ComTrade Oracle Siebel CRM/ Oracle BI Smart Plug-in for HP Software
(SPI for Siebel)

This Version 04.00 is for use with HP Operations Manager on Linux and UNIX

User's Guide

Notices

The information contained in this document is subject to change without notice.

COMTRADE D.O.O. PROVIDES THIS MATERIAL "AS IS" AND MAKES NO WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. COMTRADE D.O.O. SHALL NOT BE LIABLE FOR ERRORS CONTAINED HEREIN OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE OR USE OF THIS MATERIAL WHETHER BASED ON WARRANTY, CONTRACT, OR OTHER LEGAL THEORY.

Trademarks

HP® and OpenView® are registered trademarks of the Hewlett-Packard Company in the United States and other jurisdictions.

IBM® and AIX® are registered trademarks of the IBM Corporation.

Oracle® and Siebel™ are registered trademarks of Oracle Corporation and/or its affiliates.

Sun™ and Solaris™ are trademarks of Sun Microsystems, Inc.

UNIX® is a registered trademark in the U.S. and other countries licensed exclusively through X/Open Company, Ltd.

Microsoft®, Windows®, Windows® 2000, Windows Server™ 2003, Windows Server™ 2008, and Windows NT® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

ComTrade d.o.o.
Litijska 51
SI-1000 Ljubljana
Slovenia, Europe
www.comtrade.com

Contents

Contents

Contents

Contents

Chapter 1

Document Overview

Edition History

New editions are complete revisions of the manual. The printing dates for each edition are listed below.

Edition	Date
First Edition	June 2002
Second Edition	October 2002
Third Edition	February 2003
Fourth Edition	May 2003
Fifth Edition	July 2004
Sixth Edition	November 2004
Seventh Edition	February 2005
Eighth Edition	August 2006
Ninth Edition	December 2006
Tenth Edition	July 2007
Eleventh Edition	October 2008
Twelfth Edition	October 2009
Thirteenth Edition	June 2010
Fourteenth Edition	December 2010

Conventions

The following typographical conventions are used in this manual:

Font	Definition	Example
Italic	Product names, book or manual titles, man page names, and section, table, and figure titles.	Refer to the *SPI for Siebel Installation and Configuration Guide* for additional information.
	Emphasis.	You *must* follow these steps.
	Window and dialog box names.	In the *Node Bank* window, select a node.
Bold	Commands on menus and buttons, dialog box titles and options, menu and icon names.	In the menu, first click **Actions**, and then **Agents**.
`Computer`	File names, syntax, directory names, or text that should be entered on screen or that is displayed on the monitor.	You will receive a license activation file `siebspi_licact_new.dat` by e-mail.

Product Documentation

With SPI for Siebel, the following documentation is provided:

- *SPI for Siebel Installation and Configuration Guide*
  Installation and Configuration Guide is available in PDF format (*SIEBSPI-InstallGuideUNIX.pdf*).
- *SPI for Siebel User's Guide*
  User's guide is available in PDF format (*SIEBSPI-UserGuideUNIX.pdf*).
- *SPI for Siebel Quick Reference Guide*
  Quick reference guide is available in PDF format (*SIEBSPI-QuickReference.pdf*).
- *SPI for Siebel - Supported Siebel and HP Software Platforms*
  Supported Platforms document is available in PDF format (*SIEBSPI-SupportedPlatforms.pdf*).
- Release notes
  Release notes are available in TXT format (*siebspi-release-notes-unix.txt*).
- Readme
  Readme file is available in TXT format (*siebspi-readme.txt*).
- ComTrade software license terms file
  License file is available in TXT format (*comtrade_software_license_support_terms_signed.txt*)

Customer Support

Use the following e-mail and Web page addresses if you need help with the licensing process or while using the product, and if you would like additional information about this or other ComTrade products.

Licensing

To obtain the license activation file you can visit ComTrade licensing portal:

http://spi.comtrade.com/licensing/

or send an e-mail to the following address:

spi-licensing@comtrade.com

For more information on licensing and licensing procedure refer to *SPI for Siebel Installation and Configuration Guide*.

If you encounter any problems with the licensing process, contact the ComTrade licensing department at:

spi-licensing@comtrade.com

Contacting Support

IMPORTANT

Should you require additional assistance or information while using the product, contact the vendor that shipped the software.

If you have purchased the software directly from ComTrade, send e-mail to:

support-siebelspi@comtrade.com

Before Contacting Support

Before you contact the support department, have the following information available so that a technical support analyst can work on your problem more efficiently:

- the support files `siebspi_supp.zip` (on Windows managed nodes) and `siebspi_supp.tar.Z` (on Unix managed nodes)

To create the support file, run the **SIEBSPI-Collect Information** tool on one or more nodes. To run the tool, perform the following steps:

1. Go to the **SPI for Siebel/SIEBSPI Maintenance/SIEBSPI Support** tool group and run the **SIEBSPI-Collect Support Information** tool on the managed nodes for which you would like to collect the information. The files `siebspi_supp.zip` or `siebspi_supp.tar` with the support information are created in the following directory on the node(s):

```
<OvAgentDataDir>/siebspi/supplog on Unix
<OvAgentDataDir>\siebspi\supplog on Windows
```

- symptoms
- sequence of events leading to the problem
- commands and options that you used
- messages you have received (a description with the time and date)

General Information

For marketing or business-related issues in reference to this or other ComTrade SPIs, send e-mail to:

spi-info@comtrade.com

Product Web Sites

Visit ComTrade Smart Plug-in Web site at:

http://www.managementproducts.comtrade.com/smart_plug-in/siebel

and the company Web site at:

http://www.comtrade.com/

Chapters Summary

This guide describes how to use SPI for Siebel to monitor and manage Oracle BI and Siebel CRM application resources from the HP Software environment. It also addresses and troubleshoots some of the possible installation problems.

NOTE

This document assumes that you are familiar with the HP Operations Manager administration procedures and concepts.

The guide contains the following chapters:

Chapter 2

Getting Started

About Oracle Siebel CRM

Today's organizations must manage customer interactions across multiple communications channels. The challenge is to make it easy for customers to do business with the organization any way they want-at any time, through any channel, in any language or currency-and to make customers feel that they are dealing with a single, unified organization that recognizes them at every touch point. Oracle Siebel Customer Relationship Management (Oracle Siebel CRM) solutions, designed to fit any size organization, empower companies to deliver seamless and superior customer experiences by extending CRM to everyone in their organizations and partner networks.

The Oracle Siebel CRM represents the framework for the Siebel Products and Industry solutions that are built upon them.

Products:

- Business Analytics Applications
- Call Center And Service
- Customer Data Integration
- Customer Order Management
- Enterprise Marketing
- Partner Relationship Management
- Sales
- Self Service And Ebilling
- Loyalty Management

Typical Enterprise Setup of Oracle Siebel CRM

Typical enterprise setup of Oracle Siebel CRM consists of the following components:

- Siebel Server
- Siebel Server Components
- Gateway Name Server
- Web Server and Siebel Web Server Extension
- Siebel Database Server
- Resonate Central Dispatch (obsolete since Siebel 7.7.)
- Siebel clients:

- Siebel High Interactivity Web Clients: Java based, using Microsoft JVM.
- Siebel HTML Clients: Functionality the same as HI web client, however everything implemented with HTML. Slower, can be used from non-Windows platforms.
- Siebel Dedicated Clients: Desktop or "fat" clients - inside LAN. Java based, internally implemented with a web server. Practically obsolete by now.

Siebel Server

The Siebel Server is the middle-tier platform that supports both back-end and interactive processes for all Siebel application clients. These processes are components within the Siebel Server architecture, and support functions such as:

- Operation of business logic for Siebel Thin Clients, as well as connectivity and access to the database server and file system
- Integration with legacy or third-party data
- Automatic assignment of new accounts, opportunities, service requests, and other records
- Workflow management
- Mobile client synchronization

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

Siebel Server Components and Application Object Managers

The various programs that operate on the Siebel Server are implemented as components. A component represents only a specific type of program; a component is executed or operated as a task, or instantiation of a component, on a specific Siebel Server.

Components execute tasks in one of three run modes - background, batch, or interactive. Components are defined at the Siebel Enterprise Server level in component groups. Component groups are then assigned to one or more Siebel Servers within the Siebel Enterprise Server on which they can execute tasks.

Application Object Managers host the Business Objects layer and Data Objects layer of the Siebel CRM architecture. They primarily support Siebel Web client connections by handling multiple users simultaneously and making requests to the Siebel Server on their behalf. AOMs are hosted as components in the Siebel Server and run on the application server machine. They are providing the infrastructure for

serving multiple Siebel Web client users. A single Siebel Server can run multiple AOMs that can be configured to run as multithreaded processes on them.

Siebel Gateway Name Server

The Siebel Gateway Name Server:

- Serves as a single entry point for accessing Siebel Servers
- Provides enhanced scalability, load balancing, and high availability across the Enterprise Server

Two primary services that coordinate the Enterprise Server and Siebel Servers operate within the Gateway are:

- Name Server
- Connection Brokering

The Gateway Server maintains the configuration information for all Siebel Servers in all the Enterprise Servers it manages.

Resonate Central Dispatch

The Resonate Central Dispatch is used for:

- Connection Brokering
- Load Balancing

Connection Brokering is an optional service of the Gateway Server that uses the Resonate Central Dispatch product to distribute client connection requests across multiple Siebel Servers. Only client connections to the Siebel Object Manager (for thin clients), request processor, and request agent components (for Interactive Assignment) will be distributed by Resonate Central Dispatch.

Siebel Web Server Extension

The Siebel Web Server Extension, operating on the Web server, connects to the Application Object Manager component operating within the Siebel Server. This connection uses Siebel's application.

Web Server (for example, IPlanet)

Web Server is used with Siebel Web Server Extension. It provides a server (Web) for providing an HTTP access for Siebel Web Clients.

Siebel Database Server (for example, Oracle)

The Siebel Database Server stores the data used by Oracle Siebel CRM. Siebel dedicated clients and Siebel Server components, including those that operate in

conjunction with the Siebel Thin Client, connect directly to the Database Server and make changes in real time.

Oracle Secure Enterprise Search

Oracle Secure Enterprise Search (SES) allows you to search all your enterprise data sources from a single interface. It provides uniform search capabilities over multiple repositories. Oracle SES uses a crawler to collect data from these sources. The crawler supports a number of built-in source types, as well as a published plug-in (or connector) architecture for adding new types. Multiple Oracle SES instances can also share content through the federated source type.

Oracle SES supports numerous built-in source types: Web, table, file, e-mail, mailing list, OracleAS Portal, Oracle Calendar, Oracle Content Database, Oracle Applications, and so on.

Oracle Business Intelligence

Oracle Business Intelligence is a suite of products based around several server products and a Microsoft Windows-based administration tool:

- Oracle BI Server - Connects to a wide range of relational and OLAP datasources and provides access, via a business metadata layer, to an integrated data set including calculations, aggregations, and KPIs
- Oracle BI Presentation Server - Connects via ODBC to Oracle BI Server and provides interactive dashboards, reports, and data visualizations through a consistent, dynamic HTML interface
- Oracle BI Delivers - Works alongside Oracle BI Presentation Server to schedule reports and create workflows that perform actions based on alerts and thresholds defined by users
- Oracle BI Publisher - Provides "boardroom-quality" reports using data sourced from relational databases, Oracle BI Answers requests, Oracle BI Discoverer workbooks, and the Oracle Business Intelligence Enterprise Edition metadata layer

About SPI for Siebel

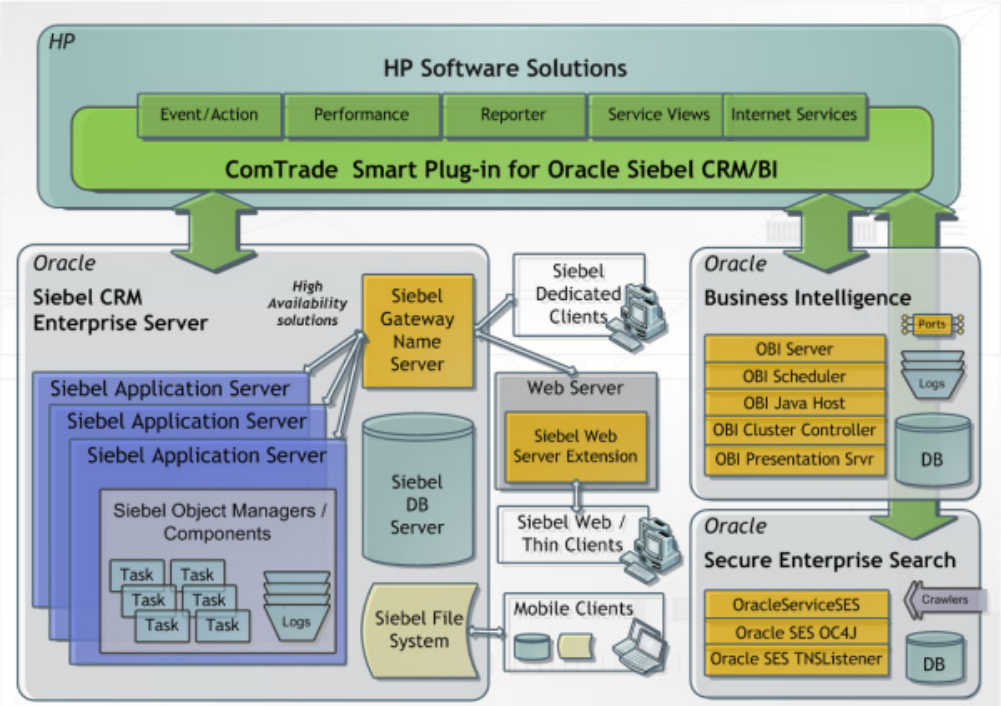
ComTrade Oracle Siebel CRM/Oracle BI Smart Plug-in for HP Software (SPI for Siebel) is designed specifically for use with Oracle Siebel CRM and BI (Oracle Business Intelligence and Siebel Analytics) in HP Software environments. Developed by ComTrade, it performs proactive system monitoring and service management while providing additional control over your computing environment.

Additional benefits of using SPI for Siebel include the following:

- **Easy installation**. The standard HPOM user interface is used for all administration and configuration tasks. SPI for Siebel also uses well-known installation procedures.
- **Seamless integration into your environment**. As a pre-configured software module, SPI for Siebel "plugs into" HP Software automatically and provides an efficient and productive link between the applications that run on your server and other server applications.
- **Consistent performance**. Because SPI for Siebel runs on standard hardware, monitoring of the Siebel system has a low impact on system performance.
- **Dependable usage**. Operators are notified when errors occur. Additionally, backup is handled through the HP Software environment.
- **Built-in security features**. SPI for Siebel is compatible with the security features pre-established in the HP Software environment.
- **Comprehensive reports**. SPI for Siebel generates detailed reports on: server, database and component activity and status; remote user client synchronization history and status; event/action history; and Siebel Web Server Extensions.
- **Includes an Intelligent Smart Probe**. This feature measures customer experience when they use the software.

High-Level Architecture

Below is the high-level diagram of SPI for Siebel architecture.



Quick Introduction to SPI for Siebel

The main components of SPI for Siebel include the following:

- HP Operations Manager Policies
- HP Operations Manager Tools
- HP Operations Manager Service Map
- HP Performance Manager Graphs
- HP Reporter Reports

For a complete list and descriptions of policies, tools, and graphs, refer to the *SPI for Siebel Quick Reference Guide*.

Policies

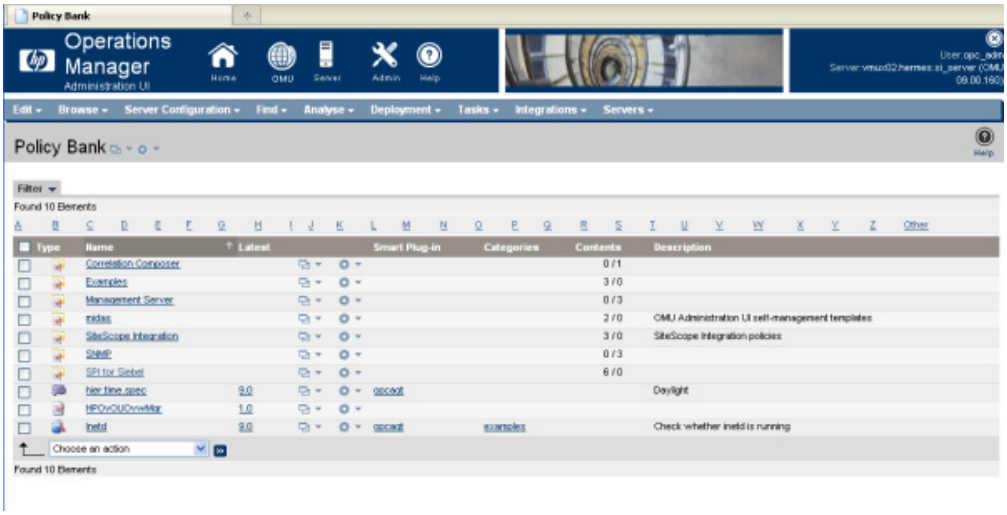
Policies instruct HP Operations Manager engines how to solve system management issues, for example, “Monitor CPU Utilization”.

SPI for Siebel policies enable you to define complex rules and instructions for monitoring different systems and services. Policies are instructions for HP Operations Manager (HPOM) agents that monitor your Siebel environment. When an issue is detected, a message is sent to the HPOM console.

In addition, you can define automated actions to be performed upon detecting a specific issue, or include instructions for operators as part of the message. Every policy can start automatic or operator initiated action when issue is detected. You can check which actions were launched when issue was detected, and check the action outcome in the message annotation.

SPI for Siebel Policies and Policy Groups

When you install SPI for Siebel, a new top level policy group is added in the HPOM Administration UI.



The **SPI for Siebel** policy group contains all policies, used for managing your Oracle Siebel CRM and BI environment. It contains the following main policy groups:

- SIEBSPI-Actuate e.Reporting Server
- SIEBSPI-Business Intelligence
- SIEBSPI-Oracle Secure Enterprise Search
- SIEBSPI-Oracle Siebel CRM
- SIEBSPI-Resonate Central Dispatch
- SIEBSPI-Web Servers

SIEBSPI-Actuate e.Reporting Server

This policy group should only be installed on a node where the Actuate Reporting Server is installed.

SIEBSPI-Business Intelligence

This policy group should be installed on a node where Oracle Business Intelligence or Siebel Analytics is installed. It contains two subgroups depending on the Business Intelligence product (SIEBSPI-Oracle Business Intelligence or SIEBSPI-Siebel Analytics), where you can find the following policy groups:

SIEBSPI-OBI Performance Data or SIEBSPI-SA Performance Data

This policy group contains policies for collecting performance data, used in HP Performance Manager or HP Reporter.

SIEBSPI-OBI Presentation Server or SIEBSPI-SA Web Server

This policy group contains policies that should be installed on a node where OBI Presentation Server or SA Web Server is installed.

SIEBSPI-OBI Scheduler or SIEBSPI-SA Scheduler

This policy group contains policies that should be installed on a node where OBI Scheduler or SA Scheduler is installed.

SIEBSPI-OBI Server or SIEBSPI-SA Server

This policy group contains policies that should be installed on a node where OBI Server or SA Server is installed.

SIEBSPI-Oracle Secure Enterprise Search

This policy group should only be installed on a node where the Oracle Secure Enterprise Search is installed.

SIEBSPI-Oracle Siebel CRM

This policy group contains the following policy groups:

SIEBSPI-Internal

This policy group contains policies that intercept internal siebspi messages.

SIEBSPI-Siebel Application Server

This policy group should only be installed on a node where the Siebel Application Server is installed. It contains the following policy groups:

- SIEBSPI-Autodiscovery
- SIEBSPI-Mobile Clients and Backlogs
- SIEBSPI-Siebel Components
- SIEBSPI-Siebel Database
- SIEBSPI-Siebel Log Files
- SIEBSPI-Siebel Server Base
- SIEBSPI-Siebel Server Performance Data
- SIEBSPI-Siebel Users Activity
- SIEBSPI-Statistics Metrics

SIEBSPI-Siebel Gateway Server

This policy group should only be installed on a node where the Siebel Gateway server is installed.

SIEBSPI-Siebel Remote Client

This policy group should only be installed on a node where a Siebel remote (mobile) client is installed.

SIEBSPI-Siebel Web Server Extension

This policy group should only be installed on a node where the Siebel Web server extension is installed.

SIEBSPI-Smart Probe

This policy group should only be installed on the nodes where the Siebel server or dedicated clients are installed.

SIEBSPI-Resonate Central Dispatch

This policy group should be installed on all nodes in the Siebel enterprise where Resonate Central Dispatch is installed. Typically, these are the nodes where the Siebel server and gateway are installed.

SIEBSPI-Web Servers

This policy group should only be installed on a node where the Siebel Web server is installed. It contains the following policy groups:

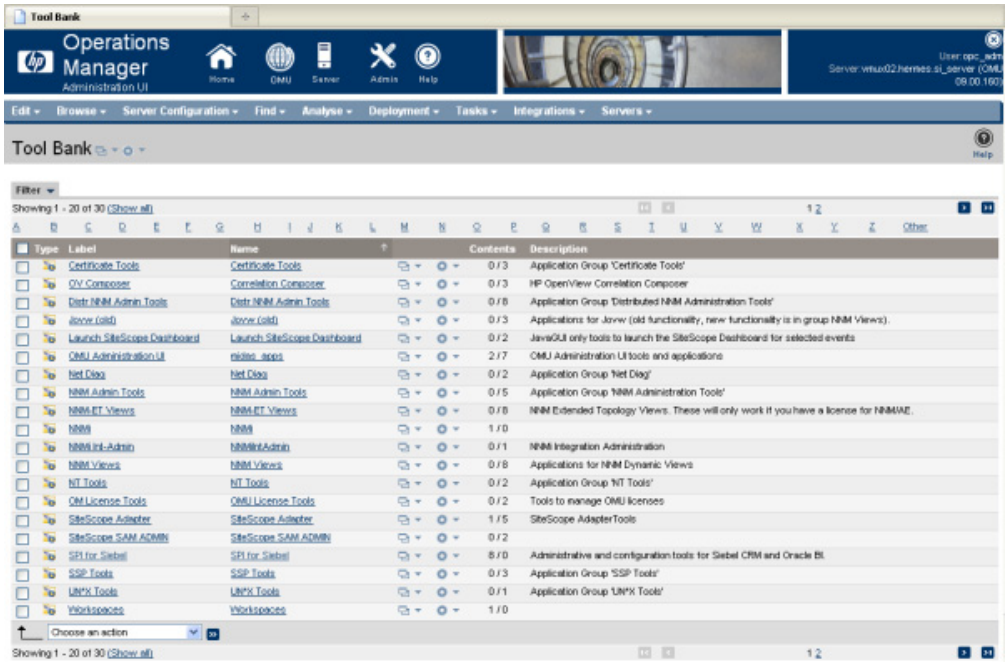
- SIEBSPI-Apache Tomcat
- SIEBSPI-IBM HTTP Web Server
- SIEBSPI-Microsoft IIS
- SIEBSPI-Sun ONE Web Server

Refer to the Technical Sales Reference Guide for ComTrade Smart Plug-ins manual for more information about all available policies and policy groups.

Tools

SPI for Siebel supplies powerful tools for monitoring and managing your Siebel environment. SPI for Siebel enable you to inspect, analyze, and manage your Siebel environment, check the current status of the environment, and react to issues in your environment.

When you install SPI for Siebel, a new top level tool group is added in the HPOM administration UI.



The **SPI for Siebel** tool group contains all tools, used for managing your Siebel environment. It contains the following tool groups:

- `SIEBSPI-Actuate`
- `SIEBSPI-Business Intelligence`
- `SIEBSPI-Maintenance`
- `SIEBSPI-Performance`
- `SIEBSPI-Resonate`
- `SIEBSPI-SARM`
- `SIEBSPI-Siebel Users Activity`
- `SIEBSPI-Siebel Tools`

Running Tools in Tool Groups

SPI for Siebel contains many tools, for example, tools for configuring SPI for Siebel, starting Siebel servers, tasks, and so on.

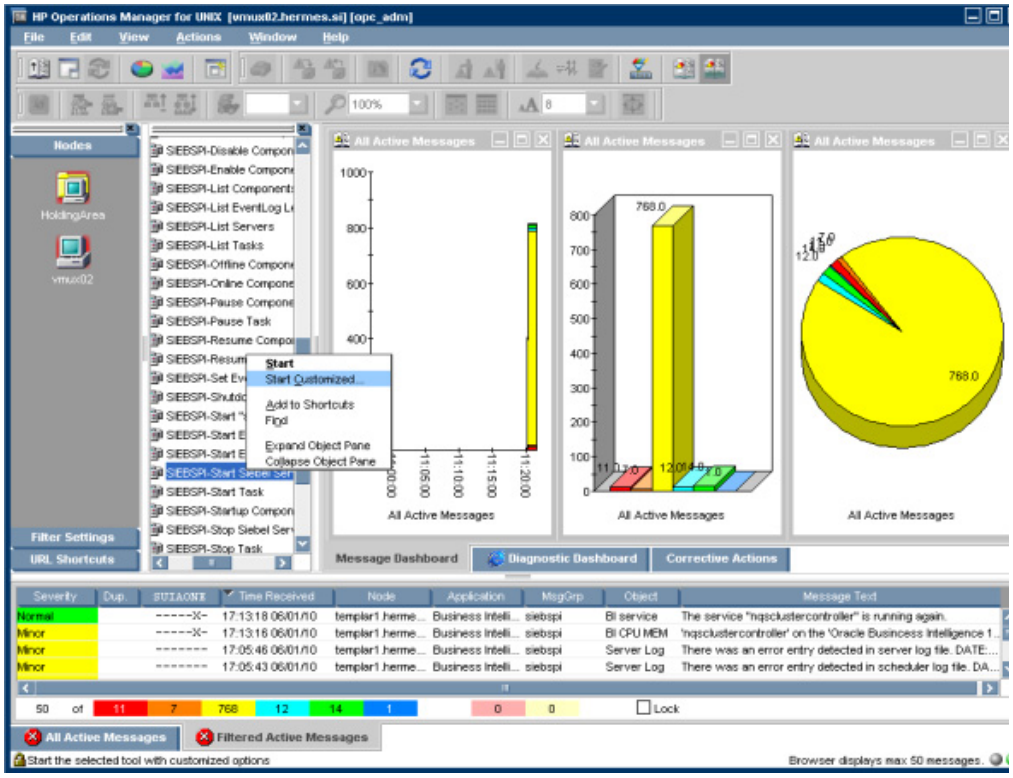
Most tools must be run as **Start Customized**, so you can add or change additional parameters. For example, if you want to start the Siebel server named `myserver`, use the Start Server tool with an additional parameter:
`-start_server "myserver"`

Example:

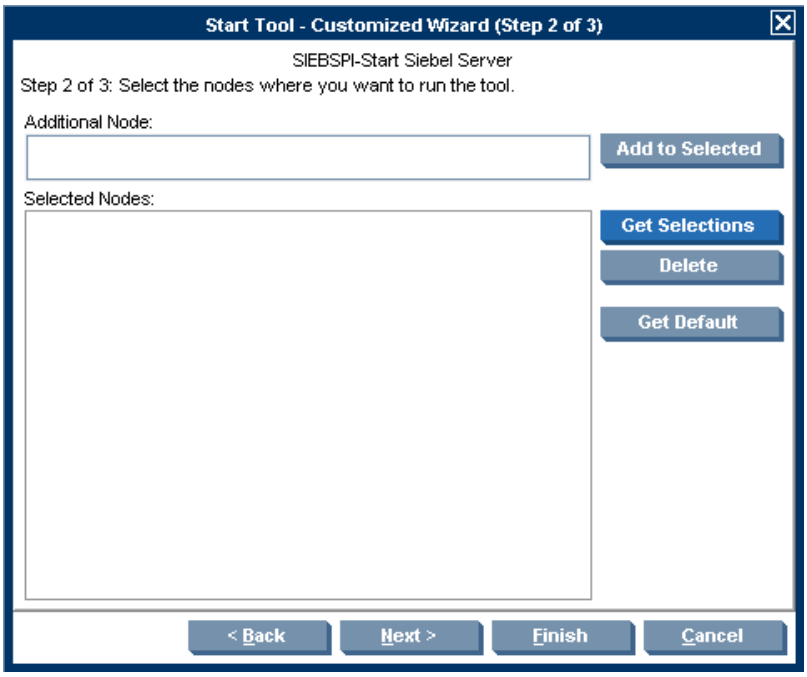
From the **SPI for Siebel/SIEBSPI-Tools** tool group, run the **SIEBSPI-Start Siebel Server** tool.

