Oracle® Solaris Cluster Data Service for Siebel Guide

SPARC Platform Edition

Part No: E72776
June 2017

Oracle Solaris Cluster Data Service for Siebel Guide

Part No: E72776

Access to Oracle Support

Oracle customers that have purchased support 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.

Référence: E72776

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation

- **Overview** – Describes how to install and configure the Oracle Solaris Cluster HA for Siebel data service.
- **Audience** – Technicians, system administrators, and authorized service providers.
- **Required knowledge** – Advanced experience troubleshooting and replacing hardware.

Product Documentation Library

Documentation and resources for this product and related products are available at http://www.oracle.com/pls/topic/lookup?ctx=E56676-01.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPTER 1

Installing and Configuring Oracle Solaris Cluster HA for Siebel

This chapter explains how to install and configure Oracle Solaris Cluster HA for Siebel (HA for Siebel).

Note - For current support information, see the Oracle Solaris Cluster 4 Compatibility Guide (`http://www.oracle.com/technetwork/server-storage/solaris-cluster/overview/solariscluster4-compatibilityguide-1429037.pdf`).

This chapter contains the following sections.

HA for Siebel Overview

HA for Siebel provides fault monitoring and automatic failover for the HA for Siebel application. High availability is provided for the HA for Siebel Gateway and HA for Siebel Server. With a HA for 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 either the global zone or a zone cluster. For updated information about supported configurations of this data service, contact your Oracle service representative or see the *Oracle Solaris Cluster 4 Compatibility Guide*.

For conceptual information about failover services, see the *Oracle Solaris Cluster 4.3 Concepts Guide*.

TABLE 1 Protection of Siebel Components

HA for SiebelComponent	Protected by
Siebel Gateway	HA for Siebel The resource type is `SUNW.sblgtwy`.
Siebel Server	HA for Siebel The resource type is `SUNW.sblsrvr`.

Installing and Configuring HA for Siebel

Table 2, "Task Map: Installing and Configuring HA for Siebel," on page 10 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

Task	Instructions
Plan the Siebel installation	"Planning the HA for Siebel Installation and Configuration" on page 11
Prepare the nodes and disks	"How to Prepare the Nodes" on page 14
Install and configure Siebel	"How to Install the Siebel Gateway on the Global File System" on page 17 "How to Install the Siebel Gateway on Local Disks of Physical Hosts" on page 18 "How to Install the Siebel Server and Siebel Database on the Global File System" on page 20 "How to Install the Siebel Server and Siebel Database on Local Disks of Physical Hosts" on page 21

Task	Instructions
Verify Siebel installation and configuration	"How to Verify the Siebel Installation and Configuration" on page 22
Register and configure HA for Siebel as a failover data service	"How to Register and Configure HA for Siebel Gateway as a Failover Data Service" on page 25 "How to Register and Configure HA for Siebel Server as a Failover Data Service" on page 28
Verify HA for Siebel installation and configuration	"How to Verify the HA for Siebel Installation and Configuration" on page 32
Maintain HA for Siebel	"Maintaining HA for Siebel" on page 33
Tune the HA for Siebel Fault Monitors	"Tuning the HA for Siebel Fault Monitors" on page 33

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 4.3 Data Services Planning and Administration Guide*.

