Oracle® Enterprise Manager

System Monitoring Plug-in Installation Guide for IBM DB2 Database

Release 12.1.0.2.0

E25215-03

September 2012

This document provides a description about the Oracle System Monitoring Plug-In for IBM DB2 Database, details on the versions the plug-in supports, prerequisites for installing the plug-in, and step-by-step instructions on how to download, install, verify, and validate the plug-in.

Description

The System Monitoring Plug-in for IBM DB2 Database extends Oracle Enterprise Manager Cloud Control to add support for managing IBM DB2 UDB (LUW) database instances. By deploying the plug-in in your Cloud Control environment, you gain the following management features:

- Monitor DB2 Database instances.
- Gather configuration data and track configuration changes for DB2 database instances.
- Raise alerts and violations based on thresholds set on monitored targets and configuration data.
- Provide rich, out-of-box reports based on the gathered data.
- Support monitoring by a remote Agent. Local Agent is an agent running on the same host as the DB2 database. Remote Agent is an agent running on a host that is different from the host where DB2 database is running.

Platforms Supported

The plug-in supports monitoring of IBM DB2 UDB (LUW) on all the platforms where IBM DB2 UDB can be installed.

Versions Supported

This plug-in supports the following versions of products:

- Enterprise Manager 12*c* Cloud Control Release 1 (12.1.0.1.0) or higher
- Single-partition IBM DB2 Universal Database (UDB) for Linux, UNIX, and Windows (LUW) Version 8.2 FixPak 2 and above (8.2.x ,9.x.x)

Prerequisites

The following prerequisites must be met before you can use the plug-in:

- Install the following:
  - Enterprise Manager 12*c* Cloud Control Release 1 (12.1.0.1.0) or higher (Oracle Management Service and Oracle Management Agent)
  - IBM DB2 Universal JDBC Type 4 driver for IBM DB2 Database (see Setting Up the JDBC Driver)
  - IBM DB2 Universal Database
- Create a suitable operating system user to access the table functions used in IBM DB2. For information about creating a user, see Using a Suitable Operating System User and Assigning Authorities and Privileges.
- To avoid metric collection errors for *Database Monitoring* metrics, create the table `STMG_DBSIZE_INFO`. For more information, see Configurations Required for Avoiding Metric Collection Errors for Database Monitoring Metrics.
- If you want to generate alerts using the IBM DB2 Diagnostic Log file (db2diag.log), then do the following:
  - Define your match patterns in the `Diag_log_file_match_pattern_file.txt` file that is present in `$ORACLE_HOME/plugins/oracle.em.sidb/scripts/emx/ibm_db2_database/`.
  - Define your ignore patterns in the `Diag_log_file_no_match_pattern_file.txt` file that is present in `$ORACLE_HOME/plugins/oracle.em.sidb/scripts/emx/ibm_db2_database/`.
  - Set the `DIAG_PATH` configuration paramater of the database manager (instance) to correspond to the monitored IBM DB2 database.

  Based on the patterns defined in the two files, the System Monitoring Plug-in for IBM DB2 parses the Diagnostic Log file and generates alerts for the satisfied conditions. First, the plug-in validates the two files to see if any patterns are defined. If no patterns are defined, then the plug-in does not parse the Diagnostic Log file. If matching patterns are not defined, but ignore patterns are defined, then the plug-in parses every entry in the Diagnostic Log file and checks if ignore patterns are satisfied. If matching patterns are also defined, then the plug-in first parses only those entries that satisfy the matching patterns, and then for those satisfied entries, the plug-in checks if ignore patterns are satisfied.

  Also, if multiple log entries having the same function name are encountered in a collection, then only one alert is generated to represent the function name. This alert is based on the last log entry with a common function name, present in the Diagnostic Log file.

  > **Note:** This feature is supported only for local monitoring, that is, when the IBM DB2 database on a host is monitored by an Oracle Management Agent that is running on the same host.

- In the IBM DB2 Database SQL Statement Performance and IBM DB2 Database Applications Lock Performance reports and the Agent Monitoring metric, in order to see the SQL statement text along with the application name, enable the instance configuration parameter DFT_MON_STMT. Otherwise, you may not see any data in the column.