To run the **SIEBSPI-Start Siebel Server** tool, perform the following steps:

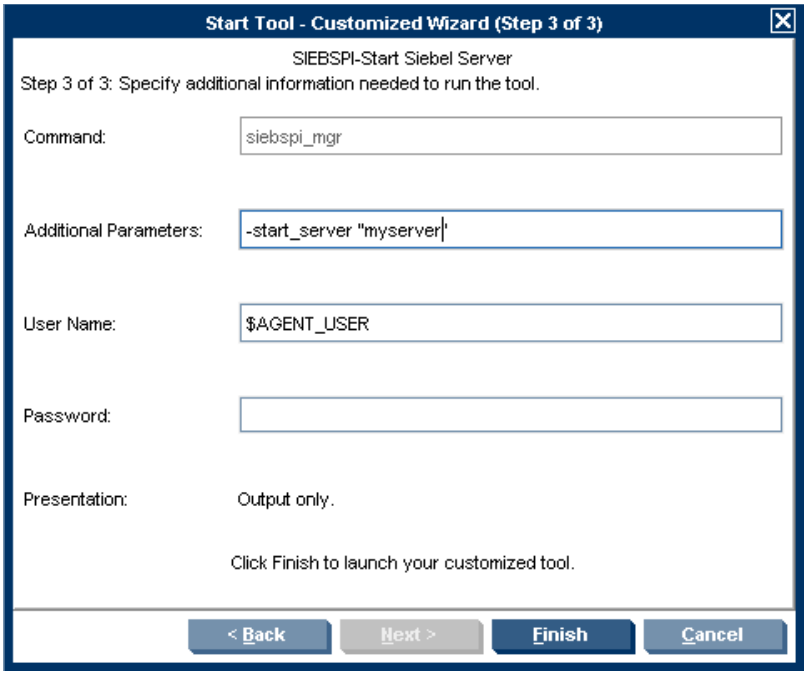
1. Start the *HPOM Operational UI* and log in as an HPOM Administrator.
2. Right-click **SIEBSPI-Start Server** and select **Start Customized**.



3. Select the node where you want to run the tool and click **Next>**.



4. In the next window, change the Application Parameters value “Siebel Server” to “myserver”:



5. Click **Finish** and wait for the tool to execute.

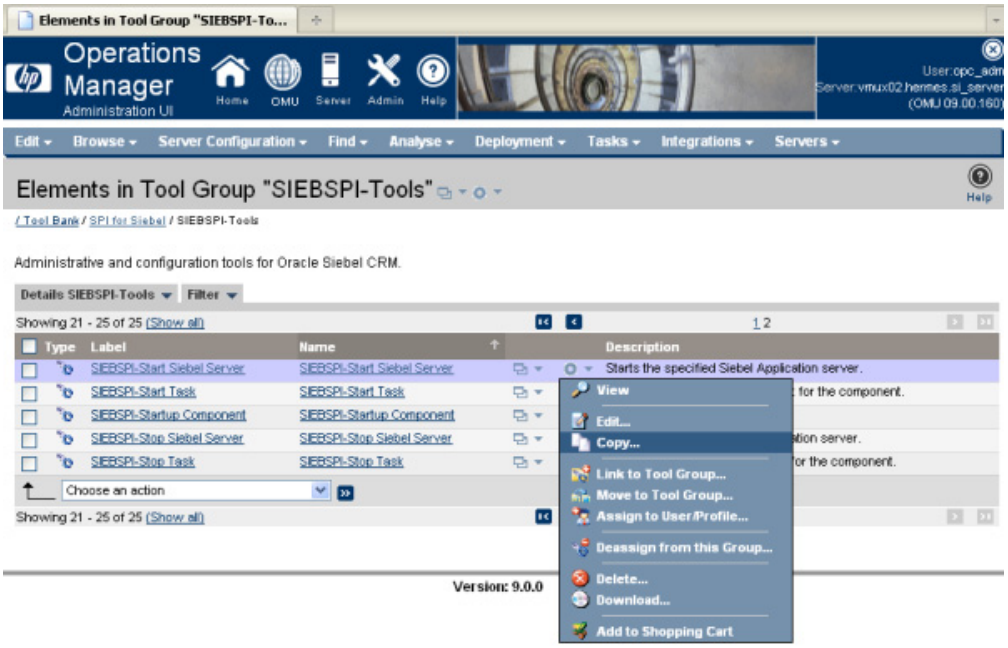
N O T E

You can customize tools to change parameters to fixed values. This can be done to enlarge your tool group with new tools, for example, "Start Server myserver1", "Start Server myserver2", and so on.

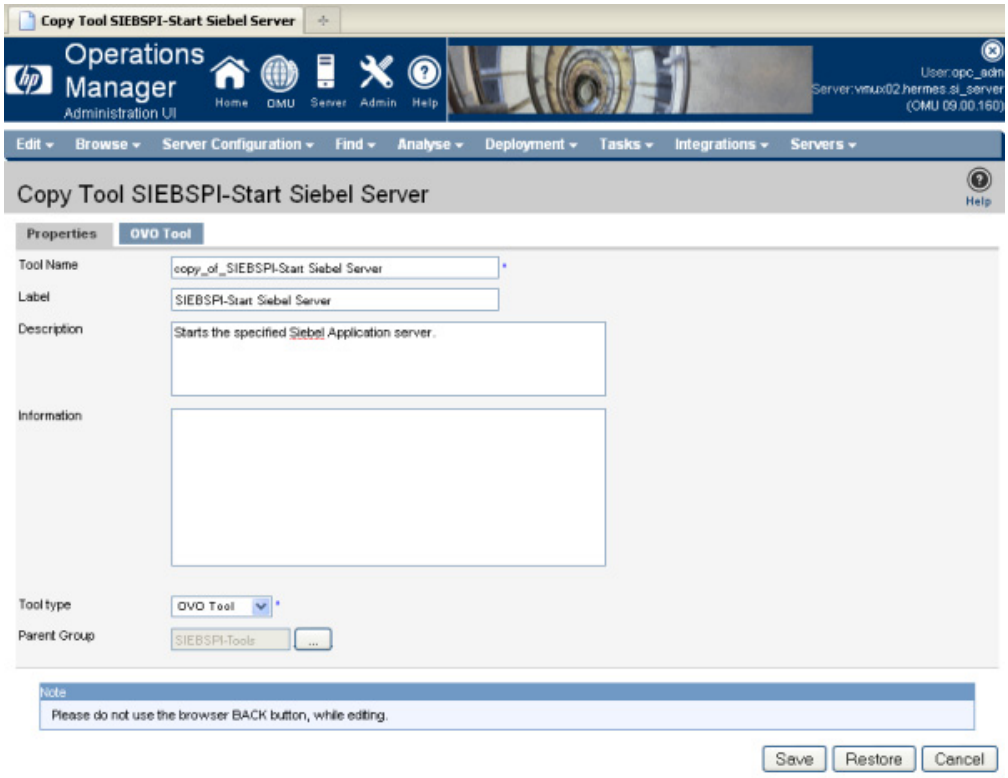
Example:

1. Start the *HP Administration UI* and log in as an HPOM Administrator (opc_adm).

1. Select **Copy** from the **Actions** menu next to the **SIEBSPI-Start Server** tool.



2. The following window opens:



3. Change the *Tool Name*, *Label*, and *Description* fields as appropriate and click **Save**.

Reports

SPI for Siebel also offers report functionality, where collected performance data can be represented in web-based reports. SPI for Siebel integrates HP Reporter.

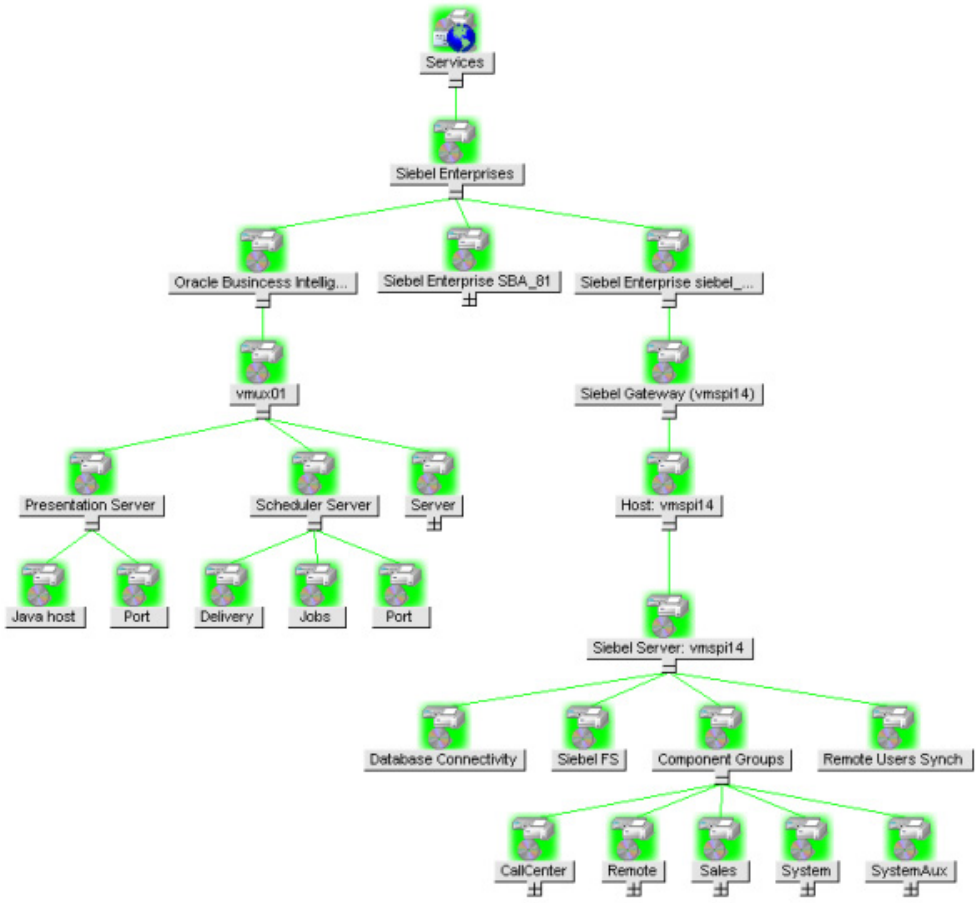
Services Map

HP Service Map View is a component of the HP Java-based operator GUI. This component enables you to manage your IT (information technology) environment while focusing on the IT services that you provide.

SPI for Siebel provides support for Service Navigator. It automatically generates a Siebel service map of the Siebel enterprise configuration, which offers complete graphical representation of your Siebel environment and its hierarchical organization. All Siebel object types (Siebel Servers, Gateway Name Servers, Components, Web Server Extensions, Actuate Reporter Server, and so on) in your environment are displayed in a tree view, which shows the components and their hierarchical dependencies.

In addition, graphical representation of your Siebel environment clearly indicates relations between Siebel environment components, how they impact one another, and which business services are affected. This enables you to effectively manage services within your information technology framework.

An example of a service map view:



Chapter 3

Setting Up the Environment

Setting Up the Siebel Environment

SPI for Siebel enables you to monitor and manage your Siebel environment from one, centralized point. For this purpose Siebel Servers are added as managed nodes on the HPOM management server.

Setting up your Siebel environment involves installing, licensing, and configuring SPI for Siebel on the HPOM management server and on the managed nodes. For more information on how to install, license and configure managed nodes refer to *SPI for Siebel Installation and Configuration Guide*.

When you successfully configured your environment, you can start using the SPI for Siebel product. For procedural information on how to:

- perform autodiscovery of Siebel components and update your configuration, refer to "Mapping the Siebel Environment" on page 29
- configure SPI for Siebel reporting functionality, refer to "SPI for Siebel Integration with HP Reporter" on page 112.

Mapping the Siebel Environment

SPI for Siebel integrates HPOM Services and supports Service View. HPOM Services is a component of the HPOM GUI. It automatically generates services MOF file of your Siebel enterprise configuration. This component enables you to manage your IT environment while focusing on the IT services that you provide.

SPI for Siebel offers complete graphical representation of your Siebel environment and its hierarchical organization. All Siebel object types (Siebel Servers, Gateway Name Servers, Components, Web Server Extensions, Actuate Reporter Server, and so on) in your environment are displayed in a tree view, which shows the components and their hierarchical dependencies.

N O T E

For additional information on the HP Operations Manager Services, refer to the HP Operations Manager manuals.

Autodiscovery

SPI for Siebel offers autodiscovery of the Oracle's Siebel Business Applications topology, comprising different Siebel object types and their dependencies. As a result, it graphically displays the business impact of Siebel lower-level components, their failures, or performance degradations.

SPI for Siebel tool group contains a tool that performs discovery of the Siebel enterprise configuration. Additionally, it monitors the configuration. If the discovered configuration has changed, a message is sent to the management server, which is automatically acknowledged if the automatic action has completed successfully. Autodicovery must be performed on the Siebel Server managed node. Autodiscovery on one Siebel Server in Siebel Enterprise performs discovery for the whole Siebel Enterprise. All Siebel Servers and Siebel Gateway that are part of the discovered Siebel Enterprise are added to a service tree. For more information about autodiscovery, refer to the *SPI for Siebel Quick Reference Guide*, to the `SIEBSPI_ENTERPRISE_CONFIGURATION` policy description.

If you want Web Servers with the Siebel Web Server Extension (SWSE) installed also to appear in a service tree, you need to add these nodes to configuration on the Siebel Server where autodiscovery will be performed. `SPI for Siebel` tool group contains a tool **SIEBSPI-Add SWSE nodes to Autodisc.** that will add SWSE nodes to autodiscovery of the Siebel enterprise configuration.

To perform autodiscovery, perform the following steps:

1. Assign the policy group **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Autodiscovery** to a node where the Siebel server is installed, and install the policy group to the node.
2. If you want SWSE nodes to appear in a service tree, run the **SIEBSPI-Add SWSE nodes to Autodisc.** tool on that node. Before performing autodiscovery, edit the tool parameter `swe_nodes` and type the nodes names, for example:

   ```
   -swe_nodes "node1,node2"
   ```
3. Run the **SIEBSPI-Autodiscovery** tool on that node.

In the *Message Browser* window, you can check whether the autodiscovery was successful or not.

N O T E

You should only assign autodiscovery policies to one node in the Siebel enterprise where the Siebel Server is installed. Additionally, to perform an autodiscovery, the policy group SPI for Siebel/SIEBSPI-Oracle Siebel CRM/ SIEBSPI-Siebel Application Server/SIEBSPI-Autodiscovery must be deployed on the node where the Siebel Application Server is installed.

By default, services are assigned to the `opc_op` user. If you want these services to also be assigned to another operator or user, you must perform the following steps:

1. Change the autodiscovery policies in the **SIEBSPI-Autodiscovery** group (refer to section *Changing the Autodiscovery Policies*).
2. Modify the **Autodiscovery** tool in the **Tool Bank** (refer to section *Modifying the Autodiscovery Tool*).

Changing the Autodiscovery Policy

To change the autodiscovery policies in the SIEBSPI-Autodiscovery group, perform the following steps:

1. Log in as `opc_adm`.
2. Open the *Message Source Policies* window.
3. Go to the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Autodiscovery** policy group.
4. Click the `SIEBSPI_ENTERPRISE_CONFIGURATION` policy.
5. Click **Conditions**.

6. Select the condition **Siebel enterprise configuration changed** and click **Modify**.
7. In the operator initiated actions field, locate the command `siebspi_autod` and change it to the following:

   ```
   siebspi_autod -op <Your operator>
   ```

8. Click **OK** to confirm the changes and close all of the windows.

N O T E

You must assign and update the policies on the nodes for the changes to take effect.

Modifying the Autodiscovery Tool

To modify the Autodiscovery tool in the Tool bank, follow the procedure below:

1. Log in as `opc_adm`.
2. Go to **SPI for Siebel/SIEBSPI-Tools** tool group.
3. Right-click the **Autodiscovery** tool and select **Modify**.
4. In the **Additional Parameters** field, type:

   ```
   -op <Your operator>
   ```

5. Click **OK** to confirm the changes.

From this point on, whenever you run autodiscovery, the Service tree of the Siebel Enterprise will be visible for **<Your operator>**.

N O T E

To perform an autodiscovery, the policy group SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Autodiscovery must be assigned and installed on the node where the Siebel server is installed.

Adding Additional Services in Service Map

If you want to include additional services in your Service View, you can manually add them in the existing Service View that was discovered by Autodiscovery.

To do this, edit the `siebspi_svc.xml` file that was generated by Autodiscovery. This file is located on the management server in the folder: `/opt/OV/siebspi/bin`. This file can be edited and then uploaded using the `opcservice` command-line tool. For

detailed information about XML format and file upload techniques, refer to the *HP Operations Manager Manual*.

Every service requires its own unique Service ID. Service IDs are defined in the policies. You can discover a Service ID by inspecting the appropriate policy for which you want to create a new service. Service IDs in Service View should not contain any HP Operations Manager variables (for example, `<$MSG_NODE_NAME>`), such as Service IDs in policies. When putting a Service ID into the Service View, replace all variables with the actual variable values.

Example: Creating a service for monitoring the Siebel Web Server Extension

Service ID in the `SIEBSPI_WEB_SERVER_STATUS` policy is:
`<$MSG_NODE_NAME>:SIEBEL_WEB_SERVER`

When creating a service in the Service View, replace the variable with the variable value. Service ID (if node name is `MYCOMPUTER`) is:
`MYCOMPUTER:SIEBEL_WEB_SERVER`

You must use this value as a Service ID in Service View.

NOTE

The same approach is applicable also for adding Actuate Reporter.

Another way of discovering the actual Service ID is by inspecting the message in the HP Operations Manager Message Browser. You can do this by double-clicking the message, where you can see the actual Service ID. You should use the same Service ID when adding a new service in the Service View.

The SPI for Siebel Support Tool

This tool is installed on the managed node and is implemented to help the support of SPI for Siebel. It collects statistics and log files from the system for easy submission to the Support Department. To use the tool, login to the management node and run it from the command-line.

Tool locations:

- Unix: <OVInstallDir>/siebspi/support/siebspi_supp
- Windows: <OVInstallDir>\siebspi\support\siebspi_supp.exe

Collected log files locations:

- Unix: <OVDataDir>/siebspi/supplog/siebspi_supplog.tar.Z
- Windows: <OVDataDir>\siebspi\supplog\siebspi_supplog.zip

Usage:

```
siebspi_supp    -status|-collect
```

`status`	Collects and displays statistical data about the installed SPI for Siebel files, the HP agent and the operating system including detailed information on the following: - The version of the SPI - HP Agent status - Operating system statistics - Deployed policies - Running processes - Installed software
`collect`	Collects and saves log files, statistical data about the installed SPI for Siebel files, the HP agent and the operating system in the `<OvAgetDir>\siebspi\supplog`

directory on the node for easy submission
to the Support Department

Collected detailed information includes the following:
- The version of the SPI
- HP Agent status
- Operating system statistics
- Deployed policies
- Running processes
- Installed software

Chapter 4

Monitoring the Availability of all Key Components of the Siebel Environment

About Monitoring the Availability

SPI for Siebel monitors availability of all key components in your Siebel Environment. These are the components that Siebel requires for correct operation. The key components are:

- Siebel Server service/daemon
- Gateway service/daemon
- Siebel Database
- Siebel shared file system
- Web services/daemons

Siebel Server Service/Daemon

To monitor availability of the Siebel Server service/daemon on a Siebel Application server, deploy `SIEBSPI_SERVER_PROCESS` and `SIEBSPI_SERVER_PROCESS_EXT` policies to the Siebel Application server.

To monitor availability of the Siebel Server and Siebel Gateway server from a Siebel server, deploy `SIEBSPI_SERVER_AVAILABILITY` and `SIEBSPI_SERVER_AVAILABILITY_EXT` policies to the Siebel Application server.

Gateway Service/Daemon

To monitor availability of the Gateway service/daemon on a Siebel Gateway server, deploy the `SIEBSPI_GATEWAY_PROCESS` policy to the Gateway server.

Siebel Database

To monitor availability of the Siebel Database from a Siebel server, deploy the `SIEBSPI_DB_CONNECTIVITY` policy to the Siebel Application server.

Siebel Shared File System

To monitor availability of the Siebel shared file system from a Siebel server, deploy the `SIEBSPI_SIEBEL_FS` and `SIEBSPI_SIEBEL_FS _EXT` policies to the Siebel Application server.

Web Services/Daemons

To monitor availability of all Web services/daemons on a Web server that is needed for Siebel Web Server Extension to work correctly, deploy `SIEBSPI_WEB_WIN_SERVER_STATUS`, `SIEBSPI_TOMCAT_PROCESS`, `SIEBSPI_WEB_SUN60_SERVER_STATUS`, `SIEBSPI_WEB_SUN61_SERVER_STATUS`, or `SIEBSPI_WEB_IBM_HTTP_SERVER_STATUS` policies to the Siebel Web Server Extension system.

In policies that check availability of the Siebel related services and daemons, you can configure operator initiated or automatic actions to restart the unavailable service or daemon.

Chapter 5

Monitoring Siebel Log Files

About Monitoring Siebel Log Files

SPI for Siebel checks for errors in the most important Siebel log files within the following components:

- Siebel Gateway
- Siebel Server
- Siebel Web Server
- Siebel Server Components

You can extend this functionality to monitor any log file on a system.

If a condition in the log file is met, a message is displayed in the message browser. By default, only Siebel messages with the following severity are sent:

- Fatal error
- Error

Siebel Gateway and Server Log Files

For the Siebel gateway and server log files, you can change the severity of messages in the log files that are reported, for example, warning, info, and so on. To perform this action, modify the following policies:

- `SIEBSPI_GATEWAY_LOG` and `SIEBSPI_GATEWAY_LOG_EXT (check NameSrvr.log)`
- `SIEBSPI_SERVER_LOG` and `SIEBSPI_SERVER_LOG_EXT (check SiebSrvr.log)`
- `SIEBSPI_SERVER_EVENT_LOG` and `SIEBSPI_SERVER_EVENT_LOG_EXT (check "<SiebEntName>_<Server_Name>.log)`

To modify a policy, perform the following steps:

NOTE

Make sure that the Siebel gateway log file exists. In Siebel, version 6.0.1, there is no gateway log file available.

1. Start the *HPOM Administration UI* and log in as an HPOM Administrator (opc_adm).
2. Go to the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM** policy group and select the required policy:
   - For Gateway Log: In the **SIEBSPI-Siebel Gateway Server** policy group, select the `SIEBSPI_GATEWAY_LOG` policy.

- For Server Log: In the **SIEBSPI-Siebel Application Server /SIEBSPI-Siebel Server Base** policy group, select the `SIEBSPI_SERVER_LOG` policy for the Siebel server log file or the `SIEBSPI_SERVER_EVENT_LOG` for the Siebel server event log file.

3. Select **Edit (raw Mode)** from the **Actions** menu, then select the **Content** tab.
4. Add the `-s` severity option and specify the required severity level. For example:
   `siebspi_extmon -srvr -m SIEBSPI_SERVER_LOG -s 3`

The default severity level is 2. You can set one of the following severity levels:

```
0: No errors are reported
1: Only fatal errors are reported
2: Errors and fatal errors are reported
3: Warnings, errors and fatal errors are reported
4: Info, warnings, errors and fatal errors are reported
5: Details, info, warnings, errors and fatal errors are reported
```

Specifying Log File Location

If the Siebel gateway or server is installed on UNIX systems, you may receive a message indicating that the log file could not be found. If this occurs, add the `path` option. To do this, perform the following steps:

1. Follow the steps 1 to 7 as described in the previous procedure.
2. In the *Monitor Program Name*, add the `-p` parameter and set the path. Note that "path" is the root path where the Siebel application is installed, for example, `c:\sba80 for Windows or /opt/siebel for UNIX`.

   Example:

   ```
   siebspi_extmon -srvr -m SIEBSPI_SERVER_LOG -p /opt/siebel
   ```

N O T E

If a message from SIEBSPI_SERVER_EVENT_LOG is received in the message browser, an operator-initiated action, which displays a detailed log of the Siebel component that produced the error, can be executed.

Siebel Server Component Log Files

To monitor component log files, use the following policies:

- `SIEBSPI_SERVER_REQ_BROKER_LOG, Service Request Broker`
- `SIEBSPI_SC_BROKER_LOG, Siebel Connection Broker`
- `SIEBSPI_SERVER_MGR_LOG, Siebel Server Manager`

To add a policy, perform the following steps:

3. Start the *HPOM Administration UI* and log in as an HPOM Administrator (opc_adm).
4. Go to the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Siebel Log Files/SIEBSPI-System Management Logs** policy group.
5. Select the `SIEBSPI_SERVER_REQ_BROKER_LOG` policy for the Siebel server log file.
6. Change the log path file to:

   ```
   <`siebspi_logn -l logfile -file SCCObjMgr_enu`>.
   ```

7. Save as `SIEBSPI_SCC_OBJ_MGR_LOG`. You can create a new policy group **SIEBSPI-Call Center Logs.**
8. You can change the severity option and specify the required severity level.

Monitoring Siebel Flight Data Recorder (FDR) Files

FDR files help you discover what happened before a system or a component server failure. These files have a `.fdr` extension and are located in: `SIEBEL_ROOT/siebsrvr/bin`

To monitor the FDR files, use the `SIEBSPI_FDR_FILES_EXT` or `SIEBSPI_FDR_FILES` policy, located in the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Siebel Log Files** policy group.

To limit the number of arriving messages, set the optional parameter `max_log_msgs` (default value is `5`).

Monitoring Siebel Crash Files

SPI for Siebel can monitor crash files on Siebel Application Servers on all Siebel platforms. Siebel Administrators can immediately respond to a component failure. When the Siebel server component failure occurs on a Siebel system, a “crash” file is created. For each component failure, one “crash” file is created. This file contains detailed information about the process and thread that caused the failure and other useful information. Administrator will be immediately informed that the new crash file is appearing. A `crash_*.txt` file on Microsoft Windows platforms, and “core.*” or “core” file on UNIX platforms.

You can find information about the latest component failure on the system in the following location:

SIEBEL_HOME\siebsrvr\bin

The SIEBSPI_CRASH_FILES and SIEBSPI_CRASH_FILES_EXT files are located in the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/ SIEBSPI-Siebel Log Files** policy group.

Customizing Policies to Monitor Crash Files

You can customize the file name, extension, and path searching conditions using parameters file, exten, and path in the "Program name" field of the SIEBSPI_CRASH_FILES policy.

To limit the number of arriving messages, use the optional parameter max_log_msgs (default value is 5).

Siebel Web Server Log File

SPI for Siebel monitors the log files for IIS on Windows and SUN One Web Server on Sun managed nodes. Only errors are reported in the HPOM message browser. To view the line in the Siebel Web server log file that produced the message, double-click the message in the message browser and click **Show Original Message**.

Resonate Log File

Central Dispatch records all of its activities in log files stored on each node in the Central Dispatch site.

The SIEBSPI_RCD_AGT_LOG file policy catches Resonate Central Dispatch Agent log file messages with severity 3 (normal), 2 (warning), and 1 and 0 (critical).

Actuate Report Server Log Files

The Actuate Report Server log files contain information on report server errors. The report server generates the file name using the process name, a report server generated integer, and date and time. The following is an example view server diagnostic log name:

viewsrv6.exe.1824.2002FEB08_09_35_02_Pacific_Standard_Time.1.log

The SIEBSPI_RPT_SRVR_LOG file policy catches report server log file messages with severity Fatal, Severe, and Warning.

Advanced Options for Monitoring Siebel Log Files and Task Issues

How to Set Rules in SPI for Siebel to Filter Error Messages

Some errors that are reported with SPI for Siebel may not be important to you. If you do not want to get messages about these errors displayed in the message browser, you can set rules so that SPI for Siebel is able to filter task errors and errors found in Siebel log files to report only errors that are important to you.

