Customer reference

Credigen Bank

Meeting local authority requirements with syslog-ng Store Box

"THE UNIQUENESS OF THE SYSLOG-NG STORE BOX LIES IN ITS FAST, SIMPLE AND EASY IMPLEMENTATION INTO ANY KIND OF IT ENVIRONMENT."

Norbert Laczfi, Head Administrator, Credigen Bank.

Credigen Bank is in 100% owned by Credit Agricole Consumer Finance Group, market leader in France and in several countries in Europe. Credigen Bank's financial background and technical support is provided by its nearly 60 year-old parent company, Sofinco S.A., which is also owned by the Credit Agricole group. Sofinco is constantly growing on the international market, it is currently present in 20 countries and counted 16.7 million customers at the end of 2007. Sofinco was bought in 1999 by Credit Agricole group, leader of the French banking market. Thus, the world's 4th largest bank is standing behind Credigen Bank, whose 160,000 employees are serving 58 million customers with 12.000 branches in 74 countries.

The challenge

CIRCUMSTANTIAL CUSTOM LOGGING AND STRICT REQUIREMENTS

The IT experts of Credigen Bank faced with several logging-related business and technical challenges in the past. Previously, logs were stored by IT systems themselves; the handling of those logs were difficult and time consuming, archiving and retrieval caused extra work due to the lack of centralized log management. Moreover, in certain cases, as a result of suddenly growing log message rates they have even experienced data loss, as well. "Formerly logs were collected by scripts that were different on each platform. Furthermore all queries had to be edited manually that required deep knowledge of the given system's logging characteristics. All this took a lot of energy and time that slowed down the work especially in case of troubleshooting." - says Norbert Laczfi, Head Administrator of Credigen Bank.

On top of the time consuming process of log extraction, the bank's experts also faced with business problems. The Hungarian Financial Supervisory Authority (HFSA), as the controlling authority of the Hungarian financial markets, has strict requirements related to the logging of banking systems and regularly audits banks' practices in this field. In addition, user needs arriving from the bank's different business areas also required an increasingly higher availability of IT systems. Therefore, to handle these complex challenges, the bank's experts looked for a new, central logging application on the market.

Credigen Bank

The Solution

LOG ANALYZING BASED ON SYSLOG-NG STORE BOX

After interviewing several partner companies and examining multiple possible solutions, finally a syslog-ng Store Box (SSB) logging server-based log analyzing application (Logness) was chosen. “The main arguments of selecting SSB were its strong HFSA references, its good value for money and the huge international knowledge base thanks to its open source edition.”- highlights Norbert Laczfi. Credigen Bank has not had experience with BalaBit before, although on their Linux servers they had already been using the free open source edition of syslog-ng (BalaBit syslog-ng Open Source Edition) as a local log collector. Similarly to BalaBit, this was their first project with PR-Audit Ltd., too, partner of BalaBit and developer of Logness log analyzing application.

Selection, planning, implementation, testing and documentation took less than 2 months. On the production environment the following setup is being used:

- on client side:
  - syslog-ng Premium Edition 4.0 log collector application
- on server side:
  - syslog-ng Store Box 2.0 logging server,
  - PR-Audit Logness v1.5 log analyzer system.

The bank has quite a heterogeneous IT environment, where Linux and Windows servers, Cisco network equipments, firewalls, different database-management systems and web servers can also be found. “The established logging solution works together with the different platforms and devices of the bank without any problem.” - adds Laczfi.

It should also be mentioned that the bank operates two business-critical applications that run on less-known database-management systems (i.e. a Linux-based Progress, and a Pervasive SQL running on Windows 2003). SSB managed to handle the logs of these systems also without any problems. Currently there are 40 devices and platforms included under the central logging infrastructure.

The Results

STRONG ANSWER TO THE COMPLEX CHALLENGES

The bank’s experts found a fully adequate solution for all of their aforementioned technical and business problems in the syslog-ng Store Box-based system. SSB fully meets both HFSA’s recommendations and the requirements for fast and efficient log collection. The system can be fine-tuned at any time based on the changes and inquiry needs. “In addition, finding correlation among logs faster has accelerated the troubleshooting process that further increased the availability of our business systems.”- highlights Norbert Laczfi.

About BalaBit

BalaBit IT Security is an innovative information security company, one of the global leaders in developing privileged activity monitoring, trusted logging and proxy-based gateway technologies to help customers be protected against insider and outsider threats and meet security and compliance regulations.

BalaBit, the second fastest-growing IT Security company in the Central European region concerning Deloitte Technology Fast 50 list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Its R&D and global support centers are located in Hungary, Europe.

More information here: www.balabit.com.

Main characteristics of syslog-ng Store Box

- Log collecting application for Unix and Windows platforms
- Encrypted, signed, compressed and timestamped storage
- Easy to integrate into the existing infrastructure
- Forwarding messages for log analyzing applications
- Easy to manage from a browser
- Automatic log archiving and backup

Learn more about syslog-ng Store Box

- syslog-ng Store Box homepage
- syslog-ng Store Box documentation
- Request a trial version
- Request a callback