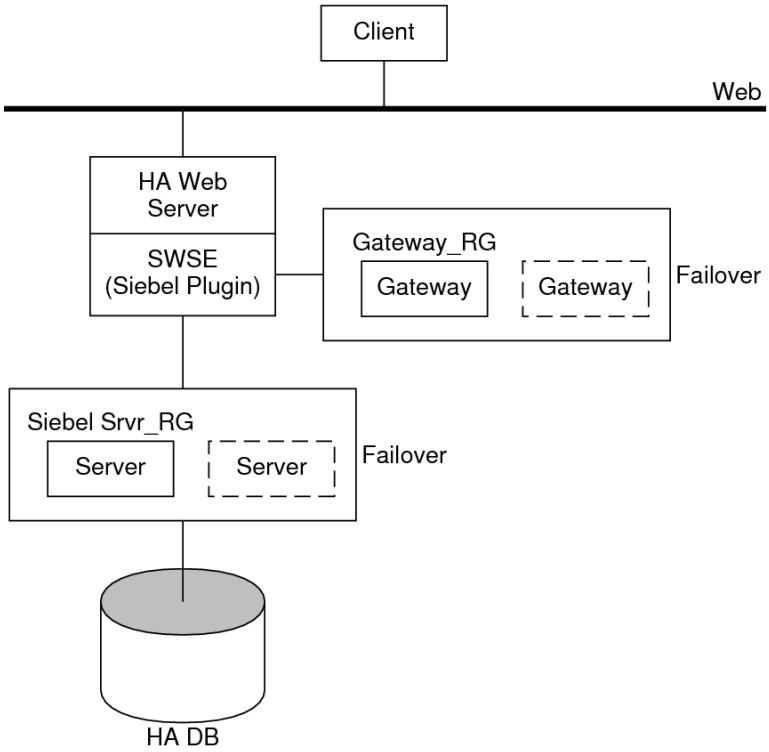
- Install each Siebel Gateway and each Siebel Server in its own Siebel root environment (each instance has its own `siebenv.sh` file). This allows each instance to be independent of others, making failovers and problem diagnosis easier.
- If more than one Siebel server will use the Siebel File System, install the Siebel File System on a global file system. This will ensure that all Siebel Server resources have access to the same file system 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, "Standard Siebel Configuration," on page 13 illustrates a possible configuration using HA for Siebel. The Siebel Server and the Siebel Gateway are configured as failover data services.

FIGURE 1 Standard Siebel Configuration



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 4.3 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.

Before You Begin Ensure that the `/etc/netmasks` file has IP-address subnet and netmask entries for all logical hostnames. If necessary, edit the `/etc/netmasks` file to add any missing entries.

1. **Assume the `root` role on all of the nodes.**

2. **Use the `svccfg` command to 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 dns
   publickey: files dns
   project:   files dns
   group:     files dns
   ```

   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` command does not refer to the NIS/NIS+ name services if the network information name service is unavailable. For more information, see the `su`(1M) man page. For more information on the `svccfg` command, see the `svccfg`(1M) man page.

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 might have a locally mounted `/home` path or you can 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.**

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:`*siebel*

   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 must 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.

10. **Bring the resource group online.**

    ```
    # clresourcegroup online -M failover-rg
    ```

11. **Repeat Step 8 through Step 10 for each logical hostname that is required.**

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 fail over 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 17
- "Installing the Siebel Server and Siebel Database" on page 19

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 17
- "How to Install the Siebel Gateway on Local Disks of Physical Hosts" on page 18

▼ 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 18.

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

1. **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`.

2. **Verify that the `siebenv.sh` file is under *gateway_root*, and is owned by the user who will launch the Siebel Gateway.**

3. **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.

4. **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*.**

5. **Stop and restart the Siebel Gateway to ensure that the Gateway is using the logical hostname.**

6. **To verify the installation and configuration of Siebel Gateway Server, execute the following command as the user who started the Siebel Gateway.**

   Ensure that the command returns a version string:

   ```
   # srvredit -q -u gateway_username -p gateway_password -g siebel_gateway -e none -z \
   -c '$Gateway.VersionString'
   ```

-u *gateway_username*	Specifies the username for Gateway authentication.
-p *gateway_password*	Specifies the password for Gateway authentication.
siebel_gateway	Logical hostname created for Siebel Gateway Server resource.

▼ 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 17.

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 cluster file system).

---

1. **Install the Siebel Gateway on any one node of the cluster 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`.

2. **Verify that the `siebenv.sh` file is under *gateway_root*, and is owned by the user who will launch the Siebel Gateway.**

3. **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.

4. **Change the `SIEBEL_GATEWAY` to the logical hostname that is selected for the Gateway in `siebenv.sh` and `siebenv.csh` files under *gateway_root*.**

5. **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. **Issue 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'
```

- *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 File System, you *must* install the Siebel File System on a global file system.

