logical hostname should match the value of the HOST_NAME parameter for the Siebel server.

# clreslogicalhostname create -g siebel-rg logical_host

  **logical_host**  Specifies an optional resource name of your choice.

4 **Bring the resource group online.**

The following command brings the resource group online on the preferred node.

# clresourcegroup online -M siebel-rg

5 **Verify that the siebenv.sh file is located under server_root.**

6 **Create a file called scsblconfig under server_root, owned by the owner of siebenv.sh.**

If the Siebel server is installed locally, create the file scsblconfig under server_root on all nodes.

For security reasons, make this file readable only by the owner.

# cd server_root
# touch scsblconfig
# chown siebel:siebel scsblconfig
# chmod 400 scsblconfig

7 **Select a database user (for example, dbuser/dbuserpassword) with permission to connect to the database for use by the HA for Siebel Fault Monitor.**

8 **Select another Siebel user (for example, sadmin/sadminpassword) with permission to run the compgrps command in srvrmgr.**

9 **Add the following entries into the scsblconfig file.**

   ```
   export DBUSR=dbuser
   export DBPWD=dbuserpassword
   export SADMUSR=sadmin
   export SADMPWD=sadminpassword
   ```
10 Optional: If you want to encrypt the scsblconfig file, perform the following steps.

a. As root user, encrypt the password file scsblconfig for the Siebel server and place the password file and the key file in the /var/cluster directory.

In the example below, the password file scsblconfig is being encrypted and sieb-rs reflects the Siebel server resource name. The key file name must be in the format /var/cluster/.siebelserver_resource_name_key. The password file name must be in the format /var/cluster/.siebelserver_resource_name_sbl_pdata. The PATH_TO_CONFIGFILE is the location of the scsblconfig file.

```
node1# dd if=/dev/urandom of=/var/cluster/.sieb-rs_key bs=16 count=1
node1# chmod 400 /var/cluster/.sieb-rs_key
node1# /usr/sfw/bin/openssl enc -aes128 -e -in 
SPATH_TO_CONFIGFILE/scsblconfig -k /var/cluster/.sieb-rs_key -out 
/var/cluster/.sieb-rs_sbl_pdata
node1# chmod 400 /var/cluster/.sieb-rs_sbl_pdata
```

b. Verify that the encrypted password can be decrypted.

```
node1# /usr/sfw/bin/openssl enc -aes128 -d -in /var/cluster/.sieb-rs_sbl_pdata 
-k /var/cluster/.sieb-rs_key -out /var/cluster/tmpfile
```

c. Repeat steps a and b on all other Oracle Solaris Cluster nodes that will host the Siebel server resource.

11 If you are using Siebel 8.1 or later version, create a file called scgtywconfig under server_root, owned by the owner of siebenv.sh.

If the Siebel server is installed locally, create the file scgtywconfig under server_root on all nodes. For security reasons, make this file readable only by the owner.

```
# cd server_root
# touch scgtywconfig
# chown siebel:siebel scgtywconfig
# chmod 400 scgtywconfig
```

12 If you are using Siebel 8.1 or later version, in the scgtywconfig file, enter the gateway user name and password that was given while configuring the gateway server enterprise.

For example: gtwyuser gtwypassword

This user name and password combination must have permission to connect to the database and also to the gateway server for use by the Sun Cluster HA for Siebel Gateway Fault Monitor.

```
export GTWYUSR=gtwyuser
export GTWYPWD=gtwyuserpassword
```
Optional: If you want to encrypt the scgtwyconfig file, perform the following steps.

a. As root user, encrypt the password file scgtwyconfig for the Siebel server using the key file /var/cluster/.siebelserver_resource_name_key. Place the password file in the /var/cluster directory.

In the example below, the password file scgtwyconfig is being encrypted and sieb-rs reflects the Siebel server resource name. The password file name must be in the format /var/cluster/.siebelserver_resource_name_gtwy_pdata. The PATH_TO_CONFIGFILE is the location of the scgtwyconfig file.

```
node1# /usr/sfw/bin/openssl enc -aes128 -e -in \
SPATH_TO_CONFIGFILE/scgtwyconfig -k /var/cluster/.sieb-rs_key -out \
/var/cluster/.sieb-rs_gtwy_pdata
```

```
node1# chmod 400 /var/cluster/.sieb-rs_gtwy_pdata
```

b. Verify that the encrypted password can be decrypted.

```
node1# /usr/sfw/bin/openssl enc -aes128 -d -in /var/cluster/.sieb-rs_gtwy_pdata \
-k /var/cluster/.sieb-rs_key -out /var/cluster/tmpfile
```

c. Repeat steps a and b on all other Oracle Solaris Cluster nodes that will host the Siebel server resource.