The following policies are now able to ignore the specified messages:

- `SIEBSPI_SERVER_EVENT_LOG`
- `SIEBSPI_SERVER_LOG`
- `SIEBSPI_GATEWAY_LOG`
- Any policy that is monitoring Siebel component and sends results to `SIEBSPI_CHECK_TASKS_EXT`, for example `SIEBSPI_SCC_OBJ_MGR_COMPONENT` or `SIEBSPI_REQ_PROC_COMPONENT`

For SPI for Siebel to be able to ignore some messages, perform the following steps:

1. Create a text file with the rules. The file can be stored on the managed node on any location on the disk. If it is stored in the SPI for Siebel configuration directory `{OVAgent InstallDir}/siebspi/conf`, the short name in the -rules parameter is enough. If it is stored on any other location on the disk, the full path is required. The file may contain several rules. Every single line in the file contains one string or regular expression.

NOTE

For regular expression syntax, refer to "Regular Expression Syntax" on page 174.

2. You can use this functionality in two ways:
   - In the file, specify all messages that you do not want to receive and change the program parameters in the policy by adding the following parameters:

     ```
     -rules <file name>
     ```

     All the error messages that match the rules defined in the `C:\rules.txt` file will be ignored.
   - In the file, specify all messages that ONLY you want to receive (others will be ignored) and change the program parameters in the policy by adding the following parameters:

     ```
     -rules <file name> [-send_filtered]
     ```

All the error messages that match the rules defined in the `C:\rules.txt` file will be sent to the HPOM console.

3. Deploy any of the policies listed above that were changed.

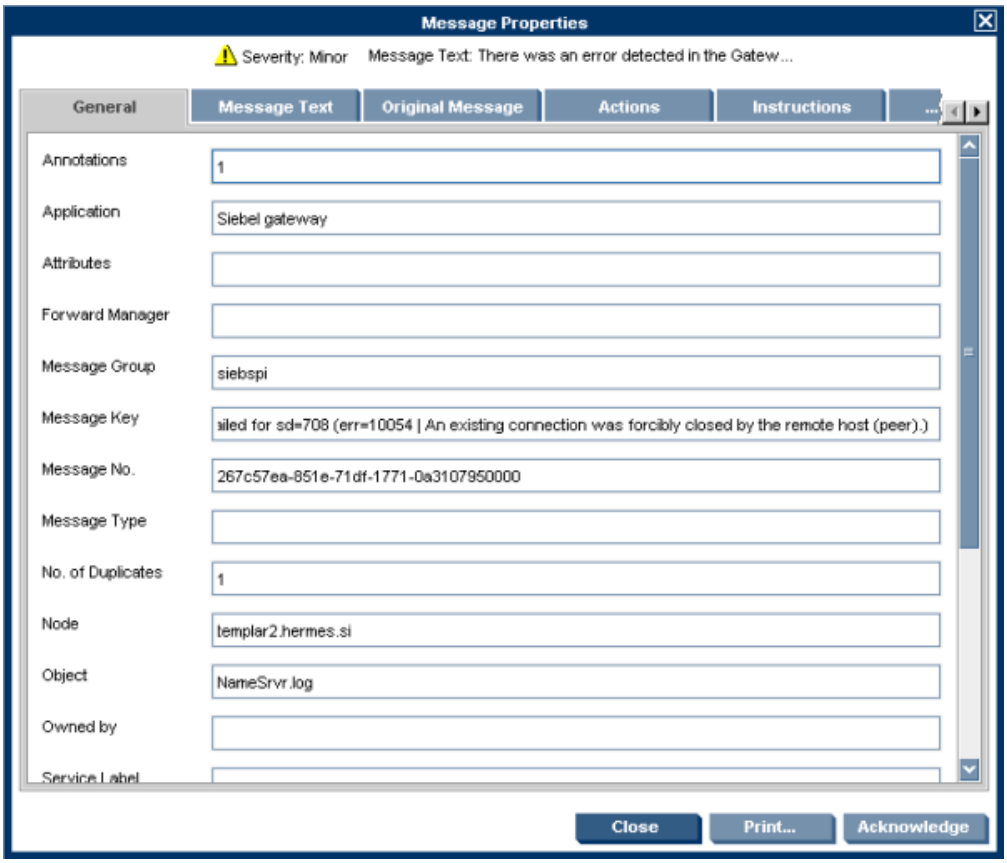
Example: How to set the rules to ignore some messages from the Siebel Gateway log file

In this example, we are getting error messages from the Siebel Gateway log file, which we want to ignore. The following entries are in the Gateway log file:

SisnTcpIp SisnSockError 1 0 2010-06-30 16:34:03 3328: [TCPIP-server] recv() failed for sd=656 (err=10054 | An existing connection was forcibly closed by the remote host (peer).)

```
SisnTcpIpSisnSockError 1 0 2010-06-30 16:34:03 4028:
[TCPIP-server] recv() failed for sd=708 (err=10054 | An existing
connection was forcibly closed by the remote host (peer).)
```

The message is then displayed in the HPOM message browser.



To ignore this message, perform the following steps:

1. Create the `{OVAgent InstallDir}/siebspi/conf/rules.txt` file on managed node with the following content:

   ```
   .*An existing connection was forcibly closed by the remote host.*
   ```

2. Change the program parameters in the `SIEBSPI_GATEWAY_LOG` policy:

   ```
   siebspi_extmon -m SIEBSPI_GATEWAY_LOG -gtwy -rules rules.txt
   ```

3. Deploy the modified policy to the Siebel Gateway server system.

Chapter 6

Monitoring Siebel Components and Tasks

About Monitoring Siebel Components and Tasks

SPI for Siebel offers monitoring of components and tasks. Components are checked for changes in their status, for example, online and offline, while tasks are monitored for errors in their exit status and for the minimum and maximum number of running tasks.

Monitoring Siebel Components and Tasks

Monitor policies for Siebel components automatically monitor different language versions of specified Siebel component. In case you do not want or do not need to monitor components in specific language versions, change the monitor policy for that specific component using the `-skip_lang` parameter.

To monitor the components and their tasks, assign and install policies from the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/ SIEBSPI-Server Components** policy group on all components that you want to monitor. In addition, the following policies from the same group must also be assigned and installed:

To monitor the tasks exit status, install the following:

- `SIEBSPI_CHECK_TASKS_EXT`

To monitor the component status, install the following:

- `SIEBSPI_COMP_STATUS_EXT`

To monitor the maximum number of running tasks on components, install the following:

- `SIEBSPI_NUM_TASKS_TOO_HIGH_EXT`

To monitor the minimum number of running tasks on components, install the following:

- `SIEBSPI_NUM_TASKS_TOO_LOW_EXT`

If you want to collect performance data for the component, you can specify this with a parameter as described below.

By default, both the change of component status and task exit status are checked. However, you can disable one of them by deleting a parameter in the *Monitor Program Name* of the policy.

The following table describes the parameters:

Parameter	What is monitored
`-status`	Status of the component
`-min_tasks N`	Minimum tasks for the component; N specifies the min threshold
`-max_tasks`	Maximum tasks for the component
`-task_exit`	Task exit status
`-perf`	Collect performance information for the component
`-skip_lang "lang1, lang2…`	Ignore the components ending with specified language extensions

If you do not want to monitor the status of the components and the exit status of tasks, you do not need to install both (`SIEBSPI_CHECK_TASKS_EXT` and `SIEBSPI_COMP_STATUS_EXT`) monitor policies. Assign and install only the required one.

When monitoring the task exit status, you can also use the following feature: In the message browser, when a message that a task has exited with error is reported, you can start an operator-initiated action to list the log file contents of the Siebel server task which produced the message as an annotation to the message.

NOTE

It is not recommended to deploy more than 10 policies for Siebel components containing -perf parameter on one managed node.

Below is an example of how to modify a monitor policy to monitor only the component status changes of the Transaction Merger component:

1. Start the *HPOM Administration UI* and log in as an HPOM Administrator (opc_adm).
2. Go to **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Siebel Components/SIEBSPI-Siebel Remote** tool group.
3. Select the `SIEBSPI_TXN_MERGE_COMPONENT` policy.
4. Select **Edit** from the **Actions** menu, then select the **Source** tab.
5. In the *Program* name, modify the command line:

```
siebspi_extmon -srvr -m SIEBSPI_TXN_MERGE_COMPONENT - component "Transaction
Merger" -status
```

6. Click [OK] to confirm the changes.

NOTE

For the changes to take effect, you must deploy the modified policy on a node where the Siebel server is installed.

Adding a Policy for Monitoring Server Statistic Metrics

SPI for Siebel can monitor Siebel Server and Component statistics on Windows and Unix platforms.

This policy group **SIEBSPI-Statistics Metrics** is located in the **SPI for Siebel/ SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server** policy group with the following policies:

- SIEBSPI_SERVER_STATS
- SIEBSPI_SERVER_STATS_EXT
- SIEBSPI_COMPONENT_STATS
- SIEBSPI_COMPONENT_STATS_EXT

NOTE

SIEBSPI_COMPONENT_STATS has additional parameter 'component' for component name:

```
siebspi_extmon -mon SIEBSPI_COMPONENT_STATS -stats_list "AvgConnTime
AvgSQLExecTime" -component "comp. alias e.g. SCCObjMgr_enu"
```

Additional statistics names (aliases) can be gathered from Siebel Server Manager (srvrmgr), with following command:

```
list statistics for server 'siebelservername' component 'componentname'
```

under the STAT_ALIAS column.

Example:

How to add a policy for monitoring statistic metrics NumDBConnRtrs and NumDLRbkRtrs for the Siebel Application Server:

1. Start the *HPOM Administration UI* and log in as an HPOM Administrator (opc_adm).
2. Go to the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Statistics Metrics** policy group.
3. Select the **SIEBSPI_SERVER_STATS** policy.

4. Select **Edit** from the **Actions** menu, then select the **Source** tab.

5. In the *Monitor name*, modify the command line:

```
siebspi_extmon -mon SIEBSPI_SERVER_STATS -stats_list "NumDBConnRtrs
NumDLRbkRtrs" -component SSEObjMgr_enu
```

6. Click **Save** to confirm the changes.

NOTE

For the changes to take effect, you must assign and install the modified monitor policy on a node where the Siebel server is installed.

Advanced Component Monitoring Options

Changing External Policy Name that will Collect Component Results

By default, all `SIEBSPI_*_COMPONENT` monitor policies send results to standard Siebel component external monitor policies (`SIEBSPI_CHECK_TASKS_EXT`, `SIEBSPI_COMP_STATUS_EXT`, `SIEBSPI_NUM_TASKS_TOO_HIGH_EXT`, `SIEBSPI_NUM_TASKS_TOO_LOW_EXT`) as described in the previous section. The common thresholds, defined in those external monitor policies, are applied to all of them.

In situations when you need to define component specific thresholds, instructions, or actions, you can use the following parameters:

Parameter	Description
`-extmon`	Custom external monitor policy
`-[status2| min_tasks2| max_tasks2| task_exit2]`	What should be monitored and sent to the custom external monitor policy

This way you define what should be monitored and to which external monitor policy the results should be sent. You can combine standard parameters and the custom one in one component policy as long as you define custom external policies.

The required postfixes for custom external monitor policies are:

- `component status external monitor policy = *_CS_EXT`
- `task exit status external monitor policy = *_TS_EXT`
- `number of tasks to low external monitor policy = *_TL_EXT`
- `number of tasks to high external monitor policy = *_TH_EXT`

Example:

Siebel component "Workflow Monitor Agent" should send status results to the custom monitor policy SIEBSPI_WORK_MON_CS_EXT. Additionally, the number of running tasks (alarm if the number of running tasks: >70%, >90%) should be monitored.

Perform the following steps:

1. Create a copy of the SIEBSPI_COMP_STATUS_EXT external policy and save it under SIEBSPI_WORK_MON_CS_EXT
2. Customize Thresholds (if required, also: Actions, Instructions, and so on)
3. Customize SIEBSPI_WORK_MON_COMPONENT policy command line to:

```
siebspi_extmon -srvr -m SIEBSPI_WORK_MON_COMPONENT -component "Workflow
Monitor Agent" -extmon SIEBSPI_WORK_MON -status2 -max_tasks
```

Using Object Name Parameter in policies

On the UNIX HPOM management server, you can use the object name parameter to define different thresholds in Siebel component external policies (SIEBSPI_CHECK_TASKS_EXT, SIEBSPI_COMP_STATUS_EXT, SIEBSPI_NUM_TASKS_TOO_HIGH_EXT, SIEBSPI_NUM_TASKS_TOO_LOW_EXT) for specific Siebel components.

To set the Siebel component alias as an object name, perform the following:

1. Create copies of all thresholds and set the object name to component alias.
2. Modify the thresholds (message, instructions...) to get specific responses for the component that is entered as the object name.

How To Create a New Policy for Monitoring Custom Component

You can create you own policies for monitoring Siebel components that are not provided out-of-the-box.

Perform the following steps:

1. Copy one of the existing policies for component monitoring.
2. Define the same name in the policy command line with the -m parameter as the name of the policy:

   ```
   -m <Monitor policy name>
   ```

3. Compare the spelling of the component name (parameter -component) in the policy command line with the output from **SIEBSPI-List Components** tool. It is very important that they match.

   ```
   -component "<long Siebel component name in Siebel>"
   ```

Example:

New policy name: `SIEBSPI_ECOMM_WIRELESS_COMPONENT`

New policy program name:
`siebspi_extmon -srvr -m SIEBSPI_ECOMM_WIRELESS_COMPONENT -component`

" eCommunications for Wireless Object Manager (ENU)"

-perf -status -task_exit

Analyzing Siebel Component Crashes

Sometimes a Siebel server component may crash while it is executing or while it is shutting down. The symptoms vary depending on the type of the component that has crashed. For example, if an Object Manager crashes, all users connected to that Object Manager will be disconnected.

After the crash (or task error), it is very useful for the Siebel administrator to find out who (which user) was responsible for the crash and what the user executed before the crash, so the problem can be analyzed and eliminated.

Note that different Siebel components have different log Event types. With a little modification of log Event types also other components can be traced.

To configure SPI for Siebel to be able to get information about the user and actions responsible for the Siebel component crashes, perform the following steps:

1. Enable user logging for the component:

   From the **SPI for Siebel/SIEBSPI-Tools** tool group, launch the **SIEBSPI-Set EventLog Level** tool and change the tool parameters to:

   ```
   4 -event_type "ObjMgrSessionLog" -comp "SCCObjMgr_enu"
   ```

2. Enable activity logging for the component:

   Launch the **SIEBSPI-Set EventLog Level** tool again and change the tool parameters to:

   ```
   4 -event_type "EventContext" -comp "SCCObjMgr_enu"
   ```

3. Add an automatic action to the `SIEBSPI_CHECK_TASKS_EXT` policy into the condition task exited with error that will find the user, actions he or she performed, and issues from the task log file:

   ```
   siebspi_catl -p <$OPTION(logpath)> -c <$OPTION(comp_alias)> -t
   <$OPTION(task_id)>
   -req_exp ".*EventContext|Siebel Id|newUser|Error.*"
   ```

4. Deploy the policies to the managed nodes.

5. Check the message annotation after the component crash (task error) that displays in the message browser and analyze the output.

If you want to reset component logging levels, perform the following steps:

1. Disable user logging for the component:

   Launch the **SIEBSPI-Set EventLog Level** tool and change the tool parameters to:

   ```
   1 -event_type "ObjMgrSessionLog" -comp "SCCObjMgr_enu"
   ```

2. Disable activity logging for the component:

   Launch the **SIEBSPI-Set EventLog Level** tool again and change the tool parameters to:

   ```
   1 -event_type "EventContext" -comp "SCCObjMgr_enu"
   ```

Chapter 7

Monitoring Siebel Database, Database Tables, and Records

About Monitoring Siebel Database, Database Tables, and Records

SPI for Siebel provides basic monitoring for database, database tables, and records in your Siebel environment.

Monitoring Database Availability, Login Time, and Transaction Time from Siebel Server System

The monitor policy `SIEBSPI_DB_CONNECTIVITY` checks database server availability and connectivity from the Siebel server systems. To obtain the database login time, you can use thee `SIEBSPI_DB_LOGIN_TIME` policy.

To obtain the transaction time, `SIEBSPI_DB_TRANSACTION_TIME` runs a synthetic transaction, which is a set of predefined SQL statements.

To obtain the number of open connections to the Siebel database you can use `SIEBSPI_DB_SESSION`. Administrators are notified if real-time response times exceed the predefined monitor thresholds or if the database is not available.

It is also possible to collect this performance data and generate reports that show you potential database problems and slowdowns in time. (for additional information, refer to "Viewing and Analyzing Historical Data from Collected Performance Data" on page 105). For this purpose you can use performance monitors:

- `SIEBSPI_DB_LOGIN_PERFORMANCE`
- `SIEBSPI_DB_TRANS_PERFORMANCE`
- `SIEBSPI_DB_SESSION_PERFORMANCE`

Users can write their own SQL queries that will be used with the `SIEBSPI_DB_TRANSACTION_TIME` monitor to measure the transaction time of the database. To measure the database transaction with your custom SQL queries, perform the following steps:

1. Save your SQL query into the following directory:
   `{OVAgent InstallDir}/siebspi/conf`
2. Open the `SIEBSPI_DB_TRANSACTION_TIME` policy.
3. Change the program parameters in the policy:

```
siebspi_dbperf -mon SIEBSPI_DB_TRANSACTION_TIME
-transaction -sql_name "your sql name"
-sql_file "SQL file to be executed"
```

4. Change the thresholds levels in the policy conditions.
5. Deploy the SIEBSPI_DB_TRANSACTION_TIME policy to the Siebel server system.

To collect the transaction data obtained with your custom SQL queries, follow these instructions:

1. Open the SIEBSPI_DB_TRANSACTION_PERFORMANCE policy.
2. Change the program parameters in the policy:
   ```
   siebspi_dbperf -mon SIEBSPI_DB_TRANSACTION_PERFORMANCE
   -transaction -sql_name "your sql name"
   -sql_file "SQL file to be executed" -p
   ```
3. Deploy the SIEBSPI_DB_TRANSACTION_PERFORMANCE policy to the Siebel server system.

Monitoring the Size of the Siebel Database Tables

The SIEBSPI_WORKFLOW_BACKLOG and SIEBSPI_TRANS_PROCESSOR_BACKLOG policies in the policy group **SIEBSPI-Mobile Clients and Backlogs** are designed to monitor the size of the Siebel database tables. It is also possible to collect this performance data with the SIEBSPI_*_BACKLOG_PERF policies and generate reports that show database backlogs trends in time.

It is also possible to monitor a specific table from the Siebel database. Refer to the instructions below about how to create a custom policy to monitor any Siebel database table.

Monitoring the Transaction Processor Backlog Table

When the **System Preference Docking:Transaction Logging** is TRUE, Oracle's Siebel Business Applications will record transactions to the transaction log table (S_DOCK_TXN_LOG). The Transaction Processor (txnproc) is responsible for deleting entries from this table, once all txnprocs in the system have copied them to the Application server TXNPROC directory. Enterprise visible data will be routed to the active mobile clients. The backlog is the number of transactions in S_DOCK_TXN_LOG. However, a backlog of 1000 transactions is not usually considered a problem.

The SIEBSPI_TRANS_PROCESSOR_BACKLOG (optionally SIEBSPI_TRANS_PROCESSOR_BACKLOG_PERF) policy must be deployed on the Siebel server system to monitor the size of the S_DOCK_TXN_LOG table.

For more information on transaction processor backlog, see the policy instructions or refer to the *Siebel Remote and Replication Manager Administration Guide*.

Monitoring the Workflow Policies Backlog Table

When the Workflow policy condition is triggered, a record is inserted in the Escalation Request table, S_ESCL_REQ. This table contains all the rows in the database that could trigger a Workflow Policy to take action. After the workflow Monitor Agent processes a request, it removes the row from this table.

If the table becomes very large, this could indicate that the number of policies being monitored is too large and a new Workflow Policies process needs to be created to share the load. If rows are being monitored and are not removed after the time interval is met, this could indicate that a policy was deactivated without removing the database triggers. The triggers continue to send data which is not processed by the Workflow Policies instance.

The SIEBSPI_WORKFLOW_BACKLOG (optionally SIEBSPI_WORKFLOW_BACKLOG_PERF) policy must be deployed on the Siebel server system to monitor the size of the S_ESCL_REQ table.

For more information on workflow backlog, see the policy instructions or refer to the *Siebel Workflow Administration Guide*.

Monitoring any Siebel Database Table for Backlogs

To monitor the size of any Siebel database table, perform the following steps:

1. Make a copy of the SIEBSPI_WORKFLOW_BACKLOG policy and rename it.
2. Change the program parameters in the policy:

   ```
   siebspi_dbperf -mon "new policy name"
   -backlog_name "your backlog name" -table "table that should be
   monitored"
   ```

3. Change the threshold levels in the policy conditions.
4. Deploy the new policy to the Siebel server system.

To collect data about the size of your table, perform the following steps:

1. Make a copy of the SIEBSPI_WORKFLOW_BACKLOG_PERF policy and rename it.
2. Change the program parameters in the policy:

   ```
   siebspi_dbperf -mon "new policy name" -backlog_name "your backlog name"
   -table "table that should be monitored" -p
   ```

3. Deploy the new policy to the Siebel server system.

Monitoring the Records Value in the Siebel Database Tables

The SIEBSPI_SYNCH_BACKLOG, SIEBSPI_SYNCH_BACKLOG_EXT, SIEBSPI_TRANS_MERGER_BACKLOG, SIEBSPI_TRANS_MERGER_BACKLOG_EXT, SIEBSPI_TRANS_ROUTER_BACKLOG and SIEBSPI_TRANS_ROUTER_BACKLOG_EXT policies in the policy group SIEBSPI-Mobile Clients and Backlogs are designed to monitor the synchronization, transaction merger, and transaction router backlogs. It is also possible to collect this performance data with the SIEBSPI_*_BACKLOG_PERF policies and generate reports that show you database record value trends in time.

These backlogs are extracted from Siebel database with predefined SQL queries, stored in the {OVAgent InstallDir}/siebspi/conf directory.

It is also possible to monitor custom backlogs. Refer to the instructions below on how to create custom policy to monitor the results from your SQL queries.

The difference between this policies and policies in the previous section is that policies in the previous section monitor the number of records in database tables, and policies in this section monitor the value for specific field in each record. For example, the number of hours from last user synchronization for each remote user, or the number of unsynchronized files on server for each remote user.

Monitoring the SYNCHRONIZATION BACKLOG

Synchronization Backlog indicates that there is a substantial amount of data that must be downloaded by a remote user. Remote users need to synchronize daily to keep the amount of data low. To monitor the number of files that need to be sent to a particular client, deploy the SIEBSPI_SYNCH_BACKLOG and SIEBSPI_SYNCH_BACKLOG_EXT (optionally SIEBSPI_SYNCH_BACKLOG_PERF) policies to the Siebel server system.

Monitoring the TRANSACTION MERGER BACKLOG

Transaction merger backlogs indicate that remote users have made changes on their local databases and uploaded the changes to the server, but these changes have not been committed to the server database yet. A high backlog here indicates that not all changes made by remote users are visible on the server. To monitor the number of files that need to be merged from a particular client, deploy the SIEBSPI_TRANS_MERGER_BACKLOG and SIEBSPI_TRANS_MERGER_BACKLOG_EXT (optionally SIEBSPI_TRANS_MERGER_BACKLOG_PERF) policies to the Siebel server system.

Monitoring the TRANSACTION ROUTER BACKLOG

Transactions are created when data is updated on the server database. These transactions need to be routed to remote users so that they can see the updates. A backlog of transactions indicates that not all of the data has been routed.

To monitor the number of transactions that need to be routed to a particular client, deploy the `SIEBSPI_TRANS_ROUTER_BACKLOG` and `SIEBSPI_TRANS_ROUTER_BACKLOG_EXT` (optionally `SIEBSPI_TRANS_ROUTER_BACKLOG_PERF`) policies to the Siebel server system.

Monitoring Any Record in Any Siebel Table for the Last Date of Change and if Any Numeric Values Exceed Threshold

Sometimes you would like to know which Siebel workflows are not processed for a certain number of days, which opportunities, contacts, or orders were not changed since the specific date or which opportunities are really big (for example, revenue is more than a certain amount of money). You can get all that information with SPI for Siebel. You can monitor any record in any Siebel table for the last date of change with SPI for Siebel tools and policies.

Use the **SIEBSPI-Pending Workflows** tool in the **SPI for Siebel/SIEBSPI-Performance/SIEBSPI-Mobile Clients and Backlogs** tool group to display workflow requests that are older than the specified number of days.

Use the **SIEBSPI-Inactive Opportunities** tool in the **SPI for Siebel/SIEBSPI-Performance/SIEBSPI-Mobile Clients and Backlogs** tool group to display opportunities that were not changed for more than the specified number of days.

You can also customize the existing tools to monitor any Siebel table for records older than the specified time or records with the value greater than the specified value.

To monitor pending workflow requests, use the `SIEBSPI_WORKFLOW_REQ` and `SIEBSPI_WORKFLOW_REQ_EXT` policies, located in the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Mobile Clients and Backlogs** policy group.

Example: How to create a tool that will report opportunities with the revenue greater than 10.000$

1. Save the SQL query bellow into the following directory and file on the managed node:

   ```
   {OVAgent InstallDir}/siebspi/conf/siebspi_big_oppty.sql
   ```

   If you use the Oracle or DB2 database type:

   ```
   SELECT    'NAME: ' || NAME || ',   ROW_ID: ' || ROW_ID AS OPPORTUNITY,
   SUM_REVN_AMT
   ```

```
FROM          %DATABASE%.S_OPTY
ORDER BY SUM_REVN_AMT DESC
```

If you use MS SQL database type:

```
SELECT     'NAME: ' + NAME + ',    ROW_ID: ' + ROW_ID AS OPPORTUNITY,
SUM_REVN_AMT
FROM          %DATABASE%.S_OPTY
ORDER BY SUM_REVN_AMT DESC
```

2. Make a copy of the Inactive opportunities tool and rename it.
3. Change the program parameters in the tool:

```
siebspi_dbperf -columns 2 -col1 1 -col2 2 -sql_file
siebspi_big_oppty.sql -print -threshold 10000
```

Parameters' descriptions:

-columns Number of columns returned by your SQL query, for example, 2

-col1 Number of column that returns a string value, for example, 1

-col2 Number of column that returns a float, integer or date-timevalue, for example, 2; this value is then compared to the threshold value.

-sql_file Name of your sql file, for example, siebspi_synch.sql

-threshold Value that must be exceeded by the "col2" value to include record to the list, for example, 300

-threshold_day Include only records with the date value in "col2" older than x days, for example, 30

-threshold_date Include only records with the date value in "col2" older than this date, for example, 10-12-2006

The following two parameters are used in policies, but not in tools:

-ext_mon Policy name, for example, SIEBSPI_SYNCH_BACKLOG

-pair Name of the backlog, for example, synchBL. This is used just in policies that writes data into performance agent (name ending with `_PERF`)

4. Launch the new tool.

Similar procedure can be used to create policies that will report records that exceed threshold into HPOM message browser. You can copy and modify the `SIEBSPI_WORKFLOW_REQ` and `SIEBSPI_WORKFLOW_REQ_EXT` policies.

Chapter 8

Monitoring Siebel Users and Siebel Applications Activity

About Monitoring Siebel Users and Siebel Applications Activity

SPI for Siebel enables you to monitor the usage of different Siebel applications and the users activity.

Monitoring Siebel Users that Are Logged into Siebel Application (Object Manager Component)

This functionality includes monitoring the number of users connected to Siebel Applications (Object Manager Components) between two monitor intervals, and the number of active users in monitoring moment. To turn this monitoring on, add a command-line parameter usercount into existing or new component monitor policies (only for Object Manager policies).

In addition to the number of users, information on when Siebel users logged in, logged out, and for how long they were connected to a Siebel Application can be collected. To turn this monitoring on, add a command-line parameter usertime into existing or new component monitors policies (only for Object Manager policies).

Example: Modifying the existing "Call Center Object Manager" component

```
siebspi_extmon -srvr -m SIEBSPI_SCC_OBJ_MGR_COMPONENT -component "Call
Center Object Manager" -perf -status -usercount -usertime
```

Example: Creating a new policy for "Call Center Object Manager" component

```
siebspi_extmon -srvr -m NEW_SCC_OBJ_MGR_COMPONENT -component "Call
Center Object Manager" -usercount -usertime
```

There are two Performance Manager graph templates available that display the number of users connected to Siebel Applications (Object Manager Components) between two monitor intervals, and the number of active users in monitoring moment. For details, reefer to "Viewing and Analyzing Historical Data from Collected Performance Data" on page 105.

