Database Performance Analyzer

Version 11.0
Table of Contents

Introduction .............................................................................................................................................. 1
DPA architecture ....................................................................................................................................... 1
  Two key functions of the DPA server ........................................................................................................ 1
  Monitored database instances .................................................................................................................. 2
  Monitored virtualization environment ........................................................................................................ 2
DPA licensing ............................................................................................................................................ 3
  Purchase licenses ..................................................................................................................................... 3
  License types .......................................................................................................................................... 3
    Database instance licenses ..................................................................................................................... 3
      Category 1 licenses ............................................................................................................................... 3
      Category 2 licenses ............................................................................................................................... 4
    Azure SQL Database license .................................................................................................................. 4
    VM Option licenses ............................................................................................................................... 4
  All licenses are floating ............................................................................................................................. 4
  Licensing recommendations for clustered environments ......................................................................... 4
View purchased licenses ............................................................................................................................ 5
Activate and allocate your licenses ........................................................................................................... 5
  Activate licenses online ............................................................................................................................ 5
  Activate licenses offline ............................................................................................................................ 6
Allocate licenses to database instances ..................................................................................................... 6
  View current license allocation ................................................................................................................ 7
  Allocate licenses to database instances to monitor and collect information ............................................. 7
Allocate VM licenses to VM database instances ........................................................................................ 7
Deallocate licenses ..................................................................................................................................... 7
Deactivate your DPA licenses ...................................................................................................................... 7
Deactivate online .............................................................. 8
Deactivate offline ............................................................ 8
Troubleshoot over-allocated licenses .................................... 8

Register a database instance for monitoring ............................ 9
  Self-Managed .................................................................... 9
  Amazon RDS .................................................................... 9
  Azure ................................................................................ 9
  Register an Oracle database .............................................. 9
  Register a SQL Server database ........................................ 13
  Register a Sybase database ............................................... 16
  Register a DB2 database .................................................. 18
  Register a MySQL database ............................................ 21
  Register an Amazon RDS for Oracle database .................. 25
  Register an Amazon RDS for SQL Server database .......... 28
  Register an Amazon RDS for MySQL or Aurora database .... 30
  Register an Azure SQL database ..................................... 34
    Enable deadlocks for read-only geo-replicas .................. 37

Update a monitored database instance ................................. 38

Unregister a monitored database instance ............................. 39

Users and groups .................................................................. 40
  Create a user .................................................................... 40
  Create a group .................................................................. 40
  User authentication options .......................................... 40
    AD user authentication .................................................. 41
    LDAP user authentication ............................................ 41
    Single sign-on ............................................................ 41
    Common Access Cards ................................................ 41
  Configure Active Directory or LDAP ................................. 41
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection information</td>
<td>41</td>
</tr>
<tr>
<td>Domain name</td>
<td>41</td>
</tr>
<tr>
<td>Port</td>
<td>42</td>
</tr>
<tr>
<td>User and Password</td>
<td>42</td>
</tr>
<tr>
<td>Did the connection test fail?</td>
<td>42</td>
</tr>
<tr>
<td>Base search location</td>
<td>42</td>
</tr>
<tr>
<td>Base DN</td>
<td>42</td>
</tr>
<tr>
<td>Advanced settings</td>
<td>42</td>
</tr>
<tr>
<td>Summary</td>
<td>43</td>
</tr>
<tr>
<td>Configure authentication and permissions for groups of users</td>
<td>44</td>
</tr>
<tr>
<td>Log in to DPA</td>
<td>44</td>
</tr>
<tr>
<td>Reports</td>
<td>45</td>
</tr>
<tr>
<td>Access reports in DPA</td>
<td>45</td>
</tr>
<tr>
<td>Report types</td>
<td>46</td>
</tr>
<tr>
<td>Create a Top SQL Statements report</td>
<td>47</td>
</tr>
<tr>
<td>Schedule a report for email delivery</td>
<td>47</td>
</tr>
<tr>
<td>Alerts</td>
<td>49</td>
</tr>
<tr>
<td>Access alerts in DPA</td>
<td>49</td>
</tr>
<tr>
<td>Alert categories</td>
<td>49</td>
</tr>
<tr>
<td>Wait Time</td>
<td>49</td>
</tr>
<tr>
<td>Resources</td>
<td>50</td>
</tr>
<tr>
<td>Administrative</td>
<td>50</td>
</tr>
<tr>
<td>Custom</td>
<td>50</td>
</tr>
<tr>
<td>Alert attributes</td>
<td>50</td>
</tr>
<tr>
<td>SNMP alerts</td>
<td>51</td>
</tr>
<tr>
<td>Create an SNMP contact</td>
<td>51</td>
</tr>
<tr>
<td>Alert on increases in SQL wait times</td>
<td>52</td>
</tr>
<tr>
<td>Determine the average execution time of your queries</td>
<td>52</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Create an alert based on the wait threshold</td>
<td>52</td>
</tr>
<tr>
<td>Advanced analysis</td>
<td>54</td>
</tr>
<tr>
<td>Stop monitoring a database instance for a period of time</td>
<td>54</td>
</tr>
<tr>
<td>Enable SNMP Monitoring in SCOM</td>
<td>54</td>
</tr>
<tr>
<td>Automatic grouping of Oracle CDBs</td>
<td>55</td>
</tr>
<tr>
<td>Turn off automatic grouping of Oracle CDBs</td>
<td>55</td>
</tr>
<tr>
<td>Link together separate DPA servers</td>
<td>56</td>
</tr>
<tr>
<td>Set up a Central Server</td>
<td>56</td>
</tr>
<tr>
<td>Configure authentication for Central Server</td>
<td>56</td>
</tr>
<tr>
<td>Log in with a SolarWinds DPA user</td>
<td>56</td>
</tr>
<tr>
<td>Log in with an Active Directory or LDAP user</td>
<td>56</td>
</tr>
<tr>
<td>Add remote DPA servers</td>
<td>57</td>
</tr>
<tr>
<td>View the Central Server page</td>
<td>57</td>
</tr>
<tr>
<td>Central Server advanced configuration</td>
<td>57</td>
</tr>
<tr>
<td>General Central Server settings</td>
<td>58</td>
</tr>
<tr>
<td>Thread pool settings</td>
<td>59</td>
</tr>
<tr>
<td>Client factory cache</td>
<td>59</td>
</tr>
<tr>
<td>Troubleshooting tips</td>
<td>61</td>
</tr>
<tr>
<td>DPA solutions</td>
<td>62</td>
</tr>
<tr>
<td>Identify the top three query problems</td>
<td>62</td>
</tr>
<tr>
<td>Correlate response time with system resources</td>
<td>64</td>
</tr>
<tr>
<td>Determine wait bottlenecks that delay response time</td>
<td>64</td>
</tr>
<tr>
<td>Identify Waits for the top SQL queries</td>
<td>66</td>
</tr>
<tr>
<td>Diagnose current performance issues</td>
<td>67</td>
</tr>
<tr>
<td>The DPA worksheet</td>
<td>68</td>
</tr>
</tbody>
</table>
**Introduction**

You can use SolarWinds Database Performance Analyzer (DPA) to monitor, diagnose, and resolve performance problems for Oracle, SQL Server, MySQL, DB2, Sybase, and Azure SQL databases.

SolarWinds DPA has [agentless architecture](#) and uses [wait-based analytics](#) for extended database monitoring. SolarWinds DPA uses less than one percent of resources on production systems.

ℹ️ For installation information, see the [DPA Installation Guide](#). To upgrade DPA, see the [DPA Upgrade Guide](#).

**DPA architecture**

SolarWinds Database Performance Analyzer consists of:

- A SolarWinds DPA server
- A SolarWinds DPA repository database
- One or more database instances you want to monitor

The SolarWinds DPA server collects performance data from a set of database instances you choose to monitor. SolarWinds DPA stores this data in the repository database.

For optimal performance, the DPA server, repository database, and the monitored database instances must reside on the same high-speed LAN. If your environment contains database instances that are on separate LANs, SolarWinds recommends [creating a repository database](#) on each LAN. For cloud monitoring, SolarWinds recommends deployment to the same region.

The SolarWinds DPA server provides a web interface that displays performance data in a web browser from any computer with access to the SolarWinds DPA server.

SolarWinds recommends installing one SolarWinds DPA instance on a computer. If you must install multiple instances on the same computer, [submit a support ticket](#).

**TWO KEY FUNCTIONS OF THE DPA SERVER**

- Collect data from the monitored database instances and store the data in the repository database.
- Provide a web interface that displays performance data from any computer with access to the SolarWinds DPA server. From this interface, you can configure monitoring, alerting, and email reports.
MONITORED DATABASE INSTANCES

SolarWinds DPA remotely connects to each database instance using Java Database Connectivity (JDBC). SolarWinds DPA causes less than 1% overhead on the instance. No software is installed on the monitored server.

MONITORED VIRTUALIZATION ENVIRONMENT

In a virtual environment, SolarWinds DPA can remotely connect to each VMware vCenter Server, ESX, or ESXi host. SolarWinds DPA causes less than 1% overhead on the monitored systems. No software is installed in the vCenter Server, ESX or ESXi host, or virtual machines.
DPA licensing

SolarWinds DPA has a 14-day evaluation license. During the evaluation period, you can monitor and view data for an unrestricted number of database instances. After the evaluation period, to continue monitoring you must purchase the correct quantity and type of licenses for your database instances.

- DPA has its own licensing and does not work with SolarWinds License Manager.

Purchase licenses

Contact our sales team to purchase licenses directly from SolarWinds.

- Only buy licenses for active database instances. Standby database instances used for disaster recovery or high availability do not need licenses.

  - Online quote tool
  - sales@solarwinds.com
  - 866.530.8100

License types

Each database instance you monitor with SolarWinds DPA requires a license. You must buy a database instance license for each database instance you monitor. In addition, you can buy virtual machine licenses to monitor the virtual infrastructure hosting a database instance.

- To purchase licenses, contact the SolarWinds sales team.

DATABASE INSTANCE LICENSES

SolarWinds sells licenses by category according to the database edition they are authorized to monitor.

CATEGORY 1 LICENSES

- Oracle: all editions except Standard and Express
- Sybase: all editions except Express
- DB2: all editions except Express
- All Category 2 database types
CATEGOR Y 2 LICENSES

- Oracle: Standard and Express editions (including Amazon RDS)
- SQL Server: all editions (including Amazon RDS)
- MySQL: all editions (including Amazon RDS and Aurora)
- Sybase: Express edition
- DB2: Express edition

If you run out of Category 2 licenses, you can use Category 1 licenses instead. Category 1 licenses can monitor all database types.

AZURE SQL DATABASE LICENSE

- Azure SQL Database: all editions, including databases in elastic pools

If you run out of Azure SQL Database licenses, you can use Category 1 or Category 2 licenses instead.

VM OPTION LICENSES

- The VM option enables the DPA virtualization feature. This license is an add-on to a Category 1 or Category 2 license.

Purchase optional VM licenses to see information related to the virtual infrastructure of database instances in the Virtualization view. You can use one license to see VM-related information for one database instance.

A VM license can be applied only to a database instance for which you purchased a database instance license.

ALL LICENSES ARE FLOATING

You can register more instances than you have licenses for. On the license allocation page, assign the licenses to the instances you want to monitor.

