Oracle Enterprise Manager

Plug-in for Oracle Secure Global Desktop User's Guide

ORACLE®

Table of Contents

Preface

The *Enterprise Manager Plug-in for Oracle Secure Global Desktop User Guide* describes how to install and use the Enterprise Manager Plug-in for Oracle Secure Global Desktop in order to monitor Oracle Secure Global Desktop (SGD) resources from within Oracle Enterprise Manager.

1 Audience

This guide is intended for administrators who are familiar with SGD and require access to the comprehensive metrics and performance data that Oracle Enterprise Manager collects for all managed Oracle systems.

2 Document Organization

The document is organized as follows:

- Chapter 1, *Introduction to the Plug-in* is an introduction to the plug-in. Supported versions and requirements are covered in this chapter.

- Chapter 2, *Installing and Configuring the Plug-in* describes how to install and deploy the plug-in. Instructions on how to how to undeploy and uninstall the plug-in are also included.

- Chapter 3, *Monitoring SGD Targets* describes the layout and content of the monitoring pages for the plug-in.

- Chapter 4, *Troubleshooting the Plug-in* includes basic troubleshooting information for the plug-in.

- Chapter 5, *Plug-in Metrics Reference* lists the metrics collected by the plug-in.

3 Related Documents

The documentation for the Oracle Secure Global Desktop product is available at:

http://www.oracle.com/technetwork/documentation/sgd-193668.html

For additional information, see the following manuals:

- *Oracle Secure Global Desktop Administration Guide*

- *Oracle Secure Global Desktop Platform Support and Release Notes*

4 Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1 Introduction to the Plug-in

The Enterprise Manager Plug-in for Oracle Secure Global Desktop extends Oracle Enterprise Manager Cloud Control to add support for monitoring an Oracle Secure Global Desktop (SGD) deployment.

A typical SGD deployment consists of one or more SGD servers, configured as an *array*. The plug-in provides a unified view of the array, helping Administrators to monitor a multi-server deployment.

The plug-in enables integration with SGD by adding an Oracle Secure Global Desktop target type, together with monitoring pages for an SGD array and related resources.

Monitoring pages show a summary of system information, user activity, resource usage, and alerts. A description of the monitoring pages is provided in Chapter 3, *Monitoring SGD Targets*.

For an overview of the architecture, terminology, and components of Oracle Enterprise Manager Cloud Control, see the Oracle Enterprise Manager Cloud Control documentation.

1.1 Requirements for the Plug-in

This section describes the requirements to enable monitoring of an SGD deployment.

1.1.1 Supported Versions

The plug-in supports the following versions of Oracle Enterprise Manager Cloud Control and Oracle Secure Global Desktop:

- Oracle Enterprise Manager Cloud Control 12c Release 4 (12.1.0.4) [1]

- Oracle Secure Global Desktop version 5.2 or later [2]

1.1.2 Prerequisites

Before you install the plug-in, verify that your environment meets these requirements:

- An Oracle Enterprise Manager installation must be running.

- An Oracle Management Agent (Management Agent) must be installed on each SGD host that you want to monitor.

For Oracle Enterprise Manager Cloud Control system requirements and installation instructions, see the Oracle Enterprise Manager Cloud Control installation documentation.

1.1.3 User Requirements

To monitor an SGD array with the plug-in, the following user requirements apply:

- On each SGD host, the Oracle Software Owner User must have an account and must be a member of the `ttaserv` UNIX group.

  The Oracle Software Owner User (typically, `oracle`) is required to install the Oracle Management Agent on the host. For details of the requirements for this user, see the Oracle Enterprise Manager Cloud Control installation documentation.

---

[1] Requires ARU 18654647.
[2] For information on earlier versions of SGD, contact Oracle Support.

The `ttaserv` group contains the SGD server system account users. Adding the Oracle Software Owner User to this group enables the Oracle Software Owner User to run `tarantella` commands.