14 Create the Siebel server resource.

```
# clresource create -g siebel-rg \
-t SUNW.sblsrvr \
-p Confdir_list=server_root \
-p siebel_enterprise=siebel enterprise name \
-p siebel_server=siebel_server_name -p siebel_version=version_number sblsrvr-rs
```

Specifying the name of the resource type for the resource.

```
-p Confdir_list
```

Specifies the path name to the Siebel server root directory.

```
-p siebel_version
```

Specifies the Siebel server version.

Caution – If you enter an incorrect value for siebel_version, you might not see errors during validation but the resource startup will fail. If siebel_version is incorrect, the probe method is not able to verify database connectivity.

```
-p siebel_enterprise
```

Specifies the name of the Siebel enterprise.

```
-p siebel_server
```

Specifies the name of the Siebel server.

```
sblsrvr-rs
```

Specifies your choice of the name of the resource to add.

The resource is created in the enabled state.
Caution – If you enter incorrect values for siebel_enterprise or siebel_server, you may not see any errors during validation. However, resource startup will fail. If siebel_enterprise is incorrect, validate method will not be able to verify database connectivity, which will result in a warning only.

**Verifying the HA for Siebel Installation and Configuration**

This section contains the procedure you need to verify that you installed and configured your data service correctly.

**How to Verify the HA for Siebel Installation and Configuration**

Use this procedure to verify that you installed and configured HA for Siebel correctly.

1. Bring the Siebel database, Siebel gateway, and Siebel server resources online on the cluster.
2. Log in to the node on which the Siebel server is online.
3. Confirm that the fault monitor functionality is working correctly.
4. Start srvrmgr and run the subcommand list compgrps.
5. Verify that the required Siebel components are enabled.
6. Connect to Siebel using a supported thin-client (browser) and run a session.
7. As user root, switch the Siebel server resource group to another node.
   ```
   # clresourcegroup switch -n node2 siebel-rg
   ```
8. Repeat Step 4, Step 5, and Step 6 for each potential node on which the Siebel server resource can run.
9. As root user, switch the Siebel gateway resource group to another node.
   ```
   # clresourcegroup switch -n node2 gateway-rg
   ```
Maintaining HA for Siebel

This section contains guidelines for maintaining HA for Siebel.

- To maintain a Siebel resource, you must disable the Siebel resource or bring the Siebel resource group to an unmanaged state using one of the following commands.
  
  - `clresource disable resource`
  - `clresourcegroup unmanage resource_group`

- To start a Siebel resource, disable the resource, but keep the logical hostname online, before starting the Siebel resource manually.

**Caution** – If the Siebel server is started manually without disabling the resource or bringing the resource group to an unmanaged state, the Siebel resource start method might “reset” the service on the node where the resource is attempting to be started under Oracle Solaris Cluster control. This may lead to unexpected results.

Tuning the HA for Siebel Fault Monitors

Fault monitoring for the HA for Siebel data service is provided by the following fault monitors:

- The Siebel server fault monitor
- The Siebel gateway fault monitor

Each fault monitor is contained in a resource whose resource type is shown in the following table.

<table>
<thead>
<tr>
<th>Fault Monitor</th>
<th>Resource Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siebel server</td>
<td>SUNW.sblsrvr</td>
</tr>
<tr>
<td>Siebel gateway</td>
<td>SUNW.sblgtwy</td>
</tr>
</tbody>
</table>

System properties and extension properties of these resources control the behavior of the fault monitors. The default values of these properties determine the preset behavior of the fault monitors. The preset behavior should be suitable for most Oracle Solaris Cluster installations. Therefore, you should tune the HA for Siebel fault monitors *only* if you need to modify this preset behavior.

Tuning the HA for Siebel fault monitors involves the following tasks:

- Setting the interval between fault monitor probes
- Setting the timeout for fault monitor probes
Defining the criteria for persistent faults
Specifying the failover behavior of a resource

For more information, see “Tuning Fault Monitors for Oracle Solaris Cluster Data Services” in Oracle Solaris Cluster Data Services Planning and Administration Guide. Information about the HA for Siebel fault monitors that you need to perform these tasks is provided in the subsections that follow.

Tune the HA for Siebel fault monitors when you register and configure HA for Siebel. For more information, see "Registering and Configuring HA for Siebel” on page 24.

Operation of the Siebel Server Fault Monitor

During a probe, the Siebel server fault monitor tests for the correct operation of the following components:

- The Siebel database
  If the Siebel database fails, the status of the Siebel server is marked as DEGRADED. When the Siebel database restarts again, the Siebel server resource probe tries to verify that the Siebel server is functioning. If this test fails, the Siebel server is restarted or failed over to another node.
  The Siebel database might not be available when the Siebel server resource is started. In this situation, the fault monitor also starts the Siebel server when the Siebel database becomes available.