To install the Siebel Server and configure the Siebel Server and Siebel Database , use one of the following procedures:

- "How to Install the Siebel Server and Siebel Database on the Global File System" on page 20

- "How to Install the Siebel Server and Siebel Database on Local Disks of Physical Hosts" on page 21

▼ 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 21.

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 for 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`/*db-password*) 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 `ServerHostAddress` parameter to the IP address of the Siebel Server's logical-hostname resource..**

```
$ srvrmgr:hasiebel> change param ServerHostAddress=lhaddr 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 20.

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 for 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`/*db-password*) 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 `ServerHostAddress` parameter to the IP address of the Siebel Server's logical host name resource.**

   ```
   $ srvrmgr:hasiebel> change param ServerHostAddress=lhaddr for server hasiebel
   ```

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

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

   ```
   # rdist -c server_root hostname:server_root
   ```

10. **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 where 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 db-password
   ```

5. **Run the `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 `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.

6. **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 Oracle Solaris Cluster HA for Siebel Package

If you did not install the Oracle Solaris Cluster HA for Siebel package during your initial Oracle Solaris Cluster installation, perform this procedure to install the package.

▼ How to Install the Oracle Solaris Cluster HA for Siebel Package

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

1. **On the cluster node where you are installing the data service package, assume the `root` role.**

2. **Ensure that the data service package is available from the configured publisher and that the `solaris` and `ha-cluster` publishers are valid.**

```
# pkg list -a ha-cluster/data-service/siebel
# pkg publisher
PUBLISHER                             TYPE     STATUS   P  LOCATION
solaris                               origin   online   F  solaris-repository
```

```
ha-cluster                        origin   online   F  ha-cluster-repository
```

For information about setting the `solaris` publisher, see "Adding, Modifying, or Removing Package Publishers" in *Adding and Updating Software in Oracle Solaris 11.3*.

Tip - Use the `-nv` options whenever you install or update to see what changes will be made, such as which versions of which packages will be installed or updated and whether a new BE will be created.

If you do not get any error messages when you use the `-nv` options, run the command again without the `-n` option to actually perform the installation or update. If you do get error messages, run the command again with more `-v` options (for example, `-nvv`) or more of the package FMRI pattern to get more information to help you diagnose and fix the problem. For troubleshooting information, see Appendix A, "Troubleshooting Package Installation and Update," in *Adding and Updating Software in Oracle Solaris 11.3*.

3. **Install the HA for Siebel software package.**

```
# pkg install ha-cluster/data-service/siebel
```

4. **Verify that the package installed successfully.**

```
$ pkg info ha-cluster/data-service/siebel
```

Installation is successful if output shows that `State` is `Installed`.

5. **Perform any necessary updates to the Oracle Solaris Cluster software.**

For instructions on updating single or multiple packages, see Chapter 11, "Updating Your Software" in *Oracle Solaris Cluster 4.3 System Administration Guide*.

Registering and Configuring HA for Siebel

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

Setting HA for Siebel Extension Properties

These sections 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 Appendix A, "Oracle 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*

`-p` *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 4.3 Data Services Planning and Administration Guide* to configure resources after the resources are created.

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

Use this procedure to configure HA for Siebel Gateway 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 and Configuring the Siebel Application" on page 16 to install the packages. Otherwise, use this procedure to configure HA for Siebel.

Before You Begin Ensure that the `/etc/netmasks` file has IP-address subnet and netmask entries for all logical hostnames. If necessary, edit the `/etc/netmasks` file to add any missing entries.

1. **On one of the nodes in the cluster that hosts the application server 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.**

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, skip to Step 6.

```
# 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.

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.

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

logical_host	Specifies an optional resource name of your choice.

5. **Bring the resource group online.**

   ```
   # clresourcegroup 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. **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.