When you add the Oracle Software Owner User to the `ttaserv` group, ensure that you preserve any existing supplementary groups for this user.

For example, if the Oracle software owner user is `oracle`:

```
# usermod -G group1,group2,ttaserv oracle
```

where *group1* and *group2* are the existing supplementary groups for the `oracle` user.

- A single dedicated SGD Administrator must be available for use with the plug-in.

  You enter the credentials for this user when you add the SGD host as a target in Oracle Enterprise Manager.

  The user must be able to authenticate to SGD using any of the enabled SGD authentication mechanisms.

  The user profile must be shareable. Ensure that the Login: Multiple (`--shared`) attribute is enabled for the user profile object.

  The user must be a member of the Enterprise Manager Agents role.

  In the following example, the user profile object `sgd-agent-user` is added as a member of the Enterprise Manager Agents role.

  ```
  # tarantella role add_member \
  --role "o=Tarantella System Objects/cn=Enterprise Manager Agents" \
  --member "o=Example/cn=sgd-agent-user"
  ```

  Verify that the SGD Administrator user can log in to SGD on each host, and that they can access the SGD Administration Console.

  For more information on how to configure SGD Administrator accounts and roles, see the *Oracle Secure Global Desktop Administration Guide*.

- To monitor an Oracle Secure Global Desktop target, an Oracle Enterprise Manager administrator must have PERFORM_OPERATION privileges for the target. See the Oracle Enterprise Manager Cloud Control documentation for more information on configuring privileges.

Chapter 2 Installing and Configuring the Plug-in

This chapter describes how to install and configure the plug-in in your Oracle Enterprise Manager environment.

> **Note**
>
> This chapter summarises the main steps required to install, deploy, and configure the plug-in. For more detailed instructions, see the Oracle Enterprise Manager Cloud Control documentation.

The following tasks are described in this chapter:

- Downloading and deploying the plug-in to Oracle Enterprise Manager.

  You deploy the plug-in to Oracle Enterprise Manager and to an SGD host.

  See Section 2.1, "Downloading and Deploying the Plug-in".

- Configuring targets for monitoring an SGD host.

  See Section 2.2, "Adding Monitoring Targets".

- Verifying the plug-in installation and deployment.

  See Section 2.3, "Verifying the Plug-in Deployment".

- Uninstalling the plug-in.

  See Section 2.4, "Uninstalling the Plug-in".

2.1 Downloading and Deploying the Plug-in

The plug-in is distributed through the Oracle Enterprise Manager Store.

For detailed steps on how to download and deploy the plug-in, see the Oracle Enterprise Manager Cloud Control Administrator's Guide.

The following is a summary of the required tasks for downloading and deploying the plug-in.

- Download the plug-in to the Management Repository.

  Plug-in Manager in the Enterprise Manager Cloud Control Console shows that the plug-in is available in your environment.

- Deploy the plug-in to Oracle Management Service (OMS).

  This enables the OMS to manage SGD server targets.

- Deploy the plug-in to a Management Agent on an SGD host.

  This enables the Management Agent to discover and monitor SGD server targets.

2.2 Adding Monitoring Targets

After the plug-in is deployed, Oracle Enterprise Manager recognizes monitoring targets of the type *Oracle Secure Global Desktop*. To monitor an SGD array, add all the members of the array individually as monitoring targets.

Before you begin, ensure you the have the credentials of the dedicated SGD Administrator user for the array.

Repeat the following steps for each member of the SGD array.

1. Log in to the Enterprise Manager Cloud Control Console.

2. In the **Setup** menu, select **Add Target**, and then select **Add Targets Manually**.

3. Select **Add Targets Declaratively by Specifying Target Monitoring Properties**.

4. In the **Target Type** list, select Oracle Secure Global Desktop.

5. In the **Monitoring Agent** field, do one of the following:

   • Enter the fully qualified host name and port of the target. For example: `boston.example.com:3872`.

