IBM Z Data Privacy for Diagnostics

Serviceability without compromising regulatory compliance

Diagnostics and Regulatory Compliance

In an open world, valuable confidential data must always be protected, but that isn't always an easy task. When using problem resolution services of third-party vendors, your data is open and vulnerable. Diagnostic reports, if taken at a certain time, can include sensitive data and when the reports are shared, the sensitive data could be accessed improperly.

Sensitive data at-rest can be protected on premises with pervasive encryption and/or other mechanisms. But if sensitive data was either in-use at the time of an error or explicitly requested by the recovery to be included in a dump, it may be captured in the resulting dump which is available to others for root cause analysis. This can pose a problem for compliance with data privacy regulations. Organizations are often forced to make a choice between serviceability or compliance. Therefore, SVC and stand-alone dumps will be updated to determine processor information and set an indicator in the dump header record to identify redactable dump taken on IBM z15™.

What is IBM Z Data Privacy for Diagnostics?

Part of the problem is that today, there isn't a way for an application to mark their memory locations containing sensitive information to tell the operating system to treat it specially when this memory is captured in a dump. Now, z/OS® will provide infrastructure to enable applications to tag sensitive data and metadata as crucial for problem diagnostics using "sensitive=no." With these tags in place, when a system dump is captured, page's sensitive attribute will also be captured in the dump (in DRPX aka dump record's meta-data). Capturing dumps already impacts system availability, so nothing more will be done at capture time to elongate elapsed time.

Instead, these dumps will be post processed (which satisfies clients requirement of having a complete dump) to redact pages marked sensitive in the resulting dump, which can then be sent to vendors for further analysis. This minimizes the impact of 'securing sensitive data in dumps' on the overall problem resolution times.

Note that only dumps (SDUMPs and stand-alone dumps) taken on z15 will be protected using this approach. Also, clients want an indication if dump has tagged data. Hence, SDUMP will be updated to determine the processor information and set an indicator in the dump header record to identify tagged dump taken on z15.

These dumps will need to be post processed to secure sensitive data before sending them to vendors.

Benefits from IBM Z Data Privacy for Diagnostics

Customized Tagging

The system, middleware, and applications will designate which memory areas contain sensitive information and which do not. Each page's data sensitivity information will be passed with the page at dump capture time. A complete dump with these tags should be post processed, which will redact (eliminate) sensitive pages and create a secondary dump that should be sent to vendors for further analysis.

Data Redaction

With IBM Z Data Privacy for Diagnostics, you maintain control when working with third-party vendors without serviceability. As the diagnostics can contain important information, you decide what sensitive data is shared with that vendor. This capability protects data by redacting anything tagged as sensitive and creating a second diagnostic dump to be shared externally.

System requirements

In order to enable IBM Z Data Privacy for Diagnostics, the following minimum system requirements are needed:

- IBM z15
- z/OS 2.4 or z/OS 2.3
- Exploiters
  - *Db2® for z/OS*
  - *IMS™*
  - *Subsection DFSMS™ components*