

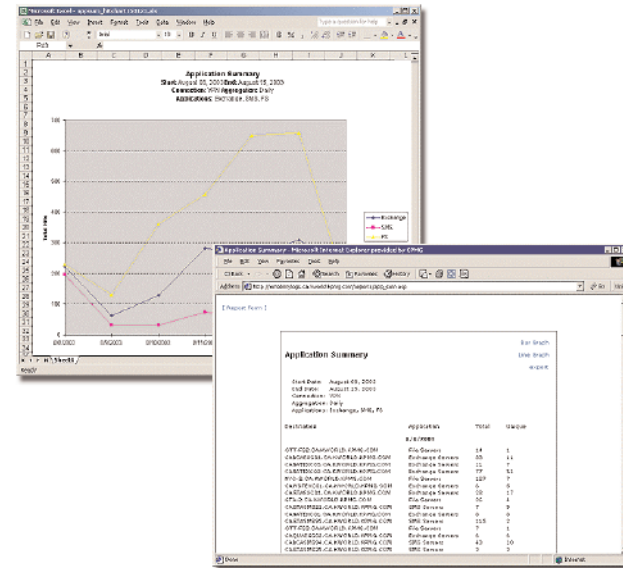


case studies



KPMG CONSULTING

GLOBAL NETWORK MONITOR



CLIENT OBJECTIVE

KPMG, a leading financial consulting firm, required an application to monitor and produce reports for all Canadian remote access activity. The client needed a system to compare historical trends and data volumes for each user and connection type in graphical and textual format.

The application requirements included:

- Next day reporting on all activity from previous day by 8:30am
- Application Summary, Detail Use Activity, Connection Summary and Connection Comparison Reports
- Detailed historical data for 60 days, Summary historical data indefinitely
- Secure report access through KPMG's national intranet
- Ability to receive and import data from EGAP, VPN, and RAS logs

CASE STUDY: KPMG: GLOBAL NETWORK MONITOR

CHALLENGES

This data system needed to gather activity data from RAS, VPN and EGAP connection types from across the KPMG network. Each one of these services has a different format so the data needed to be converted into a common format to log into the system. The various systems were located in different locations. Some log did not have any logout information.

Several hundred megabytes of data needed to be parsed and inserted into a database in less than 90 minutes to meet the requirement of next day reporting by 8:30am. This was further complicated by the complex filtering rules needed to categorize the application data.

All application activity was to be associated with a particular connected user. This was a challenge because all application activity was contained in a separate DNS log which did not have any user information.

Develop professional reports with graphical charts that could be accessed by the KPMG systems group across the country.

SOLUTION

JIG worked with the KPMG to assess the current log formats of the various connection types. This allowed JIG to develop a parser for the various formats. To overcome the challenge of varied locations JIG worked with KPMG to develop a secure mechanism to place all log data into one central location before the parsing would be done. To address the lack of logout information an algorithm was developed to associate connection timeouts with application activity.

A high performance parser was built to parse and insert data into the database. This was developed in Perl to handle the parsing and complex filtering rules. To store data on the order of 10 million records SQL server was used. This DB implementation was highly optimized with stored procedures and indexes to obtain the needed performance.

The association of user information to application activity required an IP lookup in the connection data in the database. This solution did not scale well as the database increased in size. A LIFO caching system was implemented in the parser to gain the desired parsing performance.

To allow reports to be accessed from across the country JIG developed a web based ASP.NET application. The graphs were generated using the Excel chart wizard COM object. This application was made available through a secured intranet.

Technologies Used

- ASP.NET
- Chart Wizard COM object.
- Perl
- MS SQL Server

OUTCOME

JIG's diversity of required skills across networking and application development enabled JIG to build and deploy an application that met all of KPMG's requirements. KPMG currently uses this system and has been well received by both management and operations. The data provided by the Network Monitor created by JIG allows KPMG to analyze connection patterns and application usage. This has helped to save costs and increase connection reliability by understanding what systems are under utilized and over utilized.

JIG developed this system in an object oriented manner to easily allow for additions and ongoing maintenance. New log parsers can be developed in a modular way without affecting the rest of the application.