DBPLUS
better performance

DBPLUS
Performance Monitor for Oracle
description of changes in version 2022.3

Date: October 10, 2022

DBPLUS
better performance

Table of Contents

Below is a list of changes to the DBPLUS Performance Monitor system for Oracle database monitoring.

New in 2022.3 version

1 Anomaly monitor – improvements

Anomaly monitor mechanism is a module responsible for automatic real-time detection of performance problems in the monitored database.

Report

The Anomaly Monitor report has been modified in the latest version. This report is available at the instance details level in the *Anomaly Monitor - Reports menu*. The change was to the default version of the report. Users can still create and modify their own versions of the report.

The changes concern the presentation of information on the general performance characteristics of the instance, as well as the presentation of information on the main performance problems detected in the instance in the period for which the report was prepared.

Analysis of locking problems

The problem of locks is one of the most common performance problems in relational databases. In the Performance Monitor application, there is an Anomaly Monitor module in which occurrences of events detected by the application affecting the performance of the monitored instance are presented. One of the series of events is Locks.
In the latest version, in addition to sealing the mechanism for collecting locks, functionality was added to verify the causes of locks. The following scenarios have been distinguished in the application:

High locking due to sleeping session

The problem caused by leaving an inactive session with an open transaction that holds unapproved changes in the database. The problem cannot be solved on the database server side. Application code, connection and transaction management should be verified to resolve the problem.

High locking due to long transaction

The problem caused by opening a long transaction in the database. The process causing the locking and the application code should be verified. The recommendation is to split the process into using shorter database transactions. In addition, verify the transaction isolation mode and check whether the blocked queries, used optimal execution plans.

High locking due to long running statement

A problem caused by a long-running query (or a large number of executions). Verify the query's statistics, performance and execution plan.

High locking due to long transaction or processing on application site

Problem caused by opening a long-running database transaction or application-side processing. The process and application code should be verified. Recommendation is to split the process to use shorter database transactions. In addition, verify the transaction isolation mode and check whether the blocked queries, used optimal execution plans.

High locking due to processing on application site

Problem caused by application-side processing. Verify the process and application code. In addition, check whether the blocked queries, used optimal execution plans.
If any of the scenarios occurs, information about the event will be presented in the application on the Dashboard screen, Anomaly Monitor as well as other screens available in the application.
In addition, information on the cause of the blockages will be available in the report for the period in which the problems described above occurred.

Note that information on the causes of locks requires additional data collection during monitoring. Therefore, the causes of blockages will be visible only for problems that were detected after the application was updated to the latest version.

Anomaly detection improvements

In the latest version of the application, we have improved and added several new detections and alerts. Below is a list of some of them.

High waits problem

If there is an increase in the level of waits in the instance monitoring, information about such an event will be presented in the form of an alert. Depending on the type of wait, the information on the problem is also dependent on the decrease in the performance of the instance.

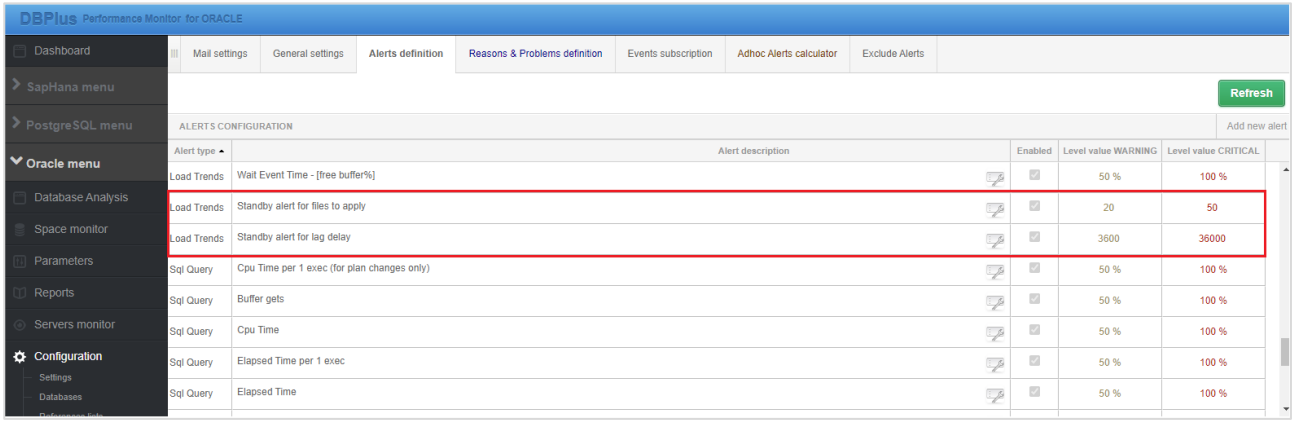
CPU problem

A new detection related to high CPU load by instances has been added. The high CPU problem will occur when the threshold of 50% of the CPU load available on the machine is exceeded, as well as when there is an increase in CPU utilization by queries executed on the monitored instance.