- As part of JDBC URL, either IP Address or host name can be provided. Ensure that the host name can be resolved consistently on the network. Standard TCP tools such as "nslookup" and "traceroute" can be used to verify the host name. Validate using the following commands on Management Agent where plug-in is deployed:

  - `nslookup <hostname>`

    This returns the IP address and fully qualified host name.

  - `nslookup <IP>`

    This returns the IP address and fully qualified host name.

Setting Up the JDBC Driver

The JDBC driver is available from IBM, and consists of the following files that the Agent must be able to access:

- `db2jcc.jar`
- `db2jcc_javax.jar`
- `db2jcc_license_cu.jar`

To set up the `AGENT_BASE_DIR` directory for the IBM DB2 Universal Type 4 JDBC driver:

1. If it does not already exist, create the directory `$AGENT_BASE_DIR/plugins/dependencies/oracle.em.sidb/jdbcdriver/`.
2. Copy the three JDBC driver files into the directory `$AGENT_BASE_DIR/plugins/dependencies/oracle.em.sidb/jdbcdriver/`.

Configure the Management Agent to Deploy the Plug-In

To configure the Agent,you must first ensure that the user starting the Agent service belongs to the Local Administrators Group. Also, you must set the preferred credentials on all Agents where you want to deploy the plug-in. To do so, follow the instructions given in the following sections.

Assigning Advanced Privileges to User

To assign advanced privileges, do the following:

1. Locally on the Microsoft Windows node hosting the Agent, check that the user starting the Agent service belongs to the Local Administrators Group. If not, add it.
2. Open the Local Security Settings Windows Tool and give the following Advanced Privileges to the user starting the Agent service:
   - Act as part of the operating system
   - Adjust memory quotas for a process
   - Logon as batch job
   - Replace a process level token

3. Restart the Agent service if it is running.

4. Set the Preferred Credentials for the Host and the Agent in Cloud Control. For more information, see Setting and Validating Preferred Credentials.

   - The OS user set in the Preferred Credentials must belong to the Local Administrators Group.
   - This OS user must have the following Advanced Privileges:
     - Act as part of the operating system
     - Adjust memory quotas for a process
     - Log on as batch job
     - Replace a process level token

Setting and Validating Preferred Credentials

To set the preferred credentials on all Agents where you want to deploy the plug-in, do the following:

1. In Enterprise Manager Cloud Control, from the **Setup** menu, select **Security**, then **Preferred Credentials**.

   The Preferred Credentials page appears, showing a table of targets.

2. Select Host target type from the table and then click **Managed Preferred Credentials**.

   The Host Preferred Credentials page appears.

3. In the Host Preferred Credentials page, in the Target Credentials section, select the host that is running the Management Agent where the plug-in has to be deployed, and click **Set**.

4. In the Select Named Credential dialog box, Select Credential as **New** and specify the user name and password and click **Test and Save**. If your test runs successfully, your credentials are set correctly.

5. Run the OS Command job for the Management Agent where the plug-in has to be deployed.

   - Log in to Enterprise Manager Cloud Control.
   - From the Enterprise menu, select **Job** and then **Activity**.
   - In the Job Activity page, from the Create Job list, select **OS Command**, and click **Go**.
   - Fill up the details required in the following pages, and click **Submit** to run the job. If the job runs successfully, your credentials are set correctly.

Using a Suitable Operating System User and Assigning Authorities and Privileges

The System Monitoring Plug-In for IBM DB2 accesses the table functions used in IBM DB2. For the plug-in to have access to the table functions, you have to use a suitable operating system user and assign this new user to a user group. The operating ssytem user must have at least the minimum privileges. In addition, you have to assign the correct authority levels to this user.

Note: IBM DB2 users must be operating system users. IBM DB2 cannot have its own database users because it relies on the host operating system for security.

If you do not have an operating system user already created, first, create one on the host where IBM DB2 is running. Then, follow these steps to assign this user to a new or existing UserGroup.