   • Click the search icon to search for an SGD host that is running the Management Agent.

6. Click **Add Manually**. The properties page for the new Oracle Secure Global Desktop target is displayed.

7. Configure the new Oracle Secure Global Desktop target.

   You must complete all of the following fields.

   • **Target Name:** A unique name to identify the monitoring target.

   • **Secure Global Desktop Administrator User Name and Password:** The credentials of the dedicated SGD Administrator for the plug-in.

   • **Secure Global Desktop Installation Directory:** The path to the SGD installation on the host. This is `/opt/tarantella` by default.

   • **Secure Global Desktop Web Services Port:** The TCP port that the SGD web server uses for unsecured web service connections on the localhost interface. This is always port 80, for a default installation of SGD.

8. Click **OK** to save details and add the new target.

9. Ensure that preferred credentials are available for the target.

   The preferred credentials must be for a user account which has privileges to run the `tarantella` command on an SGD server, and is a member of the `ttaserv` UNIX group on the SGD host.

   Credentials for the Oracle Software Owner User (`oracle`) are suitable for this purpose. See Section 1.1.3, "User Requirements" for details of how to configure the `oracle` user on an SGD host.

   For information on how to configure preferred credentials for a target, see the Oracle Enterprise Manager Cloud Control Security Guide.

2.3 Verifying the Plug-in Deployment

After you add the members of an SGD array as monitoring targets, wait at least 15 minutes for the plug-in to start collecting data. Then use the following steps to verify that Oracle Enterprise Manager is correctly monitoring the targets.

1. Log in to the Enterprise Manager Cloud Control Console.

2. From the **Targets** menu, select **All Targets**.

3. In the Refine Search pane, select **Target Type**, then **Servers, Storage and Network**, and then **Oracle Secure Global Desktop**.

   Check that the target is present and that the **Target Status** is Up.

4. Click the name of the target that you want to verify.

   The target home page is displayed.

5. From the **Oracle Secure Global Desktop** menu in the upper-left of the page, select **Monitoring**, and then select **Metric Collection Errors**.

   Check any metric collection errors listed in the table.

6. From the **Oracle Secure Global Desktop** menu, select **Monitoring**, and then select **All Metrics**.

   Click the metrics in the left-hand pane and check that data is being collected.

2.4 Uninstalling the Plug-in

The plug-in can be uninstalled from your Oracle Enterprise Manager environment.

To upgrade the plug-in, simply deploy the new version as shown in Section 2.1, "Downloading and Deploying the Plug-in". Uninstallation is not required before an upgrade.

For detailed steps on uninstalling the plug-in, see the Managing Plug-Ins chapter in the Oracle Enterprise Manager documentation.

Uninstalling the plug-in consists of the following steps:

- (Optional) Unconfigure all Oracle Secure Global Desktop targets.

  It is best to unconfigure targets, to halt data monitoring.

- Undeploy the plug-in.

  When you undeploy the plug-in, Oracle Enterprise Manager can no longer monitor an Oracle Secure Global Desktop target.

- (Optional) Remove the plug-in from the Management Repository.

Chapter 3 Monitoring SGD Targets

When you configure an SGD host as a target, the target name is shown in the All Targets page, a list of all targets that are monitored by Oracle Enterprise Manager.

To display the monitoring pages for an SGD array, select from the available Oracle Secure Global Desktop targets on the All Targets page.

An Oracle Secure Global Desktop target includes the following monitoring pages:

- **Array Overview.** An overview page for the SGD array.

  This is the home page for an Oracle Secure Global Desktop target.

  See Section 3.1, "Monitoring an SGD Array".

- **Array Member.** Monitoring data for an SGD server.

  See Section 3.2, "Monitoring an SGD Server".

- **User.** Monitoring data for users logged in to SGD.

  See Section 3.3, "Monitoring an SGD User".