You can also check who (which users) is connected to Siebel Application (Object Manager Component) at the moment and what are the users doing with the **SIEBSPI-Users Connected to Object Manager Component** tool that is located in the **SPI for Siebel/SIEBSPI-Siebel Users Activity** tool group. This information is important, for example, if something unusual is happening to the system. It can also be useful to get information about the process PID and task number for each user session in that moment.

The tool outputs the following information:

- component name and alias
- Siebel user name
- login time
- siebmtshmw process PID
- task ID
- last view accessed by user
- last applet accessed by user

Before you use the tool for the first time, you need to modify the tool program parameters with the name of the Object Manager Component for the tool that you want to monitor. For example, for Call Center Object Manager (`SCCObjMgr_enu`):
`-comp "SCCObjMgr_enu"`

If you want to have more tools for different Object Manager Components, you can make a copy of the existing tool and create a new one for each.

There are also web-based reports available that present collected data:

- Users connected to Siebel Applications (Object Manager Components), grouped by users
- Users connected to Siebel Applications (Object Manager Components), grouped by Siebel Applications
- Number of users connected to Siebel Applications (Object Manager Components)

For more information about these reports, refer to "SPI for Siebel Integration with HP Reporter" on page 112.

Monitoring Siebel Users' Last Login Time into Siebel Applications

Sales managers, business managers, and Siebel administrators can require information about the last time when Siebel users were connected into Siebel Applications.

To collect the information on inactive users, you can use the **SIEBSPI-Last Siebel User Login Time** tool. It is located in the **SPI for Siebel/SIEBSPI-Siebel Users Activity** tool group.

For reporting purposes, you can use the policy `SIEBSPI_USER_LOGIN_PERFORMANCE`, located in the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Siebel Users Activity** policy group. By default, this policy collects data on Siebel users last login time on a daily basis.

SPI for Siebel enables you to specify Siebel users not to include in the data collection and reports. The list of excluded users is located in the configuration file:

<OVInstallDir>/siebspi/conf/exclude_user.cfg

By default, the following users are excluded: GUESTCST, GUESTCP, GUESTERM, PROXYE, and UNIVERSALQUEUE. You can also deactivate or activate users in the exclusion list by adding or removing the // mark at the beginning of the line.

Available web based report to present the collected data:

- Number of days since last login of Siebel user (Top 50 inactive users)

For more information about this report, refer to "SPI for Siebel Integration with HP Reporter" on page 112.

Monitoring Last Time When a Siebel User Added or Changed Account, Contact, or Opportunity

Sales managers, business managers, and Siebel administrators can require information about the last time when Siebel users add or change account, contact, or opportunity in Siebel Applications.

To get this information, you can use **SIEBSPI-Last Siebel User Action time** tool from the **SPI for Siebel/SIEBSPI-Siebel Users Activity** tool group.

You can also use the following tools from the **SIEBSPI-Siebel Users Activity** tool group:

- **SIEBSPI-Last Account Change**
- **SIEBSPI-Last Contact Change**
- **SIEBSPI-Last Opportunity Change**

For reporting purposes, you can use the SIEBSPI_USER_ACTION_PERFORMANCE policy. It is located in the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Siebel Users Activity** policy group. By default, this policy collects data about Siebel users last action time on a daily basis.

SPI for Siebel enables you to specify Siebel users not to include in the data collection and reports. For more information, refer to "Monitoring Siebel Users' Last Login Time into Siebel Applications" on page 65.

Available web based report to present the collected data:

- Number of days since last update of account, opportunity or contact (Top 50 inactive Siebel users)

For more information about this report, refer to "SPI for Siebel Integration with HP Reporter" on page 112.

Chapter 9

Monitoring Siebel Web Server Extension (SWSE)

About Monitoring Siebel Web Server Extension (SWSE)

The Siebel Web Server Extension, operating on the Web server, connects to the Application Object Manager component operating within the Siebel Server. This connection uses Siebel's application. When accessing Siebel applications using the Web client, no components are hosted on the client. The client interacts through a Web browser.

SPI for Siebel offers tools and policies that help system administrators have a better understanding of the use of the Web server. To report current SWSE data statistics, use the **SIEBSPI-Show SWSE System and Application Statistics** tool from the **SPI for Siebel/SIEBSPI-Performance** tool group.

It outputs the current SWSE data about:

- Average response times
  This event measures the time needed to receive a callback response from the Siebel server. This event functions with CTI and internal login callbacks. A callback is a mechanism used by the Siebel Server to initiate communication with the plug-in.
- Average close session time
  This event reflects the amount of time needed to close a session.
- Average open session time
  This event reflects the amount of time needed to open a session.
- Average request time
  This event is the amount of time needed to submit a request to the Siebel Server and to get a response back. For example, if the user (on the browser) clicked on a button then the plug-in receives the request and invokes a service on the Siebel Server.
- Number of attempts to use the application
  Number of attempts to use the specified Siebel Applications
- Average time it took to open a session to specified application

To monitor this statistic data values, install the following policies from the policy group **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Web Server Extension/SIEBSPI-SWSE Statistics Page**:

- `SIEBSPI_SWSE_AVERAGE_APPLICATION_RESPONSE_TIME`
- `SIEBSPI_SWSE_AVERAGE_CLOSE_SESSION_TIME`
- `SIEBSPI_SWSE_AVERAGE_OPEN_SESSION_TIME`
- `SIEBSPI_SWSE_AVERAGE_REQUEST_TIME`
- `SIEBSPI_SWSE_AVERAGE_RESPONSE_TIME`

To collect SWSE performance statistics data, install the following policies:

- `SIEBSPI_SWSE_SYSTEM_STATISTIC_PERF`
- `SIEBSPI_SWSE_APPLICATION_STATISTIC_PERF`

Note that before you can use these policies and tools, you need to customize their command lines with the Siebel Application name that is used on your SWSE. You can get the correct application name from the url address that is used to login into your Siebel application. For example, if you use:
`http://gander/callcenter_enu/start.swe`

the name is `callcenter_enu`

To configure the `SIEBSPI_SWSE_AVERAGE_CLOSE_SESSION_TIME` policy, perform the following steps:

1. Open the policy.
2. Change the program name parameter from:

- `siebspi_web -application "Application name, e.g. callcenter_enu" -f SWSE_AVG_CLOSE_TIME -mon SIEBSPI_SWSE_AVERAGE_CLOSE_SESSION_TIME`

to:

- `siebspi_web -application " callcenter_enu" -f SWSE_AVG_CLOSE_TIME -mon SIEBSPI_SWSE_AVERAGE_CLOSE_SESSION_TIME`

To monitor SWSE log file for errors, install the following policy from the policy group **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/ SIEBSPI-Siebel Web Server Extension**:

- `SIEBSPI_WEB_SERVER_LOG`

For more information about the log file monitoring, refer to "Monitoring Siebel Log Files" on page 39.

Monitoring the Availability of Web Server Services and daemons Needed for SWSE to Work Correctly

SPI for Siebel offers tools and policies that help system administrators have all important web server services and daemons up and running.

To monitor availability of web services and daemons, install the following policies from the policy group `SPI for Siebel/SIEBSPI-Web Servers/SIEBSPI-<Web server>` (depending on the type of web server that is used):

Tomcat:
`SIEBSPI_TOMCAT_PROCESS`

MS IIS:
`SIEBSPI_WEB_WIN_SERVER_STATUS`

Sun ONE Web Server 6.0:
`SIEBSPI_WEB_SUN60_SERVER_STATUS`

Sun ONE Web Server 6.1:
`SIEBSPI_WEB_SUN61_SERVER_STATUS`

IBM HTTP Web Server:
`SIEBSPI_WEB_IBM_HTTP_SERVER_STATUS`

For starting or stopping web services, use the following tools from the **SIEBSPI-Siebel Services** tool group:

- **SIEBSPI-Start WEB Server**
- **SIEBSPI-Stop WEB Server**

If you use web server that is not supported with the provided policies and tools, SPI for Siebel offers easy customization that enables you to monitor any new web servers.

With the `-daemon` parameter, you can select which daemon process you want to monitor. To specify which daemon will be monitored, add this parameter to the policy command line, for example:

Policy: `SIEBSPI_WEB_SERVER_MYSRV_STATUS`
`siebspi_extmon -m SIEBSPI_WEB_SERVER_MYSRV_STATUS -daemon <daemon_name>`

In tools, used for starting or stopping the web server, you can also specify a daemon name that differs from the default. This name is used when performing the check if daemon is running before the start or stop. The -daemon parameter enables you to select which daemon process you want to check. The -script parameter enables you to change the web server start/stop script. To specify which script will be used, add this parameter to the tool command line, for example:

Tool: **SIEBSPI-Stop WEB Server**
`siebspi_mgr -service stop_web -script <script_name> -daemon <daemon_name>`

or

Tool: **SIEBSPI-Start WEB Server**
`siebspi_mgr -service start_web -script <script_name> -daemon <daemon_name>`

Monitoring Availability and Response Time of Ports on the Siebel Server Machine from the SWSE Machine

SPI for Siebel offers tools and policies that can be used for checking availability and response times of ports on the Siebel Server machine from the SWSE machine and contrariwise.

For monitoring port availability, install the following policies from the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Web Server Extension/ SIEBSPI-Port Response and Availability** policy group:

- `SIEBSPI_PORT_AVAILABILITY`
- `SIEBSPI_PORT_AVAILABILITY_EXT`

For monitoring port response time (ms), install the following policies from the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Web Server Extension/ SIEBSPI-Port Response and Availability** policy group:

- `SIEBSPI_PORT_RESPONSE_TIME`
- `SIEBSPI_PORT_RESPONSE_TIME_EXT`

For displaying current port response time (ms), the following tool can be used from the **SPI for Siebel/SIEBSPI-Performance** tool group:

- **SIEBSPI-Port Performance**

Note that before you can use this policies and tools, you need to customize their command lines with the port numbers that you want to monitor. For example, to configure the `SIEBSPI_PORT_AVAILABILITY` policy, open the Modify policy window and change the program name parameter from:

```
siebspi_extmon -m SIEBSPI_PORT_AVAILABILITY -target target_host -port
port1,port2,..
```

to:

```
siebspi_extmon -m SIEBSPI_PORT_AVAILABILITY -target target_host -port 80
```

Optionally you can also specify non-default time interval that policy or tool will wait for port to response, by adding the parameter `-timeout <Timeout in seconds>` into the policy or tool program name parameter.

Chapter 10

Monitoring Siebel End-User Experience and Response Times

About End-User Monitoring

Siebel Mobile and Dedicated Clients End-User Monitoring

Smart Probe is a program that runs on Siebel clients and shows the clients Siebel server availability and connectivity. It monitors the login time and transaction time with two monitors that are started every n-seconds. To obtain the transaction time, Smart Probe runs a synthetic transaction, which is a set of pre-defined client actions, for example, query for Account Names in Accounts. Administrators are notified if real-time response times exceed the predefined monitor thresholds or if the Siebel server/Siebel database is not available. Smart Probe works on any computer where a **Siebel Mobile/Dedicated web client** is installed.

The Smart Probe policy for monitoring transaction time, `SIEBSPI_SP_TRANSACTION_TIME`, or the policy for collecting performance data, `SIEBSPI_SP_PERFORMANCE` (Siebel client login and transaction time), in the policy group **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Smart Probe** can be modified to execute a different transaction.

For example, assume that you want to query the Last Names of your Contacts. You can modify the `SIEBSPI_SP_TRANSACTION_TIME` policy to monitor the transaction time of the user query by performing the following steps:

1. Start the *HPOM Administration UI* and log in as an HPOM Administrator (opc_adm).
2. Go to the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Smart Probe** policy group.
3. Click the `SIEBSPI_SP_TRANSACTION_TIME` policy.
4. In the *Monitor Program Name*, add the -busobj, -buscomp and -compfield parameters. For example:

   ```
   siebspi_sp -t -busobj "Contact" -buscomp "Contact" -compfield "Last Name"
   ```

Additionally, the `SIEBSPI_SP_PERFORMANCE` policy can be modified in the same manner.

NOTE

For the changes to take effect deploy the new policies on a node where the Siebel Mobile/Dedicated web client is installed.

OVIS Smart Probe for Siebel

Installation Instructions

For information on how to install and configure OVIS Smart Probe for Siebel, refer to *OVIS SMARTProbe for Siebel Installation and Configuration Guide*.

You can find the self-extracting installation file for HP Internet Services and OVIS Smart Probe for Siebel documentation on the SPI for Siebel download page:

- `OVISProbeforSiebel_03_20.exe`
- `OVIS_SmartProbe_for_Siebel_03_20.pdf`

OVIS SMARTProbe for Siebel target is a Web Server that is used by Siebel Web Clients to access Oracle Siebel CRM Applications. OVIS SMARTProbe for Siebel supports all Web Servers that are supported by:

- Oracle Siebel CRM Applications 7.7, 7.8, or 8.x.

Chapter 11

Using SPI for Siebel for Analyzing Siebel Application Response Measurement (SARM) Data

About Siebel ARM

Siebel ARM is a framework for capturing critical performance data in Oracle's Siebel Business Applications. Siebel ARM captures response times at key monitoring points within the Siebel Server infrastructure. These Siebel ARM monitoring points are classified in the following distinct areas within the Siebel infrastructure:

- **Web Server Time**. The time a request has spent on the Web server.
- **Infra-Network Time**. The time between a request from the Web server and the Siebel Server (including the network time).
- **Siebel Server Time**. The time Siebel Server and Database Server need to process the request (time between Server Thread (SMI) and any database-layer calls).
- **Database Time**. The time spent for any Siebel Database-layer calls.
- **Tool-Specific Time**. The time spent in tool-specific areas of the infrastructure.

The Siebel ARM feature monitors system performance in the infrastructure and tool-specific pre defined areas, which appear in Siebel ARM output.

How Can SPI for Siebel Help You Analyze Siebel Transactions

SPI for Siebel provides diagnostic tools that help administrators to correlate Oracle's Siebel Business Applications end-user performance and availability problems to their root causes within the Siebel infrastructure. These tools help you to find problematic areas in Siebel user transactions, where the most time, CPU or memory is spent. SPI also provides tolls that can be used from HPOM console for setting SARM parameters on the node, and to start or stop collecting SARM information on the node.

If you want to use SARM and SPI to analyze problematic transaction, perform the following steps:

1. If you do not want to have default values, set SARM parameters on all managed nodes that will be used by transaction (Siebel Web Server Extension, Siebel Servers) using SPI for Siebel tools.
2. Start the collection of SARM data on all involved managed nodes, using SPI for Siebel tools.
3. Execute problematic transaction (manually or using any of the automated tools for login into Siebel and performing transactions).

4. Stop the collection of SARM data on all involved managed nodes, using SPI for Siebel tools.
5. Copy SARM log files from all involved managed nodes to one location on the machine where analyzing will be performed.
6. Analyze transaction and find problematic areas and bottlenecks, using SPI for Siebel tools.

For detailed instructions on how to perform these steps, refer to the following sections. Steps are described using a real-life example. A company is having performance problem using Siebel applications for sales automation. When users try to go to Contacts View, and then to Contacts List Screen, and perform there a query by last name, it takes about 3 minutes before the results are displayed. We will try to find out where the problematic areas are.

Setting SARM Parameters Using SPI for Siebel Tools

SPI for Siebel provides tools that can be used to set all SARM parameters on managed nodes from a central point (HPOM). You can set parameters on both, Web Server and Siebel Server. The following tools are provided in the tool group **SPI for Siebel/SIEBSPI-SARM/SIEBSPI-SARM Parameters**:

- **SIEBSPI-Change SARM Buffer Size**
- **SIEBSPI-Change SARM File Size**
- **SIEBSPI-Change SARM Max Files Number**
- **SIEBSPI-Change SARM Period**

Before you use these tools, you should configure (modify) tools parameters. For the complete list and descriptions of the tools parameters, refer to the *SPI for Siebel Quick Reference Guide*.

SARM Parameters Descriptions

In SARM, the following parameters and environment variables are defined:

Parameter Display Name	Parameter Alias	Environment Variable Name
SARM Granularity Level*	SARMLevel	SIEBEL_SARMLevel
SARM Buffer Size	SARMBufferSize	SIEBEL_SARMBufferSize
SARM Period	SARMPeriod	SIEBEL_SARMPeriod
SARM Max Number of Files	SARMMaxFiles	SIEBEL_SARMMaxFiles
SARM Data File Size	SARMFileSIze	SIEBEL_SARMFileSize

*This parameter is used later for enabling/disabling SARM

SARM Buffer Size

The Siebel ARM framework uses a buffered data generation mechanism. Siebel ARM collects data and stores it in memory. After the in-memory data size reaches a threshold defined by SARM Buffer Size Siebel ARM outputs the stored data to file on a physical disk. The SARM Buffer Size parameter or environment variable is specified in bytes. The default value is 5,000,000 bytes (approximately 5 MB). The valid settings range from 100,000 bytes to 50,000,000 bytes.

Siebel ARM also outputs stored data to a file based on elapsed time, which is defined by the parameter or environment variable SARM Period. The setting of this parameter may determine the size of the data saved to the file rather than the threshold value defined by SARM Buffer Size.

For example, if SARMBufferSize is 5 MB and there are five instances (processes) of the component, then the total memory used is 25 MB.

SARM Period

Siebel ARM collects data and stores it in memory. The time period specified by the SARM Period parameter or environment variable determines when Siebel ARM outputs the stored data to a file on a physical disk regardless of the value set for `SARM Buffer Size`. The parameter is specified in minutes, and has a default value of 3 minutes. The valid settings for this parameter range from 1 minute to 60 minutes.

Only use `SARM Period` to output Siebel Server performance data based on elapsed time. Siebel ARM outputs Web server performance data based only on the `SARM Buffer Size` value.

SARM Max Number of Files

Specifies the maximum number of Siebel ARM files created per component instance. The default value is four, and there is no Siebel-specified upper limit to the number of files Siebel ARM creates. (The parameter or environment variable `SARM Data File Size` configures how large a file becomes before a new file is stored on the physical disk.)

The number of active Siebel ARM files per component process is 1 plus the value of `SARM Max Number of Files`. That is, Siebel ARM removes the oldest file for that process only after the SARM Max Number of Files-plus-1 file reaches `SARM Data File Size`.

See the description for SARM Data Size for an example on how to calculate memory usage using these parameters or environment variables.

SARM Data File Size

Specifies how large a file becomes before Siebel ARM stores data in a new file on the physical disk. The parameter is specified in bytes. The default value is 15000000 bytes (15 MB), and there is no Siebel-specified upper limit to file size.

Until the specified size is reached, Siebel ARM continues to append file segments to the current file. When the file limit is reached, Siebel ARM creates a new file. (The parameter or environment variable SARM Max Number of Files configures the number of files maintained by Siebel ARM.)

When Siebel ARM reaches the file number specified by `SARM Max Number of Files` (that is, there are SARM Max Number of Files of size SARM Data File Size), Siebel ARM removes the first (that is, the oldest) file when the next file reaches the SARM Data File Size limit. Therefore, the maximum amount of disk space used is approximately SARM Max Number of Files + 1 times SARM Data File Size bytes. This amount of memory is per-process (per component instance).

For example, if SARM Data File Size is 15 MB, SARM Max Number of Files is 4, and there are 5 instances (processes) of the component, then the maximum amount of disk space consumed is approximately 375 MB-that is, 15MB per file, times 5 files per process, times 5 processes (instances of component).

Starting the Collection of SARM Data Using SPI for Siebel Tools

SPI for Siebel provides tools that can be used to start collecting SARM data on managed nodes from a central point (HPOM). To start collecting SARM data on both, Web Server and Siebel Server, use SPI for Siebel tools for changing SARM Granularity Level. The following tools are provided in the tool group **SPI for Siebel/ SIEBSPI-SARM/SIEBSPI-SARM Parameters**:

- **SIEBSPI-Start SARM Data Collection on Level 1 (ARM)**
- **SIEBSPI-Start SARM Data Collection on Level 2 (Detail)**

Before you use these tools, you can configure (modify) tools parameters. For the complete list and descriptions of the tools parameters, refer to the *SPI for Siebel Quick Reference Guide*.

SARM Granularity Level

Specifies the amount of response measurement detail logged to Siebel ARM files and effectively enables or disables the Siebel ARM feature. This parameter or environment variable has the following settings:

- **1 (ARM)**. This setting captures general application performance and is based on the application response measurement (ARM) standard. At this level, Siebel ARM collects information such as process and component boundaries, third-party

software calls, database measurements, workflow execution, and script performance. Use this level for general performance monitoring.

- **2 (Detail)**. This setting captures the information at level 1 as well as detailed information such as steps of workflow execution, construction of large objects, reading of large files, and crossing significant architectural areas. Use this level for problem diagnostics.

Executing Problematic Siebel User Transactions

After SARM data collection is enabled, you should execute problematic transaction. You can do this manually in Siebel GUI or use any of the automated applications for login into Siebel and performing transactions.

We recommend performing transactions without any other user activity on the nodes when SARM data collection is enabled. That way the SARM log files will be smaller and analyzing will be easier and quicker.

Stopping the Collection of SARM Data Using SPI for Siebel Tools

SPI for Siebel provides tools that can be used to stop collecting SARM data on managed nodes from a central point (HPOM). To stop collecting SARM data on both, Web Server and Siebel Server, use the SPI tools for changing SARM Granularity Level to 0. This setting is the default value and disables Siebel ARM. To stop collecting SARM data, use the **SIEBSPI-Stop SARM Data Collection** tool, located in the **SPI for Siebel/SIEBSPI-SARM/SIEBSPI-SARM Parameters** tool group.

Before you use this tool, you can configure (modify) tool's parameters. For a complete list and descriptions of the tools parameters, refer to the *SPI for Siebel Quick Reference Guide*.

Copying SARM Log Files to Location for Analyzing

To get a complete picture of the complete transaction, it is important that you use SARM files from Siebel Web Server Extension and from Siebel Server(s) together when analysis is performed. Usually, those SARM files are located on several computers. In such cases, copy all files to a single computer to a directory, where analysis will be performed. Alternatively, share (NFS, SAM, and so on) remote directories where SARM files are located.

We recommend you to perform analysis on a computer that is not part of the Siebel environment, because analyzing big amount of SARM files takes a lot of time and machine resources.

Analyzing Transactions Using SPI for Siebel Tools

This is the most important step and reason that all previous steps were performed. SPI for Siebel provides two ways for analyzing SARM data:

- **Call graph workflow analysis**
  The Call Graph displays how the specific areas and methods were called within the session. It also displays the specific metric values, for example, `duration`, `cpu_time`, `cpu_perc`, `pooled_memory_usage` and `pooled_memory_calls`
- **Performance aggregation analysis**
  This analysis displays problematic areas in Siebel. The tool analyzes Siebel areas (for example, SWE) for the specific metric (for example, "total response time") maximum values. When the area is found, it analyzes the child areas to see which child area took the most time. After that, the tool calculates in which child area the calls take the most time. When the call (method) is discovered, the tool displays a performance summary for that call.

Tools for Running Call Graph Workflow Analysis

SPI for Siebel provides tools that you can use to execute Call Graph Workflow Analysis. This analysis is divided into 2 steps:

1. Create comma-separated files (CSV) from SARM binary log files. To do this, use the SPI for Siebel tool that is using Siebel tool for creating CSV files. The files are used for later analysis.

   For this purpose, the **SIEBSPI-Run Call Graph (CSV) Workflow Analysis** tool is provided in the **SPI for Siebel/SIEBSPI-SARM/SIEBSPI-Call Graph Workflow Analysis** tool group.

   The CSV files are placed in the …`/siebspi/tmp` directory.

For more information about this SARM CSV files, refer to "Siebel ARM (SARM) Reference Information" on page 168.

2. Execute analysis that shows Call graph workflow.

Use the tool **SIEBSPI-List Sessions Using CSV SARM Data** from the **SPI for Siebel/ SIEBSPI-SARM/SIEBSPI-SARM Call Graph Workflow Analysis** tool group to display all available sessions in current SARM files. This information can be later

used for running Call Graph Workflow analysis (using parameter `-session {session id}`) to filter output on one session.

The following tools are provided for displaying workflow data tree in the **SPI for Siebel/SIEBSPI-SARM/SIEBSPI-SARM Call Graph Workflow Analysis/ Show Workflow from CSV SARM Data** tool group:

- **SIEBSPI-Show Workflow Data Using All Metrics**
- **SIEBSPI-Show Workflow Data Using Metric '%CPU'**
- **SIEBSPI-Show Workflow Data Using Metric 'Count'**
- **SIEBSPI-Show Workflow Data Using Metric 'CPUTime'**
- **SIEBSPI-Show Workflow Data Using Metric 'Duration'**
- **SIEBSPI-Show Workflow Data Using Metric 'PooledMemoryCalls'**
- **SIEBSPI-Show Workflow Data Using Metric 'PooledMemoryUsage'**
- **SIEBSPI-Show Workflow Data Using Metric 'SystemMemoryCalls'**
- **SIEBSPI-Show Workflow Data Using Metric 'SystemMemoryUsage'**

It is important that you use SARM files from Siebel Web Extension and from Siebel Server(s). Usually those SARM files are located on several computers. To use SARM files from different locations, specify the directories (local or remote) using -include_sarm_dirs parameter.

Example:

```
siebspi_sarm -list_sessions
         -include_sarm_dirs /net/node/sarm,/this/too
```

Example output:

```
Session: 30969
Session: 30970
Session: 30971
Session: 30972
```

This example will use SARM files on a local computer in original Siebel log directories and the SARM files in the following directories: `/net/node/sarm and /this/too`. For example, `/net/node/sarm` is a NFS mounted directory and `/this/too` is a local temporary directory.

If you do not want to use the SARM files in original Siebel log directories on the computer where you execute the tool, specify the `-exclude_original_sarm_dirs` parameter.

Example:

```
siebspi_sarm -list_sessions
          -include_sarm_dirs /net/node/sarm,/this/too
          -exclude_original_sarm_dirs
```

In this case, only the SARM files in directories `/net/node/sarm and /this/too` will be used.

The same parameters can also be used for other tools, for example, **SIEBSPI-Run Call Graph (CSV) Workflow Analysis**.

The Call Graph displays how the specific areas and methods were called within the session. It also displays the specific metric values, for example, SystemMemoryUsage (on areas).

Analysis can be done for the specified metric and/or session.

Example command line:

```
siebspi_sarm  -call_graph
              -session 30928
              -metric Duration
```

Example output:

```
     sadmin
       |
       Session: !1.c5c.78d0 - Task ID: 30928
             |
             +- Area_SWSE.Receive request [Duration(MiliSecs): 150.515]
                |
                +- Area_SWSE.Send message to app server [Duration(MiliSecs): 8.725]
                   |
                +- Area_INFRA.Request Receipt (sessID SeqID) [Duration(MiliSecs): 112.588]
                   |  |
                   |  +- Area_OBJMGR.Service Invoke Method.Web Engine Interface
     [Duration(MiliSecs): 111.368]
                   |     |
                   |     +- Area_SWE.Invoke Applet Method.Account Entry Applet
     [Duration(MiliSecs): 110.576]
                   |        |
                    |      +- Area_OBJMGR.BusComp Write Record.Account [Duration(MiliSecs):
     105.292]
                   |        |  |
                   |        |  +- Area_OBJMGR.BusComp Write Record.Activity Plan
     [Duration(MiliSecs): 0.013]
                   |        |  |
                   |        |  +- Area_OBJMGR.BusComp Write Record.Activity Plan
     [Duration(MiliSecs): 0.005]
                   |        |  |
                   |        |  +- Area_OBJMGR.BusComp Query Execution.Activity Plan
     [Duration(MiliSecs): 4.004]
                   |        |  |  |
                   |        |  |  +- Area_OBJMGR.BusComp Write Record.Activity Plan
     [Duration(MiliSecs): 0.006]
                   |        |  |  |
               |      |  |  +- Area_DBC.Prepare SQL statement [Duration(MiliSecs): 0.328]
                  |        |  |  |
               |      |  |  +- Area_DBC.Execute SQL statement [Duration(MiliSecs): 2.535]
                   |        |  |
                   |        |  +- Area_OBJMGR.BusComp Write Record.Activity Plan
     [Duration(MiliSecs): 0.006]
                   |        |  |
                   |        |  +- Area_DBC.Get Record from DB [Duration(MiliSecs): 0.006]
                   |        |  |
                    |       |  +- Area_DBC.Write Record to DB [Duration(MiliSecs): 72.376]
                    |       |
```

```
            |       +- Area_OBJMGR.Service Invoke Method.Task Assistant UI Service
[Duration(MiliSecs): 0.044]
             |
          +- Area_INFRA.Request Receipt (sessID SeqID) [Duration(MiliSecs): 21.650]
                |
               +- Area_OBJMGR.Service Invoke Method.Web Engine Interface
[Duration(MiliSecs): 19.900]
                |
                +- Area_OBJMGR.Service Invoke Method.Task Assistant UI Service
[Duration(MiliSecs): 0.046]
                |
                +- Area_OBJMGR.Service Invoke Method.Communications Client
[Duration(MiliSecs): 0.074]
                  |
                  +- Area_CSS.Communiations Client Invoke Method.ShellUIExit
[Duration(MiliSecs): 0.029]
```

HPOM Tools for Discovering and Analyzing Problematic Siebel Areas

SPI for Siebel provides tools that can be used to discover problematic areas in Siebel transactions. This analysis is divided into 2 steps:

1. To perform the Performance Aggregation Analysis, first run the tool **SIEBSPI-Run Performance Agg. Analysis**. A result of running a performance aggregation analysis of a Siebel ARM file is an extensible markup language (XML) output file. This file contains timing data for the instrumented areas.

