Monitoring Siebel Gateway Server

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Gateway Server is a logical server that consists of the Siebel Name Server and optionally Resonate Central Dispatch. These two components can reside on separate physical servers. The Gateway Name Server is a repository for configuration information about each Siebel Server. When Siebel Servers or components come online or go offline the Name Server data is refreshed with the connect strings. Clients will also use the Gateway Name server to connect to the Siebel Servers if Resonate Central Dispatch (which is used to load balance and manage client connections to Siebel Enterprise) is not implemented.

Since the Name server component of the Gateway server maintains the connectivity information pertaining to every component in Siebel Enterprise, the 24 x 7 availability of the Name server is crucial to the functioning of the Gateway server, and also for ensuring that client connections to Siebel servers are not disrupted. This where the eG Enterprise hlps administrator!

Chapter 2: How to Monitor Siebel Gateway Server Using eG Enterprise?

eG Enterprise monitors the Siebel Gateway server in an agent based manner.

2.1 Managing a Siebel Gateway Server

eG Enterprise can automatically discover the Siebel Gateway in the environment and also let you to add the Siebel Gateway component if the server is not auto-discovered. The following steps explain you how to manage the server that is auto-discovered server and how to manually add the Siebel Gateway using the eG administrative interface.

1. Log into the eG administrative interface.
2. If a Siebel Gateway is already discovered, then directly proceed towards managing it using the **COMPONENTS – MANAGE/UNMANAGE** page (Infrastructure -> Components -> Manage/Unmanage).
3. However, if it is yet to be discovered, then run discovery (Infrastructure -> Components -> Discover) to get it discovered or add the component manually using the **COMPONENTS**page (Infrastructure -> Components -> Add/Modify). Remember that components manually added are managed automatically. Discovered components, however, are managed using the **COMPONENTS – MANAGE / UNMANAGE** page.
4. To add the component manually, follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
5. In the **COMPONENT** page that appears next, select *Siebel Gateway* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

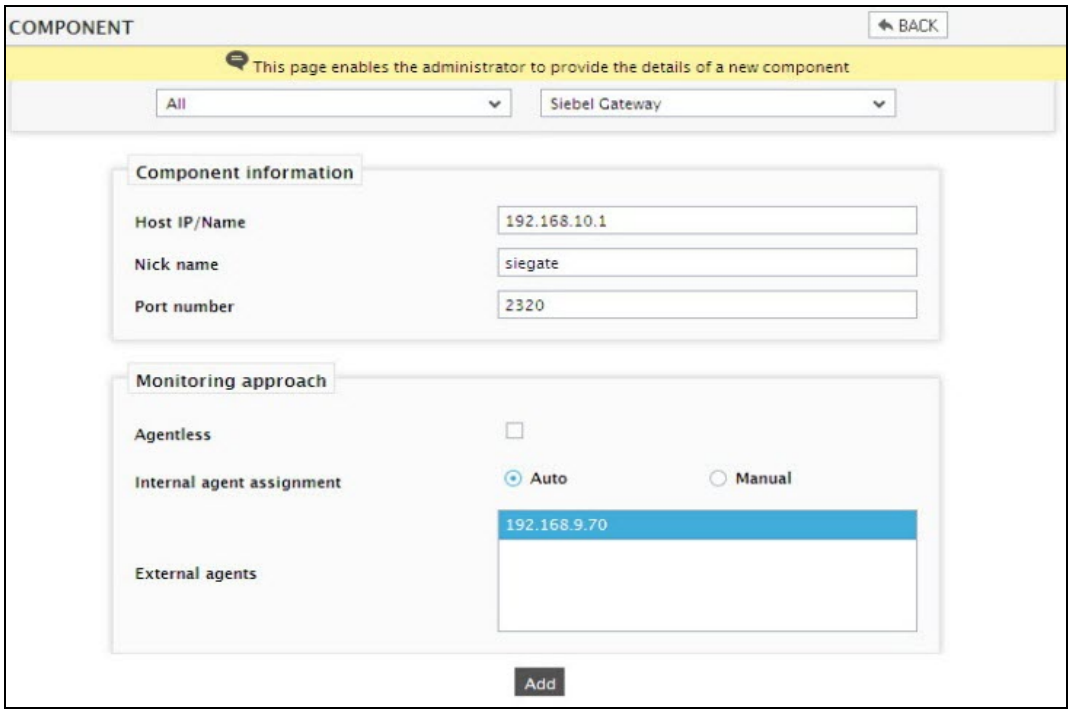

Figure 2.1: Adding a Siebel Gateway server

6. Specify the **Host IP/Name** and the **Nick name** of the Siebel Gateway in Chapter 2. Then, click the **Add** button to register the changes.
7. Next, try to sign out of the eG administrative interface. Figure 2.2 appears listing the tests to be configured for the managed Siebel gateway server.