3.1 Monitoring an SGD Array

The target home page, called the Array Overview monitoring page, provides an overview of metrics and resources for all SGD servers in the array. See Figure 3.1, "Array Overview Monitoring Page".

Figure 3.1 Array Overview Monitoring Page
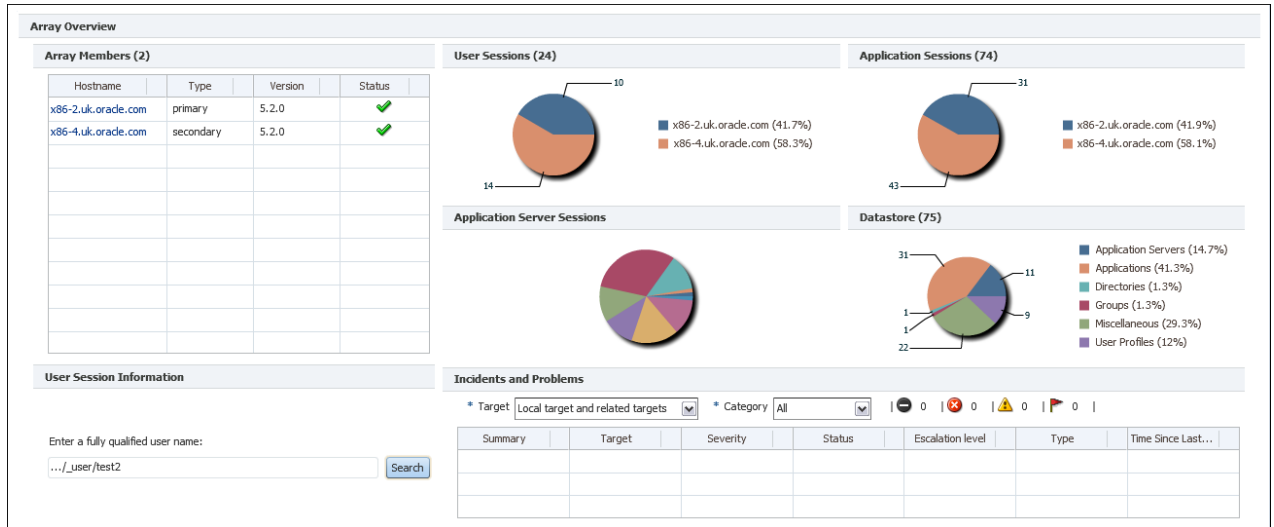
The Array Overview monitoring page includes a series of panels, as described in Table 3.1, "Panels on the Array Overview Monitoring Page".

Table 3.1 Panels on the Array Overview Monitoring Page

Panel	Description
Array Members	A table that lists information about the members of the array, including their role in the array (primary or secondary) and their current status (up or down).

Panel	Description
	The Hostname field is a link to the Array Member monitoring page, where you can view the monitoring information for that array member. See Section 3.2, "Monitoring an SGD Server".
User Session Information	A search field that returns user session and application session information for a user who is logged in to the array.
	Enter the fully qualified name for the user. For example:
	`../_user/o=organization/cn=Indigo Jones`.
	The fully qualified name for an SGD user is shown on the Detailed Diagnostics page of the user's workspace.
	Click on **Search** to display the User monitoring page, where you can view session information for the specified user. See Section 3.3, "Monitoring an SGD User".
User Sessions	A pie chart that shows the distribution of logged in users (user sessions) across the members of the array.
Application Sessions	A pie chart that shows the distribution of running applications (application sessions) across the members of the array.
Application Server Sessions	A pie chart that shows the distribution of application sessions across the application servers.
Datastore	A pie chart that shows the distribution of SGD objects in the local repository. The objects are classified according to their SGD object type.
Incidents and Problems	A table that shows system messages relating to incidents and problems for the SGD array.
	For more information about managing incidents in Oracle Enterprise Manager, refer to the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

3.2 Monitoring an SGD Server

The Array Member monitoring page enables you to view monitoring data for a specific SGD server in an array. See Figure 3.2, "Array Member Monitoring Page".