   For this purpose, the **SIEBSPI-Run Performance Agg. Analysis** tool is provided in the **SPI for Siebel/SIEBSPI-SARM/SIEBSPI-SARM Performance Agg. Analysis** tool group.

   This will generate the `siebspi_sarm_paa.xml` file that will be placed in the .../`siebspi/tmp` directory. This file is then used for displaying problematic areas.

   For more information about SARM Performance Aggregation Analysis refer to "Siebel ARM (SARM) Reference Information" on page 168.

2. Execute analysis that discovers problematic areas in Siebel transaction.

   To actually display the problematic areas, you must run the tool for a specific metric in the **SPI for Siebel/SIEBSPI-SARM/SIEBSPI-SARM Performance Aggregation Analysis/SIEBSPI-Show Problematic Areas** tool group:

   - **SIEBSPI-Average Exclusive Memory**
   - **SIEBSPI-Average Execution Time**
   - **SIEBSPI-Average Inclusive Memory**
   - **SIEBSPI-Average Recursive Time**
   - **SIEBSPI-Average Response Time**
   - **SIEBSPI-Maximum Execution Time**
   - **SIEBSPI-Maximum Recursive Time**
   - **SIEBSPI-Percent of Response Execution Time**

- **SIEBSPI-Percent of Response Recursive Time**
- **SIEBSPI-Custom Metric**
- **SIEBSPI-Total Exclusive Memory**
- **SIEBSPI-Total Execution Time**
- **SIEBSPI-Total Inclusive Memory**
- **SIEBSPI-Total Recursive Time**
- **SIEBSPI-Total Response Time**

Tools analyze Siebel areas (for example, SWE) for specific metric maximum values (for example, Average Exclusive Memory). When the area is found, it also analyses the child areas to see which child area took the most time.

After that, the tool calculates in which child area the calls take the most time. When the call (method) is discovered, the tool displays a performance summary for that call. The tool also displays performance summary for a call that had the shortest execution time.

Example:

```
siebspi_sarm   -show_problematic_area
               -metric InclusiveMemory
               -submetric Average
               -detailed
```

Example output:

```
    ============================================================
    Analyzing areas for Average InclusiveMemory
    ============================================================

    Areas Average InclusiveMemory (ordered):

    Workflow                                WORKFLOW   94464.00  bytes
    Web Server Plugin                       SWSE       80677.00  bytes
    Request Broker                          SRB        4216.00  bytes
    Database Connector                      DBC        218.00  bytes

    Area where the maximum Average InclusiveMemory was measured: Workflow(WORKFLOW)


    MaxAllocated InclusiveMemory for WORKFLOW was measured here:

    Workflow(WORKFLOW).Invoke workflow method(WORKFLOW_ENGNE_INVOKE).BusSvcMgrInit

    This call performance data:

    SarmID                      7841
    Memory                      167586  bytes
    ResponseTime                1003.068
    PercentCPU                  4.67
    SarmID                      7841
    TypeLevel                   Sarm(1)
    RootID                      7841
    ParentSarmID                0
    ParentTimeID                0
    ParentProcID                0
    AreaCodeSymbol              WORKFLOW
```

```
AreaDescription              Workflow
SubAreaCodeSymbol            WORKFLOW_ENGNE_INVOKE
SubAreaDescription           Invoke workflow method
Count                        1
Duration                     1003.068  ms
PooledMemoryUsage            197454  bytes
PooledMemoryCalls            7532
SystemMemoryUsage            167586  bytes
SystemMemoryCalls            2152
AppInt1                      0
AppInt2                      0
AppString1                   BusSvcMgrInit
AppString2


Workflow(WORKFLOW) child areas Average Memory:

Database Connector                      DBC        2.00  bytes

Child area where the maximum Average Memory was measured: Database Connector(DBC)


Workflow(WORKFLOW) child areas Average Memory/Invocations :

Database Connector                      DBC        0.00  bytes

Child area where the maximum Average Memory/Invocations was measured: Database
Connector(DBC)
```

After the first stage, if you do not want the analysis to go automatically to the area with the maximum value (in example above this is WORKFLOW), you must use the `-force_area {SARM area}` parameter.

Example:

```
siebspi_sarm   -show_problematic_area
               -metric InclusiveMemory
               -submetric Average
               -detailed
               -do_not_refresh
               -force_area SWSE
```

It is important that you use SARM files from Siebel Web Extension and from Siebel Server(s). Usually those SARM files are located on several computers. In such case, copy all files to one single computer in a temporary directory. Alternatively, share (NFS, SAMBA…) remote directories where SARM files are located. To use SARM files from different locations, specify the directories (local or remote) using the `-include_sarm_dirs` parameter.

Example:

```
siebspi_sarm   -show_problematic_area
               -metric InclusiveMemory
               -submetric Average
               -detailed
               -include_sarm_dirs /net/node/sarm,/this/too
```

This example will use SARM files on a local computer in original Siebel log directories and the SARM files in the following directories: /net/node/sarm and /this/too. For example, /net/node/sarm is a NFS mounted directory and /this/too is a local temporary directory.

If you do not want to use the SARM files in original Siebel log directories on the computer where you execute the tool, specify the -exclude_original_sarm_dirs parameter.

Example:

```
siebspi_sarm  -show_problematic_area
              -metric InclusiveMemory
              -submetric Average
              -detailed
              -exclude_original_sarm_dirs
              -include_sarm_dirs /net/node/sarm,/this/too
```

In this case, only the SARM files in directories /net/node/sarm and /this/too will be used.

Example output:

```
    ============================================================
    Analyzing areas for Average InclusiveMemory
    ============================================================

    Areas Average InclusiveMemory (ordered):

    Workflow                                WORKFLOW   94464.00  bytes
    Web Server Plugin                       SWSE       80677.00  bytes
    Request Broker                          SRB        4216.00  bytes
    Database Connector                      DBC        218.00  bytes

    Area where the maximum Average InclusiveMemory was measured: Workflow(WORKFLOW)


    Further analysis was forced with this area: SWSE



    MaxAllocated InclusiveMemory for SWSE was measured here:

    Web Server Plugin(SWSE).Receive request(SWSE_REQUEST)

    This call performance data:

    SarmID                        610212
    Memory                        269962  bytes
    ResponseTime                  120001.270
    PercentCPU                    0.00
    SarmID                        610212
    TypeLevel                     Sarm(1)
    RootID                        610212
    ParentSarmID                  0
    ParentTimeID                  0
    ParentProcID                  0
    AreaCodeSymbol                SWSE
```

```
AreaDescription              Web Server Plugin
SubAreaCodeSymbol            SWSE_REQUEST
SubAreaDescription           Receive request
Count                        1
Duration                     120001.270  ms
PooledMemoryUsage            273226  bytes
PooledMemoryCalls            1242
SystemMemoryUsage            269962  bytes
SystemMemoryCalls            276
AppInt1                      0
AppInt2                      0
AppString1
AppString2



MaxDeallocated InclusiveMemory for SWSE was measured here:

Web Server Plugin(SWSE).Receive request(SWSE_REQUEST).!1.9fc.527d

This call performance data:

SarmID                       90636
Memory                       -3056999  bytes
ResponseTime                 237.767
PercentCPU                   0.07
SarmID                       90636
TypeLevel                    Sarm(1)
RootID                       90636
ParentSarmID                 0
ParentTimeID                 0
ParentProcID                 0
AreaCodeSymbol               SWSE
AreaDescription              Web Server Plugin
SubAreaCodeSymbol            SWSE_REQUEST
SubAreaDescription           Receive request
Count                        1
Duration                     237.767  ms
PooledMemoryUsage            -3052231  bytes
PooledMemoryCalls            1443
SystemMemoryUsage            -3056999  bytes
SystemMemoryCalls            366
AppInt1                      -1
AppInt2                      0
AppString1
AppString2                   !1.9fc.527d



Web Server Plugin(SWSE) child areas Average Memory:

Web Server Plugin                       SWSE       0.00  bytes

Child area where the maximum Average Memory was measured: Web Server Plugin(SWSE)


Web Server Plugin(SWSE) child areas Average Memory/Invocations :

Web Server Plugin                       SWSE       0.00  bytes

Child area where the maximum Average Memory/Invocations was measured: Web Server
Plugin(SWSE)
```

Similarly, you can use the following parameters to force the analysis for other stages:

```
-force_child_area {SARM child area from which
                   further analysis starts on
                   the second level}

-force_child_area_per_invocations {SARM child area
                from which further analysis starts
                for metric / invocations  on the
                second level}
```

Chapter 12

Monitoring Oracle Business Intelligence and Siebel Analytics

About Monitoring Business Intelligence

SPI for Siebel provides policies and tools for monitoring the status of the Oracle Business Intelligence and Siebel Analytics key components. Business Intelligence has become the most important tool for making the correct business decisions and therefore it is very important that all key parts are running and available.

NOTE

Throughout the manual, the Business Intelligence (BI) term is used for both, Oracle Business Intelligence and Siebel Analytics products.

Autodiscovery of the Business Intelligence Environment

SPI for Siebel offers autodiscovery of the installed Business Intelligence component on a node and creates or adds components to the service tree.

SPI for Siebel also monitors any configuration changes on a managed node with Business Intelligence installed.

To perform autodiscovery of the BI environment, install the following policy from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Server** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Server** policy group:

- `SIEBSPI_BI_AUTODISCOVERY`

Run the **SIEBSPI-BI Autodiscovery** tool from the **SPI for Siebel/SIEBSPI-Business Intelligence** tool group to generate or update the service tree.

Monitoring Business Intelligence Services

SPI for Siebel monitors the status of the following services and deamons:

Oracle Business Intelligence

- Oracle BI Cluster Controller
- Oracle BI Java Host
- Oracle BI Presentation Server
- Oracle BI Scheduler
- Oracle BI Server

Siebel Analytics

- Siebel Analytics Cluster
- Siebel Analytics Web
- Siebel Analytics Scheduler
- Siebel Analytics Server

When a service is not available, a critical message is sent to the HPOM console.

To monitor BI Presentation Server services, install the following policies from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Presentation Server** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Web Server** policy group:

- `SIEBSPI_BI_PRESENTATION_SERVER_SERVICE`
- `SIEBSPI_BI_JAVA_HOST_SERVICE` (Oracle BI only)

To monitor BI Server services, install the following policies from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Server** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Server** policy group:

- `SIEBSPI_BI_SERVER_SERVICE`
- `SIEBSPI_BI_CLUSTERCONTROLLER_SERVICE`

To monitor Scheduler services, install the following policy from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Scheduler** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Scheduler** policy group:

- `SIEBSPI_BI_SCHEDULER_SERVICE`

With SPI for Siebel tools, you can check the status, start, or stop the services. For a list and descriptions of BI Services tools, refer to the *SPI for Siebel Quick Reference Guide*.

Monitoring Business Intelligence Processes

SPI for Siebel monitors CPU and memory usage for the following BI processes:

Oracle Business Intelligence

On the Windows node:

- NQSserver.exe
- NQScheduler.exe
- Sawserver.exe
- NQSClusterController.exe

- Sawjavahostsvc.exe

On the Unix node:

- Sawjavahostsvc
- nqsserver
- nqscheduler
- sawserver
- nqsclusterontroller

Siebel Analytics

On the Windows node:

- NQSComGateway.exe
- NQScheduler.exe
- Sawserver.exe
- ClusterController.exe
- Sawjavahostsvc

To monitor CPU and memory usage for the BI Presentation Server processes, install the following policies from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Presentation Server** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Web Server** policy group:

- `SIEBSPI_BI_PRESENTATION_SERVER_MEM`
- `SIEBSPI_BI_PRESENTATION_SERVER_CPU`
- `SIEBSPI_BI_JAVA_HOST_MEM` (Oracle BI only)
- `SIEBSPI_BI_JAVA_HOST_CPU` (Oracle BI only)

To monitor CPU and memory usage for the BI Server processes, install the following policies from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Server** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Server** policy group:

- `SIEBSPI_BI_SERVER_MEM`
- `SIEBSPI_BI_SERVER_CPU`
- `SIEBSPI_BI_CLUSTERCONTROLLER_MEM`
- `SIEBSPI_BI_CLUSTERCONTROLLER_CPU`

To monitor CPU and memory usage for the BI Scheduler processes, install the following policies from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Scheduler** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Scheduler** policy group:

- `SIEBSPI_BI_SCHEDULER_MEM`

- SIEBSPI_BI_SCHEDULER_CPU

By default, the policies send results to the external policy SIEBSPI_BI_CPU_MEM_EXT. To get notifications about high memory or CPU usage for one of the processes, you must have this policy deployed.

Monitoring Business Intelligence Ports

SPI for Siebel monitors the performance and availability of the following default ports:

- 9703 port: for ODBC connections on the OBI & SA Servers (NQSServer)
- 9704 port: for OC4J (Oracle Containers for java) web access
- 9705 port: for Server Scheduler (NQScheduler)
- 9706 port: for Cluster Controller Clustering port
- 9710 port: for Presentation Server (OBI) Web (SA) - Sawserver
- 9810 port: for java host

To monitor the performance and availability of the BI Presentation Server ports, install the following policies from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Presentation Server** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Web Server** policy group:

- SIEBSPI_BI_PRESENTATION_SERVER_PORT
- SIEBSPI_BI_JAVA_HOST_PORT

To monitor the performance and availability of the BI Server ports, install the following policies from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Server** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Server** policy group:

- SIEBSPI_BI_SERVER_PORT
- SIEBSPI_BI_CLUSTERCONTROLLER_PORT
- SIEBSPI_BI_OC4J_PORT

To monitor the performance and availability of the BI Scheduler ports, install the following policy from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Scheduler** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Scheduler** policy group:

- SIEBSPI_BI_SCHEDULER_PORT

Monitoring Business Intelligence Cache

SPI for Siebel provides cache monitoring, so you can make Business Intelligence more efficient.

With SPI for Siebel, you can monitor the size of cache folders which can be on different locations. To do this, set thresholds in the percentage of use in the `SIEBSPI_BI_CACHE_SIZE` policy. By default, this policy sends results to the external policy `SIEBSPI_BI_CACHE_SIZE_EXT`. To get notifications, you must have this policy deployed.

You can also monitor the percentage of queries read from cache files with the `SIEBSPI_BI_CACHE_PERCENTAGE_QUERY` policy. By default, this policy sends results to the external policy `SIEBSPI_BI_CACHE_PERCENTAGE_QUERY_EXT`. To get notifications, you must have this policy deployed.

SPI for Siebel also provides the following tools that you can use to check the size of cache folders and the percentage of cache usage:

- **SIEBSPI-Cache Size**
- **SIEBSPI-Queries Read From Cache**

Monitoring Business Intelligence Usage Tracking

Business Intelligence servers support the accumulation of usage tracking statistics, which capture valuable information about users, performance, and so on, that can be used in a variety of ways, for example, database optimization, aggregation strategies, or billing users or departments based on the resources they consume.

SPI for Siebel monitors user usage by tracking accumulated usage statistics. You can monitor:

- the percentage of queries read from cache
- the number of rows returned to client
- the average query duration

To monitor usage tracking, install the following policies from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Server** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Server** policy group:

- `SIEBSPI_BI_AVG_DURATION_QUERY`
- `SIEBSPI_BI_CACHE_PERCENTAGE_QUERY`
- `SIEBSPI_BI_RETURNED_ROWS_QUERY`

By default, these policies send results to the external policies `SIEBSPI_BI_AVG_DURATION_QUERY_EXT`, `SIEBSPI_BI_CACHE_PERCENTAGE_QUERY_EXT`, and `SIEBSPI_BI_RETURNED_ROWS_QUERY_EXT`. To get notifications, you must have these policies deployed.

SPI for Siebel provides the following tools for monitoring usage tracking:

- **SIEBSPI-Average Query Duration**
- **SIEBSPI-Number Of Returned Rows**
- **SIEBSPI-Queries Read From Cache**

Monitoring Business Intelligence Scheduler Jobs

Business Intelligence Scheduler is an extensible application and server that manages and schedules jobs. Business Intelligence Scheduler supports two kinds of jobs:

- Scripted jobs
- Unscripted jobs, called iBots

SPI for Siebel monitors scheduled and managed jobs (workflow) and reports jobs with the status `FAILED`.

To monitor BI scheduled and managed jobs, install the following policy from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Scheduler** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Scheduler** policy group:

- `SIEBSPI_BI_FAILED_JOBS_QUERY`
- `SIEBSPI_BI_FAILED_SCHEDULER_QUERY`

By default, these policies send results to the external policies `SIEBSPI_BI_FAILED_JOBS_QUERY_EXT` and `SIEBSPI_BI_FAILED_SCHEDULER_QUERY_EXT`. To get notifications, you must have these policies deployed.

SPI for Siebel provides the following tools for monitoring scheduled and managed jobs, located in the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-BI Scheduler** tool group:

- **SIEBSPI-Failed Managed Jobs**
- **SIEBSPI-Failed Scheduled Jobs**

Monitoring Business Intelligence Database

SPI for Siebel provides basic monitoring for database in your Business Intelligence environment.

To monitor BI database, install the following policies from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Server** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Server** policy group:

- `SIEBSPI_BI_DB_CONNECTIVITY`
- `SIEBSPI_BI_DB_LOGIN_TIME`
- `SIEBSPI_BI_DB_TRANSACTION_TIME`

The monitor policy `SIEBSPI_BI_DB_CONNECTIVITY` checks database server availability and connectivity from the BI systems. To obtain the database login time, you can use the `SIEBSPI_BI_DB_LOGIN_TIME` policy.

To obtain the transaction time, the `SIEBSPI_BI_DB_TRANSACTION_TIME` policy runs a synthetic transaction, which is a set of predefined SQL statements.

SPI for Siebel provides the following tools for monitoring BI database, located in the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-BI Database** tool group:

- **SIEBSPI-Database Connectivity**
- **SIEBSPI-Database Login Time**
- **SIEBSPI-Database Transaction Time**

Monitoring Business Intelligence Delivery

SPI for Siebel monitors the ftp and mail delivery.

To monitor ftp and mail delivery, install the following policies from the **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Oracle BI/SIEBSPI-OBI Server** or **SPI for Siebel/SIEBSPI-Business Intelligence/SIEBSPI-Siebel Analytics/SIEBSPI-SA Server** policy group:

- `SIEBSPI_BI_FTP_AVAILABILITY`
- `SIEBSPI_BI_MAIL_AVAILABILITY`

Chapter 13

Monitoring Oracle Secure Enterprise Search

About Monitoring Oracle Secure Enterprise Search

SPI for Siebel provides basic monitoring of Oracle Secure Enterprise Search. Currently, only monitoring of Oracle Secure Enterprise Search on Windows is supported. Provided functionalities include monitoring of Oracle Secure Enterprise Search services and crawler log files.

Monitoring Oracle Secure Enterprise Search Services

SPI for Siebel monitors the status of the following services:

- Oracle Secure Enterprise Search Service
- Oracle Secure Enterprise Search OC4J Service
- Oracle Secure Enterprise Search TNS Listener Service

When a service is not available, a critical message is sent to the HPOM console.

To monitor Oracle Secure Enterprise Search service, install the **SIEBSPI_OSES _SERVICE** policy from the **SPI for Siebel/SIEBSPI-Oracle Secure Enterprise Search** policy group.

To monitor Oracle Secure Enterprise Search OC4J service, install the **SIEBSPI_OSES_OC4J _SERVICE** policy from the **SPI for Siebel/SIEBSPI-Oracle Secure Enterprise Search** policy group.

To monitor Oracle Secure Enterprise Search TNS Listener service, install the **SIEBSPI_OSES_TNS_LISTENER _SERVICE** policy from the **SPI for Siebel/ SIEBSPI-Oracle Secure Enterprise Search** policy group.

Monitoring Oracle Secure Enterprise Search Crawler Log Files

The log file records all crawler activity, warnings, and error messages for a particular schedule. It includes messages logged at startup, runtime, and shutdown. A new log file is created when crawler is restarted. SPI for Siebel monitors crawler log files and reports to HPOM console each time a line with one of the following severities is written to a log file:

- Warning (a message with a warning severity arrives to the HPOM console)
- Error (a message with an error severity arrives to the HPOM console)
- Fatal error (a message with a critical severity arrives to the HPOM console)

A message contains following information:

- Message text from a log file
- Crawler name
- Timestamp

To monitor Oracle Secure Enterprise Search crawler log files, install the following policies from the **SPI for Siebel/SIEBSPI-Oracle Secure Enterprise Search** policy group:

- `SIEBSPI_OSES_LOG_FILES`
- `SIEBSPI_OSES_LOG_FILES_EXT`

Chapter 14

Viewing and Analyzing Historical Data from Collected Performance Data

Analyzing Historical Data from Collected Performance Data Using HP Performance Manager

HP Performance Manager provides a central point from where you can monitor and manage the performance of all networked systems in your environment. Using Performance Manager you can analyze historical data from Performance Agent systems, receive alarms generated by Performance Agent, and predict future resource usage. HP Performance Manager also allows you to perform the following functions:

- Select a data source and list the graphs associated with it
- Choose a graph to view, select how the graph will display, and change the metrics graphed
- Draw graphs
- Drill down to view detail over a period of time
- Export and import systems and graph policies
- Design graphs and save them as policies
- Receive and view alarms
- Create forecasts

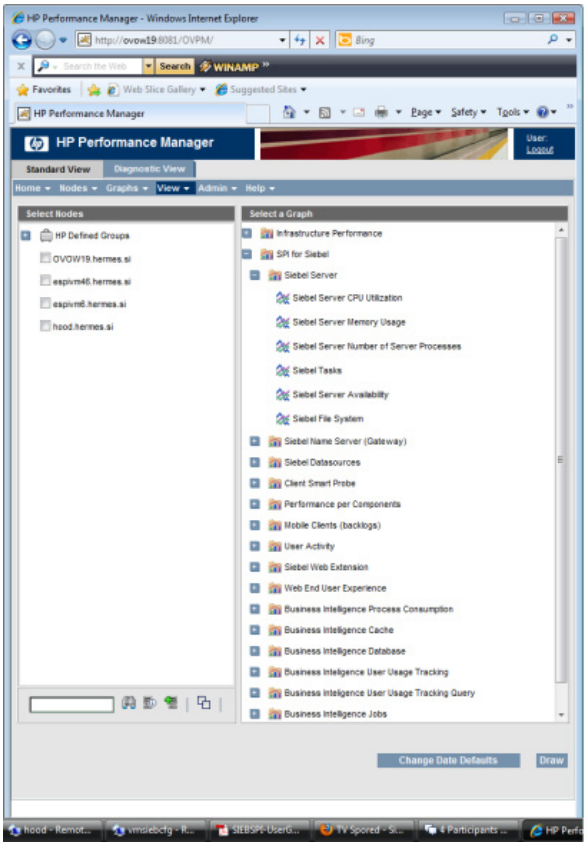
For additional information on HP Performance Manager, refer to the HP Performance Manager documentation.

HP Performance Manager User Defined Graph Templates

For easier work with Performance Manager, you can use the predefined graph templates of SPI for Siebel performance data. You can download the file with predefined Performance manger Graphs from the SPI for Siebel download web page.

Copy the `VPI_GraphsSPI_for_Siebel.txt` or `VPI_GraphsSPI for Siebel.txt` file (usually located in the `<OVInstallDir>/newconfig/OVPM` directory) into your Performance Manager's data directory to be fully integrated with them.

Note that available graphs are listed under the family **SPI for Siebel**.



The following tables list and describe graphs available for use and refer to both HP Performance Agent and CODA Agent usage.

Table 1. The SPI for Siebel family

Category	Graph Name	Description
Siebel Server		
	Siebel Server CPU Utilization	Displays Siebel server CPU utilization.
	Siebel Server Memory Usage	Displays Siebel server memory usage.
	Siebel Tasks	Displays the number of Siebel tasks, active tasks, completed tasks, and completed tasks with an error.
	Siebel Server Availability	Displays Siebel Server availability.

Category	Graph Name	Description
	Siebel File System	Includes information on Siebel file server disk usage (kb) and disk free space (%).
Siebel Name Server (Gateway)		
	Name Server CPU Utilization	Displays gateway CPU utilization.
	Name Server Memory Usage	Displays gateway memory usage.
Siebel Datasources		
	DS Login Time	Displays login time required by the DB client to connect to the database.
	DS Transaction Time	Displays transaction time.
	Workflow Policies Backlog	Displays workflow policies backlog.
	Transaction Processor Backlog	Displays transaction processor backlog.
	Database Sessions	Displays the number of database sessions.
Client Smart Probe		
	Client Smart Probe	Displays login time required by the client to connect to the server and transaction execute time from the client host.
	Login Time	Displays login time required by the client to connect to the server.
	Transaction Time	Displays transaction execute time from the client host.
Performance per Components		
	CPU Time	Displays component CPU time.
	Average SQL Times	Displays average SQL times per components.
	SQL Times	Displays SQL times per components.
	Memory Usage	Displays component memory usage.
	CPU Utilization	Displays component CPU utilization.
	Total Tasks	Displays the number of total tasks per components.
Mobile Clients (backlogs)		
	Clients not Synchronized	Displays the number of users needing to synchronize and number of remote clients on the Siebel enterprise.

Category	Graph Name	Description
	Files Transaction Router Backlogs	Displays transaction router backlogs.
	Synchronization Backlogs	Displays synchronization backlogs.
	Transaction Router Backlogs	Displays transaction router backlogs.
Siebel User Activity		
	All Active and Connected Users	Displays the number of active and connected users for Siebel Application (component).
	All Active Users	Displays the number of active users for Siebel Application (component).
	All Connected Users	Displays the number of connected users for Siebel Application (component).
Siebel Web Extension		
	Average Close Session Time	Displays the average close session time of Siebel Web Extension.
	Average Open Session Time	Displays the average open session time of Siebel Web Extension.
	Average Open Session Time per Application	Displays the average open time of the specific Siebel Web Extension Application.
	Average Request Time	Displays the average request time of Siebel Web Extension.
	Average Response Time	Displays the average response time of Siebel Web Extension.
Web End User Experience		
	Web End User Experience	Displays web end user login time, action time, and logoff time.
Business Intelligence Process Consumption		
	Business Intelligence Service Availability	Displays availability of Business Intelligence services, for example, BI Server, BI Presentation Server, BI Scheduler.
	Business Intelligence Process CPU Consumption	Displays CPU consumption for Business Intelligence processes.
	Business Intelligence Process Memory Consumption	Displays memory consumption for Business Intelligence processes.