Monitor Standby process alerts

In the latest version, we have added alerts that monitor the operation of the Standby mechanism. The alert is based on two definitions:

- Number of files to process (files to apply)
- The delay between the Standby and Primary bases (lag delay)

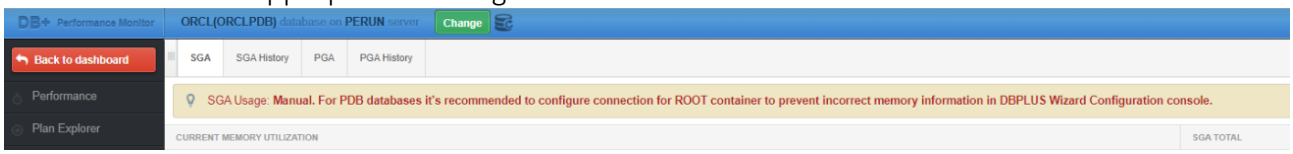


The definitions are available from the ***Configuration - Alert Settings - Alerts definition menu***. The categories have been given default predefined values: number of files - Warning value: 20 and Critical value: 50, as well as delay - Warning value: 3600 and Critical value: 36000.
The values stored in the definitions can, of course, be freely changed in the settings, globally for all monitored databases or to a single database.

Information about exceeding the alarm threshold will be presented on the Dashboard screen as well as from the level of details of a given database on the Database Load screen and Anomaly monitor (Alerts browser).

2 Memory support for container databases

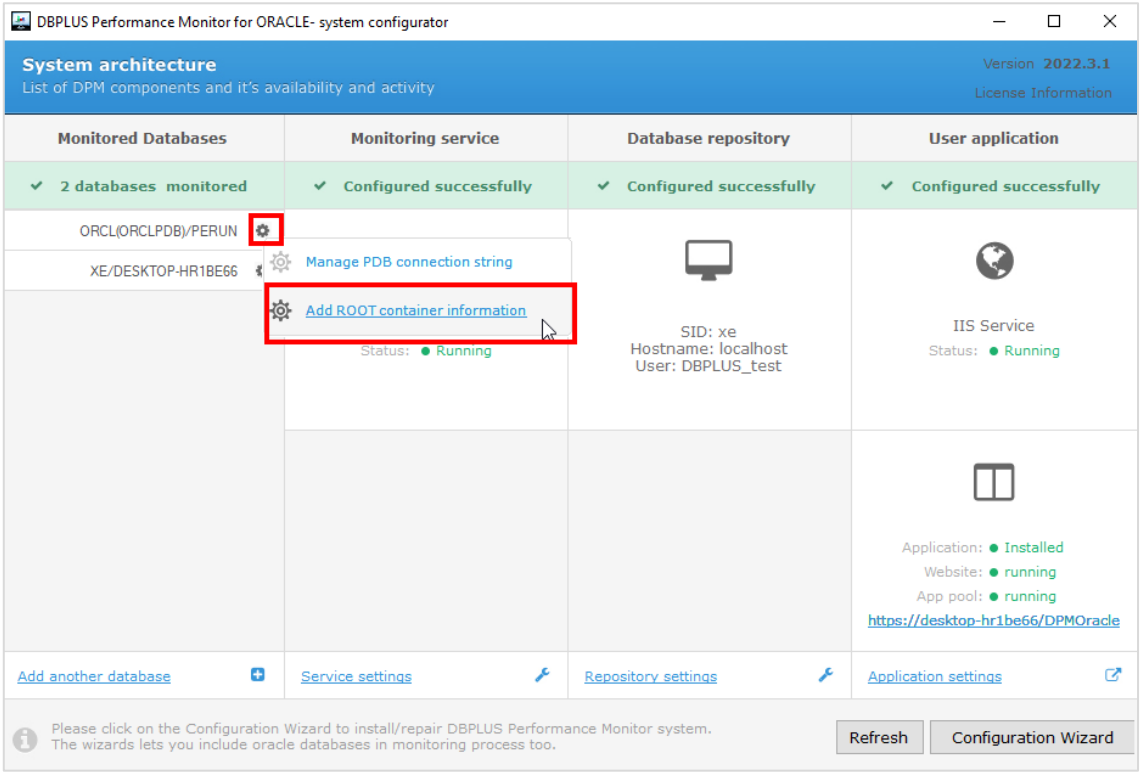
In the latest version, we have improved the memory monitoring mechanism for container databases. Memory monitoring of container databases in some cases could be incorrectly presented due to the lack of information available only from the level of the "root" database. The current mechanism verifies the status of connection of databases to the monitoring and detects whether the "root" bases are also connected to the monitoring.
In the event that the "root" database is not connected to the monitoring, then from the level of the container base the appropriate message will be visible:



For proper operation of memory monitoring for the container base, you only need to enter the configuration of the "root" database or connect the "root" database to monitoring from the Configuration Wizard level.

