Data Collection and Processing

Database Visibility

Product Overview

At AppDynamics, we offer enterprise-grade software that enables our customers to monitor and analyze the performance of their business applications and supporting infrastructure. Our Database Visibility Software monitors the performance of the database(s) that support our customer's business applications by visually displaying how database performance is impacting overall application performance, providing data to help troubleshoot database issues, and correlating database metrics with server and application KPIs. The Database Visibility Software can be deployed to customers as either an on-premise installation or as software-as-a-service (SaaS).

The information below addresses SaaS versions of the Database Visibility Software; for on-premise deployments, we do not have access to the data collected by the Database Visibility Software.

What data does the Database Visibility Software collect?

Our Database Visibility Software is designed to collect the types of performance data about a customer's database(s) listed below. Which data types set out below are actually collected and processed by a customer's unique instance of our Database Visibility Software depends on how the customer has configured the Database Visibility Software and the monitored database(s)..

Database query strings and information

This class of data can include any information that may be contained in a database query string "literal." For example, select * from user where UN="[PII]". By default, the query string literal values are replaced by "?" and the values themselves are not passed to the Database Visibility Software for processing. The customer administrator, using the role-based access controlled settings within the Database Visibility Software user interface, can choose to change the default functionality to allow the literal to be collected and sent unmasked to our SaaS infrastructure for processing.

Stored database procedures and execution plans

The Database Visibility Software collects and processes information related to how the monitored database(s) would respond to hypothetical queries. The contents of execution plans may be displayed temporarily by the Database Visibility Software in response to a user's request to view such information, but such information is not stored by the Database Visibility Software.

Database session data

The Database Visibility Software collects and processes information related to database ses- sions. The software collects the session ID and hostname/IP address of the client application machine for every observed query. In databases that support this, the client program name, module, and username are also collected. Where possible, information about blocking and blocked sessions will be collected for processing and analysis.

Database and Query metrics

The Database Visibility Software can be configured to collect the following time series metrics related to the monitored database(s): SQL calls per minute, database availability (times when database has an active connection, number of connections established between the database client and server, time the database spent executing SQL statements. Specific time series metrics can also be collected to track the internal state of the monitored database engine. Additionally, the Database Visibility Software can be configured to collect metrics about individual queries, to metrics such as the number of executions of individual queries and their hardware resource consumptions. The metrics vary between types of monitored databases.

Personal data collection and processing

AppDynamics Software does not require the collection of personal data and does not collect personal data by default. The software customer administrator can choose to configure the software to collect and process payload and parameter information within their application(s), which may contain this information. Therefore, our customer controls whether the AppDynamics Software collects and processes personal data.
For more information about our privacy practices and how we process our customers' personal data, please visit our Privacy Center at https://www.appdynamics.com/privacy.

How is access to data controlled?

We use industry-standard techniques designed to restrict access to and to prevent unauthorized use of our information systems. We require the use of individual user accounts to maintain the integrity of audit trails. User and group management is centralized using single-sign-on systems and access to systems is subject to management approval. Access to all systems that process or store customer data are reviewed and re-approval is required periodically.

How long is data retained?

Information about data retention is set out in the relevant License Entitlement located at: https://docs.appdynamics.com/display/latest/License+Entitlements+and+Restrictions .

Can I delete or rectify data?

Our customers may request information regarding the deletion of data, or make specific requests to have certain data deleted from our systems and records, by emailing privacy@appdynamics.com or opening a ticket with our support teams..

AppDynamics Software collects data from various sources as described above. If the source data are incorrect then the collected data will be incorrect. It is not possible to correct the data within the product but if the source data is corrected, the next time the product collects the data, it will be accurate. Customers can submit deletion requests for inaccurate data.

Is the data encrypted?

Yes; our SaaS software products support encryption of customer data in transit and at rest, including backups.

How secure is the data?

We are committed at all levels to the security of customer data. We have developed a comprehensive security program and organization that is supported by leadership who are committed to proactively managing cybersecurity risk. By focusing on a secure-by-design approach, we seek to weave security into our development practices early and layer security across our architecture to protect its corporate services, supply chain, software distribution, and customer-facing services.

We implement process, and technical controls designed to manage cybersecurity risks. Controls may be physical, technical or administrative in their operation, and they may be preventative, detective, corrective, deterrent or recovery focused in their intent. Controls may include hardware and software functions, processes, and procedures, as well as organizational and managerial structures. Controls are reviewed periodically to ensure they are still appropriate.

We maintain a SOC 2 Type II certification. For more information please visit https://www.appdynamics.com/security

Third parties

We engage third-party service providers to help us provide our products and related services. We maintain an up-to-date list of such third parties and a description of their activities at https://www.appdynamics.com/privacy/subprocessors.