Category	Graph Name	Description
Business Intelligence Cache		
	Business Intelligence Cache Size and Used Cache	Displays cache size and used cache for Business Intelligence.
	Cache Consumption	Displays cache consumption for Business Intelligence in percentage.
	Cache Performance (Inserts)	Displays cache performance (inserts) for Business Intelligence.
	Cache Performance (Hits)	Displays cache performance (hits) for Business Intelligence.
	Cache Performance (Hits and Inserted)	Displays cache performance (hits and inserted) for Business
Business Intelligence Database		
	Database Transaction Time	Displays Business Intelligence database transaction time.
	Database Login Time	Displays Business Intelligence database login time.
	Database Login Time vs. Transaction Time	Displays Business Intelligence database login time vs. transaction time.
Business Intelligence User Usage Tracking		
	Number of Users	Displays the number of users connected to Business Intelligence.
	Number of Queries	Displays the number of executed queries.
	Max Total Time vs. Average Total Time	Displays query maximal total time vs. query average total time of usage tracking.
	Sum Total Time	Displays the sum of total time.
	Total Time, Compile Time, Time in DB	Displays total time, compile time, and time in database.
	Number of Rows Returned by the Back-End Database	Displays the number of rows returned by the back-end database.
	Number of Rows Returned to the Client	Displays the number of rows returned to the client.
Business Intelligence User Usage Tracking Query		

Category	Graph Name	Description
	Longest Running Queries	Displays the longest running queries.
	Query Analysis	Displays query analysis.
Business Intelligence Jobs		
	Business Intelligence Jobs	Displays Business Intelligence jobs statistics.

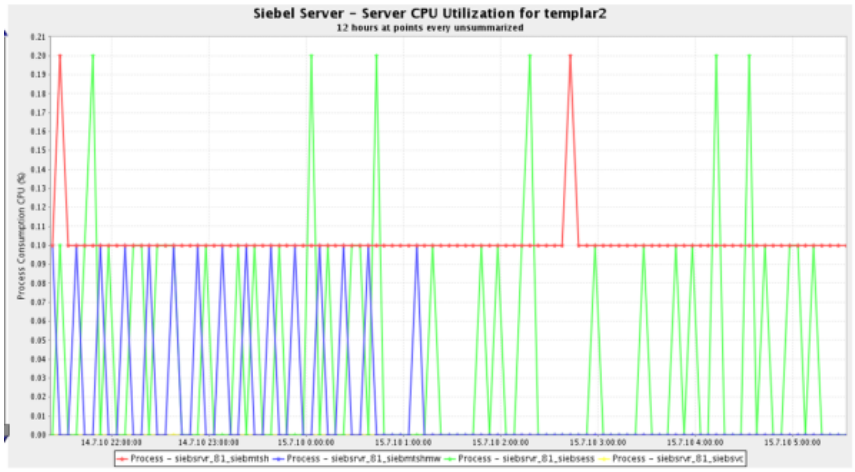
Sample Graph Output

Below are two sample graphs that can be produced. Both graphs relate to the Siebel Enterprise graph group.

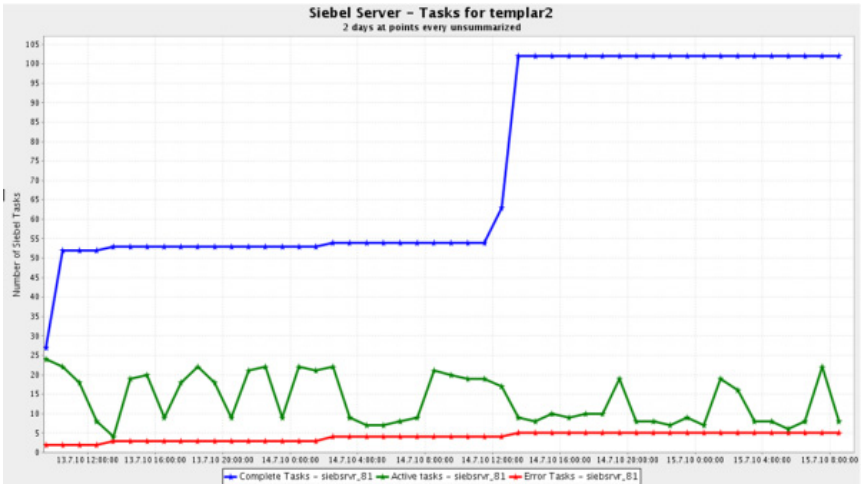
N O T E

All graphs display output in similar format to that shown in the sample graphs here.

The following graph reflects Siebel Application Server CPU utilization statistics.



The following graph displays Siebel Server tasks information.



SPI for Siebel Integration with HP Reporter

HP Reporter creates Web-based reports from data derived from the targeted systems that it "discovers". Discovery of a system can occur if the system is running the HP Performance Agent software (formerly known as OVPA or MWA agents) or CODA Agent (part of the HPOM Agent).

After Reporter has run through its discovery, it gathers data based on pre-defined and user-specified lists of metrics. This data is then used to generate reports. From the data it collects, Reporter automatically generates many different reports, providing critical information about the systems in your computing environment.

Deploying Policies and Collecting Performance Data

To produce reports, policies must be deployed. After the policies are successfully deployed, the CODA or MWA agent begins to collect performance data. For all Siebel systems where MWA or CODA agents are collecting data, HP Reporter can be used to generate reports.

How HP Reporter Creates Reports

HP Reporter follows the steps below when producing reports:

1. "Perform System Discovery" on page 113
2. "Gather Performance Data" on page 113

3. "Generate Reports" on page 114

Perform System Discovery

HP Reporter creates Web-based reports from data derived from the targeted systems that it "discovers". During a system discovery, Reporter looks for systems that are specified in the Discovery Area, and which have a CODA or HP Performance Agent agent installed on them. It then adds those systems to the Discovered Systems group.

Note that the following group is created automatically for SPI for Siebel purposes: `Siebel`

If you want to create this group manually, follow these steps:

1. In the left pane, right-click [Discovered Systems].
2. Select **Add Group**.
3. In the **Add Group** dialog box, type the new group name **Siebel**.
4. Click `[Add]`.

Gather Performance Data

After Reporter has run through its discovery, it gathers performance data from each discovered system and places it in a local database. Additionally, Reporter collects data only for those metrics that it knows about. These metrics are specified under **Metrics Lists**.

Metric lists control what information is gathered from a system into the Reporter's database. A metric list groups metrics from a single metric class supplied by the performance agent for UNIX or Windows. The metric list can also select the degree of summarization (points every 5 minutes, hour, day, and so on) and how much data to gather and retain in the database. The shorter the interval, the more records collected. The default summarization level is one hour. Metric lists are tightly connected to Data Source and Objects within that Data Source on each system.

The following metric lists are created for SPI for Siebel reports:

- `SIEBEL_COMP`
- `SIEBEL_APP`
- `SIEBEL_AMO`
- `SIEBEL_UL`
- `SIEBEL_UA`
- `SIEBEL_TR`
- `SIEBEL_BL`
- `SIEBEL_DS`
- `SIEBEL_SP`

- SIEBEL_GW
- SIEBEL_ENT_STATS
- SIEBEL_ENT_PROC
- SIEBEL_ENT_AVAIL
- SIEBEL_ENT_TASKS
- SIEBEL_ENT_FS
- SIEBEL_ENT_REMOTE
- SIEBEL_SWE1
- SIEBEL_SWE2
- SIEBEL_SWE_API
- BI_PROC_UTIL
- BI_CACHE
- BI_CACHE1
- BI_DBPERF_TRNS
- BI_DBPERF_LOGIN
- BI_JOBS
- BI_JOBS1
- BI_USAGE_QUERY

More information about metrics that are contained in this metric list is explained in the chapter "Collecting Performance and Other Metrics from Siebel Environment" on page 119.

Generate Reports

Reporter generates HTML reports based on the data available in the local Reporter database.

The following report family is created for SPI for Siebel purposes:

- Siebel

Reports are divided into the following categories:

Siebel Enterprise

- Gateway CPU utilization
  Shows the average CPU consumption of the Siebel gateway server processes during the reporting interval
- Gateway memory utilization
  Shows the amount of physical memory in use for Siebel gateway server processes during the reporting interval
- Siebel servers & file system usage

Shows the number and percent of running servers during the interval and the size of the Siebel file system

- Siebel Clients
  Shows the number of remote clients and the number of clients that must perform synchronization

Siebel Servers

- Siebel Server CPU utilization
  Shows the average CPU utilization of all Siebel server processes and the average CPU utilization of the siebmtsh and siebses processes separately
- Siebel Server Memory Usage
  Shows the average memory usage of all Siebel server processes and the average memory usage of the siebmtsh and siebses processes separately
- Siebel Server Tasks
  Shows the average number of tasks started for server components, average number of active tasks, completed tasks, and tasks completed with an error
- Siebel Server Messages
  Shows the average size and average number of reply (request) messages sent (received) by the servers during the interval
- Siebel Object Manager Sessions
  Shows the average connect and response time for Object Manager sessions, average number of requests per Object Manager session, and the average number of errors during the Object Manager session.
- Siebel Server SQL Operations
  Shows the average time and average number of SQL execute, fetch, and parse operations for Siebel servers during the interval.

Siebel Components

- Siebel Component CPU utilization
  Shows the average CPU utilization for the Siebel components during the reporting interval
- Siebel Component Memory Usage
  Shows the average memory usage for the Siebel components during the reporting interval
- Siebel Component SQL Operations
  Shows the average time and average number of SQL execute, fetch, and parse operations for the Siebel components during the interval

- Siebel Component Tasks
  Shows the number of total tasks for the Siebel components during the reporting interval

Siebel Clients

- Siebel Clients Response
  Shows the average response time for Siebel clients during the reporting interval
- Synchronization Backlogs
  Shows the number of files that need to be sent to the particular client
- Transaction Merger Backlogs
  Shows the number of files that need to be merged from the particular client
- Transaction Router Backlogs
  Shows the number of transactions that need to be routed to the particular client

Siebel Datasources

- Siebel DB Login Time
  Shows the average DB login time for Siebel servers during the reporting interval
- Siebel DB Transaction Time
  Shows the average DB transaction time during the reporting interval
- Siebel DB Table Size Growth
  Shows the average number of records in the Siebel database tables during the reporting interval

Siebel Users Activity

- Users connected to Siebel Applications (Object Manager Components) grouped by users
  Shows Siebel user activity in Siebel Applications. The first part of the report focuses on determining top/bottom 30 users by the time spent using Siebel Applications. The second part of the report shows in detail for each user when they logged in, logged out and for how long they were connected to a Siebel Application. Grouping is performed by Siebel Enterprises and Siebel Servers.
- Users connected to Siebel Applications (Object Manager Components) grouped by Siebel Applications
  Shows Siebel users activity in Siebel Applications. The first part of the report focuses on summary connection time for Siebel Applications and summary number of Siebel users' connections to Siebel Application. The second part of the report shows in detail for each Siebel Application when users logged in, logged out, and for how long they were connected to the Siebel Application. Grouping is

performed by Siebel Enterprise and Siebel Servers.

- Number of users connected to Siebel Applications (Object Manager Components)
  Shows the number of users connected to Siebel Applications (Object Manager Components) between two monitor intervals, and the number users active in monitoring moment. First part of the report focuses on determining the top/ bottom 30 Siebel Applications and Siebel Servers by the number of the Siebel user's connections. The second part of the report shows in detail how the number of connected users between the two intervals varied in time.
- Number of days since last update of account, opportunity or contact (Top 50 inactive Siebel users)
  Shows the date and time a Siebel user last added or changed an account, contact or opportunity, and the number of days since the last action, for the top 50 inactive Siebel users. Graph shows the top 20 inactive users.
- Number of days since last login of Siebel user (Top 50 inactive users)
  Shows how many days ago a Siebel user last logged in, and the last login time, for the top 50 inactive Siebel users. Graph shows the top 20 users.

Chapter 15

Collecting Performance and Other Metrics from Siebel Environment

About Collecting Performance and Other Metrics from the Siebel Environment

SPI for Siebel provides integration into both embedded (Embedded Performance Component of the HPOM Agent - CODA) and full-functioning (HP Performance Agent) performance management.

Integration with HP Performance Manager requires that HP Performance Agent or an Embedded Performance Component of the HPOM Agent is running on the managed node.

HP Performance Agent

HP Performance Agent (formerly OVPA or MWA) collects, summarizes, time stamps, and detects alarm conditions on current and historical resource data across a system. It also provides performance, resource, and end-to-end transaction response time measurements, and supports network and database measurement information.

Data collected outside of HP Performance Agent can be integrated using data source integration (DSI) capabilities. For example, network, database, and your data from SPI for Siebel, can be assimilated through DSI and used similarly as other data collected by HP Performance Agent. All DSI data is logged, time stamped, and can be setup for alarms. For additional information about Performance Agent, refer to the *HP Performance Agent: Data Source Integration Guide*.

All data collected or received by HP Performance Agent can be analyzed using spreadsheet programs, or HP or other third-party analysis products.

The data logged by HP Performance Agent allows you to perform the following tasks:

- Characterize environmental workloads
- Analyze resource usage for load balancing
- Perform trend analysis
- Perform service-level management based on transaction response time
- Perform capacity planning
- Respond to alarm conditions
- Solve system management problems before they arise

HP Performance Agent also gathers information on system activity and allows for customization. You can accept default configurations, or set parameters to collect data for specific conditions.

For additional information on HP Performance Agent, refer to the HP Performance Agent manuals.

Embedded Performance Component (CODA) of the HPOM Agent

Integration of SPI for Siebel performance data is also possible with the Embedded Performance Component of the HP Performance Agent of the HP Agent.

In this case, performance metrics are collected by the Embedded Performance Component, which is part of the HPOM agents. The performance component collects performance instance and counter and information from many sources, mainly operating systems. The collected values are stored in a proprietary persistent data store from which they are gathered and changed into presentation values. Programs including HP Reporter and HP Performance Manager for Windows can use these values.

NOTE

You cannot extract, export, view, or aggregate the data directly on a managed node.

The Embedded Performance Component is a powerful API and the data collection tool distributed with HP Operations Manager. The Embedded Performance Component collection is the preferred data collection mechanism and is always used when the Embedded Performance Component is installed on the managed node. For compatibility, some wrapper functions are used that provide the same interface as HP Performance Agent; however, the Embedded Performance Component is actually used.

In summary, the HP Operations Agent or Embedded Performance Agent is available with the HPOM agent. It provides the following:

- Lightweight system performance metric collection and storage via a Coda subagent
- Data can be visualized from HP Operations Manager, HP Performance Manager, and HP Reporter
- Its Black Box Communication (BBC) datacomm requires less ports through a firewall

Using SPI for Siebel with HP Performance Agent (MWA)

Data Source Integration (DSI) technology allows you to use HP Performance Agent to log data, define alarms, and access metrics from new data sources beyond the

metrics logged by the HP Performance Agent scopeux collector. Metrics can be acquired from data sources such as databases, LAN monitors, and end-user applications.

Make sure that you have selected the `MWA - HP Performance Agent` option for the performance agent when configuring the SPI for Siebel. Otherwise, use the **SIEBSPI-Configure-direct** tool for selecting it.

For collecting performance data, you can use all policies described in "Metrics Collected with the SPI for Siebel Policies" on page 122.

Using SPI for Siebel with Embedded Performance Agent (CODA)

IMPORTANT

Make sure that you have read the Software Requirements section in *SPI for Siebel Installation and Configuration Guide*. You will need the "SPI Data Collector" instrumentation deployed on your managed node before proceeding.You will need the "HP OpenView Smart Plug-ins DSI-to-DDF wrapper utilities" instrumentation deployed on your management server before proceeding.

Data Source Integration To Dynamic Data Feed (DSI2DDF) technology provides a command-line interface to the Embedded Performance Component (EPC) and passes the performance data to the EPC agent.

For this purpose, you can use the same policies in SPI for Siebel that you use for collecting performance data into HPPA, which is described in the next section *Metrics Collected with the SPI for Siebel Policies*. However, be sure that you have selected the **CODA - Embedded Performance Agent** option for the performance agent when configuring the SPI for Siebel. Via that configuration the policies collect data from the Siebel environment and store it in CODA.

Metrics Collected with the SPI for Siebel Policies

Policies Used for Collecting Performance Data

Policy name	Description	Metric Group
SIEBSPI_SERVER_AVAILABILITY_PERFORMANCE	Collects the performance data for the Siebel Servers Availability	SIEBEL_ENT_AVAIL
SIEBSPI_SERVER_FS_PERFORMANCE	Collects the performance data of the Siebel server filesystem	SIEBEL_EMT_FS

Policy name	Description	Metric Group
SIEBSPI_SERVER_PROCESS_PERFORMANCE	Collects the performance data of the Siebel server processes	SIEBEL_ENT_PROC
SIEBSPI_SERVER_REMOTE_PERFORMANCE	Collects the performance data of the Siebel remote clients	SIEBEL_ENT_REMOTE
SIEBSPI_SERVER_STATS_PERFORMANCE	Collects the performance data of the Siebel server statistics	SIEBEL_ENT_STATS
SIEBSPI_SERVER_TASKS_PERFORMANCE	Collects the performance data of the Siebel server tasks	SIEBEL_ENT_TASKS
SIEBSPI_GATEWAY_PERFORMANCE	Collects the performance data for the Siebel Gateways	SIEBEL_GW
SIEBSPI_SP_PERFORMANCE	Collects Smart Probe performance data	SIEBEL_SP
SIEBSPI_DB_TRANS_PERFORMANCE	Collects database transaction performance data	SIEBEL_TR
SIEBSPI_DB_SESSION_PERFORMANCE	Collects database sessions performance data	SIEBEL_BL
SIEBSPI_DB_LOGIN_PERFORMANCE	Collects database login performance data	SIEBEL_DS
SIEBSPI_*_COMPONENT with "-perf" option	Collects Siebel Components performance data	SIEBEL_COMP
SIEBSPI_*_COMPONENT with “-usercount” option	Collects data about number of Siebel users active on Siebel Components	SIEBEL_APP
SIEBSPI_*_COMPONENT with "-usertime" option	Collects data about Siebel users activity (login) on Siebel Components	SIEBEL_AMO
SIEBSPI_SYNCH_BACKLOG_PERF SIEBSPI_TRANS_MERGER_BACKLOG_PERF SIEBSPI_TRANS_PROCESSOR_BACKLOG_PERF SIEBSPI_TRANS_ROUTER_BACKLOG_PERF SIEBSPI_WORKFLOW_BACKLOG_PERF	Collects database tables backlog data	SIEBEL_BL
SIEBSPI_USER_LOGIN_PERFORMANCE	Collects data about Siebel users last login time	SIEBEL_UL
SIEBSPI_USER_ACTION_PERFORMANCE	Collects data about Siebel users last update of account, opportunity or contact	SIEBEL_UA
SIEBSPI_SWSE_SYSTEM_STATISTIC_PERF	Collects SWSE System statistics performance data	SIEBEL_SWE1
SIEBSPI_SWSE_APPLICATION_STATISTIC_PERF	Collects SWSE Application statistics performance data	SIEBEL_SWE2

Policy name	Description	Metric Group
SIEBSPI_SWSE_LIST_*_PERF	Collects the performance data for Siebel Web Server extension action (List - Accounts, Contacts, or Opportunities)	SIEBEL_SWE_API
SIEBSPI_BI_PROCESS_PERF	Collects the performance data for BI processes.	BI_PROC_UTIL
SIEBSPI_BI_CACHE_PERF	Collects the cache performance data.	BI_CACHE
SIEBSPI_BI_CACHE_TRACKING_PERF	Collects the usage tracking cache performance data.	BI_CACHE1
SIEBSPI_BI_DB_LOGIN_PERF	Collects the database login time performance data.	BI_DBPERF_LOGIN
SIEBSPI_BI_DB_TRANSACTION_PERF	Collects the database transaction time performance data.	BI_DBPERF_TRNS
SIEBSPI_BI_JOBS_PERF	Collects the scheduled jobs performance data.	BI_JOBS, BI_JOBS1
SIEBSPI_BI_USAGE_TRACKING_GENERAL_PERF	Collects the usage tracking performance data for all queries.	BI_USAGE_QUERY
SIEBSPI_BI_USAGE_TRACKING_PERF	Collects the usage tracking performance data.	BI_USAGE_QUERY

Metrics Collected with SIEBSPI_SERVER_STATS_PERFORMANCE

Metric group SIEBEL_ENT_STATS

Metric Name	Metric Label	Description
ST_SRVR_NAME	Server Name	Siebel Server Name
ST_ENT_NAME	Enterprise Name	Siebel Enterprise Name
ST_AVG_CONN_TIME	Avg. Connect Time	Average connect time for Object Manager sessions
ST_AVG_CPU_TIME	Avg. CPU Time	Total CPU time for component tasks (in seconds)
ST_AVG_R_TIME	Avg. Response Time	Average Object Manager response time
ST_AVG_REP_SIZE	Avg. Reply Size	Average size of reply messages (in bytes)
ST_AVG_REQ_P_S	Avg. Req. Per S	Average number of requests per Object Manager session

Metric Name	Metric Label	Description
ST_AVG_REQ_SIZE	Avg. Request Size	Average size of request messages (in bytes)
ST_AVG_SQL_EXE_T	Avg. SQL Execute Time	Average time for SQL execute operations (in seconds)
ST_AVG_SQL_F_T	Avg. SQL Fetch Time	Average time for SQL fetch operations (in seconds)
ST_AVG_SQL_P_T	Avg. SQL Parse Time	Average time for SQL parse operations (in seconds)
ST_AVG_THINK_TIME	Avg. Think Time	Average end-user think time between requests
ST_ELAPSED_TIME	Elapsed Time	Total elapsed (running) time for component tasks (in seconds)
ST_NUM_DBCON_RET	Num of DBConn Retr.	Number of re-tries due to DB connection loss
ST_NUM_DLRBK_RET	Num of DLRbk Re.	Number of re-tries due to deadlock rollbacks
ST_NUM_EXHAS_RET	Num of Exhausted Re.	Number of times all re-tries are exhausted
ST_NUM_OF_SLEEPS	Num of Sleeps	Total amount of sleep time for component tasks (in seconds)
ST_NUM_SQL_EXECS	Num of SQL Exec.	Total number of SQL execute operations
ST_NUM_SQL_FETCHES	Num of SQL Fetch.	Total elapsed time for SQL fetch operations (in seconds)
ST_NUM_SQL_PARSES	Num of SQL Parses	Total elapsed time for SQL parse operations (in seconds)
ST_OBJ_MANAGER_ERR	Object Manager Err.	Number of errors encountered during Object Manager session
ST_REPLY_MESSAGES	Reply Messages	Number of reply messages sent by the server
ST_REQ_MESSAGES	Request Messages	Number of request messages received by the server
ST_SIEB_FS_FREE	Sieb FS free (%)	Siebel file server disk free space (%)
ST_SIEB_FS_SIZE	Sieb FS size (kb)	Siebel file server disk usage (kb)
ST_SLEEP_TIME	Sleep Time	Total amount of sleep time for component tasks (in seconds)

Metric Name	Metric Label	Description
ST_SQL_EXEC_TIME	SQL Execute Time	Total elapsed time for SQL execute operations (in seconds)
ST_SQL_FETCH_TIME	SQL Fetch Time	Total elapsed time for SQL fetch operations (in seconds)
ST_SQL_PARSE_TIME	SQL Parse Time	Total elapsed time for SQL parse operations (in seconds)
ST_TOT_REPLY_SIZE	Total Reply Size	Total size (in bytes) of reply messages
ST_TOT_REQ_SIZE	Total Request Size	Total size (in bytes) of request messages
ST_TOT_RESP_TIME	Total Response Time	Total Object Manager response time (in seconds)
ST_TOT_TASKS	Total Tasks	Total number of tasks started for server components
ST_TOT_THINK_TIME	Total Think Time	Total end-user think time (in seconds)

Metrics Collected with SIEBSPI_SERVER_AVAILABILITY _PERFORMANCE

Metric group SIEBEL_ENT_AVAIL

Metric Name	Metric Label	Description
ENTA_SRVR_NAME	Server Name	Siebel Server name
ENTA_ENT_NAME	Enterprise Name	Siebel Enterprise name
ENTA_SRV_AVAIL	Server Av.(%)	Percent of running servers (%)
ENTA_NUM_SRV	Num of Servers	Number of Siebel servers in the Siebel Enterprise

Metrics Collected with SIEBSPI_SERVER_FS _PERFORMANCE

Metric group SIEBEL_ENT_FS

Metric Name	Metric Label	Description
ENTF_SRV_PATH	Srv & FS Path	Siebel Server and file system SPI ID
ENTF_SRVR_NAME	Server Name	Siebel Server name
ENTF_NAME	Enterprise Name	Siebel Enterprise name
ENTF_FS_PATH	FS Path	Siebel file system path

ENTF_FS_FREE	Sieb FS free (%)	Siebel file server disk free space (%)
ENTF_FS_SIZE	Sieb FS size (kb)	Siebel file server disk usage (kb)

Metrics Collected with SIEBSPI_SERVER_PROCESS_PERFORMANCE

Metric group SIEBEL_ENT_PROC

Metric Name	Metric Label	Description
ENTP_SRV_PROC	Srv & Proc. Name	Siebel Server and process SPI ID
ENTP_SRVR_NAME	Server Name	Siebel Server name
ENTP_NAME	Enterprise Name	Siebel Enterprise name
ENTP_PROC_NAME	Process Name	Siebel process name
ENTP_PROC_CNT	Num. Oof Proc.	Number of running processes on Siebel server
ENTP_CPU_UTIL	Proc CPU Util.(%)	Siebel process CPU utilization (%)
ENTP_MEM_USG	Proc Mem Usage(kb)	Siebel process memory Usage (kb)

Metrics Collected with SIEBSPI_SERVER_PROCESS_PERFORMANCE

Metric group SIEBEL_ENT_PROC

Metric Name	Metric Label	Description
ENTP_SRV_PROC	Srv & Proc. Name	Siebel Server and process SPI ID
ENTP_SRVR_NAME	Server Name	Siebel Server name
ENTP_NAME	Enterprise Name	Siebel Enterprise name
ENTP_PROC_NAME	Process Name	Siebel process name
ENTP_PROC_CNT	Num. Oof Proc.	Number of running processes on Siebel server
ENTP_CPU_UTIL	Proc CPU Util.(%)	Siebel process CPU utilization (%)
ENTP_MEM_USG	Proc Mem Usage(kb)	Siebel process memory Usage (kb)

Metrics Collected with SIEBSPI_SERVER_TASKS_PERFORMANCE

Metric group SIEBEL_ENT_TASKS

Metric Name	Metric Label	Description
ENTT_SRVR_NAME	Server Name	Siebel Server name
ENTT_NAME	Enterprise Name	Siebel Enterprise name
T_NUM_OF_TASKS	Num of Tasks	Number of Siebel tasks on a Siebel
T_NUM_ACTIVE_TASKS	Num of Act. Tasks	Number of active tasks on a Siebel server
T_NUM_CMPLET_TASKS	Num of Completed T.	Number of completed tasks on a Siebel server
T_NUM_EXIT_ERR_T	Num Exit Error T.	Number of completed tasks with an error on a Siebel server

Metrics Collected with SIEBSPI_SERVER_REMOTE_PERFORMANCE

Metric group SIEBEL_ENT_REMOTE

Metric Name	Metric Label	Description
ENTR_SRVR_NAME	Server Name	Siebel Server name
ENTR_NAME	Enterprise Name	Siebel Enterprise name
R_NUM_REM_CLIENTS	Num of Remote Cli.	Number of remote clients on a Siebel enterprise
R_NUM_USR_NEED_SYNC	Clients Need Sync.	Number of users needing to synchronize

Metrics Collected with SIEBSPI_GATEWAY_PERFORMANCE

Metric group SIEBEL_GW

Metric Name	Metric Label	Description
GW_ENT_NAME	Enterprise Name	Siebel Enterprise Name
GW_NAME	Gateway Server Name	Siebel Gateway Server Name
GW_SERVER_CPU	Gateway Server CPU%	Siebel Gateway name server CPU utilization (%)
GW_SERVER_MEM	Gateway Srv. MEM (kb)	Siebel Gateway name server memory Usage (kb)

Metrics Collected with SIEBSPI_SP_PERFORMANCE

Metric group SIEBEL_SP

Metric Name	Metric Label	Description
SP_INSTANCE	Instance ID	Siebel mobile client SPI ID
SP_ENT_NAME	Enterprise Name	Enterprise Name
SP_CL_HOST_NAME	Client Host Name	Mobile client host name
SP_CL_DB_LOGIN_T	Client Login Time(ms)	Login time required by the client to connect to the database
SP_CL_DB_SQL_EXEC_T	Client SQL Time(ms)	Transaction execute time from the client host
SP_TRANS_STRING	Transaction String	The name of Siebel's business component, business object and filed name

Metrics Collected with SIEBSPI_DB_LOGIN_PERFORMANCE

Metric group SIEBEL_DS

Metric Name	Metric Label	Description
DS_ENT_NAME	Enterprise Name	Enterprise Name
DS_HOST_NAME	Host Name	DB client host name
DS_DB_LOGIN_T	DB Login Time(ms)	Login time required by the DB client to connect to the database