DPA does not collect data from registered database instances that are not licensed. You can view previously collected data on those instances, however.

LICENSING RECOMMENDATIONS FOR CLUSTERED ENVIRONMENTS

To get the maximum value from DPA, SolarWinds recommends:

- For SQL Server availability groups (AGs), use either of the following options:
  - Register each SQL Server instance in the cluster. This option is recommended if there are multiple AGs in the cluster, because it ensures that DPA does not monitor the same instance more than once. DPA monitors all activity on each instance, including primary and secondary AG activity.
With this option, DPA does not follow AGs when they fail over. Therefore, monitor all instances in the cluster to ensure monitoring continuity when failovers occur.

- Register the AG listener.
  Use this option if you want to monitor activity on the instance that contains the primary replica of an AG. When the AG fails over, DPA follows the listener and begins monitoring the SQL Server instance that now contains the primary replica.
  SolarWinds recommends registering only one listener per cluster unless you can ensure the primary replica of multiple AGs will not be on the same instance. If you register multiple listeners whose primary replica could be on the same instance, this results in duplicate monitoring which is not recommended.

SQL Server logins are not automatically replicated. To enable DPA to continue monitoring after a failover, you must manually create the DPA login on all instances in the cluster.

- For Oracle RAC, register every instance in the cluster.
- For Oracle RAC with Data Guard, register both environments but only monitor the primary one. If a failover occurs, simply reassign the licenses to the instances in the secondary RAC environment.

Every environment is different, so talk with your SolarWinds representative for other options.

View purchased licenses

View your SolarWinds DPA licenses in the SolarWinds Customer Portal.

The licenses for your SolarWinds DPA product are in the License Management section of the Customer Portal. The licenses are listed by category.

- Category 1 is for Oracle, Sybase, and DB2.
- Category 2 is for Oracle Standard and Express, SQL Server, MySQL, Sybase Express, and DB2 Express.
- Azure SQL Database is for all editions of Azure SQL, including databases in elastic pools.

Activate and allocate your licenses

ACTIVATE LICENSES ONLINE

2. Choose License Management > License Management.
3. Locate the license, and expand it.
4. Copy the activation key.
5. On the SolarWinds DPA home page, click License Management. Then click License Manager.
6. Click Enter Activation Key.
7. Select Online Activation, and click Next.
8. On the Online Activation page, paste the activation key into the correct field.
9. In the Amount to Activate section, select All Available or Specify Amount.

Unactivated licenses can be activated later. You can reuse an activation key on a different SolarWinds DPA server and activate remaining licenses there.

10. Enter the remaining information, and click Activate.

### ACTIVATE LICENSES OFFLINE

Offline activation requires a transfer of files between the SolarWinds DPA server and a computer connected to the Internet. You can use email, shared storage, or a USB flash drive.

1. In SolarWinds DPA, click License Management > License Manager.
2. Click Enter Activation Key.
3. Select Offline Activation, and click Next.
4. On the Offline Activation page, copy the text string next to the license type you want to activate, and save it to a text file. This is your unique machine ID. Include the brackets. For example:
   
   `[7R12-X2QN-U8XM-WXTD-23H7-0TD7-59QH-6ERF-5BRN-2M17-328G-0DT2-MNMS-005C-000Z-04Q2-0000]`

5. Transfer this text file to a computer with Internet access.
7. Locate the license, and expand it.
8. Click Activate license manually.
9. Paste the text string into the Unique Machine ID field, and enter the other required information.
10. Click Generate License File to download the license file.
11. Transfer the license file to the SolarWinds DPA server.
12. On the Offline Activation page, click Choose File and browse to the license file you just transferred.
13. Click Activate.

### ALLOCATE LICENSES TO DATABASE INSTANCES

Use License Allocation to configure how your licenses are allocated to database instances. Allocate your SolarWinds DPA licenses to your registered database instances. SolarWinds DPA starts monitoring new instances immediately after you allocate your licenses. Category 1, Category 2, and Azure SQL Database licenses collect the data shown in the Performance view. VM licenses collect the data shown in the Virtualization view.
VIEW CURRENT LICENSE ALLOCATION

1. On the DPA home page, click License Management.
2. See the current license allocations in the summary boxes near the top of the License Allocation page.

ALLOCATE LICENSES TO DATABASE INSTANCES TO MONITOR AND COLLECT INFORMATION

1. On the License Allocation page, find the instance you want in the list of registered database instances.
2. Select the Cat 1, Cat 2, or Azure check box next to the instance.
3. Click Save.
   The license count is updated after you allocate a license.

ALLOCATE VM LICENSES TO VM DATABASE INSTANCES

If you have VM licenses, you must allocate a license to each database instance you want to collect virtual infrastructure-related data from. VM licenses are an addition to the regular SolarWinds DPA licenses required to normally monitor the database instance.

1. On the License Allocation page, locate a VM-hosted database instance that has a Category 1 or 2 license allocated to it.
2. Select the VM check box next to the instance.
3. Click Save.

DEALLOCATE LICENSES

Deallocate licenses to make licenses available to register other database instances. Clear the Cat 1, Cat 2, or Azure check box to deallocate licenses.

If you clear a Category 1 or 2 license from an instance that also has a VM license, SolarWinds DPA automatically clears the VM license as well.

Deactivate your DPA licenses

Deactivate licenses on a SolarWinds DPA server to make the licenses available elsewhere.

If your DPA server has direct access to the internet, you can deactivate licenses online.

Evaluation licenses and temporary keys cannot be deactivated. License deactivation is supported in DPA 9.0 and later.
DEACTIVATE ONLINE

1. On the DPA home page, click License Management > License Manager.
2. In the Licenses section, locate the License Key you want to deactivate.
3. Click Deactivate.

DEACTIVATE OFFLINE

To deactivate a license offline in SolarWinds DPA 10.0 or earlier, contact SolarWinds customer support.

To deactivate a license offline in SolarWinds DPA 10.1 and later:

1. From the SolarWinds DPA home page, click License Management > License Manager.
2. Click Deactivate next to the license.
3. Click Yes to confirm the offline deactivation, and download the deactivation receipt file.
4. Log in to the SolarWinds Customer Portal, and go to the License Management page.
5. Select the DPA instance, and click Deactivate license manually.
6. On the Manage License Deactivation page, browse for the deactivation receipt file, and click Upload.

Troubleshoot over-allocated licenses

A red banner displays on the home page if SolarWinds DPA is monitoring more registered database instances than you have licenses to monitor. This can happen in two situations:

- A license expires when you have unexpired licenses of the same type on the server.
- You deactivate a license and have other licenses of the same type on the server.

If SolarWinds DPA licenses are over-allocated, you cannot view or analyze your database instances until you deallocate the extra licenses. SolarWinds DPA continues monitoring the databases, so you will not lose data while you bring the allocated licenses to an allowable level.

To correct an issue of over-allocated licenses, deallocate database instances until you reach the proper number of licenses. If Category 2 licenses are over-allocated, assign available Category 1 licenses to cover the shortage. If Azure SQL Database licenses are over-allocated, assign Category 1 or 2 licenses to cover the shortage.

1. On the DPA home page, click License Management.
2. Locate the over-allocated license type on the allocations chart. Over-allocated license types are shown in red.
3. Clear Cat 1, Cat 2, Azure, or VM check boxes until the chart is no longer red.
4. Click Save.
   You should now see your database instances in your views.
Register a database instance for monitoring

Select the type of database instance you want to register for monitoring by DPA:

**SELF-MANAGED**

- Oracle
- Microsoft SQL Server
- SAP Sybase ASE
- DB2 UDB
- MySQL

**AMAZON RDS**

- Amazon RDS for Oracle
- Amazon RDS for SQL Server
- Amazon RDS for MySQL or Aurora

**AZURE**

- Azure SQL DB

**Register an Oracle database**

To register an Oracle database for DPA to monitor:

1. On the DPA home page, click Register DB Instance for Monitoring.
2. Under Self-Managed, click Oracle.
3. Click Next.
4. Complete the wizard panels as described in the following table.
## Panel: Enter Monitored Database Instance Connection Information

**Instructions:**

SolarWinds DPA monitors all databases within the instance. If more than one instance exists on the server, you must register each instance separately in DPA.

Oracle database instances have three connection options:

- **Direct Connect**
- **Transparent Network Substrate (TNS) Connect Descriptor**
- **Lightweight Directory Access Protocol (LDAP) or TNS Name**

### Direct Connect

Enter the Service Name or System Identifier (SID), host name or IP address, and port. The default port is 1521.

### TNS Connect Descriptor

The Connect Descriptor value contains everything after `NAME=` in the `tnsnames.ora` file. The beginning `(DESCRIPTION=` is necessary. For example:

```sql
(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = demo.confio.com)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = demo)))
```

### LDAP OR TNS Name

To use this option, Oracle Name Resolution must be configured. For instructions, see [Connect to Oracle using name resolution](#).

After you configure Oracle Name Resolution, you can use the LDAP/TNS Name when registering additional monitored database instances.

SolarWinds DPA uses the Oracle network configuration `.ora` files to connect to the database instance.

If connection information other than the name has changed, update the `.ora` files. SolarWinds DPA detects changes to these files automatically. You do not have to update the connection information through this wizard.

If the name has changed, update the `.ora` files. Then select the check box next to LDAP/TNS Name, and update the value.
<table>
<thead>
<tr>
<th><strong>Panel</strong></th>
<th><strong>Instructions</strong></th>
</tr>
</thead>
</table>
| Enter Monitored Database Instance Connection Information (continued) | **RAC Instances**  
If this is an Oracle Real Application Clusters (RAC) instance, there may be listener configuration changes needed if you are not listening on the physical IP address. SolarWinds recommends:  
- If you are registering pluggable databases (PDBs) on a RAC instance, consider registering with the physical IP address of the host.  
- If you are registering a non-PDB RAC instance, consider registering with the SID.  
- If you are using the Service Name, consider using the physical IP address of the host. Do not use the virtual IP address (VIP) or the Oracle Single Client Access Name (SCAN) IP address. |
| **DBA User** | Enter DBA credentials for SolarWinds DPA to register the database instance. |
| Enter the Monitoring User | **Create or specify the account that DPA will use to gather information. To ensure that the account has the required permissions, SolarWinds recommends creating a new account.**  
To create a new account:  
1. Next to Create Monitoring User, click Yes.  
2. Enter the user name and password.  
3. Select a Tablespace and Temp Tablespace on the monitored database. This is primarily used for gathering Explain Plan data for monitored queries.  
To specify an existing account:  
1. Next to Create Monitoring User, click No.  
2. Enter the user name and password.  
If you create the user manually, DPA uses the default Tablespaces for that user.  
If you are registering multiple Oracle Real Application Clusters (RAC) nodes, you may receive an error that the user already exists. You can create a different monitoring user or clear the Create a New Monitoring User check box and continue. |
<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
</table>
| Oracle Monitoring Information| If the monitored instance contains the Oracle E-Business Suite, SolarWinds DPA can collect additional information about the suite. SolarWinds DPA can capture Oracle E-Business data to identify the screens, modules, and users generating the database requests. This gives you increased visibility into the causes of performance problems in the Oracle E-Business Suite, Oracle Enterprise Resource Planning (ERP), and Oracle Applications environments. The SYS password is requested only if remote login as SYS is enabled on the monitored Oracle instance. This option is not available for Amazon RDS instances. If you do not have remote SYS access to the computer, click the link to open the Manual Steps for Monitored Database Instance Registration. You can run a script to run on the monitored instance to install a utility package for SolarWinds DPA that grants Execute permissions for that package to the monitoring user. To register the monitored database instance manually:  
1. Click Register the monitored database instance manually.  
2. Click Select All, copy the script, and paste it into a text file.  
3. As an Oracle Administrator, log in as SYS to the database instance to be monitored.  
5. Execute the script. |
| Oracle Repository Tablespace | If your repository database is not Oracle, the wizard skips this step. Choose the tablespace in the repository database to store DPA performance data for this monitored instance. By default, the performance data is stored in the default tablespace of the repository user. However, data for monitored instances can be stored in separate tablespaces. |
| Select the Alert Groups      | If you have no Alert Groups set up, or if this new database instance does not match the database type of the Alert Group, the wizard skips this step. Alert Groups simplify alert configuration and help make alerting more consistent across the monitored database instances. Select the Alert Groups you want the new database instance to join. |
| Summary                      | Review the information and click Register Database Instance. |
Register a SQL Server database

To register a SQL Server database for DPA to monitor:

1. On the DPA home page, click Register DB Instance for Monitoring.
2. Under Self-Managed, click Microsoft SQL Server.
3. Click Next.
4. Complete the wizard panels as described in the following table.

