ICZ Log Manager 2

SECURITY INFORMATION AND EVENT MANAGEMENT

DO YOU KNOW WHERE YOUR LOGS ARE LOCATED? CAN YOU FIND IMPORTANT INFORMATION IN YOUR LOGS? DO YOU KNOW WHO LOCKED YOUR ACCOUNT? WHO USED A SPECIFIC SERVICE YESTERDAY? HOW OFTEN SPECIFIC EVENTS OCCUR? OUR SOLUTION HELPS YOU FIND ANSWERS TO THESE AND SIMILAR QUESTIONS.

The recent intensive development of information technologies has resulted in a significant increase in the volume of recorded activities in the form of events. The records of many activities are usually stored somewhere but are hard to find, and only stored for a limited period for operational reasons. This is due to the complexity of analyses of large data volumes and the impossibility of maintaining ever-growing data volumes.
It is therefore important to establish a strategy for managing, i.e. collecting, normalizing, saving, archiving and evaluating the events in time.

[ICZ LOG MANAGER]

ICZ Log Manager provides a comprehensive and highly efficient way to work with events. It is based on a NoSQL database with full-text search support. The saved events are accessible through a modern web interface with ad-hoc search support and dashboards for repetitive activities. The dashboards use a wide range of visualizations, particularly various graph types and geographic information displayed on maps.

Collected events are normalized into a uniform JSON dictionary to unify the significance of the individual event fields independently from their origin, and to ensure coherent event evaluation regardless of device type.

Events are further supplemented with categorizing metadata and any missing DNS names and IP addresses.

FEATURES AND BENEFITS

- Collection of system and application events from Windows, Linux and VMware
- Event receiving through the Syslog protocol
- Event format normalization providing for easy evaluation of same-type events across different device types
- Event saving in a NoSQL database with full-text search
- Modern web interface for events search and visualization with dashboards for repeating activities
- Events archiving in JSON format for long-term storage independent from the tool used for their processing

[LEGAL REQUIREMENTS]

Many legal standards (Cyber Security Act, Privacy Protection Act, GDPR) require organizations to collect, archive and evaluate events. ICZ Log Manager is designed to comply with the requirements applicable in the EU.

[EVENTS COLLECTION]

ICZ Log Manager enables the collection of events by means of the Syslog protocol, and includes agents for Windows, Linux, VMware vSphere and vCenter to collect system and application logs as text files. The solution can be enhanced with agents for collecting logs stored in SQL databases.

ICZ Log Collector can be used in large-scale networks for collecting local events and sending them to the central ICZ Log Manager. In the event of communication problems. it saves events to disk and uploads them after the connection has been restored.

[EVENTS NORMALIZATION Í]

ICZ Log Manager normalizes events into a single dictionary with the following structure:

- Event metadata.
- Information about the device that created the event.
- Information about the subject that originated the event.
- Information about any object influenced by the event.

[EVENTS SUPPLEMENTATION]

Events are further supplemented with the following metadata and information:

- **Categories**, enabling the classification of events into areas (network, virtualization, computer, application, etc.), the assignment of a uniform action type (log on, access, modification), their results (successful, denied, error) and importance (information, warning, error).
- IP addresses and DNS names - these will be added if missing, DNS names are supplemented with the domain.

[LOG ARCHIVING]

- Events in JSON format are archived as compressed text files that can be further processed according to the customer's requirements.

[EVENTS STORAGE IN A DATABASE]

- Events in the JSON format are stored in a NoSQL database for a specified period and automatically deleted after its expiration. Older events can be inserted from the archive into the database, if necessary.

[EVENTS EVALUATION]

- The web interface enables ad-hoc events evaluation and dashboard creation for regularly repeating activities. ICZ Log Manager includes a ready set of visualizations and dashboards, while users can also create their own.

[MODULAR SOLUTION]

- ICZ Log Manager is a modular system that can be adapted to the customer's needs - from a single-server solution for a single location to a large-scale network solution using a server cluster for performance and/or capacity scaling and events collecting from a large number of locations.

COMMERCIAL CONTACT

S.ICZ a.s. Na hrebenech II 1718/10
140 00 Prague 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@i.cz