1. Open the IBM DB2 Control Center.
2. From the tree view, select the database or database alias to which you want to connect.
3. Connect as an admin user.
4. From the tree view, select **User and Group Objects**.
5. From the right pane, select the already-created operating system user.
6. From the Authorities panel, select **Connect to Database**.
7. To verify the applied changes, try connecting to the database.

Note: These steps can also be performed from command line using IBM DB2 SQL.

Also, assign authorities and privileges for the operating system UserGroup. The authorities supported with IBM DB2 are SYSADM, SYSCTRL, SYSMAINT, DBADM, and LOAD. The SYSADM, SYSCTRL, and SYSMAINT authorities cannot be granted using the GRANT SQL statement. These special authorities can only be set from the database manager configuration file. DBADM privilege can only be granted by user at SYSADM authorization level.

SYSMON authority level is required to monitor IBM DB2. This level is required to access the table functions, such as SYSPROC.SNAPSHOT_DATABASE, which are used in IBM DB2.

Follow these steps to set SYSMON authority level to your UserGroup:

1. At the db2=> prompt, run the following commands:

   ```
   db2=> update dbm cfg using sysmon_group USERGROUP
   db2 => db2stop
   db2 => db2start
   ```

2. To check whether the changes are effective, run the following command:

   ```
   db2 => get dbm cfg
   ```

   The following will be the output of the previous command:

   ```
   Database Manager Configuration
   Node type = Enterprise Server Edition with local and remote clients
   .....
      SYSADM group name     (SYSADM_GROUP)   =
      SYSCTRL group name    (SYSCTRL_GROUP)  =
      SYSMAINT group name   (SYSMAINT_GROUP) =
      SYSMON group name     (SYSMON_GROUP)   = USERGROUP
   ......
   ```

Note: To understand how authorities and privileges are implemented in IBM DB2, access the IBM web site.

Deploying the Plug-in

See the *Plug-in Manager* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to deploy the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm

Configuring IBM DB2 for Health Indicator Metrics and Database Monitoring Metrics

The following sections explain the postinstallation configuration steps you need to perform on IBM DB2.

Configurations Required for Health Indicator Metrics

The health indicators for instance and database objects are enabled and disabled using the database manager configuration parameter -- HEALTH_MON. Then, the table functions -- HEALTH_TBS_HI, HEALTH_DB_HI, and HEALTH_DBM_HI get populated. These functions are used by the plug-in to show the alerts triggered based on the thresholds of health indicators.

Note: Enabling these settings may result in some overheads, such as CPU and memory. Therefore, follow these steps only if you want to view the Health Indicator metrics.

To enable or disable the `HEALTH_MON` by CLP (Command Line Processor), run the following command:

```
db2==> update dbm cfg using HEALTH_MON [on;off]
```

To check if your changes are effective, run the following command:

```
db2==> get dbm cfg
```

The following is the output:

```
.....
.....
.....
Monitor health of instance and databases (HEALTH_MON) = ON
.....
.....
.....
```

For more information, access the IBM web site.

Configurations Required for Avoiding Metric Collection Errors for Database Monitoring Metrics

To avoid metric collection errors for for the "Database Monitoring" metrics, make a call to the GET_DBSIZE_INFO package so that the STMG_DBSIZE_INFO table gets created and populated with the required data.

The GET_DBSIZE_INFO procedure calculates the database size and maximum capacity. The calculated values are returned as procedure output parameters and cached in the SYSTOOLS.STMG_DBSIZE_INFO table. The procedure caches these values because the calculations are costly.

The SYSTOOLS.STMG_DBSIZE_INFO table is created automatically the first time the procedure runs. If there are values cached in the SYSTOOLS.STMG_DBSIZE_INFO table and they are current enough, as determined by the snapshot-timestamp and refresh-window values, then these cached values are returned.

If the cached values are not current enough, new cached values are calculated, inserted into the SYSTOOLS.STMG_DBSIZE_INFO table and returned, and the snapshot-timestamp value is updated. The last parameter in the GET_DBSIZE_INFO call is refresh window.

Default value refresh window (time difference between successive calls) is 30 minutes. If your database is growing at a faster rate, then you can set a lower value.