<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Instance Registration Complete</td>
<td>Click Finish to return to the DPA homepage.</td>
</tr>
<tr>
<td>Panel</td>
<td>Instructions</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| Enter Monitored Database Instance Connection Information | 1. Enter connection information for the SQL Server instance:  
- If the SQL Server Browser service is running, enter the server name or IP address and the instance name in this format: Server\Instance.  
- If the SQL Server instance contains one or more Availability Groups, click Note for Availability Groups for instructions on how to register primary and secondary replicas.  
- Otherwise, enter the server name or IP address and the port number.  
- SolarWinds DPA monitors all databases within the instance. If more than one instance exists on the server, you must register each instance separately in DPA. |
| | 2. Select the type of authentication you want to use. If Mixed Mode was selected during the SQL Server installation, you can choose either option. |
| | 3. Enter a SYSADMIN login that DPA can use to register the instance.  
- DPA does not use or store these credentials after you complete the wizard.  
- For Windows authentication, enter <DOMAIN>\<username> in the SYSADMIN User field.  
- For SQL Server authentication, enter the credentials that you enter on the Connect to Server dialog in SQL Server Management Studio (with Database Engine as the Server type). |
<p>| | SSL is requested by default. If the server does not support SSL, a plain connection is used. |
| | Are you receiving errors? See <a href="#">DPA for SQL Server installation troubleshooting</a>. |</p>
<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
</table>
| Enter the Monitoring User         | Create or specify the account that DPA will use to gather information. To ensure that the account has the required permissions, SolarWinds recommends creating a new account.  
  To create a new account:  
  1. Click Yes.  
  2. Select SQL Server as the authentication method. (DPA cannot create a new Windows account.)  
  3. Enter a user name and password for the new account, or accept the default values.  
  To specify an existing account:  
  1. Click No.  
  2. Select either authentication method.  
  3. Enter the user name and password of an existing account.  
  For Windows authentication, enter `<DOMAIN>\<username>` in the Monitoring User field.  
  You can also authenticate using a [Windows Computer Account](https://support.microsoft.com).  
  For SQL Server authentication, only the user name is required. Do not specify a domain.                                                                                                                   |
| Oracle Repository Tablespace      | If your repository database is not Oracle, the wizard skips this step.  
  Choose the tablespace in the repository database to store DPA performance data for this monitored instance.  
  By default, the performance data is stored in the default tablespace of the repository user. However, data for monitored instances can be stored in separate tablespaces.                                                                                     |
| Select the Alert Groups           | If you have no Alert Groups set up, or if this new database instance does not match the database type of the Alert Group, the wizard skips this step.  
  Alert Groups simplify alert configuration and help make alerting more consistent across the monitored database instances.  
  Select the Alert Groups you want the new database instance to join.                                                                                                                                  |
| Summary                           | Review the information and click Register Database Instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
Register a Sybase database

To register a Sybase database for DPA to monitor:

1. On the DPA home page, click Register DB Instance for Monitoring.
2. Under Self-Managed, click SAP Sybase ASE.
3. Click Next.
4. Complete the wizard panels as described in the following table.

<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Instance Registration Complete</td>
<td>Click Finish to return to the DPA homepage.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Monitored Database Instance Connection Information</td>
<td>Enter the server name or IP address and port of the Sybase server. SolarWinds DPA monitors all databases within the instance. If more than one instance exists on the server, you must register each instance separately in DPA. Enter SA_ROLE credentials for SolarWinds DPA to register the database instance. The Sybase Monitor Server does not need to be configured for SolarWinds DPA to monitor the database.</td>
</tr>
<tr>
<td>PANEL</td>
<td>INSTRUCTIONS</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Enter the Monitoring User    | Create or specify the account that DPA will use to gather information. To ensure that the account has the required permissions, SolarWinds recommends creating a new account.  
To create a new account:  
1. Next to Create Monitoring User, click Yes.  
2. Select the Authentication method, and enter the user name and password.  
To specify an existing account:  
1. Next to Create Monitoring User, click No.  
2. Enter the user name and password.  
SolarWinds DPA requires the monitoring user to have SA_ROLE and MON_ROLE privileges for data collection.  
SolarWinds DPA ignores data on the monitored database instance from the specified monitoring user. Make sure the monitoring user will not cause load on the monitored instance. |
| Oracle Repository Tablespace | If your repository database is not Oracle, the wizard skips this step.  
Choose the tablespace in the repository database to store DPA performance data for this monitored instance.  
By default, the performance data is stored in the default tablespace of the repository user. However, data for monitored instances can be stored in separate tablespaces. |
| Select the Alert Groups      | If you have no Alert Groups set up, or if this new database instance does not match the database type of the Alert Group, the wizard skips this step.  
Alert Groups simplify alert configuration and help make alerting more consistent across the monitored database instances.  
Select the Alert Groups you want the new database instance to join. |
| Summary                      | Review the information and click Register Database Instance.                                                                                                                                               |
| Database Instance Registration Complete | Click Finish to return to the DPA homepage.                                                                                                                                                           |
Register a DB2 database

To register a DB2 database for DPA to monitor:

1. On the DPA home page, click Register DB Instance for Monitoring.
2. Under Self-Managed, click DB2 UDB.
3. Click Next.
4. Complete the wizard panels as described in the following table.

<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2 Configuration Settings</td>
<td>SolarWinds DPA requires the DB2 instance-wide parameter <code>{DFT_MON_STMT}</code> to be turned on to collect monitoring data. Follow the on-screen instructions to check and set the parameter. If <code>{DFT_MON_STMT}</code> is set to OFF, you can use SolarWinds DPA to register the database instance. Later, you can set it to ON and restart the database instance during an approved maintenance window. In the meantime, the database shows a status of Idle.</td>
</tr>
<tr>
<td>PANEL</td>
<td>INSTRUCTIONS</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| Enter Monitored Database Instance Connection Information | Enter the host name or IP address and port of the DB2 server. Enter the DB2 database for SolarWinds DPA to monitor in the Database field. SolarWinds DPA collects information from all DB2 instances in a cluster configuration for the specified database. If the connection information changes for the DB2 server, all databases on that instance must be updated separately through the Update Database Instance Connection Wizard. SolarWinds DPA can monitor all databases in the specified instance, or an individual database.  
  - SolarWinds DPA 9.0 and later monitors all DB2 databases in the specified instance.  
  - Do you want to monitor a single database in an earlier version of SolarWinds DPA? See [Switch to DB2 instance-wide monitoring](#).  
  - To monitor a single database, each database must be registered separately through this wizard, even if multiple databases are contained on a single DB2 server instance.  
  - For instance-wide monitoring, one database must be registered for the SolarWinds DPA connection. |
<p>| | Enter SYSADM credentials for SolarWinds DPA to monitor the database instance. Do you want more information on the DB2 permissions needed by SolarWinds DPA for the monitoring user? See <a href="#">Required DB2 permissions needed by DPA for monitoring</a>. |</p>
<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
</table>
| Enter the Monitoring User                            | Create or specify the account that DPA will use to gather information. To ensure that the account has the required permissions, SolarWinds recommends creating a new account.  
  
  To create a new account:  
  1. Next to Create Monitoring User, click Yes.  
  2. Select the Authentication method, and enter the user name and password.  
  
  To specify an existing account:  
  1. Next to Create Monitoring User, click No.  
  2. Enter the user name and password.  
  
  SolarWinds DPA requires the monitoring user to have SA_ROLE and MON_ROLE privileges for data collection.  
  
  SolarWinds DPA ignores data on the monitored database instance from the specified monitoring user. Make sure the monitoring user will not cause load on the monitored instance. |
| Oracle Repository Tablespace                         | If your repository database is not Oracle, the wizard skips this step.  
  
  Choose the tablespace in the repository database to store DPA performance data for this monitored instance.  
  
  By default, the performance data is stored in the default tablespace of the repository user. However, data for monitored instances can be stored in separate tablespaces. |
| Select the Alert Groups                               | If you have no Alert Groups set up, or if this new database instance does not match the database type of the Alert Group, the wizard skips this step.  
  
  Alert Groups simplify alert configuration and help make alerting more consistent across the monitored database instances.  
  
  Select the Alert Groups you want the new database instance to join. |
| Summary                                              | Review the information and click Register Database Instance.                                                                                                                                                                                                                      |
| Database Instance Registration Complete              | Click Finish to return to the DPA homepage.                                                                                                                                                                                                                                      |
Register a MySQL database

To register a MySQL database for DPA to monitor:

1. On the DPA home page, click Register DB Instance for Monitoring.
2. Under Self-Managed, click MySQL.
3. Click Next.
4. Complete the wizard panels as described in the following table.
| Panel |
---|---|
Enter Monitored Database Instance Connection Information | Enter the host name or IP address and port of the server. SolarWinds DPA monitors all databases within the instance. If more than one instance exists on the server, you must register each instance separately in DPA. SolarWinds DPA ignores data generated by the monitoring user on the monitored database instance. For this reason, do not specify a user that causes load on the monitored instance. SolarWinds recommends creating a separate account for the monitoring user. To create a new account:

1. Click Provide a privileged user.
2. Enter the credentials of an existing user with privileges to create the monitoring user and to grant the required permissions. The credentials for the privileged user are not used or stored after the registration.
   
   The privileged user requires the CREATE USER permission and must be able to grant the following permissions:
   
   ```
   PROCESS on *
   SELECT & UPDATE on performance_schema.*
   ```
   
   To enable the retrieval of query execution plans, this privileged user must be able to grant the following permissions:
   
   ```
   SELECT, INSERT, UPDATE, DELETE on *.*
   ```
   
3. Enter credentials for the monitoring user. You can create a new user or use an existing one.

To specify an existing account:

1. Click Provide the monitoring user.
2. Enter credentials. DPA encrypts the password.

Alternatively, you can use the script that DPA provides to create a monitoring user.