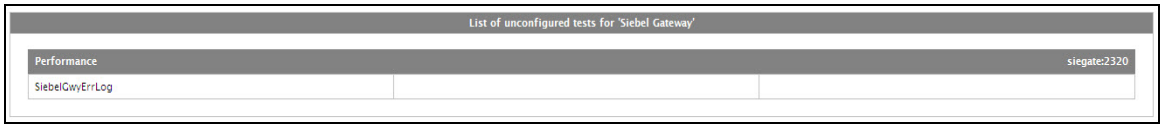

Figure 2.2: The list of unconfigured tests for the Siebel Gateway server

8. Click on the **Siebel Gateway Errors** test to configure it. Refer to the Section **3.3** to know how to configure this test.
9. Then, signout of the eG administrative interface.

Chapter 3: Monitoring Siebel Gateway Server

eG Enterprise offers a specialized *Siebel Gateway* monitoring model (see Figure 3.1), which runs periodic availability checks on the Gateway server to determine the availability of its Name server component and related services. This way, availability issues can be proactively detected and resolved before they affect the end-user experience.

Besides, additions to the Siebel Gateway server's log files are also closely monitored, so that potential threats to the health of the Gateway server can be promptly detected, and administrators immediately alerted.

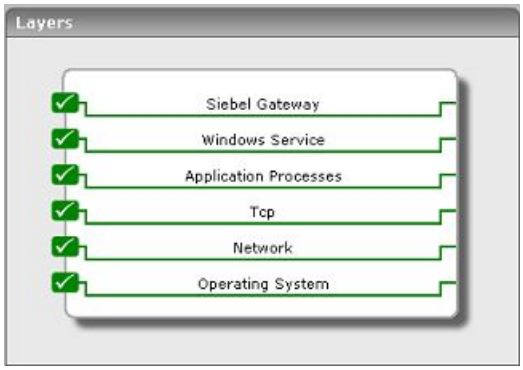

Figure 3.1: Layer model of the Siebel Gateway Server

The eG agent executes the tests mapped to each layer of the layer model to determine the following:

- Are too many errors logged in the error log? If so, what are they?
- Is the Siebel Gateway server up and running currently?
- Is the Siebel Gateway Name Server service available? If so, is it consuming too much CPU?

The sections to come will discuss the first 2 layers of Figure 3.1 alone, as the remaining layers have been elaborately discussed in the *Monitoring Unix and Windows Servers* document.

3.1 The Windows Service Layer

This layer determines the availability of the Name server service executing on the Gateway server.

Figure 3.2: shows the tests associated with the Windows Service Layer

The **Windows Services** test, its parameters, and the measures it reports have been dealt with extensively in the *Monitoring Unix and Windows Servers* document.

3.2 The Siebel Gateway Layer

Using the **Siebel Gateway Errors** test, this layer monitors the error logs and indicates whether any new errors occurred on the Gateway server (see Figure 3.3).

Figure 3.3: The tests associated with the Siebel Gateway layer

3.3 Siebel Gateway Errors Test

This test provides the status of errors logged in the Siebel gateway server log files.

Target of the test : A Siebel Gateway server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every log file, log file directory, or *LogFilePath:PatternName* monitored on the Siebel Gateway server.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The hostname (or IP address) of the Siebel web server.
Port	The port number on which the Siebel web server is listening.
AlertFile	Specify the path to the log file to be monitored. For eg., *C:/sea703/SWEBApp/LOG/Siebel_Web_log.txt*. Multiple log file paths can be provided as a comma-separated list. Also, instead of a specific log file path, the path to the directory containing log files can be provided - eg., *C:/sea703/SWEBApp/LOG*. This ensures that eG Enterprise monitors the most recent log files in the specified directory. Specific log file name patterns can also be specified. For example, to monitor the latest log files with names containing the strings 'siebel' and 'log', the parameter specification can be, *C:/sea703/SWEBApp/LOG/*siebel*,C:/sea703/SWEBApp/LOG/*log**. Here, '*' indicates leading/trailing characters (as the case may be). In this case, the eG agent first enumerates all the log files in the specified path that match the given pattern, and then picks only the latest log file from the result set for monitoring. You can also configure the path in the following format:*Name@logfilepath*. Here, Name represents the display name of the path being configured. Accordingly, the parameter specification for the 'siebel' and 'log' example discussed above can be: *siebel@C:/sea703/SWEBApp/LOG/*siebel*,log@C:/sea703/SWEBApp/LOG/*log** . In this case, the display names 'siebel' and 'log' will alone be displayed as descriptors of this test. Every time this test is executed, the eG agent verifies the following: • Whether any changes have occurred in the size and/or timestamp of the log files that were monitoring during the last measurement period; • Whether any new log files (that match the alertfile specification) have been newly added since the last measurement period; If a few lines have been added to a log file that was monitored previously, then the eG agent monitors the additions to that log file, and then proceeds to monitor newer log files (if any). If an older log file has been overwritten, then, the eG agent monitors this log file completely, and then proceeds to monitor the newer log files (if any).
SearchPattern	Enter the specific patterns of alerts to be monitored. The pattern should be in the following format: *<PatternName>:<Pattern>*, where *<PatternName>* is the pattern name that will be displayed in the monitor interface and *<Pattern>* is an expression of the form -