Configuration of the "root" database

From the Configuration Wizard, click from the [Settings] button for the container database. Then select options to [Add ROOT conteiner information].



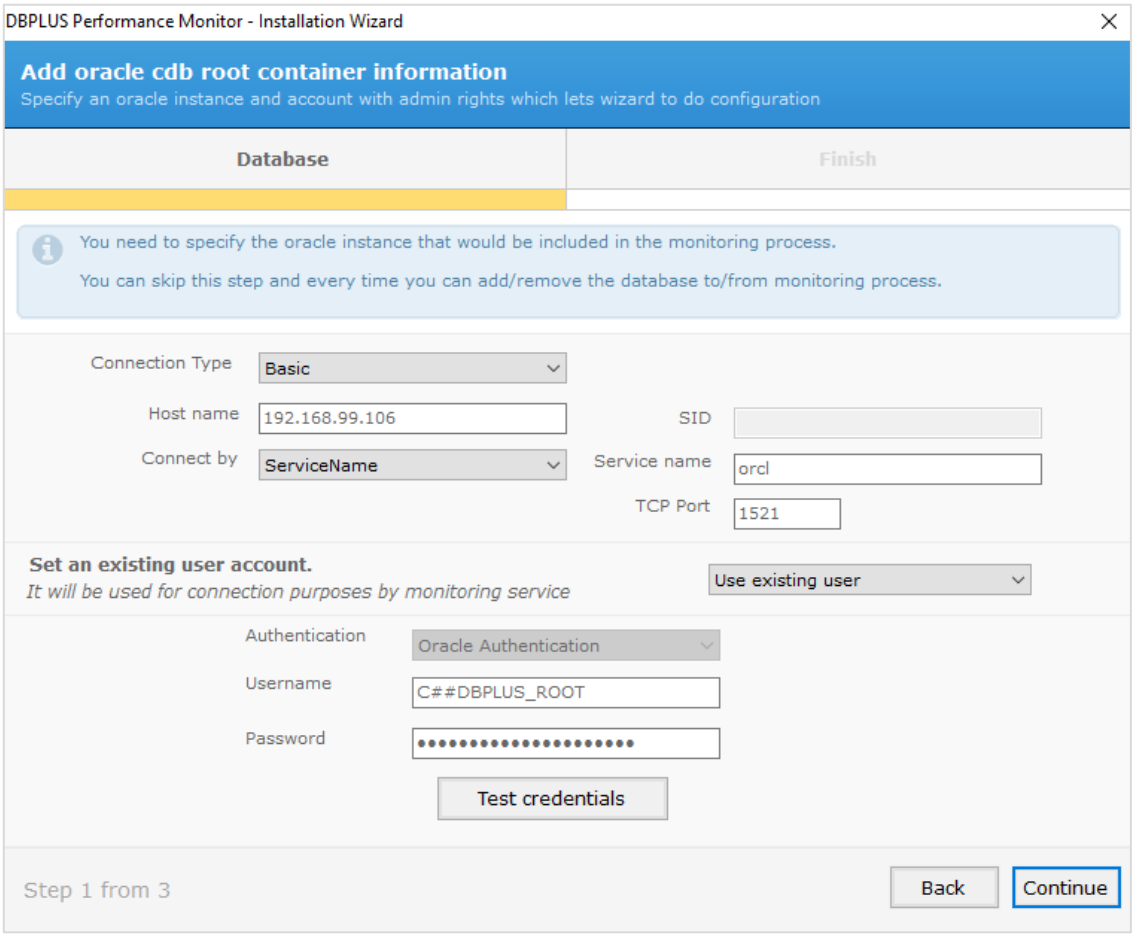
A standard configuration window will open in which we enter the data needed to connect to the ROOT database. We have two standard connection options to choose from:
- adding a new user

- using an existing user

If you choose an existing user, he/she must meet the minimum permissions:

- CONNECT
- SELECT_CATALOG_ROLE

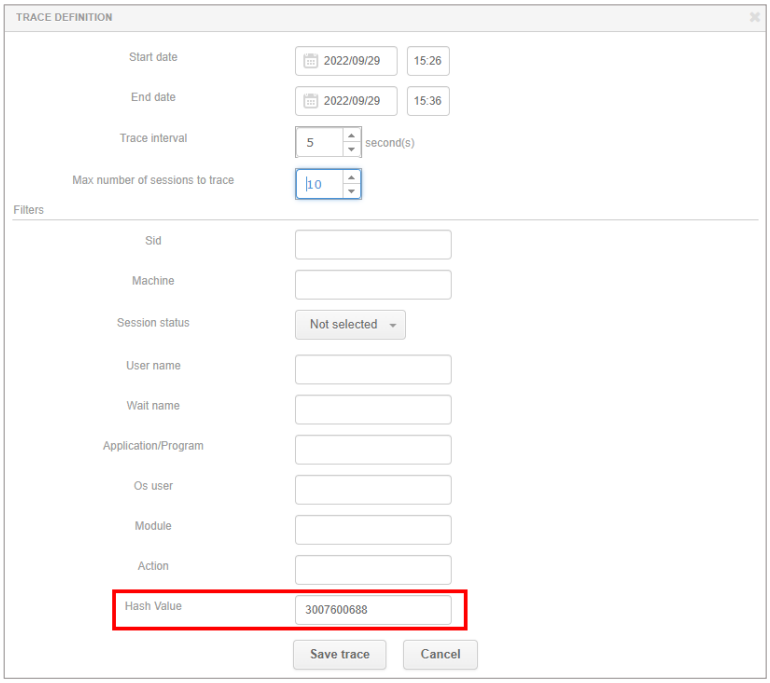
Note: Configuration of the ROOT base from the container base does not require an additional license. ROOT base is not monitored



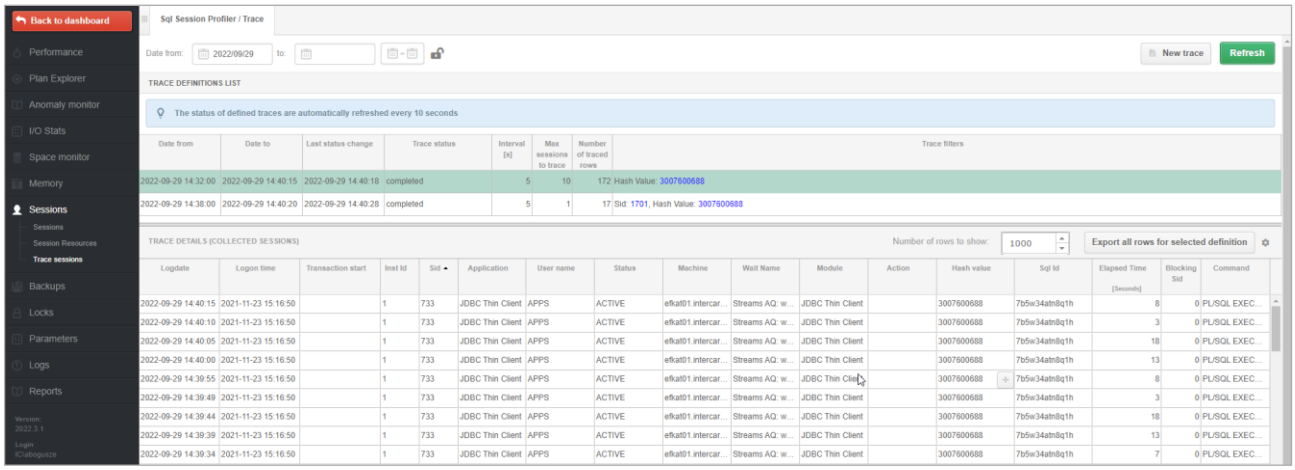
In the scenario when the ROOT database is also connected to the monitoring, you do not need to additionally configure the connection from the container base. The application will detect the configurations on its own.

3 Trace session - filter by Hash value

In the latest version, the mechanism has been extended by the possibility to search for user sessions which, at the time of verification, execute the query indicated in the filter. The collected data can be analyzed from the application level or exported to *.csv file.



Result for trace using Hash value in filter:



4 Query advisor functionality update

In the latest version of the application, we have introduced further changes to the automatic query performance verification mechanism. In the new version, a verification of the query plan with which the query is currently executed and a comparison with the one generated by the Query Advisor algorithm has been added. The mechanism now calculates its query plan and compares it with the current plan with which the query is executed on the database. If a more optimal path is detected, such information will be presented on the application screen.

Another change is to improve the algorithm that calculates HINT suggestions for queries.
In addition, in case a query is executed outside the monitored database (the REMOTE option in the execution plan), such queries will not be taken into account by the Query Advisor algorithm.

The functionality is available from the details of a given query on the SQL Details - Show Plan Objects - Parse SQL Query screen.

5 Improvements and enhancements

5.1. Dashboard screen host name update fix.

The problem of updating database and server names has been fixed. The problem was related to the scenario of switching databases between a server. On the Dashboard screen, the server name was not refreshed after switching.

5.2. Improved functionality of Standby Monitor

We corrected a problem related to the operation of the Standby mechanism causing a problem with the collection of data on the performance of the monitored instance.