1. Click Monitoring User Creation Script, and follow the on-screen instructions.
2. Copy the edited script to the MySQL console, and run it.
3. Provide this user as your monitoring user.

SolarWinds DPA ignores data on the monitored database instance from the specified monitoring user. Make sure the monitoring user will not cause load on the monitored instance.
<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
</table>
| Oracle Repository Tablespace | If your repository database is not Oracle, the wizard skips this step.  

Choose the tablespace in the repository database to store DPA performance data for this monitored instance.  

By default, the performance data is stored in the default tablespace of the repository user. However, data for monitored instances can be stored in separate tablespaces.                                                                                                                                                                                                                                                                 |
| Select the Alert Groups   | If you have no Alert Groups set up, or if this new database instance does not match the database type of the Alert Group, the wizard skips this step.  

Alert Groups simplify alert configuration and help make alerting more consistent across the monitored database instances.  

Select the Alert Groups you want the new database instance to join.                                                                                                                                                                                                                                                                                                                                         |
## MySQL Configuration for Monitoring

Select a Typical or Custom configuration. SolarWinds recommends the Typical configuration.

- The DPA Recommended option is used for Performance Schema setup.
- `EXPLAIN` can be run on `SELECT` statements.

Select Custom to change the Performance Schema setup and to allow `EXPLAIN` to be run on different statements.

### PERFORMANCE SCHEMA SETUP

Specify what data the Performance Schema collects and maintains. This table shows which consumers and instruments each option enables.

> 1. The MySQL Performance Schema must be enabled. If you select Leave As Is, verify that Global Instrumentation and Thread Instrumentation are enabled in the existing Performance Schema configuration.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>SERVER DEFAULT</th>
<th>DPA RECOMMENDED</th>
<th>DETAILED</th>
<th>LEAVE AS IS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer Global Instrumentation</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NC</td>
</tr>
<tr>
<td>Consumer Thread Instrumentation</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NC</td>
</tr>
<tr>
<td>Consumer Statement Digest</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NC</td>
</tr>
<tr>
<td>Consumer Statement (Current)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NC</td>
</tr>
<tr>
<td>Consumer Wait (Current)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NC</td>
</tr>
<tr>
<td>Instrument Wait (Lock/*)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NC</td>
</tr>
<tr>
<td>Instrument Wait (I/O table)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NC</td>
</tr>
<tr>
<td>Instrument Wait (I/O/file)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NC</td>
</tr>
<tr>
<td>Instrument Wait (I/O/socket)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NC</td>
</tr>
<tr>
<td>Instrument Wait (Synch/*)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>NC</td>
</tr>
</tbody>
</table>
MySQL Configuration for Monitoring (continued)

✔ = Enabled.
NC = No change. DPA does not change the existing Performance Schema configuration.

* Values that are outside of the MYSQL_PERFORMANCE_SCHEMA configuration scope of DPA are not changed. For example, an instrument named stage exists in the MySQL Performance Schema. If you enable or disable that instrument, DPA will not change it.

ALLOW EXPLAIN TO BE RUN ON

This section is displayed if you specified a privileged user to create the DPA monitoring user.

Select what type of statements you want DPA to collect execution plans for. The monitoring user can run EXPLAIN on the selected statement types.

<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL Configuration for Monitoring (continued)</td>
<td>✔ = Enabled. NC = No change. DPA does not change the existing Performance Schema configuration. * Values that are outside of the MYSQL_PERFORMANCE_SCHEMA configuration scope of DPA are not changed. For example, an instrument named stage exists in the MySQL Performance Schema. If you enable or disable that instrument, DPA will not change it.</td>
</tr>
</tbody>
</table>

Summary

Review the information and click Register Database Instance.

Database Instance Registration Complete

Click Finish to return to the DPA homepage.

Register an Amazon RDS for Oracle database

To register an Amazon RDS for Oracle database for DPA to monitor:

1. On the DPA home page, click Register DB Instance for Monitoring.
2. Under Amazon RDS, click Amazon RDS for Oracle.
3. Click Next.
4. Complete the wizard panels as described in the following table.
<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Monitored Database Instance Connection Information</td>
<td>Amazon Relational Database Service (RDS) for Oracle database instances have three connection options:</td>
</tr>
<tr>
<td></td>
<td>• Direct Connect</td>
</tr>
<tr>
<td></td>
<td>• Transparent Network Substrate (TNS) Connect Descriptor</td>
</tr>
<tr>
<td></td>
<td>• Lightweight Directory Access Protocol (LDAP) or TNS Name</td>
</tr>
<tr>
<td>DIRECT CONNECT</td>
<td>Enter the Service Name or System Identifier (SID), host name or IP address, and port. The default port is 1521.</td>
</tr>
<tr>
<td>TNS CONNECT DESCRIPTOR</td>
<td>The Connect Descriptor value contains everything after <code>NAME=</code> in the <code>tnsnames.ora</code> file. The beginning <code>DESCRIPTION=</code> is necessary. For example:</td>
</tr>
<tr>
<td></td>
<td><code>(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = demo.confio.com)(PORT = 1521)))(CONNECT_DATA = (SERVICE_NAME = demo)))</code></td>
</tr>
<tr>
<td>LDAP OR TNS NAME</td>
<td>To use this option, Oracle Name Resolution must be configured. For instructions, see <a href="#">Connect to Oracle using name resolution</a>.</td>
</tr>
<tr>
<td></td>
<td>After you configure Oracle Name Resolution, you can use the LDAP/TNS Name when registering additional monitored database instances.</td>
</tr>
<tr>
<td>RAC INSTANCES</td>
<td>If this is an Oracle Real Application Clusters (RAC) instance, there may be listener configuration changes needed if you are not listening on the physical IP address. SolarWinds recommends:</td>
</tr>
<tr>
<td></td>
<td>• If you are registering pluggable databases (PDBs) on a RAC instance, consider registering with the physical IP address of the host.</td>
</tr>
<tr>
<td></td>
<td>• If you are registering a non-PDB RAC instance, consider registering with the SID.</td>
</tr>
<tr>
<td></td>
<td>• If you are using the Service Name, consider using the physical IP address of the host. Do not use the virtual IP address (VIP) or the Oracle Single Client Access Name (SCAN) IP address.</td>
</tr>
<tr>
<td>DBA USER</td>
<td>Enter DBA credentials for SolarWinds DPA to register the database instance.</td>
</tr>
<tr>
<td><strong>Panel</strong></td>
<td><strong>Instructions</strong></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Enter the Monitoring User</strong></td>
<td>Create or specify the account that DPA will use to gather information. To ensure that the account has the required permissions, SolarWinds recommends creating a new account.</td>
</tr>
<tr>
<td></td>
<td>To create a new account:</td>
</tr>
<tr>
<td></td>
<td>1. Next to Create Monitoring User, click Yes.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the user name and password.</td>
</tr>
<tr>
<td></td>
<td>3. Select a Tablespace and Temp Tablespace on the monitored database. This is primarily used for gathering Explain Plan data for monitored queries.</td>
</tr>
<tr>
<td></td>
<td>To specify an existing account:</td>
</tr>
<tr>
<td></td>
<td>1. Next to Create Monitoring User, click No.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the user name and password.</td>
</tr>
<tr>
<td></td>
<td>If you create the user manually, DPA uses the default Tablespaces for that user.</td>
</tr>
<tr>
<td><strong>Oracle Monitoring Information</strong></td>
<td>If the monitored instance contains the Oracle E-Business Suite, SolarWinds DPA can collect additional information about the suite.</td>
</tr>
<tr>
<td></td>
<td>SolarWinds DPA can capture Oracle E-Business data to identify the screens, modules, and users generating the database requests. This gives you increased visibility into the causes of performance problems in the Oracle E-Business Suite, Oracle Enterprise Resource Planning (ERP), and Oracle Applications environments.</td>
</tr>
<tr>
<td></td>
<td>The SYS password option is not available for Amazon RDS instances.</td>
</tr>
<tr>
<td><strong>Oracle Repository Tablespace</strong></td>
<td>If your repository database is not Oracle, the wizard skips this step.</td>
</tr>
<tr>
<td></td>
<td>Choose the tablespace in the repository database to store DPA performance data for this monitored instance.</td>
</tr>
<tr>
<td></td>
<td>By default, the performance data is stored in the default tablespace of the repository user. However, data for monitored instances can be stored in separate tablespaces.</td>
</tr>
<tr>
<td><strong>Select the Alert Groups</strong></td>
<td>If you have no Alert Groups set up, or if this new database instance does not match the database type of the Alert Group, the wizard skips this step.</td>
</tr>
<tr>
<td></td>
<td>Alert Groups simplify alert configuration and help make alerting more consistent across the monitored database instances.</td>
</tr>
<tr>
<td></td>
<td>Select the Alert Groups you want the new database instance to join.</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td>Review the information and click Register Database Instance.</td>
</tr>
</tbody>
</table>
Register an Amazon RDS for SQL Server database

To register an Amazon RDS for SQL Server database for DPA to monitor:

1. On the DPA home page, click Register DB Instance for Monitoring.
2. Under Amazon RDS, click Amazon RDS for SQL Server.
3. Click Next.
4. Complete the wizard panels as described in the following table.

<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Monitored Database Instance Connection Information</td>
<td>Enter the server name or IP address and port.</td>
</tr>
<tr>
<td></td>
<td>SolarWinds DPA monitors all databases within the instance. If more than one instance exists on the server, you must register each instance separately in DPA.</td>
</tr>
<tr>
<td></td>
<td>SSL is requested by default. If the server does not support SSL, a plain connection is used.</td>
</tr>
<tr>
<td></td>
<td>Enter an Amazon RDS Master User for SolarWinds DPA to register the database instance. If you do not want to enter the Master User that created the database instance, use the SQL statement below to create a new Master User. Replace dpa with the new user name.</td>
</tr>
<tr>
<td></td>
<td><strong>CREATE LOGIN [dpa] WITH PASSWORD=N'Password1';</strong></td>
</tr>
<tr>
<td></td>
<td><strong>GRANT ALTER ANY LOGIN TO dpa;</strong></td>
</tr>
<tr>
<td></td>
<td><strong>GRANT VIEW SERVER STATE TO dpa WITH GRANT OPTION;</strong></td>
</tr>
<tr>
<td></td>
<td><strong>GRANT VIEW ANY DEFINITION TO dpa WITH GRANT OPTION;</strong></td>
</tr>
<tr>
<td></td>
<td><strong>GRANT VIEW ANY DATABASE TO dpa WITH GRANT OPTION;</strong></td>
</tr>
<tr>
<td></td>
<td><strong>ALTER SERVER ROLE [processadmin] ADD MEMBER [dpa];</strong></td>
</tr>
<tr>
<td><strong>Panel</strong></td>
<td><strong>Instructions</strong></td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Enter the Monitoring User | Create or specify the account that DPA will use to gather information. To ensure that the account has the required permissions, SolarWinds recommends creating a new account.  
To create a new account:  
1. Click Yes.  
2. Select SQL Server as the authentication method. (DPA cannot create a new Windows account.)  
3. Enter a user name and password for the new account, or accept the default values.  
To specify an existing account:  
1. Click No.  
2. Select either authentication method.  
3. Enter the user name and password of an existing account. 
For Windows authentication, enter `<DOMAIN>\<username>` in the Monitoring User field. 
You can also authenticate [using a Windows Computer Account](#).  
For SQL Server authentication, only the user name is required. Do not specify a domain. |
| Oracle Repository Tablespace | If your repository database is not Oracle, the wizard skips this step.  
Choose the tablespace in the repository database to store DPA performance data for this monitored instance.  
By default, the performance data is stored in the default tablespace of the repository user. However, data for monitored instances can be stored in separate tablespaces. |
| Select the Alert Groups | If you have no Alert Groups set up, or if this new database instance does not match the database type of the Alert Group, the wizard skips this step.  
Alert Groups simplify alert configuration and help make alerting more consistent across the monitored database instances.  
Select the Alert Groups you want the new database instance to join. |
| Summary | Review the information and click Register Database Instance. |
Register an Amazon RDS for MySQL or Aurora database

To register an Amazon RDS for MySQL or Aurora database for DPA to monitor:

1. On the DPA home page, click Register DB Instance for Monitoring.
2. Under Amazon RDS, click Amazon RDS for MySQL.
3. Click Next.
4. Complete the remaining wizard panels as described in the following table.