Parameter	Description
	expr or *expr* or **expr* or *expr**, etc. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. For example, say you specify Gen_errors:Generic* in the SearchPattern text box. This indicates that "Gen_errors" is the pattern name to be displayed in the monitor interface. "Generic*" indicates that the test will monitor only those lines in the log which start with the term "Generic". A single pattern may also be of the form e1+e2, where + signifies an OR condition. That is, the *<PatternName>* is matched if either e1 is true or e2 is true. Multiple search patterns can be specified as a comma-separated list. For example: *Gen_errors:Generic*,Critical_errors:*Error**. If the AlertFile specification is of the format *Name@logfilepath*, then the descriptor for this test in the eG monitor interface will be of the format: *Name:PatternName*. On the other hand, if the Alertfile specification consists only of a comma-separated list of log file paths, then the descriptors will be of the format: *LogFilePath:PatternName*.
Lines	Specify two numbers in the format **x:y**. This means that when a line in the log file matches a particular pattern, then x lines before the matched line and y lines after the matched line will be reported in the detail diagnosis output (in addition to the matched line). The default value here is *0:0*. Multiple entries can be provided as a comma-separated list. If you give *1:1* as the value for LINES, then this value will be applied to all the patterns specified in the SearchPattern field. If you give *0:0*, *1:1* as the value for Lines and if the corresponding value in the SearchPattern filed is like Gen_errors:Generic*,Critical_errors:*Error*, then: *0:0* will be applied to the Gen_errors:Generic*pattern *1:1* will be applied to the Critical_errors:*Error*pattern
ExcludePattern	Provide a comma-separated list of patterns to be excluded from monitoring in the ExcludePattern text box. For example **critical*,*exception**. By default, this parameter is set to '*none*'
UniqueMatch	By default, the UniqueMatch parameter is set to **False**, indicating that, by default, the test checks every line in the log file for the existence of each of the configured SearchPatterns. By setting this parameter to **True**, you can instruct the test to ignore a line and move to the next as soon as a match for one of the configured patterns is found in that line. For example, assume that *Pattern1:*Generic*,Pattern2:*Error** is the SearchPattern that has been configured. If UniqueMatch is set to **False**, then the test will read every line in the log file completely to check for the existence of messages

Parameter	Description
	embedding the strings 'Generic' and 'Error'. If both the patterns are detected in the same line, then the number of matches will be incremented by 2. On the other hand, if UniqueMatch is set to **True**, then the test will read a line only until a match for one of the configured patterns is found and not both. This means that even if the strings 'Generic' and 'Error' follow one another in the same line, the test will consider only the first match and not the next. The match count in this case will therefore be incremented by only 1.
RotatingFile	This flag governs the display of descriptors for this test in the eG monitoring console. If this flag is set to true and the AlertFile text box contains the full path to a specific (log/text) file, then, the descriptors of this test will be displayed in the following format: *Directory_containing_monitored_file:<SearchPattern>*. For instance, if the AlertFile parameter is set to *c:\eGurkha\logs\syslog.txt*, and RotatingFile is set to **True**, then, your descriptor will be of the following format: *c:\eGurkha\logs:<SearchPattern>*. On the other hand, if the RotatingFile flag had been set to **False**, then the descriptors will be of the following format: *<FileName>:<SearchPattern>* - i.e., *syslog.txt:<SearchPattern>* in the case of the example above. If this flag is set to **True** and the AlertFile parameter is set to the directory containing log files, then, the descriptors of this test will be displayed in the format: *Configured_ directory_path:<SearchPattern>*. For instance, if the AlertFile parameter is set to *c:\eGurkha\logs*, and rotatingfile is set to **True**, then, your descriptor will be: *c:\eGurkha\logs:<SearchPattern>*. On the other hand, if the RotatingFile parameter had been set to **False**, then the descriptors will be of the following format: *Configured_ directory:<SearchPattern>* - i.e., *logs:<SearchPattern>* in the case of the example above. If this flag is set to **True** and the AlertFile parameter is set to a specific file pattern, then, the descriptors of this test will be of the following format: *<FilePattern>:<SearchPattern>*. For instance, if the AlertFile parameter is set to *c:\eGurkha\logs*sys**, and RotatingFile is set to **True**, then, your descriptor will be: **sys*:<SearchPattern>*. In this case, the descriptor format will not change even if the RotatingFile flag status is changed.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