Figure 3.2 Array Member Monitoring Page

The Array Member monitoring page includes a series of panels, as described in Table 3.2, "Panels on the Array Member Monitoring Page".
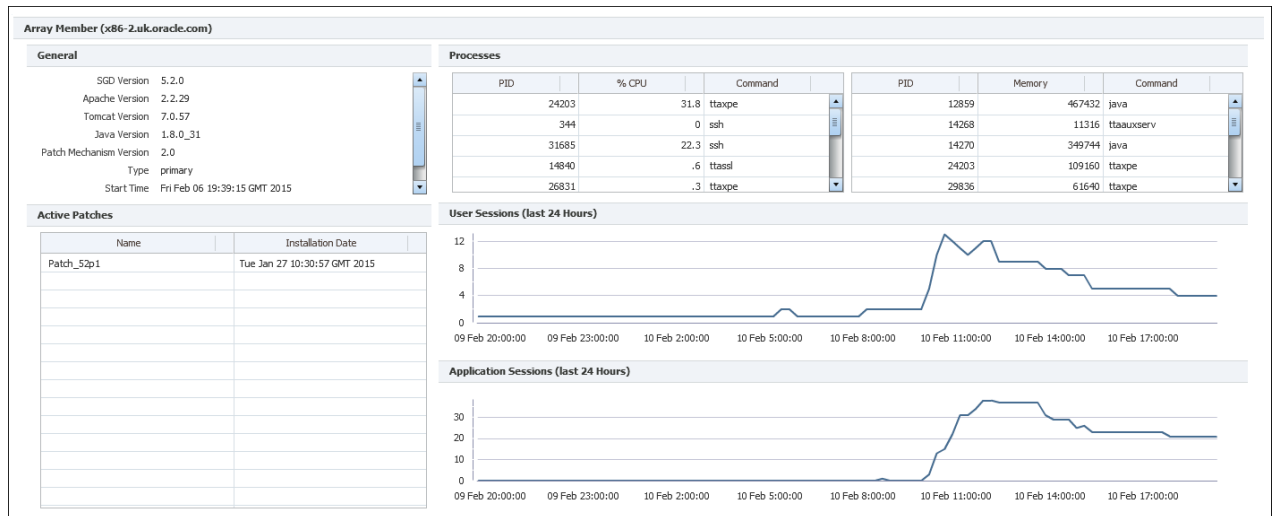
Table 3.2 Panels on the Array Member Monitoring Page

Panel	Description
General	Shows software versions and status information for the array member.
User Sessions (last 24 hours)	A line chart that shows the number of user sessions running on the array member. The chart shows the history of session statistics over the last 24 hours.
Application Sessions (last 24 hours)	A line chart that shows the number of application sessions running on the array member. The chart shows the history of session statistics over the last 24 hours.
Processes	A table that shows CPU and memory usage statistics for SGD processes running on the array member. The 10 processes with the highest CPU and memory usage are displayed.
Active Patches	A table that shows details of the SGD software patches installed on the array member.

3.3 Monitoring an SGD User

The User monitoring page shows real-time monitoring data for an SGD user who is logged in to the array. Information on user session activity and applications started by the user are displayed on this page. See Figure 3.3, "User Monitoring Page".

This page is shown when you search for user details, using the User Session Information search field on the Array Overview page. See Section 3.1, "Monitoring an SGD Array".

