

DATABASE

TRENDS AND APPLICATIONS

Solutions for the Information Project Team • www.dbta.com

Volume 22, Number 1 • March 2008

Power Company Works to Secure Oracle Data

By Elliot King

The South Mississippi Electric Power Association (SMEPA) is a not-for-profit cooperative that generates, transmits and sells electric energy on a wholesale basis to 11 member distribution cooperatives. The member systems own and maintain around 54,500 miles of distribution lines and provide service to more than 405,000 electric meters in 56 counties in Mississippi.

SMEPA has an intriguing past. In 1936, Congress passed the Rural Electrification Act, which provided low-cost loans to fund the electric power infrastructure in rural America. At the time, less than one percent of rural Mississippians had electricity. By 1940, at least 24 electric cooperatives were formed and the following year, SMEPA was chartered by seven member associations. The plans were sidetracked by World War II and the discovery of new energy sources in Mississippi. In 1958, SMEPA began to implement its charter. It now currently employs about 300 people and it generates in excess of \$600 million in revenue. "Our mission is to get the best wholesale rate for our members," said Carl Lindau, the IT manager.

In 2007, SMEPA began an implementation of Oracle E-Business Suite. It installed a range of modules from HR to Financial to Project Costing to Inventory. The implementation was designed to replace an array of legacy systems, including several that required custom reports. "The company as a whole was grinding to a halt from a process-efficiency standpoint with all

the manual processes," Lindau said.

While the need to move to a more modern, integrated system was clear, the change raised several issues. "The legacy payroll system was on its own server," said Ann Goff, an Oracle DBA and system administrator. "It was totally secure." The scenario is different with the E-Business Suite. The application modules run on the same server and the databases are potentially accessible to a wider community of users.

Security Issues

Goff and Lindau knew that they had to take pro-active steps to address the security issues and protect social security numbers, salary information and other sensitive information.

At the time, Goff became aware of security solutions offered by MentiSoftware. Founded by information security experts, MENTIS provides a strategic set of intelligent controls for companies using Oracle-based systems. Within weeks, Rajesh Parathasarathy, MENTIS founder, CEO and a recognized security expert, assessed SMEPA's security needs. He was able to alert the SMEPA team to several security risks that had not yet been considered. Goff and Lindau had focused their attention on salary and social security information. Parathasarathy pointed out several other fields that could be protected in different ways. He also suggested different approaches to protecting data and different ways to scramble the information. "It was eye-opening," Lindau said.

SMEPA plans to use iScramble, an enterprise-class, full-security data scrambling product that protects non-production databases while maintaining full database functionality, for its test and development systems. Non-production (or "cloned") databases contain all of the sensitive data in the production databases at the time of their creation. Protecting clones is a major gap in most overall IT security strategies. iScramble covers that gap.

SMEPA will use MENTIS' iMask for the production database. iMask protects sensitive data with authorization rules for connections made directly to the database. It can determine who sees either "masked" or "unmasked" data. Finally, SMEPA is experimenting with iProtect, which controls the users that have access to the database. "You have a lot of different options as to how you want to protect your system," said Goff.

"We have a small staff so we need this to be seamless and fold into our processes," added Lindau. "We wanted an audit tool that describes what we are protecting and how we are protecting it - who can access the database and who can't. It gives us the granularity. If there is ever an audit or a disclosure of this sensitive information, we can say how we set up the security. For auditors, we can show the rules and responsibilities - the who, what, when and where of what has been done."

The implementation of the software went very smoothly, taking only a day or so. "We are going above and beyond what we have to," said Goff.