To make a call to GET_DBSIZE_INFO by CLP (Command Line Processor), run the following command:

```
db2==>CALL GET_DBSIZE_INFO(?, ?, ?, -1)
```

In this case, the refresh window is 30 minutes.

For more information, access the following page on the IBM Web site:

http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.sql.rtn.doc/doc/r0011863.html

Adding Instances for Monitoring

After successfully deploying the plug-in, follow these steps to add the plug-in target to Cloud Control for central monitoring and management:

1. From the **Setup** menu, select **Add Target** and then **Add Targets Manually**.
2. In the Add Targets Manually page, select **Add Non-Host Targets by Specifying Target Monitoring Properties**, select **Target Type** as **IBM DB2 Database**, select a **Monitoring Agent** and click **Add Manually**.
3. Provide the following information for the properties:
   - **Target Name** — Name for the plug-in
   - **JDBC URL** — URL name for the IBM DB2 JDBC Driver connectivity.

     For example,

     `jdbc:db2://<server>:<port>/<database>`

     The JDBC URL argument represents a data source. Parameter definitions are as follows:

  - **jdbc:db2** — Indicates that the connection is to a DB2 UDB server.
  - server — Domain name or IP address of the database server.
  - port — TCP/IP server port number assigned to the database server, which is an integer between 0 and 65535.
  - database — Database alias, which refers to the DB2 database catalog entry on the DB2 client.

    database is the database name defined during DB2 UDB (LUW) installation.

- **JDBC Driver** — (Optional) Name of the DB2 Universal JDBC Driver.

  For example:

  ```
  com.ibm.db2.jcc.DB2Driver
  ```

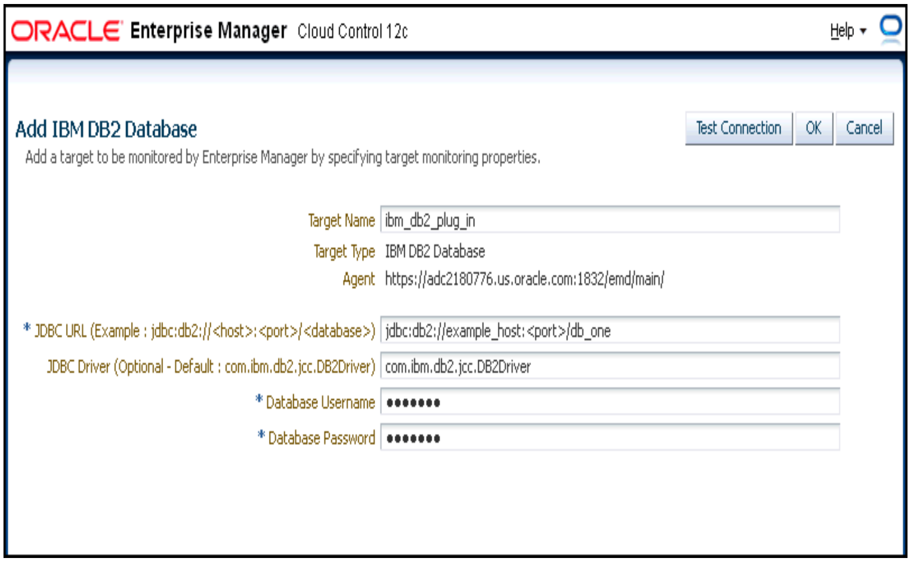
- **Database Username** — Valid user name for the database.

  For more information, see Using a Suitable Operating System User and Assigning Authorities and Privileges.

- **Database Password** — Password for the user.

4. Click **Test Connection** to make sure the parameters you entered are correct.

Figure 1 Add IBM DB2 Database



Add IBM DB2 Database

Add a target to be monitored by Enterprise Manager by specifying target monitoring properties.

Target Name	ibm_db2_plug_in
Target Type	IBM DB2 Database
Agent	https://adc2180776.us.oracle.com:1832/emd/main/
* JDBC URL (Example : jdbc:db2://<host>:<port>/<database>)	jdbc:db2://example_host:<port>/db_one
JDBC Driver (Optional - Default : com.ibm.db2.jcc.DB2Driver)	com.ibm.db2.jcc.DB2Driver
* Database Username	•••••••
* Database Password	•••••••

Note: After you deploy and configure the plug-in to monitor one or more targets in the environment, you can customize the monitoring settings of the plug-in. This alters the collection intervals and threshold settings of the metrics to meet the particular needs of your environment. If you decide to disable one or more metric collections, this could impact the reports that the metric is a part of.