Figure 3.3 User Monitoring Page
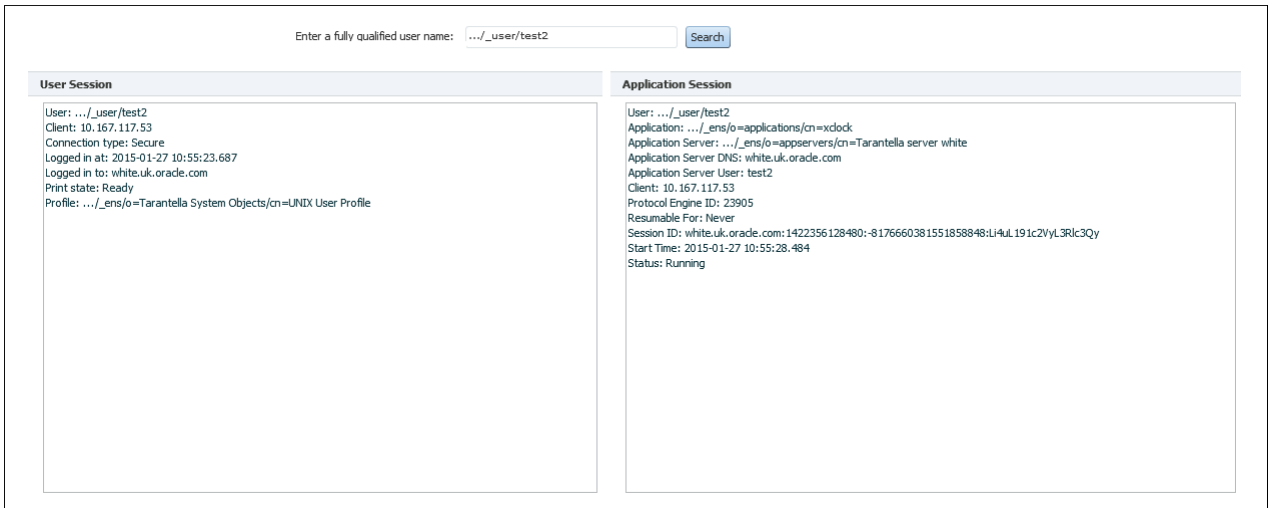
The User monitoring page includes a series of panels, as described in Table 3.3, "Panels on the User Monitoring Page".

Table 3.3 Panels on the User Monitoring Page

Panel	Description
User Search	A search field that returns user session and application session information for a user who is logged in to the array.
	Enter the fully qualified name for the user. For example:
	`../_ens/o=organization/cn=Indigo Jones`.
	The fully qualified name for an SGD user is shown on the Detailed Diagnostics page of the user's workspace.
User Session	Shows details for the user session associated with the specified user.
Application Session	Shows details of current application sessions for the specified user.

Chapter 4 Troubleshooting the Plug-in

This chapter provides basic information and links to additional resources to assist you in troubleshooting issues with the plug-in and tuning the performance of the plug-in.

4.1 Plug-in Log Files

When you are troubleshooting issues with the plug-in, the following logs may contain useful information.

- **Oracle Enterprise Manager Cloud Control logs.** Logging is available for the Oracle Management Service (OMS) and Management Agents.

  For more details about Oracle Enterprise Manager logging, see the Locating and Configuring Enterprise Manager Log Files chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

- **SGD web server logs.** Log messages for the Tomcat JSP technology container component of the SGD web server are written to log files in the `/opt/tarantella/webserver/tomcat/tomcat-version/logs` directory on the SGD host.

4.2 Plug-in Installation and Deployment Issues

The following topics describe how to troubleshoot issues when installing and deploying the plug-in.

4.2.1 Oracle Enterprise Manager Installation Issues

If you encounter problems during installation of the plug-in, verify that all prerequisites are met. See Section 1.1, "Requirements for the Plug-in".

For information on installing Oracle Enterprise Manager, refer to the Oracle Enterprise Manager Cloud Control documentation.

4.2.2 Plug-in Deployment Issues

The following troubleshooting tips may apply when you are having issues with deploying the plug-in:

- If you encounter problems when adding an SGD target, verify the settings for communication between the Management Agent and the SGD host. See Section 2.2, "Adding Monitoring Targets".

