













Eg: Jdbc\_Example\_With\_Prepared\_Statement

//go through the code

Eg: Jdbc\_Example\_With\_Prepared\_Statement\_Eg2

// go through the code

Eg: Jdbc\_Example\_With\_Prepared\_Statement\_Eg3

// go through the code

Advantages of PreparedStatement:

1. Performance is very high compared to Statement approach because query will be compiled only once.

2. Since we don't send the query multiple times b/w java application and database traffic will be reduced.

3. inputs to the query need not be supplied at the beginning dynamically we can supply the inputs.

4. inputs to the query can be supplied just like java style, no need to perform formatting as per the DB specification.

5. Best suitable for inserting Date values.

6. Best suitable for insertion of BLOB's and CLOB's (image and pdf files).

7. It prevents SQLInjection Attack.

Limitation of PreparedStatement :

Statement stmt = connection.createStatement();

stmt.executeUpdate("insert into student values () ... ");

stmt.executeQuery("select \* from student");

stmt.executeUpdate("delete from student where .... ");

One statement object can be used to execute mulitple query but with no change in inputs.

PreparedStatement pstmt = connection.prepareStatement("select \* from student");

pstmt.executeQuery();

One PreparedStatement object is restricted to only one query, that query can be executed multiple times with change in input.

Which of the following represent valid statements ?

1. delete from employee where ename = ?(valid)

2. delete from employee ? ename = ? (invalid)

3. delete from ? where ename = ? (invalid)

4. delete ? employees where ename = ?(invalid)

Note: we can use ? only in the place of input values and we cannot use in the place of sql keywords, tablenames and column names.

Static query vs Dynamic query

The sql query without positional parameter(?) is called static query.

eg: delete from employee where ename = 'sachin';

The sql query with positional parameter(?) is called dynamic query

eg: delete from employee where ename = ?

select eid,ename,esal from employee where esal > ?

Note:

Simple Statement object can be used for static queries, where as Preparedstatement object can be used for static queries and dynamic queries also.