Parameter	Description
	• The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Recent errors	Indicates the total number of recent errors logged in the log file.	Number	The value of this measure is a clear indicator of the number of “new” alerts that have come into the log file of the monitored server.

Chapter 4: Troubleshooting

If the tests related to the Siebel web server are not running, then first, try connecting to the following URL, and check whether it takes you to a page that lists the session-related and other web server-specific metrics for a configured ApplicationName: http://<IPoftheSibelWebServer>/<applicationnameconfiguredforthetest>/_ stats.swe?verbode=high. For instance, if the IP address of the Siebel web server is, 192.168.10.12, and the ApplicationName configured for a Siebel web server-related test is callcenter, the URL will be: http://192.168.10.12/callcenter/_stats.swe?verbose=high.

If the URL does not result in the display of the desired web page, then proceed to check whether the **AllowStats** and **SessionMonitor** flags in the eapps.cfg file (in the <siebel_ install_ dir>\sea<SIEBEL_VERSION>\SWEApp\BIN directory) are set to true. To know how, refer to .

Also, you can verify the values reported by the tests associated with the Siebel application server component, using the **srvrmgr.exe** in the <SIEBEL_INSTALL_DIR>\sea<Siebel_version>\BIN directory. The syntax for the command is:

```
srvrmgr.exe /g <IPoftheGatewayServer> /e <SiebelEnterpriseServerNameconfiguredforthetest>
/u <UsernameoftheSiebelAdministrator> /p <PasswordoftheSiebelAdministrator> /c "<sub-
command>"
```

For instance, to check whether the statistics reported by the SiebelTasks test are accurate or not, do the following:

- Go to the command prompt of the Siebel application server.
- Switch to the <SIEBEL_INSTALL_DIR>\sea<Siebel_version>\BIN directory.
- Assume that the Siebel Tasks test takes the following parameters:

  GATWAYSERVER- 192.168.10.58

  ENTERPRISESERVER - siebel

  USERNAME - sadmin

  PASSWORD - sadmin

- Then, execute the following command on it:

  ```
  srvrmgr.exe /g 192.168.10.58 /e siebel /u sadmin /p sadmin /c "list tasks",
  ```

  where "list tasks" is the sub-command that is executed for viewing task-related metrics.

Similarly, the command for the SiebelStats test, will be:

```
srvrmgr.exe /g 192.168.10.56 /e siebel /u sadmin /p sadmin /c "list stats"
```

The following command will have to be executed for viewing the list of object managers configured on the Siebel server:

```
srvrmgr.exe /g 192.168.10.56 /e siebel /u sadmin /p sadmin /c "list comps"
```

- For the SiebelNet test, on the other hand, a utility named **visutl.exe** will have to be run from the <SIEBEL_INSTALL_DIR>\sea<SIEBEL_VERSION>\SWEApp\BIN directory. The syntax of this command is:

```
visutl.exe /u <SiebelAdministratorName> /p <SiebelAdministratorPassword> /c
<ODBCDatasourceNameconfiguredforthetest> /d <Tableownernameconfiguredforthetest> /n
<Nodenameconfiguredforthetest>
```

- For instance, assume that you want to verify the accuracy of the measures reported by the SiebelNet test, which takes the following parameters:

  USERNAME - sadmin

  PASSWORD - sadmin

  SIEBELDATASOURCENAME - SiebSrvr_siebel

  TABLEOWNERNAME - siebel

  NODENAME - siebel

  To achieve this, execute the following command from the <siebel_install_dir>\sea<SIEBEL_VERSION>\SWEApp\BIN directory:

```
visutl.exe /u sadmin /p sadmin /c SiebSrvr_siebel /d siebel /n siebel
```

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.