<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Instance Registration Complete</td>
<td>Click Finish to return to the DPA homepage.</td>
</tr>
</tbody>
</table>
### Enter Monitored Database Instance Connection Information

- **Enter the host name or IP address and port of the server.**

  SolarWinds DPA monitors all databases within the instance. If more than one instance exists on the server, you must register each instance separately in DPA.

  SolarWinds DPA ignores data generated by the monitoring user on the monitored database instance. For this reason, do not specify a user that causes load on the monitored instance. SolarWinds recommends creating a separate account for the monitoring user.

  **To create a new account:**

  1. Click **Provide a privileged user.**
  2. Enter the credentials of an existing user with privileges to create the monitoring user and to grant the required permissions.

     The credentials for the privileged user are not used or stored after the registration.

     The privileged user requires the `CREATE USER` permission and must be able to grant the following permissions:

     - `PROCESS` on `*.*`
     - `SELECT` & `UPDATE` on `performance_schema.*`

     To enable the retrieval of query execution plans, this privileged user must be able to grant the following permissions:

     - `SELECT`, `INSERT`, `UPDATE`, `DELETE` on `*.*`

  3. Enter credentials for the monitoring user. You can create a new user or use an existing one.

  **To specify an existing account:**

  1. Click **Provide the monitoring user.**
  2. Enter credentials. DPA encrypts the password.

  Alternatively, you can use the script that DPA provides to create a monitoring user.

  1. Click **Monitoring User Creation Script**, and follow the on-screen instructions.
  2. Copy the edited script to the MySQL console, and run it.
  3. Provide this user as your monitoring user.

  SolarWinds DPA ignores data on the monitored database instance from the specified monitoring user. Make sure the monitoring user will not cause load on the monitored instance.
<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
</table>
| Oracle Repository Tablespace | If your repository database is not Oracle, the wizard skips this step.  
Choose the tablespace in the repository database to store DPA performance data for this monitored instance.  
By default, the performance data is stored in the default tablespace of the repository user. However, data for monitored instances can be stored in separate tablespaces. |
| Select the Alert Groups   | If you have no Alert Groups set up, or if this new database instance does not match the database type of the Alert Group, the wizard skips this step.  
Alert Groups simplify alert configuration and help make alerting more consistent across the monitored database instances.  
Select the Alert Groups you want the new database instance to join. |
**MySQL Configuration for Monitoring**

Select a Typical or Custom configuration. SolarWinds recommends the Typical configuration.

The DPA Recommended option is used for Performance Schema setup. Select Custom to change the Performance Schema setup.

**PERFORMANCE SCHEMA SETUP**

Specify what data the Performance Schema collects and maintains. This table shows which consumers and instruments each option enables.

> The MySQL Performance Schema must be enabled. If you select Leave As Is, verify that Global Instrumentation and Thread Instrumentation are enabled in the existing Performance Schema configuration.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>SERVER DEFAULT</th>
<th>DPA RECOMMENDED</th>
<th>DETAILED</th>
<th>LEAVE AS IS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer Global Instrumentation</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>NC</td>
</tr>
<tr>
<td>Consumer Thread Instrumentation</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>NC</td>
</tr>
<tr>
<td>Consumer Statement Digest</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>NC</td>
</tr>
<tr>
<td>Consumer Statement (Current)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>NC</td>
</tr>
<tr>
<td>Consumer Wait (Current)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>NC</td>
</tr>
<tr>
<td>Instrument Wait (Lock/*)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>NC</td>
</tr>
<tr>
<td>Instrument Wait (I/O table) (I/O/file)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>NC</td>
</tr>
<tr>
<td>Instrument Wait (I/O/socket)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>NC</td>
</tr>
<tr>
<td>Instrument Wait (Synch/*)</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>NC</td>
</tr>
</tbody>
</table>
Register an Azure SQL database

To register multiple Azure SQL databases using the Mass Registration feature, follow the instructions in this KB article.

To register a single Azure SQL database for DPA to monitor:

1. On the DPA home page, click Register DB Instance for Monitoring.
2. Under Azure, click Azure SQL DB.
3. Click Next.
4. Complete the wizard panels as described in the following table.

<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL Configuration for Monitoring (continued)</td>
<td>✔ = Enabled. NC = No change. DPA does not change the existing Performance Schema configuration. * Values that are outside of the MYSQL_PERFORMANCE_SCHEMA configuration scope of DPA are not changed. For example, an instrument named stage exists in the MySQL Performance Schema. If you enable or disable that instrument, DPA will not change it.</td>
</tr>
<tr>
<td>Summary</td>
<td>Review the information and click Register Database Instance.</td>
</tr>
<tr>
<td>Database Instance Registration Complete</td>
<td>Click Finish to return to the DPA homepage.</td>
</tr>
<tr>
<td>PANEL</td>
<td>INSTRUCTIONS</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Enter Monitored Database Instance Connection Information | Enter the server name, port, and database name. You cannot use an IP address in the Server Name field.  
Choose a method for creating or configuring the monitoring user.  
To create a new account:  
1. Click Let DPA create a new contained user or configure an existing contained user for me.  
2. Enter the credentials of an existing user with privileges to create the monitoring user and to grant the required permissions.  
The privileged user must be a member of the db_owner role.  
The credentials for the privileged user are not used or stored after the registration.  
To specify an existing account:  
1. Click I'll create the database user.  
2. Enter credentials. DPA encrypts the password.  
Alternatively, you can use the script that DPA provides to create a monitoring user.  
1. Click Monitoring User Creation Script, and follow the on-screen instructions.  
2. Copy and run the edited script on your Azure SQL database.  
3. Provide this user as your monitoring user. |
<table>
<thead>
<tr>
<th>PANEL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the Monitoring User</td>
<td>DPA gathers information through this user from the monitored database. You can create a monitoring user through DPA or use an existing user, such as for read-only replica databases.</td>
</tr>
<tr>
<td></td>
<td>To register a read-only geo-replica, you must create a monitoring account through the primary server first.</td>
</tr>
<tr>
<td></td>
<td>SolarWinds recommends creating a new account because DPA requires special permissions that existing users may not have.</td>
</tr>
<tr>
<td></td>
<td>To create a new account:</td>
</tr>
<tr>
<td></td>
<td>1. Click Let DPA create a new contained user.</td>
</tr>
<tr>
<td></td>
<td>2. Enter credentials.</td>
</tr>
<tr>
<td></td>
<td>To specify an existing account:</td>
</tr>
<tr>
<td></td>
<td>1. Run the following SQL statement on the Azure SQL database:</td>
</tr>
<tr>
<td></td>
<td>CREATE USER [USERNAME] WITH PASSWORD=N'PASSWORD';</td>
</tr>
<tr>
<td></td>
<td>ALTER ROLE db_owner ADD member &lt;USERNAME&gt;;</td>
</tr>
<tr>
<td></td>
<td>2. Click Let DPA configure an existing contained user.</td>
</tr>
<tr>
<td></td>
<td>3. Enter credentials.</td>
</tr>
<tr>
<td>Oracle Repository Tablespace</td>
<td>If your repository database is not Oracle, the wizard skips this step.</td>
</tr>
<tr>
<td></td>
<td>Choose the tablespace in the repository database to store DPA performance data for this monitored instance.</td>
</tr>
<tr>
<td></td>
<td>By default, the performance data is stored in the default tablespace of the repository user. However, data for monitored instances can be stored in separate tablespaces.</td>
</tr>
<tr>
<td>Select the Alert Groups</td>
<td>If you have no Alert Groups set up, or if this new database instance does not match the database type of the Alert Group, the wizard skips this step.</td>
</tr>
<tr>
<td></td>
<td>Alert Groups simplify alert configuration and help make alerting more consistent across the monitored database instances.</td>
</tr>
<tr>
<td></td>
<td>Select the Alert Groups you want the new database instance to join.</td>
</tr>
<tr>
<td>Summary</td>
<td>Review the information and click Register Database Instance.</td>
</tr>
</tbody>
</table>
Database Instance Registration Complete

Click Finish to return to the DPA homepage.

ENABLE DEADLOCKS FOR READ-ONLY GEO-REPLICAS

To enable the deadlock feature for read-only geo-replica Azure SQL databases, you must create and enable an Extended Event Session (EES).

If you registered the primary server first, an EES is already created and synced. Skip to step 2.

Otherwise, connect to the primary server first to create an EES.

1. Run the following SQL statement:

   ```sql
   CREATE EVENT SESSION [dpa_deadlock_capture] ON DATABASE
   ADD EVENT sqlserver.xml_deadlock_report
   ADD TARGET package0.ring_buffer(SET max_events_limit=(1000),
   max_memory=(256))
   WITH (MAX_MEMORY = 256KB,
   EVENT_RETENTION_MODE = ALLOW_SINGLE_EVENT_LOSS,
   MAX_DISPATCH_LATENCY = 30 SECONDS,
   MAX_EVENT_SIZE = 0KB,
   MEMORY_PARTITION_MODE = NONE,
   TRACK_CAUSALITY = OFF,
   STARTUP_STATE = ON);
   -- ALTER EVENT SESSION [dpa_deadlock_capture] ON DATABASE STATE = START;
   ```

2. Connect to the read-only replica database.
3. Click Extended Events > Sessions.
4. Enable the dpa_deadlock_capture session.
Update a monitored database instance

If connection or user information changes with one of your monitored database instances, you must update that information in DPA.

1. Click Options > Update Connection Info.
2. Select the database instance, and click Next.
3. Select the check box next to the property, update the value, and click Next.
   For database-specific connection information, see the following:
   - Oracle
   - SQL Server
   - Azure SQL
   - Sybase
   - DB2
   - MySQL
   - Amazon RDS for Oracle
   - Amazon RDS for SQL Server
   - Amazon RDS for MySQL
4. Confirm the connection information, and click Update Connection.
5. Click Finish, or Update Another Database Instance to continue updating.
Unregister a monitored database instance

If you want to remove one of your monitored database instances from DPA, you must unregister it.

⚠️ If you unregister a monitored database instance, DPA stops monitoring the instance and removes all historical performance data from the repository.