- If a target is shown as down in the Enterprise Manager Cloud Control Console, try the following:

  - Check the status of the SGD server on the target host.

    Run the `tarantella status` command on the SGD host.

    For more information about troubleshooting SGD issues, see the *Oracle Secure Global Desktop Administration Guide*.

  - Verify that the plug-in is working correctly and that metrics are being collected.

    Display the All Metrics page for the target and click on a metric in the left-hand pane.

    An error message is shown if there is an issue with metrics data collection.

4.3 Configuring Metrics Collection

The following topics describe how to configure and tune metrics collection for the plug-in.

4.3.1 Changing Metrics Collection Intervals

All metrics collection intervals are configurable. To set a different collection schedule for a target, do the following:

- Display the Metric and Collection Settings page for the target.

  In the target menu, select **Monitoring**, then select **Metric and Collection Settings**.

- Change the collection interval for one or more metrics.

  In the **Collection Schedule** column, click a collection interval to change the setting.

4.3.2 Changing Event Thresholds

Many metrics collected by the plug-in have predefined thresholds and incident messages. When a threshold is crossed, an incident is reported by means of an alert message in the Incidents and Problems table for the target.

To change an event threshold for a target, do the following:

- Display the Metric and Collection Settings page for the target.

  In the target menu, select **Monitoring**, then select **Metric and Collection Settings**.

- Change the thresholds for an event.

  Edit the settings in the **Warning Threshold** or **Critical Threshold** columns.

4.3.3 Viewing Real-Time Metrics Data

The data displayed on the monitoring page for a target is retrieved from the Management Repository. This is not real-time information.

To see the real-time metrics data, as it is collected by the Monitoring Agent, view the All Metrics page for the target.

4.4 Metrics Collection Issues

The following issues are related to error messages shown when collecting metrics.

Duplicate Request ID Error

Problem: The following error is shown when loading the home page for a Secure Global Desktop target.

```
Error during operation: MetricDataService.getMetricData
Duplicate Request ID (hostname-metadata)
```

where *hostname* is the name of the array member.

The Array Member table on the home page does not display any information.

Cause: This error is shown when multiple targets have been configured to monitor the same array member.

Solution: The workaround is to delete any redundant targets for the array member. Configure a single target only for each array member.

Chapter 5 Plug-in Metrics Reference

This section contains a list of metrics collected by the plug-in. Examples of typical metrics are included.

Plug-in metrics data can be processed by reporting tools such as Oracle Business Intelligence Publisher.

The following types of metrics are collected by the plug-in:

- **Performance metrics.** Examples of performance metrics include user session and application session data.

  Performance metrics are typically collected at short intervals, such as every 15 minutes.

  See Section 5.1, "Performance Metrics".

- **Configuration metrics.** Examples of configuration metrics include SGD patch and component software versions.

  Performance metrics are typically collected at long intervals, such as every 24 hours.

  See Section 5.2, "Configuration Metrics".

5.1 Performance Metrics

The following performance metrics are collected by the plug-in.

AppServerSessions

Column	Type	Description	Example
AppServer	STRING (KEY)	Host name of application server	app1.example.com
EmulatorSessionCount	NUMBER	Number of running application sessions (emulator sessions) for the application server	*number*
XProtocolEngineCount	NUMBER	Number of running X Protocol Engines for the application server	*number*
CharacterProtocolEngineCount	NUMBER	Number of running Character Protocol Engines for the application server	*number*

ArrayMembers

Column	Type	Description	Example
Hostname	STRING (KEY)	Host name of the array member	newyork.example.com
Type	STRING	Whether the array member is a primary sever or secondary server	primary
Status	STRING	Current status for the array member	accepting_std_ssl
StartTime	STRING	When the array member was started	Wed Jul 16 13:09:04 BST 2014