Metrics Collected with SIEBSPI_DB_TRANS_ACTION_PERFORMANCE

Metric group SIEBEL_TR

Metric Name	Metric Label	Description
TR_ENT_NAME	Enterprise Name	Enterprise name
TR_HOST_NAME	Host Name	Mobile client host name
TR_DB_SQL_NAME	DB SQL Name	Name of SQL
TR_DB_SQL_EXEC_T	Client SQL Time(ms)	SQL execute time

Metrics Collected with SIEBSPI_*_BACKLOG_PERF

Metric group SIEBEL_BL

Metric Name	Metric Label	Description
BL_INSTANCE	Instance ID	Siebel mobile client SPI ID
BL_ENT_NAME	Enterprise Name	Enterprise Name
BL_HOST_NAME	Host Name	Mobile client host name
BL_DB_BACKLOG_NAME	Backlog Name	Name of backlog
BL_DB_BACKLOG_VALUE	Backlog Value	Backlog value
BL_DB_BACKLOG_STRING	Backlog String	Additional backlog string value

Metrics Collected with SIEBSPI_*_COMPONENT with the "-perf" Parameter Specified

Metric group SIEBEL_COMP

Metric Name	Metric Label	Description
CS_AVG_SQL_EXE_T	Avg. SQL Execute Time	Average time for SQL execute operations (in seconds)
CS_AVG_SQL_F_T	Avg. SQL Fetch Time	Average time for SQL fetch operations (in seconds)
CS_AVG_SQL_P_T	Avg. SQL Parse Time	Average time for SQL parse operations (in seconds)
CS_COM_NAME	Component Name	Siebel Component Name
CS_CPU_UTIL	Component CPU Util.	Siebel Component CPU utilization (CPU%)
CS_CPU_TIME	Component CPU Time	Siebel Component CPU Time
CS_ELAPSED_TIME	Elapsed Time	Total elapsed (running) time for component tasks (in seconds)
CS_ENT_NAME	Enterprise Name	Siebel Enterprise Name
CS_NUM_OF_SLEEPS	Num of Sleeps	Total amount of sleep time for component tasks (in seconds)
CS_NUM_SQL_EXECS	Num of SQL Exec.	Total number of SQL execute operations

CS_NUM_SQL_FETCHES	Num of SQL Fetch.	Total elapsed time for SQL fetch operations (in seconds)
CS_NUM_SQL_PARSES	Num of SQL Parses	Total elapsed time for SQL parse operations (in seconds)
CS_MEM_USAGE	Srv. Mem Usage	Siebel component memory usage (kb)
CS_SLEEP_TIME	Sleep Time	Total amount of sleep time for component tasks (in seconds)
CS_SQL_EXEC_TIME	SQL Execute Time	Total elapsed time for SQL execute operations (in seconds)
CS_SQL_FETCH_TIME	SQL Fetch Time	Total elapsed time for SQL fetch operations (in seconds)
CS_SQL_PARSE_TIME	SQL Parse Time	Total elapsed time for SQL parse operations (in seconds)
CS_SRVR_NAME	Server Name	Siebel server name
CS_TOT_TASKS	Total Tasks	Total number of tasks for Siebel component

Metrics Collected with SIEBSPI_*_COMPONENT with the "-usercount" Parameter Specified

Metric group SIEBEL_APP

Metric Name	Metric Label	Description
APP_ENT_NAME	Enterprise Name	Enterprise Name
APP_SRVR_NAME	Server Name	Siebel Server name
APP_APPLICATION	Siebel Appl Name	Siebel Application (Component) name
APP_ACT_USER_COUNT	Active users counter	Count of all Siebel users logged to Siebel Application in monitoring moment
APP_ALL_USER_COUNT	Users counter	Count of all Siebel users logged to Siebel Application between two monitoring intervals

Metrics Collected with SIEBSPI_*_COMPONENT with the "-usertime" Parameter Specified

Metric group SIEBEL_AMO

Metric Name	Metric Label	Description
AMO_ENT_NAME	Enterprise Name	Enterprise Name
AMO_SRVR_NAME	Server Name	Siebel Server name
AMO_APPLICATION	Siebel Appl Name	Siebel Application (Component) name
AMO_USER	Siebel User Name	Siebel user name
AMO_STARTTIME	Login time	Time when Siebel user log into Siebel Application
AMO_STOPTIME	Logout time	Time when Siebel user log out from Application

Metrics Collected with SIEBSPI_USER_LOGIN_PERFORMANCE

Metric group SIEBEL_UL

Metric Name	Metric Label	Description
UL_ENT_NAME	Enterprise Name	Enterprise Name
UL_USER	Siebel User Name	Siebel user name
UL_LAST_LOGIN	Last login time	Siebel user last login time

Metrics Collected with SIEBSPI_USER_ACTION_PERFORMANCE

Metric group SIEBEL_UA

Metric Name	Metric Label	Description
UA_ENT_NAME	Enterprise Name	Enterprise Name
UA_USER	Siebel User Name	Siebel user name
UA_LAST_ACCOUNT	Last account change	Time when Siebel user last time changed account
UA_LAST_OPPORTUNITY	Last opportunity change	Time when Siebel user last time changed opportunity
UA_LAST_CONTACT	Last contact change	Time when Siebel user last time changed contact

Metrics Collected with SIEBSPI_SWSE_SYSTEM_STATISTIC_PERF

Metric group SIEBEL_SWE1

Metric Name	Metric Label	Description
SWE1_ENT_NAME	Enterprise Name	Enterprise Name
SWE1_AR_TIME	Avg Response Time	Average response time
SWE1_AC_SESS_TIME	Avg Close Sess Time	Average close session time
SWE1_AO_SESS_TIME	Avg Open Sess Time	Average open session time
SWE1_ARQ_TIME	Avg Request Time	Average request time

Metrics Collected with SIEBSPI_SWSE_APPLICATION_STATISTIC_PERF

Metric group SIEBEL_SWE2

Metric Name	Metric Label	Description
SWE2_ENT_NAME	Enterprise Name	Enterprise Name
SWE2_APPLICATION	Siebel Appl Name	Siebel Application name
SWE2_AO_SESS_TIME	Avg Open Sess Time	Average open session time

Metrics Collected with SIEBSPI_SWSE_LIST_* _PERF

Metric group SIEBEL_API

Metric Name	Metric Label	Description
SWE_HOST_WSRV_ACT	Host&Web&Action Key	Siebel Spi ID (host, websrv,action)
SWE_ACTION	SWE action command	SWSE action commadn (list accounts,contacts, opportunities)
SWE_WSRV_NAME	Web Srv. Name	Siebel Web Server name
SWE_HOST_NAME	Host Name	Host Name
SWE_APPLICATION	SWE Application	Siebel web Server Application Name
SWE_TIME	SWE Action Time	Total time for Siebel Web Client action (ms)
SWE_USER_NAME	SWE User Name	Siebel Client User Name

Metrics Collected with SIEBSPI_BI_PROCESS_PERF

Metric group BI_PROC_UTIL

Metric Name	Metric Label	Description
PROC_NAME	Process Name	Business Intelligence process name
PROC_NODE_NAME	BI Node Name	Business Intelligence node name
PROC_CPU	CPU (%)	Business Intelligence process CPU utilization (%)
PROC_MEM	MEM (kb)	Business Intelligence process memory usage (kb)
PROC_AVAIL	Process Availability	Business Intelligence process availability

Metrics Collected with SIEBSPI_BI_CACHE_PERF

Metric group BI_CACHE

Metric Name	Metric Label	Description
CACHE_PATH	Cache Path	Business Intelligence cache path
CACHE_NODE_NAME	BI Node Name	Business Intelligence Node name
CACHE_SIZE	Cache Size (kb)	Business Intelligence Cache size (kb)
CACHE_USED_PERC	Cache Used (%)	Business Intelligence Cache consumption (%)
CACHE_USED_KB	Cache Used (kb)	Business Intelligence Cache used (kb)

Metrics Collected with SIEBSPI_BI_CACHE_TRACKING_PERF

Metric group BI_CACHE1

Metric Name	Metric Label	Description
CACHE1_NODE_NAME	BI Node Name	Business Intelligence node name
CACHE_COUNT_ALL	Count all queries	Count of all queries
CACHE_COUNT_INSERT	Num of Inserts	Number of all inserted queries
CACHE_COUNT_HITS	Num of Hits	Number of all hits

CACHE_INSERTED	Cache Inserted(%)	Percentage of queries inserted into cache
CACHE_HITS	Cache Hits(%)	Percentage of query hits (read from cache)

Metrics Collected with SIEBSPI_BI_LOGIN_PERF

Metric group BI_DBPERF_LOGIN

Metric Name	Metric Label	Description
LOGIN_NODE_NAME	BI Node Name	Business Intelligence node name
LOGIN_TIME	DB Login Time (ms)	Login time required by the DB client to connect to the database

Metrics Collected with SIEBSPI_BI_TRANSACTION_PERF

Metric group BI_DBPERF_TRNS

Metric Name	Metric Label	Description
TRNS_NAME	Transaction Name	Name of the executed SQL transaction
TRNS_NODE_NAME	BI Node Name	Business Intelligence node name
TRNS_TIME	DB Trans Time (ms)	SQL execute time

Metrics Collected with SIEBSPI_BI_CACHE_TRACKING_PERF

Metric group BI_CACHE1

Metric Name	Metric Label	Description
CACHE1_NODE_NAME	BI Node Name	Business Intelligence Node name
CACHE_COUNT_ALL	Count All Queries	Count of all queries
CACHE_COUNT_INSERT	Num of Inserts	Number of all inserted queries
CACHE_COUNT_HITS	Num of Hits	Number of all hits
CACHE_INSERTED	Cache Inserted(%)	Percentage of queries inserted into cache
CACHE_HITS	Cache Hits(%)	Percentage of query hits (read from cache)

Metrics Collected with SIEBSPI_BI_JOBS_PERF

Metric group BI_JOBS

Metric Name	Metric Label	Description
JOBS_NAME_AND_ID	Job Name and ID	Job Name Siebel SPI ID
JOBS_NODE_NAME	BI Node Name	Business Intelligence node name
JOBS_JOB_NAME	Job Name	Business Intelligence Scheduler job name
JOBS_JOB_ID	Job ID	Business Intelligence Job ID
JOBS_JOB_STATUS	Job Status	Current status of a job
JOBS_LAST_RUN_TIME	Job Last Runtime	The last time the job was executed
JOBS_NEXT_RUN_TIME	Job Next Runtime	The next time of job execution
JOBS_SCRIPT_TYP	Job Script Type	Job Script type
JOBS_TIMEZONE	Job Timezone	Job time zone
JOBS_USER_ID	Job User Name	Job user name
JOBS_ERR_TEXT	Job Error Text	Job error text

Metric group BI_JOBS1

Metric Name	Metric Label	Description
JOBS1_NODE_NAME	BI Node Name	Business Intelligence node name
JOBS1_TOTAL	Total Num. of Jobs	Total number of jobs
JOBS1_FAILED	Num. of Failed Jobs	Number of failed jobs

Metrics Collected with SIEBSPI_BI_USAGE_TRACKING_GENERAL_PERF
Metrics Collected with SIEBSPI_BI_USAGE_TRACKING_PERF

Metric group BI_USAGE_QUERY

Metric Name	Metric Label	Description
QUERY_QUERY_NAME	Query	The SQL submitted for the query
QUERY_NODE_NAME	BI Node Name	Business Intelligence node name
QUERY_QUERY_ID	Query Hash ID	Unique query hash ID
QUERY_QUERY_COUNT	Query Count	Total query count

QUERY_USERS_COUNT	Users Count	Total Users Count
QUERY_MAX_TOT_TIME	Max Tot. Time (s)	Max total time (sec)
QUERY_AVG_TOT_TIME	Avg Tot. Time (s)	Average total time (sec)
QUERY_SUM_TOT_TIME	Sum Tot. Time (s)	Sum total time (sec)
QUERY_MAX_ROW_COUNT	Max Row Count	Max number of row count returned to the client
QUERY_AVG_ROW_COUNT	Avg Row Count	Average number of row count returnrd to the client
QUERY_MAX_NUM_DB_ROW	Max Num DB Row	Max number of row count returned by the database
QUERY_AVG_NUM_DB_ROW	Avg Num DB Row	Average number of row count returned by the database
QUERY_MAX_COMP_TIME	Max Comp. Time(s)	Max query compile time (sec)
QUERY_AVG_COMP_TIME	Avg Comp. Time(s)	Average query compile time (sec)
QUERY_MAX_DB_TIME	Max Time in DB(s)	Max query time spent in the DB (sec)
QUERY_AVG_DB_TIME	Avg Time in DB(s)	Average query time spent in the DB (sec)
QUERY_SUM_DB_TIME	Sum Time in DB(s)	Total query time spent in the DB (sec)
QUERY_SUM_DB_QUERY	Total Num Query	Total number of queries
QUERY_AVG_DB_QUERY	Avg Num Query	Average number of queries
QUERY_SUM_CACHE_INS	Tot. Cache Ins.	Total cache inserts
QUERY_SUM_CACHE_HITS	Tot. Cache Hits	Total cache hits

Chapter 16

Customizing SPI for Siebel

Message Correlation and State-based Browser

Message correlation helps to prevent your message browser from becoming cluttered with messages that describe the same problem. SPI for Siebel generates messages with pre-configured "Message Keys" and "Acknowledging Messages with Message Keys" properties. These make implementation of the concept for threshold as easy as possible.

NOTE

This feature is implemented in the most important policies.

About State-based Browsers

When you acknowledge messages automatically, a maximum of one message per managed object exists in the browser. This message reflects the current status of the object. Thus, the message browser has become a state-based browser. SPI for Siebel has many *Message Key* and *Acknowledge messages* with message key properties within policies. For additional information, refer to one of the policies in the list below. (Note that this list is just a representative sample of all available message keys.)

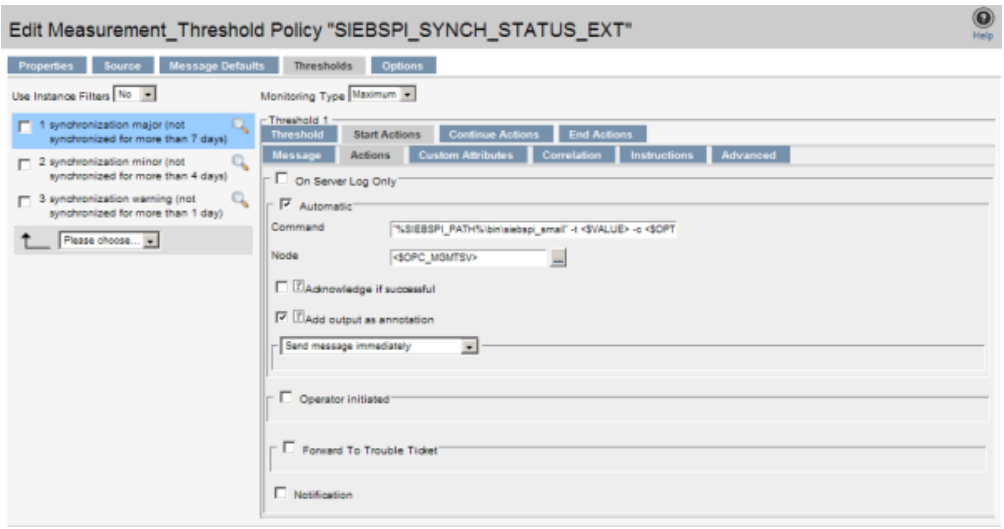
- `SIEBSPI_SERVER_AVAILABILITY_EXT`
- `SIEBSPI_SERVER_PROCESS_EXT`
- `SIEBSPI_SIEBEL_FS`
- `SIEBSPI_NUM_TASKS_TOO_HIGH_EXT`
- `SIEBSPI_COMP_STATUS_EXT`
- `SIEBSPI_CHECK_TASKS_EXT`
- `SIEBSPI_GATEWAY_PROCESS`
-

Changing E-mail for Synchronization Status Reporting

By default, an e-mail notification with information that a remote user has not synchronized for the specified amount of time is sent only to that user. If you want that e-mail to be sent also to a fixed e-mail address (for example, a Siebel administrator) or only to a fixed e-mail address, modify the `SIEBSPI_SYNCH_STATUS_EXT` policy, located in the **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Mobile Clients and Backlogs** policy group.

Changing E-mail

E-mail must be changed in all three options of the `SIEBSPI_SYNCH_STATUS_EXT` policy. (Refer to the figure below.)



Note that every threshold level contains an automatic command that is used for sending the e-mail to the recipient. The complete automatic action command is: `%SIEBSPI_PATH%\bin\siebspi_smail" -t <$VALUE> -c <$OPTION(user)> -m <$OPTION(email)>`. The e-mail address of a recipient is specified with the `-m` parameter.The default value is:
`-m <$OPTION(email)>`

This indicates that e-mail is sent only to the user who was not synchronized for the specified amount of time.

Examples

Example 1:

```
-m "<$OPTION(email)>,name1@dom1.com,name2@dom2.com"
```

This will send an e-mail message to the user who was not synchronized for the specified amount of time, and also to the following e-mail addresses:
`name1@dom1.com`
`name2@dom2.com`

Example 2:

```
-m name@domain.com
```

This will send an e-mail message only to the `name@domain.com` email address.

Sending E-mail for Synchronization Status from the Managed Node

By default, e-mail messages are sent from the management server, which requires that the management server has sendmail configured. Additionally, you can configure SPI for Siebel to send e-mail messagess from the managed nodes where the Siebel Servers are installed. Follow the procedure below:

1. Start the *HPOM Administration UI* and log in as an HPOM Administrator (opc_adm).
2. Go to **SPI for Siebel/SIEBSPI-Oracle Siebel CRM/SIEBSPI-Siebel Application Server/SIEBSPI-Mobile Clients**, **Backlogs** policy group.
3. Select the `SIEBSPI_SYNCH_STATUS_EXT` monitor policy.
4. You should see a window with three conditions listed. Change each of these conditions.
5. Delete the `<$OPC_MGMTSV>` string in the **Node** field. Additionally, change the data listed in the **Command** field as follows:

   ```
   siebspi_smail -t <$VALUE> -c <$OPTION(user)> -m <$OPTION(email)> -
   node
   ```

6. To confirm the changes, click **OK**.

NOTE

Assign and install the monitor policy on a node where the Siebel server is installed for the changes to take effect.

Managing Multiple Siebel Enterprise Environments Concurrently

By default, the SPI for Siebel configuration file `spi.cfg` is prepared and maintained on the management server. This file is deployed with the Instrumentation to the managed nodes where the SPI for Siebel configuration is updated.

To manage multiple Siebel enterprise environments at the same time, you need to prevent those automatic SPI for Siebel configuration updates from occurring. For this purpose you can use the configuration entry `MANUAL_CONFIGURATION` in the SPI for Siebel configuration file. To prevent automatic updates of the SPI for Siebel configuration, set this flag to `Y (Yes)`. Note that the default value is `N (NO)`.

Example:

```
MANUAL_CONFIGURATION=Y
```

Renaming SPI for Siebel Policies

SPI for Siebel supports changing the name of any policy that comes with SPI for Siebel. However, renaming a policy can have side effects, so this should be done very carefully following the instructions and rules described in this chapter.

Renaming Policies That Are Using siebspi_extmon Program for Monitoring Siebel Environment

You can rename any of the SPI for Siebel policies. When renaming a policy, add a new parameter to the policy `program name` parameter, called `-func {functionality}` or `-f {functionality}`. The value of the `-f` parameter must be the original policy name without the prefix `SIEBSPI_`.

Example:

Original policy: `SIEBSPI_SERVER_AVAILABILITY`

Original policy program name:

```
siebspi_extmon -srvr -m SIEBSPI_SERVER_AVAILABILITY
```

New policy name: `MY_SIEBSPI_SERVER_AVAILABILITY`

New policy program name:

```
siebspi_extmon -srvr -m MY_SIEBSPI_SERVER_AVAILABILITY \
-f SERVER_AVAILABILITY
```

Some SPI for Siebel policies send monitor messages to other SPI for Siebel policies, which are collecting data and reacting to issues. These pairs of policies usually have similar names with added postfix `_EXT`.

For example, the policy `SIEBSPI_SERVER_AVAILABILITY` checks the Siebel Servers availability. The results are sent to the policy `SIEBSPI_SERVER_AVAILABILITY_EXT`. In case you rename an external monitor policy, it is important to follow the next rules.

The easiest way to rename an external monitor is adding the `_EXT` postfix to the name specified with the `-m` parameter.

Example:

Policy A: `MY_SIEBSPI_SERVER_AVAILABILITY`

External policy B: `MY_SIEBSPI_SERVER_AVAILABILITY_EXT`

Policy A command:

siebspi_extmon -srvr -m `MY_SIEBSPI_SERVER_AVAILABILITY`

The external monitor can also have a different name than its paired policy. In this case, you must use the `-extmon` parameter.

Example:

Policy A: `MY_SIEBSPI_SERVER_AVAILABILITY`

External policy B: `NEW_SIEBSPI_SERVER_AVAILABILITY_EXT`

Policy A command:

```
siebspi_extmon -srvr -m MY_SIEBSPI_SERVER_AVAILABILITY \
-extmon NEW_SIEBSPI_SERVER_AVAILABILITY_EXT
```

Renaming Policies That Monitor the Siebel Server Components

Policies that monitor Siebel Components do not require the `-f` parameter for functionality description. Functionality is recognized automatically from the `-component` parameter, which is always present in the command line.

The old mandatory mask for the component the policy name (`SIEBSPI_*_COMPONENT`) is obsolete. The policy name can be any chosen name but must be specified with the `-m` parameter in the command line:

New policy name: `NEW_SIEBSPI_SCC_OBJ_MGR_COMPONENT`

New policy program name:

```
siebspi_extmon -srvr -m NEW_SIEBSPI_SCC_OBJ_MGR_COMPONENT -component
"Call Center Object Manager" -perf -status -max_tasks -task_exit
```

By default, all `SIEBSPI_*_COMPONENT` monitor policies send results to standard Siebel component external monitor policy (`SIEBSPI_CHECK_TASKS_EXT`, `SIEBSPI_COMP_STATUS_EXT`, `SIEBSPI_NUM_TASKS_TOO_HIGH_EXT`, `SIEBSPI_NUM_TASKS_TOO_LOW_EXT`). Therefore common thresholds, defined in those external monitor policies, are applied to all of them.

In situations when you renamed component external monitor policies or you need to define component specific thresholds, instructions, or actions, you can use the following parameters:

Parameter	Description
-extmon	Custom external monitor policy.
-[status2 | min_tasks2 | max_tasks2 | task_exit2]	What should be monitored and sent to custom external monitor policy.

This way you define what should be monitored and to which external monitor policy the results should be sent. You can combine standard parameters and the custom one in one component policy as long as you define custom external policies.

The required postfixes for custom external monitor policies are:

- component status external monitor policy = `*_CS_EXT`
- task exit status external monitor policy = `*_TS_EXT`
- number of tasks too low external monitor policy = `*_TL_EXT`
- number of tasks too high external monitor policy = `*_TH_EXT`

Example:

Siebel component "Workflow Monitor Agent" should send status results to custom monitor policy `SIEBSPI_WORK_MON_CS_EXT`. Additionally, the number of running tasks should be monitored (alarm if the number of running tasks: >70%, >90%).

Perform the following steps:

- Create a copy of the `SIEBSPI_COMP_STATUS_EXT` external monitor policy and save it as `SIEBSPI_WORK_MON_CS_EXT`
- Customize Thresholds (if needed, also: Actions, Instructions…)
- Customize the `SIEBSPI_WORK_MON_COMPONENT` policy command line to:

```
siebspi_extmon -srvr -m SIEBSPI_WORK_MON_COMPONENT -component
"Workflow Monitor Agent" -extmon SIEBSPI_WORK_MON -status2 -
max_tasks
```

Renaming Policies That Are Using siebspi_sp Program for Monitoring Siebel Environment

A new parameter `-m` is introduced in `siebspi_sp` program. If the policy is renamed, this parameter is set to the new monitor policy name. Functionality is recognized automatically from other parameters, and the `-f` parameter is not required.

Example:

Original policy: `SIEBSPI_SP_LOGIN_TIME`

Original policy program name:
`siebspi_sp -l`

New policy name: `MY_SIEBSPI_SP_LOGIN_TIME`

New policy program name:
`siebspi_sp -l -m MY_SIEBSPI_SP_LOGIN_TIME`

Renaming Policies That Are Using siebspi_ressvc Program for Monitoring Siebel Environment

This program is used only by log file policy SIEBSPI_RCD_AGT_LOG in automatic actions for conditions number 2 in 3. All messages this policy finds in a log file are sent to the external monitor SIEBSPI_RES_SVC_EXT. In case you rename this external monitor, you should use the additional -extmon parameter in this two automatic actions commands.

Example:

Original external policy name: SIEBSPI_RES_SVC_EXT

Original SIEBSPI_RCD_AGT_LOG policy automatic action command:
```
siebspi_ressvc -s 1 -m "<subfacility>: <message>" -c <facility>
```

New external policy name: MY_SIEBSPI_RES_SVC_EXT

New SIEBSPI_RCD_AGT_LOG policy automatic action command:
```
siebspi_ressvc -s 1 -m "<subfacility>: <message>" -c <facility> -extmon
MY_SIEBSPI_RES_SVC_EXT
```

Renaming Policies That Are Used in Autodiscovery Process

You can perform auto discovery using the "Autodiscovery" policy, or the policy SIEBSPI_ENTERPRISE_CONFIGURATION. Both send new and changed Siebel service tree configuration to external monitor policy SIEBSPI_CONF_UPD_EXT.

In case you rename the external monitor policy SIEBSPI_CONF_UPD_EXT, two actions are required:

- The autodiscovery tool command line should be updated with the -extmon parameter to specify the new external monitor name
- Program command-line in the SIEBSPI_ENTERPRISE_CONFIGURATION policy should be updated with the -extmon parameter to specify the new external monitor name

Example:

Original external policy name:SIEBSPI_CONF_UPD_EXT

Original SIEBSPI_ENTERPRISE_CONFIGURATION policy program name:
```
siebspi_extmon -srvr -m SIEBSPI_ENTERPRISE_CONFIGURATION
```

Original Autodiscovery tool command line:
```
siebspi_autod
```

New external policy name: MY_SIEBSPI_CONF_UPD_EXT

New SIEBSPI_ENTERPRISE_CONFIGURATION policy program name:
```
siebspi_extmon -srvr -m SIEBSPI_ENTERPRISE_CONFIGURATION -extmon
MY_SIEBSPI_CONF_UPD_EXT
```

New Autodiscovery tool command line:
```
siebspi_autod -extmon MY_SIEBSPI_CONF_UPD_EXT
```

Renaming SPI for Siebel Internal Monitor Policy

SPI for Siebel is using one internal monitor policy for intercepting some common problems that can occur in the SPI programs. Default name for this policy is SIEBSPI_INT_MESSAGE_EXT and can be found in the SIEBSPI-Internal policy group.

Renaming this policy is a special case. In case you change the name for this policy, the new name must be written in the SPI for Siebel configuration file on the managed node:
```
<AgentInstallDir>/siebspi/conf/spi.cfg
```

You must add a new parameter called "INT_MESSAGE_EXT" to this file:
```
INT_MESSAGE_EXT = <NEW_NAME>
```

Example:
```
INT_MESSAGE_EXT = INT_MESSAGE_EXT
```

Checking Mechanism for Policy Consistency

Some SPI for Siebel policies send monitor messages to other SPI for Siebel policies, which are collecting data and reacting to issues. These pairs of policies usually have similar names with added postfix _EXT.

For example, the policy SIEBSPI_SERVER_AVAILABILITY checks the Siebel Servers availability. The results are sent to the policy SIEBSPI_SERVER_AVAILABILITY_EXT.

It is important that you deploy both policies to the system. If you deployed the first policy to the system, you should also deploy the second policy.

SPI for Siebel is able to check if all external policies that are used by policies deployed on the managed node are also deployed to the node (consistency checking). By default, consistency checking is disabled (MONITOR_CHECK = N). This is only necessary when a new policy is deployed to the managed node.

You can enable consistency checking to ensure everything is deployed to the managed node. Consistency checking is enabled by setting MONITOR_CHECK = Y in SPI for Siebel configuration file on the managed node:
```
<AgentInstallDir>/siebspi/conf/spi.cfg
```

To disable consistency checking, set `MONITOR_CHECK = N` in the SPI for Siebel configuration file on the managed node.