- The Siebel gateway
  If the Siebel gateway fails, the status of the Siebel server is marked as DEGRADED. When the Siebel gateway restarts again, the Siebel server resource probe tries to verify that the Siebel server is functioning. If this test fails, the Siebel server is restarted or failed over to another node.
  The Siebel gateway might not be available when the Siebel server resource is started. In this situation, the fault monitor also starts the Siebel server when the Siebel gateway becomes available.

- The Siebel server and all its enabled components
  If the Siebel server fails, it is restarted or failed over. If any Siebel component fails, a partial failure is reported. The fault monitor counts this partial failure as 10% of a complete failure.

Note – The fault monitor of the Siebel server can detect component failures only in English language installations of Siebel.
Operation of the Siebel Gateway Fault Monitor

The Siebel gateway fault monitor monitors the Siebel gateway process. If the Siebel gateway process dies, the fault monitor restarts it, or fails it over to another node.

Upgrading the HA for Siebel Resource Types

You should upgrade the SUNW.sblgtwy and SUNW.sblsrvr resource types if the following conditions apply:

- You are upgrading from an earlier version of the HA for Oracle Web Tier data service.
- You need to use the new features of this data service.

For general instructions on upgrading a resource type, see “Upgrading a Resource Type” in Oracle Solaris Cluster Data Services Planning and Administration Guide.

▼ How to Upgrade to a New Version of HA for Siebel

Note – Before you perform this procedure, determine if your current HA for Siebel resources have been modified to have specific timeout values that suit your deployment. If timeout values were previously adjusted, you should reapply those timeout values to your new HA for Siebel resources.

1 On a cluster member, assume a role that provides solaris.cluster.modify RBAC authorization.

2 Disable the Siebel gateway and Siebel server resources.
   
   # cresource disable sblgtwy-rs
   # cresource disable sblsrvr-rs

   Use the cresource type show command to determine the version of the registered resource type. The resource type registration (RTR) files for the SUNW.sblgtwy and SUNW.sblsrvr resource types are /opt/SUNWscsbl/gateway/etc/SUNW.sblgtwy and /opt/SUNWscsbl/sblsrvr/etc/SUNW.sblsrvr, respectively.

3 Install the new version of HA for Siebel on each cluster node.
   For more information, see “How to Install the HA for Siebel Packages” on page 23.

4 Migrate instances of the HA for Siebel resource types.
   - The following example shows how to modify the SUNW.sblgtwy resource named sblgtwy-rs:
The `Type_version` property of this resource is set to the value of a (hypothetical) newer release 4.0.

The following example shows how to modify the `SUNW.sblsrvr` resource named `sblsrvr-rs`:

```bash
# clresource set -p Type_version=4.0 sblsrvr-rs
```

The `Type_version` property of this resource is set to the value of a (hypothetical) newer release 4.0.
Extension properties for HA for Siebel resource types are described in the following sections.
- “SUNW.sblsrvr Extension Properties” on page 37
- “SUNW.sblgtwy Extension Properties” on page 39

For details about system-defined properties, see the `r_properties(5)` man page and the `rg_properties(5)` man page.

**SUNW.sblsrvr Extension Properties**

The SUNW.sblsrvr resource type represents the Siebel server in a Oracle Solaris Cluster configuration. The extension properties of this resource type are as follows:

**Confdir_list**
This property is the path name to the Siebel server root directory.

**Data Type:** String array

**Default:** None

**Tunable:** At creation

**Monitor_retry_count**
This property controls the restarts of the fault monitor. It indicates the number of times the fault monitor is restarted by the process monitor facility and corresponds to the `-n` option passed to the `pmfd(1M)` command. The number of restarts is counted in a specified time window (see the property `Monitor_retry_interval`). Note that this property refers to the restarts of the fault monitor itself, not the Siebel server. Siebel server restarts are controlled by the system-defined properties `Thorough_Probe_Interval`, `Retry_Interval`, and `Retry_Count`, as specified in their descriptions. See `r_properties(5)`.

**Data Type:** Integer
Default: 4  
Tunable: Any time

Monitor_retry_interval
Indicates the time in minutes, over which the failures of the fault monitor are counted, and corresponds to the -t option passed to the pmfadm command. If the number of times the fault monitor fails exceeds the value of Monitor_retry_count, the fault monitor is not restarted by the process monitor facility.

Data Type: Integer
Default: 2
Tunable: Any time

Probe_timeout
This property is the timeout value (in seconds) used by the fault monitor to probe a Siebel server instance.

Data Type: Integer
Default: 300
Tunable: Any time

Siebel_enterprise
This property is set to the name of the Siebel enterprise.