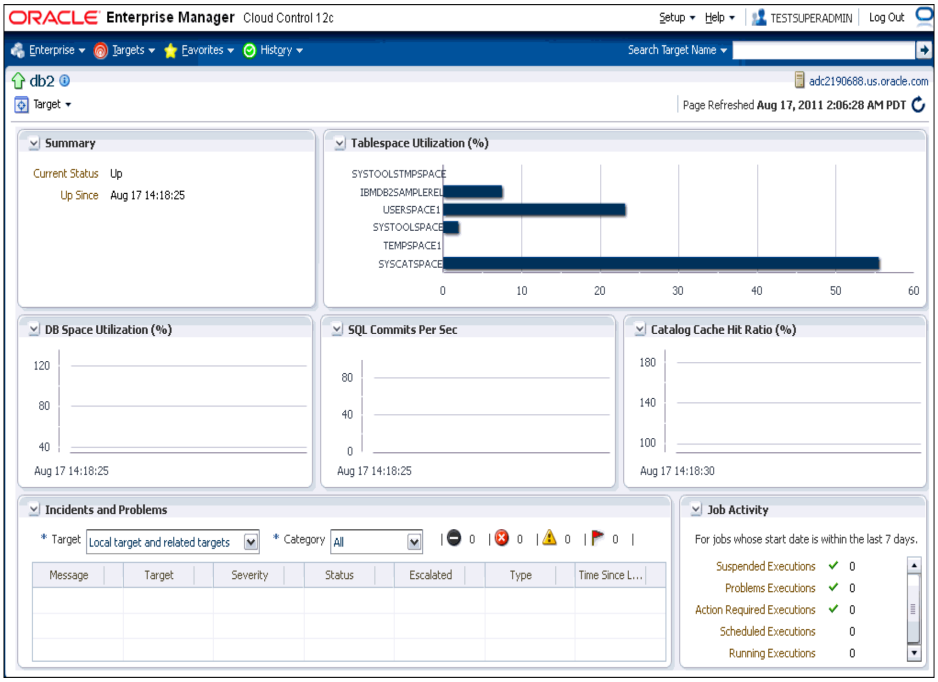
Verifying and Validating the Plug-in

After waiting a few minutes for the plug-in to start collecting data, follow these steps to verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. Click the IBM DB2 Database target link from the All Targets page.

   The IBM DB2 Database home page appears.

Figure 2 IBM DB2 Database Home Page



Page Refreshed **Aug 17, 2011 2:06:28 AM PDT**

Current Status Up

Up Since Aug 17 14:18:25

* Target Local target and related targets

* Category All

| 0 | 0 | 0 | 0 |

Message	Target	Severity	Status	Escalated	Type	Time Since L...

For jobs whose start date is within the last 7 days.

Suspended Executions	✓	0
Problems Executions	✓	0
Action Required Executions	✓	0
Scheduled Executions		0
Running Executions		0

2. Verify that no metric collection errors are reported by clicking **Monitoring** and then **Metric Collection Errors** from the **Target** menu.

3. Ensure that reports can be seen and no errors are reported by clicking **Information Publisher Reports** in the **Target** menu and viewing reports for the IBM DB2 Database target type.

4. Ensure that configuration data can be seen by clicking **Configuration** and then **Last Collected** in the **Target** menu. If configuration data does not immediately appear, click **Refresh** in the Latest Configuration page.

Undeploying the Plug-in

See the *Plug-in Manager* chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to deploy the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm

Troubleshooting the Plug-In

For information about the troubleshooting scenarios that you might encounter while working with the System Monitoring plug-ins, see the *Oracle Enterprise Manager System Monitoring Plug-in Troubleshooting Guide*.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

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

System Monitoring Plug-in Installation Guide for IBM DB2 Database, Release 12.1.0.2.0
E25215-03