

Data Collection and Processing

Server 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 Server Visibility Software monitors the performance of the server infrastructure that supports our customer's business application(s) by presenting an overview of the entire server landscape in a logical hierarchy, and providing server-related metric data like CPU, memory, disk and networks usage summaries and trends. The Server 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 Server Visibility Software; for on-premise deployments, we do not have access to the data collected by the Server Visibility Software.

What data does the Server Visibility Software collect?

By default, the Server Visibility Software does not collect any parameter or payload values from within the server infrastructure components it is configured to monitor. Our customers' Server Visibility Software administrator may choose to change the default setting and enable the Server Visibility Software to collect command line arguments (outlined below), which, depending on how such arguments are written, may contain personal data. For customers who choose to collect command line arguments for processing, we offer API-driven functionality that allows a customer administrator to exclude certain parameter values within the command line arguments from being sent to our SaaS environment.

Our Server Visibility Software is designed to collect the types of performance data about our customers' server infrastructure listed below. Which data types below are actually collected and processed by a customer's unique instance of our Server Visibility Software depends on how the customer has configured the Server Visibility Software and the monitored server infrastructure components.

Resource utilization data The following types of metric resource performance data about the monitored server(s) can be collected by the Server Visibility Software: CPU usage, disk and memory utilization, number of/status of processes running on the monitored server(s). The AppDynamics Documentation provides an updated and complete list of these hardware resources metrics, available at <https://docs.appdynamics.com> .

Command line arguments The Server Visibility Software can be configured to collect command line arguments that reflect the processes running on the monitored server(s); API-driven filtering is supported to help the customer administrator control what data within the command line arguments are passed to our SaaS infrastructure.

Service availability data A customer administrator of the Server Visibility Software can choose to collect service availability data, which consists of the text response from the service(s), metric representations of the uptime/downtime data for HTTP services hosted on the monitored server(s), information about microservices running within the server(s) (e.g., docker container information and kubernetes labels), and, for servers running on Amazon Web Services (AWS), the relevant AWS tag(s).

Personal data collection and processing

The Server Visibility Software does not require the collection of personal data and does not collect personal data by default. Customer administrators of the Server Visibility Software can choose to configure the Server Visibility Software to collect and process command line arguments (described above), and therefore our customers controls whether the Server Visibility Software collects and processes personal data.

Where a customer administrator chooses to configure the Server Visibility Software to collect and process personal data, we comply with applicable law when we make international transfers of such personal data. For international transfers, we employ the following legally-recognized data transfer mechanisms: the EU-US Privacy Shield, the Swiss-US Privacy Shield, and Standard Contractual Clauses (also commonly referred to as EU Model Clauses).

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> .

Where are data processed?

For most SaaS deployments, the AppDynamics controller resides either in our co-located data center located in Chicago, IL, United States or Amazon Web Services (AWS) regions located in the United States. Additionally, AppDynamics offers a number of geographic hosting options where the AppDynamics controller is deployed in Amazon Web Services locations worldwide. For a list of the current deployment options or details about an existing deployment, customers should contact their account manager.

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 are data retained?

Information about data retention for the Server Visibility 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.

The Server Visibility 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 are corrected, the next time the product collects the data, it will be accurate. Customers can submit deletion requests for inaccurate data.

Are 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>.