1. Click Options > Unregister.
2. Select a database instance, and click Next.
3. Select the database instance objects to be removed, and click Next.
   Depending on the database type, you can remove one or both of the following objects:
   - **Monitoring User**: You can remove the monitoring user if no other applications, including other installations of DPA, are using this user.
   - **DPA Database Objects**: This refers to tables that are created in the schema of the monitoring user. If you remove the monitoring user, these objects are removed since they are owned by the monitoring user. You can remove these objects if no other installations of DPA are monitoring this instance.

⚠️ You cannot remove objects on certain database types, such as read-only replicas.

4. Confirm the unregistration information, and click Unregister Database Instance. This may take several minutes.
5. Click Finish to complete the unregistration.
Users and groups

Create a user

Create and manage different types of users who can access repository data. Assign users access to only view data, to start and stop monitoring database instances, or to change the monitoring parameters. Each user must have a unique user name.

1. Click Options > Administration > User Administration.
2. Click Create User.
3. Enter a name and password, and select a role. Permissions are set based on role.
4. Customize permissions by selecting or clearing check boxes for one or more database instances.
5. Click Save.

If you configured DPA to point to your Active Directory or LDAP server, you will see an option to either create a user or a group. The group corresponds to a group in Active Directory or LDAP.

Create a group

Create groups to send alert notifications to several contacts at once.

1. Click Options > Administration > Contacts and Contract Groups.
2. Click Create Contact.
3. Add the name and email of a user you want to notify, and click Save.
4. If you want to send DPA alerts as SNMP traps to your Network Management System (NMS), create an SNMP contact.
5. Click Create Group.
6. Enter a name and description.
7. Add available contacts, and click Save.

User authentication options

SolarWinds DPA supports Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) authentication. Using your existing authentication infrastructure eliminates the need to duplicate your user accounts in DPA. After you configure AD or LDAP authentication, users can log in with their domain account or a custom user account created by DPA.
AD USER AUTHENTICATION

DPA integrates with Windows Active Directory (AD). DPA uses the security group information from AD to assign permissions to groups. To configure DPA user authentication and permissions using AD, see Configure Active Directory or LDAP.

If your repository database is Azure SQL and you are monitoring one or more Azure SQL databases, you can use Azure AD authentication in DPA. To configure DPA user authentication and permissions using Azure AD, see Use Azure AD authentication in DPA.

LDAP USER AUTHENTICATION

DPA integrates with most LDAP implementations to assign permissions to groups. To configure DPA user authentication and permissions using LDAP, see Configure Active Directory or LDAP.

SINGLE SIGN-ON

Using single sign-on (SSO), your AD users can log in to DPA without re-entering the domain credentials they used to log in to their operating system. Before you configure DPA for SSO, configure DPA for AD authentication.

COMMON ACCESS CARDS

You can use a Common Access Card (CAC) to log in to Windows and DPA. Before using a CAC, configure DPA for AD, and then for SSO as described in the sections above.

Configure Active Directory or LDAP

To use AD or LDAP user authentication in DPA:

1. Gather the following information from your domain administrator:
   - Directory service type: AD or LDAP
   - Domain name
   - Port number: Used to connect to the directory service
   - User: The domain user DPA uses to query the directory for users and groups
   - Password: The password of the domain user, preferably one that does not expire
2. Click Options > Administration > Configure AD/LDAP.
3. Select the type of directory service you have: Active Directory or LDAP.
4. Click Next.

CONNECTION INFORMATION

DOMAIN NAME

Enter the domain name.
SolarWinds recommends using a domain name, not the name of a specific domain controller.

DO YOU HAVE MULTIPLE DOMAINS?

If your domain users authenticate from a different domain other than the domain specified here, you must connect to the global catalog ports 3268 or 3269. The domain users must belong to a universal group, and that universal group must be added under Options > Administration > User Administration.

PORT

Select the port number.

If you use a unique port, select Other non-standard port. Enter the port number, and select SSL if required.

USER AND PASSWORD

DPA uses this user to search the directory service for users and groups.

ACTIVE DIRECTORY USER NAME

For the AD user name, use one of the following formats:

- Distinguished Name (DN): cn=BobSmith,cn=Users,dc=domain,dc=local
- User Principal Name (UPN): bsmith@domain.local

LDAP USER NAME

For the LDAP user name, use the following format:

- Distinguished Name (DN): cn=BobSmith,cn=Users,dc=domain,dc=local

DID THE CONNECTION TEST FAIL?

If you use an SSL port and the verification fails, DPA must import its certificate. Click Yes on the confirmation window to try again.

BASE SEARCH LOCATION

BASE DN

USE THE DEFAULT

SolarWinds recommends selecting the default, so DPA uses the detected base DN from the previous step.

Example of default base DN: dc=east,dc=acme,dc=com
USE A CUSTOM VALUE

You may use a value other than the default base DN. For example: You use a global catalog that supports multiple domains, and you want to broaden the scope of the search.

Example for multiple domains: dc=acme,dc=com

ADVANCED SETTINGS

If this is your first time using this wizard, do not use the advanced settings.

Only use advanced settings if you completed this wizard and you experience slow domain user logins or group searches.

ARE DOMAIN USER LOGINS SLOW?

Set the User Search Base value if domain user logins take a long time.

If your company has one domain, specify the location in the directory tree that contains all of the domain users that will use SolarWinds DPA.

If you do not know what to put here, ask the domain administrator of your company the following questions:

"What folder, or organization unit (OU), in the directory tree of the domain contains all of the users? I must specify a search base for users. What is the distinguished name of the folder?"

Example: cn=users OR ou=users

ARE DOMAIN GROUP SEARCHES SLOW?

Set the Group Search Base value if domain group searches in User Administration take a long time.

Specify the location in the directory tree that contains all of the groups to which SolarWinds DPA users belong.

If your company has multiple domains, you can enter the group search bases individually. After you add groups to SolarWinds DPA using the group search base from one domain, update this wizard to specify a group search base in another domain.

If you do not know what to put here, ask your the domain administrator of your company the following:

"What folder, or organization unit (OU), in the directory tree of the domain contains all of the groups? I must specify a search base for groups. What is the distinguished name of the folder?"

Example: cn=groups OR ou=groups

SUMMARY

Confirm the information for configuring DPA with your directory service, and click Finish.

You must restart the DPA server for the settings to take effect.
CONFIGURE AUTHENTICATION AND PERMISSIONS FOR GROUPS OF USERS

After you have set up DPA to use Active Directory or LDAP, do the following:

1. In AD or LDAP, determine which groups contain the users that you want to grant access to DPA. You may need to create a group if a suitable group does not exist.
2. In DPA, click Options > Administration > User Administration.
3. Click Add Active Directory Group or Add LDAP Group.
4. Click Search for a Group.
5. Find and select the group you want and click Save.
6. Assign privileges to the group, just as you would for a user. This assigns those permissions to the domain users who are members of the group.

   DPA does not support single sign-on (SSO) for individual accounts. It only supports AD or LDAP groups.

7. Click Save.
   All domain users in the selected group can log in to DPA using their domain credentials. The users have the privileges you set up for the group in DPA.

You can add multiple AD or LDAP groups in DPA. If a domain user is a member of more than one group, DPA grants them the combined privileges from all of their groups.

LOG IN TO DPA

When you enter the domain user name and password in the DPA login screen, DPA searches your directory service for a matching user name, and then authenticates using the password. If the domain user belongs to one of the groups that you configured as a DPA custom user, the login succeeds.

NAME FORMATS FOR AD LOGIN

DPA supports three types of login name formats for Active Directory:

- **SAM account name**: `username`
- **User principal name**: `username@domain.local`
- **NT/AD**: `domain\username`

USER NAME FOR LDAP

The user name used by DPA is the LDAP user object `uid` attribute.
Reports

Use reports to communicate the long-term performance of your databases across your organization. You can capture the results of performance tuning, important database resources, and database trends. You can send reports to managers, team members, and customers. Reports supply evidence to support your work across the organization by highlighting database trends. Report examples include the top five resource bottlenecks and the highest SQL statement utilization.

Reports are different from the detailed data displayed in DPA charts. Detailed repository data are accessible for a shorter data storage period, typically 30 days. Reports can show data captured over longer intervals and display long-term trends.

To generate reports, DPA summarizes repository data to make long-term information available in a manageable size. The data are summarized by hour and available for 90 days. After 90 days, the data are summarized by day and available for five years.

Reports show data trends over hours, days, months, and years. DPA requires a one-hour minimum of collection. Detailed repository data, with information down to the second, display information within 10 minutes of initial collection. SolarWinds recommends letting the repository collection run for 24 hours before creating a report.

Access reports in DPA

Click Reports from the top of the SolarWinds DPA home page.

Reports tab

Under Create a New Report, select a Database Instance and Report Type. Some report types require an additional parameter, such as Wait Event or SQL Hash Value.

Click Report Options to change the default parameters, such as date range, interval, and time of day.

Under Reports, view saved reports. Filter reports by database instance.

Report Groups tab

A report group is a group of reports that are displayed together. Group reports together to see related data on one page.

Report Schedules tab

Report schedules are used to automatically email a report (or group of reports) at regular intervals. For example, you can create a schedule to email a list of the top 10 worst performing SQL statements every Monday at 9:00 a.m.
Report types

SolarWinds DPA has many standard reports that include the most commonly used wait time statistics. You can customize the reports to see more detailed trends in your databases. Available reports include:

**Top SQLs**

This report shows the top five SQL statements ranked by total wait time across a custom interval. You can change the report to display the top 10 or select specific SQL statements from the SQL Statements tab on the Report Properties dialog. The report will show a descriptive name for the SQL if it has been defined.

**Top Waits for single SQL**

This report identifies the top wait events (up to 50), ranked by wait time, for a specific SQL statement.

**Top SQLs for single Wait**

This report identifies the top SQL statements for a single database wait.

**Typical Day of Wait**

This report displays a bar graph showing the average hourly wait time for a database. It displays the distribution of average wait time versus time of day.

**Typical Day of Wait for single SQL**

This report displays a stacked graph showing average hourly wait time for the top waits contributing to the total wait time for an individual SQL statement. The top of the bar is the sum of all other waits. This report can identify the peak loads during your business hours based on long-term observation of the system.

**Top Waits**

This report charts waits for an entire database. SolarWinds DPA displays the waits with the highest accumulated wait time.

**Top Programs**

This report displays the total accumulated wait time for programs.

**Top Files**

This report displays the busiest files ranked by total I/O wait time. SolarWinds DPA calculates the total wait time for all I/O operations on each file for selected intervals.
Create a Top SQL Statements report

1. Click Reports from the top of the SolarWinds DPA home page.
2. Select the Database Instance, and select Top SQLs from the Report Type list.
3. Click Preview Report.
4. Click Save As, enter a report name and description, and click OK.

Schedule a report for email delivery

1. Click Reports on the DPA menu bar.
2. Click the Report Schedules tab.
3. Click Create Schedule.
4. Name the schedule and enter an email subject and body text.

5. Specify when you want the report delivered and click Add. You can specify multiple delivery times.

6. Under Available Reports, select the reports or report groups and click Add.
7. Under Available Contacts, select the recipients of the report and click Add.  
   If you have not added the recipients as contacts in DPA, click Add Contact or Add Contact Group.

8. Click Create Schedule.  
   Your schedule is added to the list of report schedules.

Does your network or firewall require an internal SMTP server? If so, see SMTP mail server for outgoing email.
Alerts

SolarWinds DPA alerts give you proactive control of your databases, notifying you of issues before they become problems for your customers.

