precisely

Case Study:
Campbell County, Wyoming

Journal Audit Reporting Solution Brings IT Staff Unexpected Benefits

Gillette, Wyoming is the county seat of Campbell County, and because it sits on vast quantities of coal, oil and gas, it's known as the "Energy Capital of the Nation." Rocky Marquiss, a Senior Programmer Analyst for Campbell County, along with two other IBM i programmers, are responsible for providing IT services for the busy county administration offices. With all of the usual departments, offices and branches needed to keep county government operations running efficiently, its IBM i programmers don't have time to waste on inefficient audit reporting and security management.

Problem

Periodically users will request information about who made changes to a record and what the changes consisted of. For example, the County Assessor would request information concerning who made changes to a property parcel – often 2-3 months after the fact. Each request requires numerous hours sifting through the long string texts of journal data, parsing and grouping the data, then formatting in a way that an administrator could read to determine who changed what data and when. Despite having a security compliance software package installed, it didn't include capabilities to help with this tedious auditing job.

The Solution

Marquiss learned that Precisely's Assure Monitoring and Reporting generates accurate, fast and readable reports on any database or system journaling activity, and decided to install the product. Says Marquiss, "Assure Monitoring and Reporting now saves us countless hours when we get audit requests that require going back to database journals. I use its query function to show me specific data from selected windows of time and within 30 minutes I have a nicely formatted PDF report delivered to the department head."

Using the IBM i journaling functionality to record system events and database changes, Assure Monitoring and Reporting allows companies to meet regulatory compliance by detecting fraudulent activity through the easy generation of accurate, relevant, and readable reports on database and system activity. IBM i journals are the only accepted audit source for the majority of regulatory standards.

Easily scalable and with minimum impact on system

Fast Facts

Campbell County's IT department runs an IBM Power Systems server with 700 gigabytes of disk storage, two IBM i LPARS, an AIX partition and 1 Linux partition. A JD Edwards ERP application runs in an IBM i environment to manage accounting activities such as payables and receivables, and several homegrown IBM i applications manage the processing of motor vehicles, property taxes and assessment transactions.

The Campbell County programming team had its hands full sifting through database journals to find information required for audit reporting, watching for security breaches, and worrying about downtime and the risk of data loss in the event of a disaster. They needed a way to report efficiently on the audit data contained in journals, set and monitor security policies, and ensure optimal journal management for disaster recovery purposes.

> "Assure Monitoring and Reporting now saves us countless hours when we get audit requests... within 30 minutes I have a nicely formatted PDF report delivered to the department head."
>
> – Rocky Marquiss, Sr. Programmer Analyst, Campbell County, Wyoming

performance, Assure Monitoring and Reporting can be used by companies of all sizes and is fully compatible with all the most commonly used ERP systems on the IBM i.

An Unexpected Bonus

Marquiss evaluated other products but chose Assure Monitoring and Reporting when he discovered to his surprise how the product efficiently handles journal receiver storage requirements.

Campbell County uses a data vaulting product to augment its disaster recovery capabilities. This product relies on system and database journals to recreate data in the event of a system or site disaster. For auditing purposes, Marquiss was required to maintain six months of journal receivers on his production system, which was dramatically impacting the amount of data that could be recovered after a disaster. The reason for the impact: IBM i journaling processes need to track the state of all journals on the system which significantly slows down the frequency that journal data can be prepared by the vaulting product and sent to the offsite DR repository. This in turn constrained the vaulting product to transmitting its data recovery information from the production server to the offsite storage location at three hour intervals. Therefore, in the event of a disaster, Campbell County could lose up to three hours worth of transactions, which was a large data-loss exposure.

When Assure Monitoring and Reporting was installed for journal audit reporting, Marquiss discovered that the product had the ability to filter journal receivers and transform the parsed data into secured physical files. This allowed him to reduce the journal receiver storage on the production system from six months worth of journal receivers to two days, which instantly changed his disaster recovery data-loss exposure from three hours to 30 minutes. In addition, it significantly reduced the disk space required to store journal information.

"We went from 66% of disk storage utilization to 48% after converting journal receivers with Assure Monitoring and Reporting", Marquiss says. "In addition, the system is realizing measurably better performance. Plus, I now can do audits on the production system going back 10 months instead of six while still saving a huge amount of disk storage. It's been a win-win: I use less disk space, the system run faster, I can prepare audit reports for management more quickly, and mydisaster recovery situation is much improved. Assure Monitoring and Reporting quickly paid for itself."

Consolidated IBM i Security Management from Precisely

Marquiss and his team were so happy with the performance of Assure Monitoring and Reporting and the support they received from Precisely they decided to replace their security policy and access control product with Assure System Access Manager so as to centralize security management with a single vendor.

"Assure System Access Manager is far more flexible and robust than our previous product. Because of that it took a little more time to configure, but having a more feature-rich product is well worth it," Marquiss says. A big benefit of Assure System Access Manager for the Campbell County IT team is its command line data point access, which allows them to manage security policies for IBM i commands. Marquiss concedes, "Sure, I can secure command line functions through IBM i security, but it's nice to have everything available in one set of tools."

Marquiss found that Assure System Access Manager has less impact on performance than their previous access-control product. He also likes many of its features, including the product's ability to block and audit the SQL engine based on pre-defined policies; its more flexible rules that include a large vocabulary for rule definition; and its ability to produce reports in a wide range of formats including .XLS, .CSV and .PDF.

Says Marquiss, "Assure System Access Manager runs in real time and lets me know about exceptions that occur to my security policies so I can decide if I need to lock something down. It also shows me any violations so I can document them and report to management."

Marquiss has two nightly reports automatically generated and sent to him by email: one displays a summary of journal entries archived from the previous day, and the other shows all policy violations. He can also get real-time alerts that notify him of security policy violations.

Simulation Mode

"Another great feature of Assure System Access Manager is its simulation mode," adds Marquiss. "In minutes I can generate and test a new policy rule. Simulation mode is a great way to see how a new security policy will affect users without having to actually lock down the system and as a result field a bunch of angry phone calls. Only when the policy is fully tested and fine-tuned do we deploy it into the live environment."

Marquiss and his team no longer waste hours sorting through cryptic journal data, worry about security administration, or face exposures to significant data-loss after a disaster. Concludes, Marquiss: "With Assure Security, we were able to solve a myriad of problems with proven solutions from a single vendor that continually enhances its products and gives us great support."