When consistency checking is enabled and any of the used external policies are missing, a message is sent to the SPI for Siebel internal policy (by default `SIEBSPI_INT_MESSAGE_EXT`). The message contains the following attributes:

- message group: `siebspi_int`
- tool: `SPI for Siebel`
- object: `policy problem`

message text: `SIEBSPI-018: Policy "XY" that is used by another policy is not deployed on the system.`

Chapter 17

The SPI for Siebel Service

The SPI for Siebel Service

The SPI for Siebel service is an interface between Siebel's srvrmgr tool and the SPI for Siebel executables that request information from it. Therefore, the SPI for Siebel service is installed only on managed nodes where the Siebel server is installed. The main benefit of the service is that you do not need to start the srvrmgr command-line tool each time you require some data from the Siebel enterprise.

The SPI for Siebel service is located in:

- on Windows nodes in
  `{HPOM Agent install dir}\siebspi\bin\siebspi_svc.exe`
- on AIX nodes in `/usr/lpp/OV/siebspi/bin/siebspi_svc`
- on other UNIX nodes in `/opt/OV/siebspi/bin/siebspi_svc`

You can use several tools and commands to manage the SPI for Siebel service. From the HPOM management server, you can use the following tools from the **SPI for Siebel/SIEBSPI-Maintenance/SIEBSPI-SPI for Siebel Service** tool group:

- **SIEBSPI-Start SPI for Siebel Service**
- **SIEBSPI-Stop SPI for Siebel Service**
- **SIEBSPI-Restart SPI for Siebel Service**
- **SIEBSPI-SPI for Siebel Status**

The described tools use the following commands, which can also be started manually:

- `siebspi_mgr -service start_spisvc`
  Starts the SPI for Siebel Service
- `siebspi_mgr -service stop_spisvc`
  Stops the SPI for Siebel Service
- `siebspi_mgr -service restart_spisvc`
  Restarts the SPI for Siebel Service
- `siebspi_mgr -service spisvc_status`
  Displays the status of the SPI for Siebel Service

You can also use the following commands on Windows Nodes:

- `siebspi_svc -install`
  Installs the SPI for Siebel Service
- `siebspi_svc -remove`
  Removes the SPI for Siebel Service

and on UNIX Nodes:

- `siebspi_svc -start`
  Starts the SPI for Siebel Service
- `siebspi_svc -stop`
  Stops the SPI for Siebel Service
- `siebspi_svc -status`
  Displays the status of the SPI for Siebel Service

N O T E

On UNIX nodes, "SPI for Siebel Service" is not started automatically after the system starts. Therefore, start this service manually using the tools described above.
Make sure that the "SPI for Siebel Service" on UNIX nodes is started with the appropriate {siebel user name} if other than root. For starting and stopping the services, use the full path (for example, to start on the AIX nodes: `/usr/lpp/OV/siebspi/bin/siebspi_svc -start`)

Monitoring the SPI for Siebel Service

The SPI for Siebel Service is monitored if you deploy the **SIEBSPI-Internal** policy group.

If the SPI for Siebel Service is stopped, you will receive a critical error message in your message browser. The message instructions will tell you to start the service using the commands described in the previous section.

SPI for Siebel Service Error Messages

Descriptions of SPI for Siebel Service error messages:

SPISVC-001: Check if the Siebel gateway service is running. Also make sure that the configuration parameters are correct.

You should check if the Siebel gateway service is running. If it is, check if the SPI for Siebel configuration file (`spi.cfg`) parameters on the node are correct.

Check the `SIEBEL_ENTERPRISE`, `SIEBEL_GATEWAY` and `ADMIN_USERNAME` parameters. Also make sure that you entered the right administrator password for Siebel Enterprise.

SPISVC-002: Internal SPI for Siebel service/daemon error.

Could not execute the command.

An internal error has occurred. Check the SPI for Siebel error log file on the managed node.

SPISVC-003: Cannot connect to the SPI for Siebel service/daemon (`siebspi_svc`). Check if the service/daemon is running.

Refer to "Troubleshooting" on page 155 for additional information.

SPISVC-004: SPI for Siebel Service is stopping.

If you receive this message, an attempt was made to make a request on the service while it was stopping.

SPISVC-005: SPI for Siebel Service is busy. Maximum number of connections reached.

This message indicates that the maximum number of requests is being handled and therefore the request for executing a command was rejected. If you consistently receive this message, you should reduce the number of policies on the managed node.

SPISVC-006: Timeout occurred. The request could not be processed in the specified time.

You will receive this message in the SPI for Siebel error log file if a request that has been made could not be processed in a specified timeframe. If you receive this message often, most likely the machine is very slow (check the resources usage) or there is a problem with the Siebel Gateway service.

SPISVC-007: No 'srvrmgr' available on host. Executing 'srvrmgr' commands is not allowed.

You will receive this message if a request has been made to execute a 'srvrmgr' command and there is no 'srvrmgr' tool available on the machine. If you receive this message on a machine where only the Siebel Application Server is installed, this is probably a SPI for Siebel configuration error. If you receive these messages on a machine with only Siebel gateway installed, you probably installed policies for the Siebel Server on the Siebel Gateway node.

Chapter 18

Troubleshooting

Errors and Problems

This section provides information relating to the logging and tracking of errors. It also describes the possible errors that can occur during SPI for Siebel usage, and how to resolve any problems if encountered.

Error Logging and Tracing

By default, error logging is on at all times. Additionally, errors are logged to the error log files at the following location:

On UNIX systems:

`<OVDataDir>/siebspi/log/error`

On Windows systems:

`<OVDataDir>\siebspi\log\error`

Each SPI for Siebel binary/executable on the managed node in the cmds, actions and monitor directories can be executed with the `-trace` option. All errors and additional "trace" information will be printed to the console and logged at the following location:

On Unix systems:

`<OVDataDir>/siebspi/log/trace`

On Windows systems:

<OVDataDir>\siebspi\log\trace

Miscellaneous Troubleshooting

Deleting the Files Needed for SIEBSPI on the Management Server

SPI for Siebel has known problems with the de-installation of the product when the managed Siebel server and the HPOM management server are installed on the same computer. If this situation exists, do not perform the procedure "Uninstalling SPI for Siebel from the Managed Nodes" on the HPOM management server. Additionally, do not run the tool **SIEBSPI-Remove from Node** on the HPOM management server as a de-installation from the management server node also deletes the files that are needed for SIEBSPI on the management server. In case this occurs, perform the "Re-installing the SPI for Siebel" procedure.

Correcting Corruption of the spi.cfg File

When using the **SIEBSPI-Change Configuration** tool, immediately after entering new configuration values, if you use editing keys, for example, **[Backspace]**, **[Delete]**, and arrow keys, the configuration file, `spi.cfg` may become corrupted with the addition of special characters. Refer to the example below for a listing of how the file could appear:

```
SIEBEL_ENTERPRISE"sieb621_[D_[D_[D_[D_[D_[C_[C621"
SIEBEL_GATEWAY"yabg_[d_[d_[c_[c_[d_[d_[d_[c_[c_[c_[d_
[d_xxx_[d_[dngtzee"
SIEBEL_DATABASE_NAME"_[D_[D_[C_[D_[D_[D_[D_[C_[C_[C_[Csieb_[D_[D_[D_
[D sieb621"
```

A workaround to this problem is to use the `siebspi_configure` executable tool from the console.

SPISVC-003: Cannot connect to SPI for Siebel service/daemon (siebspi_svc). Check if the service/daemon is running.

If you receive this message in your message browser, you should check if the SPI for Siebel service/daemon is running. If it is not, you should start it by executing the **SIEBSPI-Start SPI for Siebel Service** tool in the **SPI for Siebel/SIEBSPI-Maintenance/SIEBSPI-SPI for Siebel Service** tool group.

If the SPI for Siebel service/daemon is running and you still receive these messages, check the SPI for Siebel error log file on the managed node where the messages came from. Look for entries in the log file such as: "Could not connect to pipe". If the error code number (errno) is 231 (`ERROR_PIPE_BUSY`) on Windows nodes or ECONNREFUSED (146 on Solaris, 79 on AIX or 239 on HP-UX) on UNIX nodes, this indicates that temporarily resources could not be allocated. This means that no new connections to the SPI for Siebel service/daemon could be established.

You should check if you receive the same messages if you install only a few policies from the **SPI for Siebel/SIEBSPI-Siebel *.*.* Server** policy group and the utilization of the Siebel server is low. If you still receive these kind of messages or, if the error code number in the SPI if Siebel error log file is other than described, you should try restarting the SPI for Siebel service/daemon either with the **SIEBSPI-Restart SPI for Siebel Service** tool or manually by starting the `siebspi_mgr -service restart_spisvc` command.

If you still encounter problems with the SPI for Siebel service/daemon, contact the Support Department.

Some Tools Do Not Work on UN*X Nodes

Some SPI for Siebel tools may not work correctly on UN*X nodes if the user name used to install Oracle's Siebel Business Applications is other than root. Therefore, the following tools must be modified by replacing the user name in the Target tab of the tools with the {siebel user name}:

- All of the tools in the **SPI for Siebel/SIEBSPI-Tools** tool group that are started with the `root` user
- **SPI for Siebel/SIEBSPI-Maintenance/SIEBSPI-SPI for Siebel Service/SIEBSPI-Start SPI for Siebel Service**
- **SPI for Siebel/SIEBSPI-Maintenance/SIEBSPI-SPI for Siebel Service/SIEBSPI-Restart SPI for Siebel Service**

In addition, the SPI for Siebel Service must be started with the same {siebel user name}. For more information, see also "SPI for Siebel Service on UN*X Nodes" on page 158.

SPI for Siebel Service on UN*X Nodes

If the username used to install Oracle's Siebel Business Applications is other than root, make sure that the SPI for Siebel Service is started with the `{siebel user name}` to work properly.

After installation, the SPI for Siebel Service is started automatically with the root user so you must first stop it with the **SPI for Siebel/SIEBSPI-Maintenance/SIEBSPI-SPI for Siebel Service/SIEBSPI-Stop SPI for Siebel Service** tool. After the SPI for Siebel Service has stopped, modify the **SPI for Siebel/SIEBSPI-Maintenance/SIEBSPI-SPI for Siebel Service/SIEBSPI-Start SPI for Siebel Service** tool, change the user name from `root` to `{siebel user name}`, and run the tool to start the SPI for Siebel Service with the user name that you provided.

For details about the other tools that should be changed, refer to "Some Tools Do Not Work on UN*X Nodes" on page 158.

Timeouts

This section provides information relating to the timeout settings.

Predefined Timeouts

Some SPI for Siebel executables contain different predefined timeouts that define timeframes (in seconds) in which they expect certain results to be returned from other executables or triggered actions to be completed. Those timeout parameters are exported in four configuration files on every managed node:

`<OVInstallDir>/siebspi/conf/siebspi_svc.cfg`

`<OVInstallDir>/siebspi/conf/siebspi_extmon.cfg`

`<OVInstallDir>/siebspi/conf/siebspi_mgr.cfg`

`<OVInstallDir>/siebspi/conf/siebspi_dbperf.cfg`

Configuration settings are read from these files only if the parameter is set to `Manual_configuration=Y`. Otherwise executables will use their predefined timeouts.

NOTE

Settings in these timeout configuration files should not be changed without prior approval from SPI for Siebel Support.

Appendix A

File Locations

File Tree on the Management Server

The /var/opt/OV/share/tmp/OpC_appl/SIEBSPI directory is created when installing the bundle from the SIEBSPI depot on the HP Operations Manager management server. It contains multiple subdirectories that contain the siebspi configuration files for HP Operations Manager.

Platform dependent files (those for deployment on the management node) are copied to the HP Operations Manager Instrumentation folder. The Instrumentation directory is usually located in the following location:

/var/opt/OV/share/databases/OpC/mgd_node/customer

/opt/OV/siebspi/bin

siebspi_configure

siebspi_smail

siebspi_svcupd

siebspi_licmgr

icudt26l.dll

icuin26.dll

icuio26.dll

icuuc26.dll

\siebspi\conf

spi.cfg

\siebspi\locale

intmc_en.res

\siebspi\msg

email.msg

SPI for Siebel - Reports

The self-extracting file for HP Reporter:

/etc/opt/OV/share/siebspi/reports

- siebspi-reports_04.00_Windows_NT.exe

OVIS Smart Probe for Siebel

The self-extracting file for HP Internet Services:

/etc/opt/OV/share/siebspi/ovis

- OVISProbeforSiebel_03_20.exe
- OVIS_SmartProbe_for_Siebel_03_20.pdf

Documentation

/opt/OV/siebspi/doc

SIEBSPI-InstallGuideUNIX.pdf

SIEBSPI-UserGuideUNIX.pdf

siebspi-release-notes-unix.txt

siebspi-readme.txt

comtrade_software_license_support_terms_signed.txt

Description of Directory Structures on the Managed Node

The files associated with the HTTPS agent are in the following directory structures:

<OVInstallDir>

HP-UX, Solaris: /opt/OV

AIX: /usr/lpp/OV

Windows: <ProgramFilesDir>\HP OpenView

<OVDataDir>

HP-UX, Solaris, Linux, AIX: /var/opt/OV

Windows: <ProgramFiles>\HP OpenView\data

The files associated with the DCE and NCS agents are in the following directory structures:

<OVInstallDir>

HP-UX, Solaris: /opt/OV

AIX: /usr/lpp/OV

Windows: c:\usr\OV

<OVDataDir>

HP-UX, Solaris, Linux, AIX: `/var/opt/OV`

Windows: `c:\usr\OV`

File Tree on the Managed Node

After the installation of SPI for Siebel on the managed node, the following directories are created on the managed node file system:

`<OVInstallDir>/siebspi`

`<OVInstallDir>/siebspi/bin`

`<OVInstallDir>/siebspi/cluster`

`<OVInstallDir>/siebspi/conf`

`<OVInstallDir>/siebspi/lib` (on Unix nodes)

`<OVInstallDir>/siebspi/locale`

`<OVInstallDir>/siebspi/locale/6.0.x`

`<OVInstallDir>/siebspi/locale/7.0.4`

`<OVInstallDir>/siebspi/locale/7.5.2`

`<OVInstallDir>/siebspi/locale/7.7`

`<OVInstallDir>/siebspi/locale/7.8`

`<OVInstallDir>/siebspi/msg`

`<OVInstallDir>/siebspi/support`

`<OVDataDir>/siebspi`

`<OVDataDir>/siebspi/tmp`

`<OVDataDir>/siebspi/log`

`<OVDataDir>/siebspi/siebspi_perf`

SPI for Siebel files are also copied to the HPOM instrumentation directories on the managed node:

On HP-UX:

DCE and NCS agents

`/var/opt/OV/bin/OpC/actions`

`/var/opt/OV/bin/OpC/cmds`

`/var/opt/OV/bin/OpC/monitor`

HTTPS agents

/var/opt/OV/OpC/bin/instrumentation

On IBM AIX systems:

DCE agents

/var/lpp/OV/bin/instrumentation

HTTPS agents

/var/opt/OV/OpC/bin/instrumentation

On Windows 2000/2003 systems:

DCE agents

C:\Program Files\HP OpenView\Installed Packages\{790c06b4-844e-11d2-972b-080009ef8c2a}\bin\instrumentation

HTTPS agents

/var/opt/OV/bin/instrumentation/

On Sun Solaris systems:

DCE agents

/var/opt/OV/bin/instrumentation

HTTPS agents

/var/opt/OV/bin/instrumentation

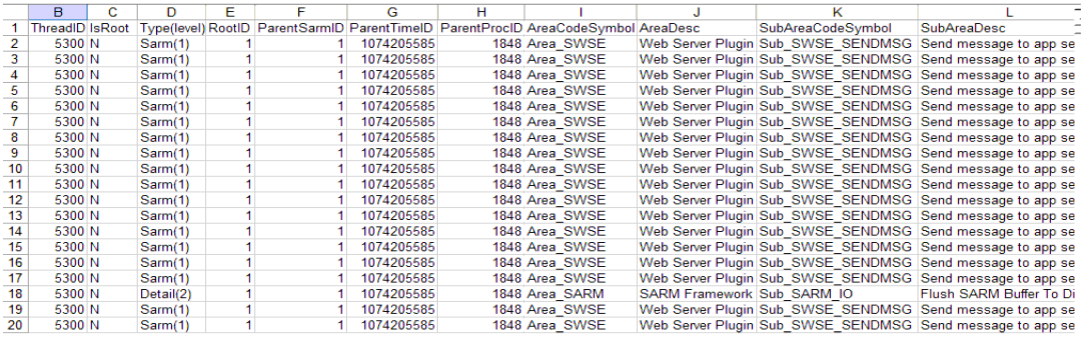
Appendix B

SARM Reference Information

Siebel ARM (SARM) Reference Information

About Siebel ARM to CSV Conversion Data (used for Call Graph)

CSV format is a comma-separated file without any interpretation or aggregation. The CSV file contains data organized under column headers. Use third-party software applications to view this output, for example, a spreadsheet.



	B	C	D	E	F	G	H	I	J	K	L
1	ThreadID	IsRoot	Type(level)	RootID	ParentSarmID	ParentTimeID	ParentProcID	AreaCodeSymbol	AreaDesc	SubAreaCodeSymbol	SubAreaDesc
2	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
3	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
4	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
5	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
6	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
7	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
8	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
9	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
10	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
11	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
12	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
13	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
14	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
15	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
16	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
17	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
18	5300	N	Detail(2)	1	1	1074205585	1848	Area_SARM	SARM Framework	Sub_SARM_IO	Flush SARM Buffer To Di
19	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se
20	5300	N	Sarm(1)	1	1	1074205585	1848	Area_SWSE	Web Server Plugin	Sub_SWSE_SENDMSG	Send message to app se

Tag	Description
SarmNode	Data contained within this tag represents an instance of a Siebel ARM node, which is an instrumented area of the Siebel ARM architecture. Each Siebel ARM node can have zero to many nodes as its descendants.
SarmID	A unique number representing the Siebel ARM node.
`TypeLevel`	The granularity level at which Siebel ARM records the Siebel ARM node information.
`RootID`	The SarmID of the root Siebel ARM node.
`ParentSARMID`	The parent SarmNode from which the request traveled.
`ParentTimeID`	A unique ID number that generates from the starting time of the corresponding parent Siebel ARM node.
`ParentProcID`	The parent process ID, that is, the OS (operating system) process ID for the Siebel component.

Tag	Description
AreaCodeSymbol	Symbol of the instrumentation area within the Siebel architecture.
AreaDescription	Name of the instrumentation area within the Siebel architecture.
SubAreaCodeSymbol	Symbol of the subarea within an area of the Siebel architecture.
SubAreaDescription	Name of the subarea within an area of the Siebel architecture.
Count	Number of times Siebel ARM accesses this Siebel ARM Node.
Duration	Total time to execute the instrumented area.
PooledMemoryUsage	Amount of memory consumed from or released to the Siebel High Performance memory allocator.
PooledMemoryCalls	The number of calls made to the High performance memory allocator.
SystemMemoryUsage	Amount of memory consumed from or released to the operating system.
SystemMemoryCalls	The number of calls made to the operating system.
AppInt1 and AppInt2	Context integer value captured at the point of instrumentation. The value depends on the instrumented area.
AppString1 and AppString2	Context string value captured at the point of instrumentation. The value depends on the instrumented area. For example, the name of the method invoked or workflow process initialized.
+<ChildNode>	Expand this tag to reveal performance details on descendent nodes of the given node. The descendent nodes are defined the same as the parent node, that is, the tag definitions are the same as above.

About Performance Aggregation Analysis and Data

Performance aggregation analysis is a compilation of the data contained in a Siebel ARM binary file. Siebel ARM files group performance data based on the instrumented areas.

A result of running a performance aggregation analysis of a Siebel ARM file is an extensible markup language (XML) output file. This file contains timing data for the instrumented areas.

The amount of information contained in the performance aggregation analysis XML output is dependent on the argument used for the `-a` flag when performing the analysis (either AREA or DETAILS) and the setting for the SARM Granularity Level parameter.

The performance aggregation XML output file contains the following tag schema when the `-a` flag argument is set to **DETAILS**. If the `-a` flag argument is set to **AREA** when running the analysis, the tag schema is the same minus the **<NumberOfSubAreas>** and **<SubArea>** information.

```
<Area>
   <Name>
   <Symbol>
   <NumberOfSubAreas>
   <Invocations>
      <Recursive>
      <NonRecursive>
   <ResponseTime>
      <Total>
      <Average>
      <StandardDeviation>
      +<Maximum>
      +<Minimum>
   <ExecutionTime>
      <Total>
      <Calls>
      <Average>
      <Maximum>
      <Minimum>
      <PercentOfResponse>
   <RecursiveTime>
      <Total>
      <Calls>
      <Average>
      <Maximum>
      <Minimum>
      <PercentOfResponse>
   <InclusiveMemory>
      <Total>
      <Average>
      <StandardDeviation>
      +<MaxAllocated>
      +<MaxDeallocated>
   <ExclusiveMemory>
```

```
   <Total>
   <Average>
   <StandardDeviation>
   +<MaxAllocated>
   +<MaxDeallocated>
<SubArea>
   <Name>
   <Symbol>
   <NumberOfInstances>
   +<Invocations>
   +<ResponseTime>
   +<ExecutionTime
   +<Memory>
   +<Instance>
   +<Parents>
   +<Children>
<Parents>
   <NumberOfParents>
   <ParentArea>
      <Name>
      <Symbol>
      +<InvocationsFromParents>
      +<ResponseTime>
      +<Memory>
<Children>
   <NumberOfChildren>
   <ChildArea>
      <Name>
      <Symbol>
      +<InvocationsOfChild>
      +<ResponseTime>
      +<Memory>
```

Appendix C

Regular Expression Syntax

Regular Expression Syntax

A regular expression is a pattern of text that consists of ordinary characters (for example, letters a through z) and special characters, known as metacharacters. The pattern describes one or more strings to match when searching a body of text. The regular expression serves as a policy for matching a character pattern to the string being searched.

Here are some examples of regular expression you might encounter:

Regular expression	Matches
\bError\b	Find "Error" but ignore strings like "SocketError"
"\d{2}-\d{5}	"Validate an ID number consisting of 2 digits, a hyphen, and another 5 digits.
"<(.*)>.*<\/\1>	"Match an HTML tag.

The following table contains the complete list of metacharacters and their behavior in the context of regular expressions:

Character	Description
\	Marks the next character as either a special character, a literal, a backreference, or an octal escape. For example, 'n' matches the character "n". '\n' matches a newline character. The sequence '\\' matches "\" and "\(" matches "(".
^	Matches the position at the beginning of the input string.
$	Matches the position at the end of the input string.
*	Matches the preceding subexpression zero or more times. For example, zo* matches "z" and "zoo". * is equivalent to {0,}.

Character	Description
+	Matches the preceding subexpression one or more times. For example, 'zo+' matches "zo" and "zoo", but not "z". + is equivalent to {1,}.
?	Matches the preceding subexpression zero or one time. For example, "do(es)?" matches the "do" in "do" or "does". ? is equivalent to {0,1}
{n}	n is a nonnegative integer. Matches exactly n times. For example, 'o{2}' does not match the 'o' in "Bob," but matches the two o's in "food".
{n,}	n is a nonnegative integer. Matches at least n times. For example, 'o{2,}' does not match the "o" in "Bob" and matches all the o's in "foooood". 'o{1,}' is equivalent to 'o+'. 'o{0,}' is equivalent to 'o*'.
{n,m}	m and n are nonnegative integers, where n <= m. Matches at least n and at most m times. For example, "o{1,3}" matches the first three o's in "fooooood". 'o{0,1}' is equivalent to 'o?'. Note that you cannot put a space between the comma and the numbers.
?	When this character immediately follows any of the other quantifiers (*, +, ?, {n}, {n,}, {n,m}), the matching pattern is non-greedy. A non-greedy pattern matches as little of the searched string as possible, whereas the default greedy pattern matches as much of the searched string as possible. For example, in the string "oooo", 'o+?' matches a single "o", while 'o+' matches all 'o's.

Character	Description
.	Matches any single character except "\n". To match any character including the '\n', use a pattern such as '[.\n]'.
(pattern)	Matches pattern and captures the match. To match parentheses characters ( ), use '\(' or '\)'.
(?:pattern)	Matches pattern but does not capture the match, that is, it is a non-capturing match that is not stored for possible later use. This is useful for combining parts of a pattern with the "or" character (|). For example, 'industr(?:y|ies) is a more economical expression than 'industry|industries'.
(?=pattern)	Positive lookahead matches the search string at any point where a string matching pattern begins. This is a non-capturing match, that is, the match is not captured for possible later use. For example 'Windows (?=95|98|NT|2000)' matches "Windows" in "Windows 2000" but not "Windows" in "Windows 3.1". Lookaheads do not consume characters, that is, after a match occurs, the search for the next match begins immediately following the last match, not after the characters that comprised the lookahead.

Character	Description
(?!pattern)	Negative lookahead matches the search string at any point where a string not matching pattern begins. This is a non-capturing match, that is, the match is not captured for possible later use. For example 'Windows (?!95|98|NT|2000)' matches "Windows" in "Windows 3.1" but does not match "Windows" in "Windows 2000". Lookaheads do not consume characters, that is, after a match occurs, the search for the next match begins immediately following the last match, not after the characters that comprised the lookahead.
x|y	Matches either x or y. For example, 'z|food' matches "z" or "food". '(z|f)ood' matches "zood" or "food".
[xyz]	A character set. Matches any one of the enclosed characters. For example, '[abc]' matches the 'a' in "plain".
[^xyz]	A negative character set. Matches any character not enclosed. For example, '[^abc]' matches the 'p' in "plain".
[a-z]	A range of characters. Matches any character in the specified range. For example, '[a-z]' matches any lowercase alphabetic character in the range 'a' through 'z'.
[^a-z]	A negative range characters. Matches any character not in the specified range. For example, '[^a-z]' matches any character not in the range 'a' through 'z'.
\b	Matches a word boundary, that is, the position between a word and a space. For example, 'er\b' matches the 'er' in "never" but not the 'er' in "verb".

Character	Description
\B	Matches a nonword boundary. 'er\B' matches the 'er' in "verb" but not the 'er' in "never".
\cx	Matches the control character indicated by x. For example, \cM matches a Control-M or carriage return character. The value of x must be in the range of A-Z or a-z. If not, c is assumed to be a literal 'c' character.
\d	Matches a digit character. Equivalent to [0-9].
\D	Matches a nondigit character. Equivalent to [^0-9].
\f	Matches a form-feed character. Equivalent to \x0c and \cL.
\n	Matches a newline character. Equivalent to \x0a and \cJ.
\r	Matches a carriage return character. Equivalent to \x0d and \cM.
\s	Matches any whitespace character including space, tab, form-feed, etc. Equivalent to [\f\n\r\t\v].
\S	Matches any non-whitespace character. Equivalent to [^ \f\n\r\t\v].
\t	Matches a tab character. Equivalent to \x09 and \cI.
\v	Matches a vertical tab character. Equivalent to \x0b and \cK.
\w	Matches any word character including underscore. Equivalent to '[A-Za-z0-9_]'.
\W	Matches any nonword character. Equivalent to '[^A-Za- z0-9_]'.

Character	Description
\xn	Matches n, where n is a hexadecimal escape value. Hexadecimal escape values must be exactly two digits long. For example, '\x41' matches "A". '\x041' is equivalent to '\x04' & "1". Allows ASCII codes to be used in regular expressions.
\num	Matches num, where num is a positive integer. A reference back to captured matches. For example, '(.)\1' matches two consecutive identical characters.
\n	Identifies either an octal escape value or a backreference. If \n is preceded by at least n captured subexpressions, n is a backreference. Otherwise, n is an octal escape value if n is an octal digit (0-7).
\nm	Identifies either an octal escape value or a backreference. If \nm is preceded by at least nm captured subexpressions, nm is a backreference. If \nm is preceded by at least n captures, n is a backreference followed by literal m. If neither of the preceding conditions exist, \nm matches octal escape value nm when n and m are octal digits (0-7).
\nml	Matches octal escape value nml when n is an octal digit (0-3) and m and l are octal digits (0-7).
\un	Matches n, where n is a Unicode character expressed as four hexadecimal digits. For example, \u00A9 matches the copyright symbol (©).