Set thresholds on key wait time statistics or on standard administration indicators. That way the DBA group receives an early warning of potential problems, and can take steps to solve the underlying issue before it affects users.

The result is improved customer service, fewer help desk tickets, and increased compliance with database service-level agreements.

Access alerts in DPA

Click Alerts from the top of the SolarWinds DPA home page.

Alert Status tab
View the status and frequency of saved alerts. Filter alerts by database instance.

Manage Alerts tab
Under Create a New Alert, select an Alert Category and Alert Type.
Under Alerts, view and edit saved alerts.

Alert Groups tab
An alert group defines a set of alerts to be run against a set of database instances.

Alert Blackouts tab
If you want to stop alerting for a period of time, create a blackout.

Alert categories

You can use the out-of-the-box alerts in DPA, or customize them to meet your needs. There are four preconfigured DPA alert categories.

WAIT TIME

Wait Time alerts are based on the amount of time users or applications waited on the database. For example, the Average SQL Wait Time alert fires when a SQL statement causes wait time that exceeds a threshold. These alerts are critical because they ensure that you are only alerted when users and applications are affected.
RESOURCES

These alerts are based on the alarm thresholds of resource metrics, such as CPU utilization and memory usage. For example, the Single Resource Metric alert notifies you when the values of the specified resource metric exceed the thresholds.

ADMINISTRATIVE

Administrative alerts are typical alerts surrounding the health of the database system. For example, the Database Parameter Changes alert notifies you when any database parameter has changed. The Database Availability alert notifies you when the database instance is no longer accessible.

CUSTOM

Custom alerts are user-specified queries that are run against the monitored database or the DPA repository. The query returns a number (or set of numbers) that may trigger an alert depending on user-defined threshold settings.

For example, you can enter a query to detect the number of canceled orders in the last 10 minutes:

```sql
select count(*) from orders where status='CANCELLED' and date > sysdate - 10/1440;
```

You can write a SQL query to set alerts on SQL Server health metrics.

```sql
select order_type, count(*) from orders where status='CANCELLED' and date > sysdate - 10/1440 group by order_type;
```

You may want to use complex logic to determine if an order has truly been canceled. In this case, you can write a function or procedure on the monitored database instance.

- **Oracle**: select mycustomfunction(param1) from dual
- **SQL Server**: select mycustomfunction(param1)
- **Sybase**: mycustomprocedure(param1)
- **DB2**: select dbo.mycustomfunction(param1) from SYSIBM.SYSDUMMY1
- **MySQL**: mycustomprocedure(param1)
- **Azure SQL**: select mycustomfunction(param1)

These functions or procedures are written in the native programming language of the database.

**Alert attributes**

When creating an alert, you must specify the following attributes:
Active

Active alerts are executed by SolarWinds DPA. Clear the Active check box to disable an alert but not delete it.

Execution Interval

The interval indicates how often the alert is run. SolarWinds recommends a 10-minute interval so the alert does not put too much load on the monitored database instance. For Wait Time alerts, this value also indicates the time period DPA uses to examine data, from the time the alert runs. For example, if the execution interval is 10 minutes, DPA executes the alert every 10 minutes and also queries the last 10 minutes of performance data as alert input.

Notification Text

This text is sent with the notification email or page. You can include an explanation of the alert and the suggested resolution.

Database Instances to monitor

Specify the database instances to be monitored with this alert. You can add multiple database instances with certain alert types.

Alert Levels

Alert levels specify the ranges of values that will trigger an alert notification. For example, a SQL statement has a service-level agreement to execute in under four seconds, but typically executes in less than two seconds. Enter 2 as the Min value and 4 as the Max value.

Notification Group or Contact

DPA can send alerts to an individual, a group, or an enterprise management console such as SolarWinds Server & Application Monitor using SNMP traps.

Notification Policy

You can change the notification policy by editing a single alert, or globally in Advanced Options.

SNMP alerts

You can configure DPA alerts to send SNMPv2c traps to an SNMP-enabled Network Management System (NMS) when an alert level is reached. The trap contains the name of the monitored database, alert name, alert level, and response instructions.

CREATE AN SNMP CONTACT

The NMS that will receive the trap is represented as an SNMP contact in DPA.
1. Click Options > Administration > Contact and Contact Groups.
2. Click Create SNMP Contact.
3. Enter the required information, and click Save.
   The SNMP is now available as a notification group or contact.

**Alert on increases in SQL wait times**

Use the steps below to determine the average execution response time of your SQL queries, and then create an alert to warn you of significant deviations.

**DETERMINE THE AVERAGE EXECUTION TIME OF YOUR QUERIES**

1. On the DPA home page, click a Database Instance.
2. Select the first query from the View Historical Charts for SQL list.
3. Scroll down to the Average Wait Time per Execution chart.
   This chart shows the average execution time for the SQL statement on each day. The black bar denotes the average wait for this query across the days in the chart.
4. Point the cursor to each bar to see details for the day.
5. Point the cursor to the black bar to see the baseline of average wait time for this query for all executions for the month.
   SolarWinds recommends alerting if the average wait time is twice as long as this baseline. For example, if the baseline of average wait time for the month is 1.5 seconds, set the alert to 3 seconds.

Identify the top three queries and estimate the typical wait time. Choose a threshold, approximately twice as long, that you will use to create alerts.

**CREATE AN ALERT BASED ON THE WAIT THRESHOLD**

1. Click Alerts > Manage Alerts.
2. Verify Wait Time is selected as the Alert Category.
3. Select Average Wait Time for a Single SQL from the Alert Type list.
4. Click Create Alert.
5. Name the alert and enter notification text.
6. Set the Execution Interval to 10 minutes or more. This allows time for valid samples and prevents unnecessary alerts from a single slow execution.
7. Select an Available Database Instance, and click Add.
8. Under Alert Parameters, search for one of the three SQL queries you identified earlier.
   
   ▰ SolarWinds DPA always returns the hash value from a search, even when you select a named query.

9. Under Alert Levels & Notifications, choose an alert level and enter a minimum time in seconds. This
value should be twice as long as the baseline of average wait time for this query.

The average wait time is specific to the execution interval. If the interval is 10 minutes, SolarWinds DPA looks at the average wait time for the SQL statement chosen for that 10-minute period and compares these values to your thresholds.

10. Select a Notification Group or Contact.
11. Click Test Alert, and verify you received the email.
12. Click Save.
13. Repeat steps 3 - 13 for the other two SQL queries you identified.
Advanced analysis

The DPA home page displays a table of the monitored database instances where you can see all of the database types. Click Action to start or stop monitoring.

Instance Groups

You can group monitored databases using the Instance Groups feature. Click ⌁ to add, modify, or delete an Instance Group.

SolarWinds DPA automatically groups Oracle Real Application Clusters (RAC) instances, but does not automatically group other databases.

In addition, SolarWinds DPA 10.1 and later automatically groups Oracle multitenant container databases (CDB) containing pluggable databases (PDB).

Monitoring

Monitoring is always active after it is started. It is not necessary to restart the SolarWinds DPA monitor if the repository instance or the monitored database instance was unavailable for a period of time. Monitoring resumes when both are available again.

If there is a period of time when monitoring should not occur, you can stop monitoring a database instance.

Logs

Next to a database instance, click Action > Log to see the SolarWinds DPA monitoring log. This helps determine why the monitor cannot start, or if data are missing.

Click Options > Support tab > Utilities > Log Viewer to see log entries for all monitored database instances.

Stop monitoring a database instance for a period of time

A blackout is a period of time when SolarWinds DPA stops monitoring a certain database instance.

1. Click Options > Monitor Blackout Periods.
2. Select a database instance from the list on top.
3. Set a day and time to stop and start monitoring, and click Add New Blackout Period.

Enable SNMP Monitoring in SCOM

You can set up SolarWinds DPA to use SNMP to monitor System Center Operations Manager (SCOM).
1. Click Options > Administration > Contacts and Contact Groups.
2. Click Create SNMP Contact.
3. Enter the SCOM host IP address and port in the Trap Receiver fields. The default port is 162.
4. Enter the community string that was set up on the SNMP Service on the SCOM host. 
   - This string is case sensitive.
5. On the SolarWinds DPA server, make sure the SNMP service is running and the community string set matches the string you entered in the SNMP Contact window.

Automatic grouping of Oracle CDBs

SolarWinds DPA 10.1 and later automatically groups Oracle multitenant container databases (CDB) containing pluggable databases (PDB).

Newly registered PDB instances are automatically grouped by the corresponding CDB. If a DBA moves a PDB to a new CDB, SolarWinds DPA processes and groups the instance.

SolarWinds DPA creates a group for a CDB when you monitor two or more PDBs in the CDB. This group is used for all registered PDBs from the CDB.

TURN OFF AUTOMATIC GROUPING OF ORACLE CDBS

1. Click Options > Administration > Advanced Options.
2. Click the ORACLE_CDB_AUTO_GROUP system option.
3. Select False from the New Value list, and click Update.

After you set this option to false, grouping of registered database instances does not change. Only newly registered or updated database instances are affected, and are not grouped.
Link together separate DPA servers

Use Central Server mode to link separate SolarWinds DPA servers together. This is useful if:

- You want to monitor more than 250 database instances. You can divide monitoring tasks between different DPA servers.
- Your monitored databases are distributed geographically. You can install separate DPA servers in each location.

The Central Server collects information from your remote servers and consolidates the data into a single interface. The Central Server has low overhead and no additional information is added to its repository database.

Set up a Central Server

1. Install SolarWinds DPA on a server. This will be your Central Server.
2. Log in to that instance as an administrator.
3. Click Options > Administration > Manage Central.
   Your SolarWinds DPA server should be listed as the Central DPA Server in the list of Registered Servers.

Configure authentication for Central Server

You can authenticate to the Central Server and the remote servers using one account. The account must be added to each server as a SolarWinds DPA user, or through an Active Directory (AD) or LDAP group.

LOG IN WITH A SOLARWINDS DPA USER

You must create the user on the Central Server and each remote server. See Create a user for more information.

The password must match on all servers.

Read-only permissions are sufficient to view data from the remote repositories.

LOG IN WITH AN ACTIVE DIRECTORY OR LDAP USER

You must first set up AD or LDAP on the Central Server and each remote server. See User authentication options for more information.

Next, create the AD or LDAP group of the user on the Central Server and each remote server. See Create a group for more information.

Read-only permissions are sufficient to view data from the remote repositories.
Add remote DPA servers

The user credentials for the Central and remote DPA servers must match. See Configure authentication for Central Server for more information.

1. Click Options > Administration > Manage Central.
2. Click Add Server.
3. Enter information about the remote SolarWinds DPA server.
4. Click Test connection, and click Save.

A successful test indicates that SolarWinds DPA can communicate with the remote server through the provider host and port. It does not indicate that DPA can authenticate users.

If the test fails, check the host name in the Server Name field. Does it contain an underscore (_) character? An underscore is not valid for host names. If you cannot rename the host, enter the IP address.

5. Repeat steps 1 - 4 for the remaining remote SolarWinds DPA servers.

The details of your remote SolarWinds DPA servers are not stored in the repository, but in a file on your Central Server, located here:

<DPA_Home>/iwc/tomcat/ignite_config/iwc/central/RemoteRepositories.json

This is a plain-text JavaScript Object Notation (JSON) file. No sensitive data is stored in this file.