ArraySummary

Column	Type	Description	Example
ArrayMembersCount	NUMBER	Number of array members	*number*
WebtopSessionCount	NUMBER	Number of running user sessions (webtop sessions) for the array	*number*
EmulatorSessionCount	NUMBER	Number of running application sessions (emulator sessions) for the array	*number*
XProtocolEngineCount	NUMBER	Number of running X Protocol Engines for the array	*number*
CharacterProtocolEngineCount	NUMBER	Number of running Character Protocol Engines for the array	*number*

DatastoreApplicationCount

Column	Type	Description	Example
Total	NUMBER	Number of application objects in the SGD datastore	*number*

DatastoreApplicationServerCount

Column	Type	Description	Example
Total	NUMBER	Number of application server objects in the SGD datastore	*number*

DatastoreDirectoryCount

Column	Type	Description	Example
Total	NUMBER	Number of directory service objects in the SGD datastore	*number*

DatastoreGroupCount

Column	Type	Description	Example
Total	NUMBER	Number of group objects in the SGD datastore	*number*

DatastoreObjectCount

Column	Type	Description	Example
Total	NUMBER	Number of objects of all types in the SGD datastore	*number*

DatastoreUserProfileCount

Column	Type	Description	Example
Total	NUMBER	Number of user profile objects in the SGD datastore	*number*

ProcessesByCPU

The 10 SGD processes with the highest CPU usage.

Column	Type	Description	Example
ID	STRING (KEY)	Unique ID for the process, between 1 and 10. Corresponds to the CPU usage ranking.	*5*
PID	NUMBER	Process ID for the process	*number*
User	STRING	User who owns the process	ttasys
CPU	NUMBER	CPU usage for the process, as a percentage	0.3
MEM	NUMBER	Memory usage for the process, in bytes	57732
Command	STRING	Command line for the process	/opt/tarantella/bin/bin/ttaxpe /opt/tarantella/var/log

ProcessesByMEM

The 10 SGD processes with the highest memory usage.

Column	Type	Description	Example
ID	STRING (KEY)	Unique ID for the process, between 1 and 10. Corresponds to the memory usage ranking.	*5*
PID	NUMBER	Process ID for the process	*5*
User	STRING	User who owns the process	ttasys
CPU	NUMBER	CPU usage for the process, as a percentage	0.3
MEM	NUMBER	Memory usage for the process, in bytes	57732
Command	STRING	Command line for the process	/opt/tarantella/bin/bin/ttaxpe /opt/tarantella/var/log

Response

Column	Type	Description	Example
Status	NUMBER	Whether the SGD server is up or down	1

SessionsCount

Column	Type	Description	Example
SGDServer	STRING (KEY)	Host name of the SGD server	newyork.example.com
WebtopSessions	NUMBER	Number of running user sessions (webtop sessions) for the SGD server	*number*
EmulatorSessions	NUMBER	Number of running application sessions (emulator sessions) for the SGD server	*number*

Column	Type	Description	Example
XApplications	NUMBER	Number of running graphical applications for the SGD server	*number*
CharacterApplications	NUMBER	Number of running character applications for the SGD server	*number*

5.2 Configuration Metrics

To process configuration metrics data, use the `OSGD` plug-in tag with the table name. For example, to process version metrics use the following string:

```
OSGD_VERSIONS
```

The following configuration metrics are collected by the plug-in.

PATCHES

Column	Type	Description	Example
PATCH_NAME	STRING (KEY)	Name of installed SGD software patch	Patch_50p1
INSTALL_DATE	STRING	Date and time when patch was installed	Tue Jan 21 16:18:08 GMT 2014

VERSIONS

Column	Type	Description	Example
SGD_VERSION	STRING	SGD version	5.10.907
JAVA_VERSION	STRING	Java technology version	1.7.0_65
APACHE_VERSION	STRING	Apache web server version	2.2.24
TOMCAT_VERSION	STRING	Tomcat JSP container version	7.0.42
PATCH_MECH_VERSION	STRING	SGD patch mechanism version	1.3