Data Type: String array
Default: None
Tunable: At creation

Siebel_server
This property is set to the name of the Siebel server.

Data Type: String array
Default: None
Tunable: At creation

Siebel_version
This property is set to the Siebel server version.

Data Type: String
Default: 8.2
Tunable: When Disabled
The SUNW.sblgtwy resource type represents the Siebel gateway in an Oracle Solaris Cluster configuration. The extension properties of this resource type are as follows:

**Confdir_list**
This property is the path name to the Siebel gateway root directory.

- **Data Type:** String array
- **Default:** None
- **Tunable:** At creation

**Monitor_retry_count**
This property controls the restarts of the fault monitor. It indicates the number of times the fault monitor is restarted by the process monitor facility and corresponds to the -n option passed to the `pmfd(1M)` command. The number of restarts is counted in a specified time window (see the property `Monitor_retry_interval`). Note that this property refers to the restarts of the fault monitor itself, not the Siebel gateway. Siebel gateway restarts are controlled by the system-defined properties `Thorough_Probe_Interval` and `Retry_Interval`, as specified in their descriptions. See `r_properties(5)`.

- **Data Type:** Integer
- **Default:** 4
- **Tunable:** Any time

**Monitor_retry_interval**
Indicates the time (in minutes) over which the failures of the fault monitor are counted, and corresponds to the -t option passed to the `pmfadm` command. If the number of times the fault monitor fails exceeds the value of `Monitor_retry_count` within this period, the fault monitor is not restarted by the process monitor facility.

- **Data Type:** Integer
- **Default:** 2
- **Tunable:** Any time

**Probe_timeout**
Indicates the timeout value (in seconds) used by the fault monitor to probe a Siebel gateway instance.

- **Data Type:** Integer
- **Default:** 120
- **Tunable:** Any time
Siebel_version
This property is set to the Siebel server version.

Data Type: String
Default: 8.2
Tunable: When Disabled
Index

C
Confdir_list extension property
SUNW.sblgtwy resource type, 39
SUNW.sblsrvr resource type, 37
configuring
HA for Siebel, 25–27
Siebel server, 27–31

E
extension properties
SUNW.sblgtwy resource type, 39–40
SUNW.sblsrvr resource type, 37–38

F
fault monitors
Siebel gateway, 34
Siebel server, 33–34
tuning, 32–34
files
.hushlogin
Siebel gateway user, 17
Siebel server user, 19, 20

G
global zone, 9, 23

H
HA for Siebel
See also Siebel
configuration
planning, 11–13, 13
requirements, 11, 12
standard, 12
fault monitors, 32–34
installing, 22–24
planning, 11–13
maintaining, 32
overview, 9–10
protection of Siebel components, 10
registering and configuring, 25–27
Siebel server, 27–31
software packages, installing, 22–24
verifying installation, 31
HA for Siebel resource types, upgrading, 34–35
help, 7–8
.hushlogin file
Siebel gateway user, 17
Siebel server user, 19, 20

I
installing
HA for Siebel, 22–24
Siebel gateway
global file system, 16–17
local disks of physical hosts, 17–18
prerequisites, 16
installing (Continued)
  Siebel server and Siebel database
    global file system, 19–20
    local disks of physical hosts, 20–21
  prerequisites, 16

L
  local zones, See non-global zone

M
  maintaining, HA for Siebel, 32
  Monitor_retry_count extension property
    SUNW.sblgtwy resource type, 39
    SUNW.sblsrvr resource type, 37
  Monitor_retry_interval extension property
    SUNW.sblgtwy resource type, 39
    SUNW.sblsrvr resource type, 38

N
  non-global zone, 9, 23

O
  overview, HA for Siebel, 9–10

P
  packages, 22–24
  Probe_timeout extension property
    SUNW.sblgtwy resource type, 39
    SUNW.sblsrvr resource type, 38

R
  registering
    HA for Siebel, 25–27, 27–31

S
  Siebel
    See also HA for Siebel
    installing
      on global file system, 16–17, 19–20
      on local disks of physical hosts, 17–18, 20–21
      overview, 16–21
      preparing nodes for, 14–16
      Siebel gateway, 16–18
      Siebel server and Siebel database, 18–21
      verifying installation, 21–22
      Siebel_enterprise extension property, 38
      Siebel_server extension property, 38
      Siebel_version extension property, 38, 39
    software packages, 22–24
    SUNW.sblgtwy resource type, extension
      properties, 39–40
    SUNW.sblsrvr resource type, extension
      properties, 37–38
    system properties, effect on fault monitors, 32

T
  technical support, 7–8
  tuning, fault monitors, 32–34

U
  upgrading, HA for Siebel resource types, 34–35
V
verifying
  HA for Siebel,  31
  Siebel installation,  21–22

Z
zones,  9,23