View the Central Server page

The default home page of a Central Server is the SolarWinds DPA home page. Navigate to the Central Server page to see database information from all registered remote servers.

1. Log in to your DPA Central Server as an administrator.
2. Click Options > Administration > Manage Central.
3. Click the Central button.

Central Server advanced configuration

You may need to change the Central Server configuration to make it run more efficiently in your environment.

To change the default behavior, you can edit the system.properties file in the /iwc/tomcat/ignite_config/idc directory of your Central Server and add the desired setting.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.confio.iwc.central.enabled</td>
<td>true</td>
<td>Enables or disables the use of Central Server mode.</td>
</tr>
<tr>
<td></td>
<td>(default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>com.confio.iwc.token.login.supported</td>
<td>true</td>
<td>Enables or disables the use of encrypted login tokens when jumping from the Central Server to a remote instance.</td>
</tr>
<tr>
<td></td>
<td>(default)</td>
<td>If true, a web service call authenticates the user and creates a temporary token to identify the incoming user and bypass the login process.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>If false, the user is always prompted to log in to the remote instance.</td>
</tr>
<tr>
<td>com.confio.iwc.show.all.errors</td>
<td>true</td>
<td>Determines which users see failures in the Unavailable SolarWinds DPA Servers section.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>If true, all users see failures for all instances.</td>
</tr>
<tr>
<td></td>
<td>(default)</td>
<td>If false, only administrators see failures. Set this option to false if you do not want all users to know about other SolarWinds DPA instances in the organization.</td>
</tr>
<tr>
<td>com.confio.iwc.automatic.update</td>
<td>true</td>
<td>Enables or disables a process that performs simple checks on the file when SolarWinds DPA starts.</td>
</tr>
<tr>
<td></td>
<td>(default)</td>
<td>For example, flagging any local instances as the Central Server.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>com.confio.iwc.alarm.level</td>
<td>Warning</td>
<td>The minimum message level to include on the Alarm Details tab. Valid values are below. If (empty) is set, details are disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (empty)</td>
</tr>
<tr>
<td>com.confio.iwc.alarm.count</td>
<td>200</td>
<td>The number of detail rows to show on the Alarm Details tab.</td>
</tr>
</tbody>
</table>
THREAD POOL SETTINGS

These settings control the number of threads that are used by the Central Server to make web service calls to other remote servers. The default settings are set for a few concurrent users hitting up to 100 remote instances. If you have more than 100 instances or many concurrent users, SolarWinds recommends adjusting these settings higher.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.confio.iwc.centralServiceTaskExecutor.corePoolSize</td>
<td>20</td>
<td>The core number of threads that Central Server uses to make web service calls to remote servers.</td>
</tr>
<tr>
<td>com.confio.iwc.centralServiceTaskExecutor.maxPoolSize</td>
<td>40</td>
<td>The maximum number of threads that Central Server uses to make web service calls to the remote servers. Central Server adds more threads only when all core threads are in use and the task queue is full.</td>
</tr>
<tr>
<td>com.confio.iwc.centralServiceTaskExecutor.queueCapacity</td>
<td>1000</td>
<td>The maximum number of requests in the queue before Central Server either creates new threads to help with the work or rejects the request. Tasks are rejected if all 40 threads cannot keep up with the requests being made.</td>
</tr>
<tr>
<td>com.confio.iwc.centralServiceTaskExecutor.keepAliveSeconds</td>
<td>120</td>
<td>The number of seconds to keep an idle thread before removing it.</td>
</tr>
</tbody>
</table>

CLIENT FACTORY CACHE

A client factory creates web service clients that talk to remote instances on a per-user basis. One client factory is created per host:port combination (not per user), so the same factory is used to create individual clients for different users. Factory creation is resource-intensive because an initial handshake is done between the client and server, and kept in a cache for reuse.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.confio.iwc.client.factory.cache.size</td>
<td>100</td>
<td>The maximum number of client factories held in the cache.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is 100, which equates to 100 unique remote SolarWinds DPA instances.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Increase this value if you are connecting to more than 100 remote instances.</td>
</tr>
<tr>
<td>com.confio.iwc.client.factory.cache.timeout</td>
<td>1800</td>
<td>The number of seconds a client factory remains in the cache without being used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is 1800 seconds, which is equal to 30 minutes.</td>
</tr>
<tr>
<td>com.confio.iwc.client.factory.connection.timeout</td>
<td>15</td>
<td>The number of seconds a client attempts to establish a connection before it times out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is 15.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zero (0) specifies that the client will continue to attempt to open a connection indefinitely.</td>
</tr>
<tr>
<td>com.confio.iwc.client.factory.read.timeout</td>
<td>30</td>
<td>The number of seconds the client waits for a response before it times out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default is 30 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zero (0) specifies that the client will wait indefinitely.</td>
</tr>
<tr>
<td>com.confio.iwc.client.factory.enable.chunking</td>
<td>true</td>
<td>Enables or disables HTTP chunking.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>False is the safer option.</td>
</tr>
<tr>
<td>com.confio.iwc.client.factory.enable.log</td>
<td>true</td>
<td>Enables logging of inbound and outbound messaging to capture the web service calls.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Log levels are still controlled in the log4j.xml file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set this value to false to disable logging.</td>
</tr>
</tbody>
</table>
Troubleshooting tips

View logs in the `installDir/iwc/tomcat/logs/` directory.

Make sure a firewall is not running on the computer.

Make sure another process is not using the default SolarWinds DPA ports. If the ports are being used by another process:

- Change the default ports of 8123, 8124, and 8127 by opening the following file in a text editor:
  `installDir/iwc/tomcat/conf/server.xml`

- Update the following lines with new port numbers:

```xml
<Server port="8127" shutdown="SHUTDOWN">
  <Connector port="8123"/>
  <Connector port="8124"/>
</Server>
```
DPA solutions

Answer critical performance questions about your database with SolarWinds Database Performance Analyzer. SolarWinds DPA helps you find the root cause of database delays that affect business applications.

In this section, you will learn how to:

- Identify the top three queries that delay application response time.
- Correlate these queries with system resources to gain perspective.
- Determine the wait bottlenecks that delay response time.
- Diagnose current performance issues.

DPA is an agentless solution that causes less than 1% load on each monitored database. Best results are seen on a heavily used database with problems to solve.

This section assumes DPA is installed and you are monitoring a database.

Record your results at each step of the process. To help you track your progress and record important information, use the DPA worksheet.

Identify the top three query problems

The efficiency of processing SQL queries is one of the most important indicators of database performance. SolarWinds recommends determining which queries are creating the largest delays in the database. The response-time measure is critical because it reflects where users wait on the database. Identifying and improving response time for SQL queries has the biggest effect on the service delivered by your database.

Before continuing, let SolarWinds DPA capture at least two days of performance data so you have a representative sample.
1. Locate the Instances with Highest Wait Time resource on the home screen. The legend entries are sorted by total database wait time.

![Instances with Highest Wait Time](image)

2. Pick a day, and click the bar that represents the instance with the highest wait time.

3. The Trends view displays the top SQL statements for the day.
   The length of each bar represents the total wait time across all sessions. The longer the bar, the longer the users had to wait for a response from the database. The colors represent the individual SQL queries, identified by hash values accumulating the response time delay.

![Top SQL Statements](image)

4. Note the top three SQL query hash values with the highest performance priority, and enter this information into the DPA worksheet.

5. Click the first SQL hash number in the legend to load the SQL Properties dialog.

6. Assign a name to the query, and click OK. This name makes the query more recognizable in DPA reports.

7. Repeat steps 5 and 6 for the second and third hash numbers.
Correlate response time with system resources

You can compare the response time results with system resource usage such as CPU, I/O, and memory. You will learn if specific response time spikes are related to server resources by comparing chart results at the same times.

1. On the home screen, click an entry in the Database Instance list.
2. Below the Top SQL Statements chart, click the Resources tab to see the default resources. Make changes with the controls to the right of each resource.

Viewing the top Wait Types/Events will help you determine which resources have the biggest effect on database response time. For example, if you have db_filesequential_read as a top Wait Type/Event, you should monitor storage layer resource metrics.

3. Click Add Resource Chart, and select the two or three resources of most interest.
4. Note the resource names in the DPA worksheet.

Determine wait bottlenecks that delay response time

After you identify the problematic SQL queries based on response time analysis, you can drill down for details about the problem and identify the cause of the bottleneck.

1. Locate the Instances with Highest Wait Time resource on the home screen.
2. Pick a day, and click the bar that represents the instance with the highest wait time.
   The daily wait time chart loads, which shows the response time delay in each hour of the day and the SQL queries that created the delay.
3. Select a value from the Interval list to adjust the time interval.
4. Is there an hour that had problems or that represents commonly found problems? Click an hour, such as 9PM above, for more information.

5. This view ranks the query bottlenecks in the chosen period. The SQL queries with the most accumulated wait time across all sessions are charted to show the total delay.

6. Click a name or hash on the left to see details on the SQL query.
7. Click the Programs tab to see which programs were executing that query.
8. Note the program name in the SolarWinds DPA worksheet.

IDENTIFY WAITS FOR THE TOP SQL QUERIES

Now that you have detailed visibility to the problematic SQL query, you can identify the cause of the bottleneck.

1. Use the breadcrumb trail in the top banner to go to the previous screens.

2. Click the time interval to return to the Top SQL Statements for that period.
3. For the first query, note how the majority of the bar corresponds to a Wait called db file sequential read. This is the item causing delay in this example.
4. Click the Wait in the legend on the right to see an explanation of the bottleneck and solutions.
5. SolarWinds DPA isolated the top SQL queries creating increased user response time and displayed the Waits responsible for the response time in each one.
6. For the three SQL queries, identify the two or three Waits that comprise more than 75% of the total response time. Enter this information into the DPA worksheet. In many cases, one wait bottleneck is responsible for most of the delay.

**Diagnose current performance issues**

When a problem is occurring, you must be able to diagnose it immediately.

1. Locate the Instances with Highest Wait Time resource on the home screen.
2. For today's date, click the bar that represents the instance with the highest wait time.
3. Click the Current view to examine response time and resources from the past hour.
4. Click an interval, such as 9:50AM above, to drill down into the top SQL queries and performance for smaller time increments.
5. Click the Timeslice tab to see a per-minute breakdown of the response time and resource data.
6. Examine the response time charts, and scroll down to the Resources section to identify a possible correlation.
7. Record current queries and wait events that show performance problems in the DPA worksheet.
The DPA worksheet

Record your actions from the preceding pages.

Identify the top three query problems

Record three SQL statements by hash value:

1.
2.
3.

Assign names to the three SQL statements identified above:

1.
2.
3.

Correlate response time with system resources

Record the system resources that correlate with bottlenecks in response time:

1.
2.
3.

Determine wait bottlenecks that delay response time

Record the program generating the most wait time:

- .

Record the top waits for each SQL query:

SQL1 name:

<table>
<thead>
<tr>
<th>WAIT</th>
<th>PERCENTAGE OF TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SQL2 name:
### Diagnose current performance issues

Record current queries and wait events:

<table>
<thead>
<tr>
<th>CURRENT QUERIES</th>
<th>CURRENT WAIT EVENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>