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

8. **In the `scgtwyconfig` file, enter the gateway user name and password that was given while configuring the Gateway Server enterprise.**

   For example: `gtwyuser` *gtwy-user-password*

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

   ```
   export GTWYUSR=gtwyuser
   export GTWYPWD=gtwy-user-password
   ```

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-rs` 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.

```
node1# dd if=/dev/urandom of=/var/cluster/.gtwy-rs_key bs=16 count=1
node1#  chmod 400 /var/cluster/.gtwy-rs_key
node1#  /usr/sfw/bin/openssl enc -aes128 -e -in \
$PATH_TO_CONFIGFILE/scgtwyconfig -k \
/var/cluster/.gtwy-rs_key -out /var/cluster/.gtwy-rs_gtwy_pdata
node1#  chmod 400 /var/cluster/.gtwy-rs_gtwy_pdata
```

b. Verify that the encrypted password can be decrypted.

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

c. Repeat these steps on all other Oracle Solaris Cluster nodes that will host the Gateway Server resource.

10. Create the Siebel Gateway resource.

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

`-t SUNW.sblgtwy`	Specifies 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. If you enter an incorrect value for `Siebel_version`, you might not see errors during validation, but the resource startup will fail. If the `Siebel_version` property 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 HA for Siebel Server as a Failover Data Service

Use this procedure to configure HA for Siebel Server 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 and Configuring the Siebel Application" on page 16 to install the packages. Otherwise, use this procedure to configure HA for Siebel.

Before You Begin Ensure that the `/etc/netmasks` file has IP-address subnet and netmask entries for all logical hostnames. If necessary, edit the `/etc/netmasks` file to add any missing entries.

1. **Add the resource type for the Siebel Server.**

```
# clresourcetype register 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, skip to Step 5.

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

-n *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`/*db-user-password*) with permission to connect to the database for use by the HA for Siebel Fault Monitor.**

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

9. **Add the following entries to the `sbsblconfig` file.**

   ```
   export DBUSR=dbuser
   export DBPWD=db-user-password
   export SADMUSR=sadmin
   export SADMPWD=sadmin-password
   ```

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 \
       $PATH_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. Create a file called `scgtwyconfig` under *server_root*, owned by the owner of `siebenv.sh`.

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

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

12. In the `scgtwyconfig` file, enter the Gateway user name and password that was given while configuring the Gateway Server enterprise.

For example: `gtwyuser` *gtwyuser-password*

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

```
export GTWYUSR=gtwyuser
export GTWYPWD=gtwyuser-password
```

13. (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 \
```

```
$PATH_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
```

`-t SUNW.sblsrvr`	Specifies 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. If you enter an incorrect value for `Siebel_version`, you might not see errors during validation, but the resource startup will fail. If the `Siebel_version` property 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 might 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.

15. **Verify that the resource group and the Siebel Server resource are online by using `cluster status -t resourcegroup,resource` and `ps –ef` commands.**

Verifying the HA for Siebel Installation and Configuration

This section contains the procedure 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 can 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 3 Resource Types for HA for Siebel Fault Monitors

Fault Monitor	Resource Type
Siebel Server	`SUNW.sblsrvr`
Siebel Gateway	`SUNW.sblgtwy`

Standard 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 4.3 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.

♦ ♦ ♦ APPENDIX A

Oracle HA for Siebel Extension Properties

Extension properties for HA for Siebel resource types are described in the following sections:

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 command. For more information, see the rpc.pmfd(1M) man page. 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 the r_properties(5) man page.

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 supported Siebel Server version, for example, 8.1.1.14 or 8.2.2.2.

Data Type: String

Default: 8.2

Tunable: When Disabled

SUNW.sblgtwy Extension Properties

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 thepmfd command. See the rpc.pmfd(1M) man page for more information. The number of restarts is counted in a specified time window (see the Monitor_retry_interval property). 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 the r_properties(5) man page.

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 supported Siebel Server version, for example, 8.1.1.14 or 8.2.2.2.

Data Type: String

Default: 8.2

Tunable: When Disabled

Index

M

O

P

R

S

T

V

Z