Information Technology Company

Government Accountability Office Uses System z® to Support Federal Government Performance and Accountability

review

Challenge

The U.S. Government Accountability Office (GAO) — Congress's investigative arm and watchdog — monitors how the vast federal government spends trillions of taxpayer dollars, providing timely and objective information to Congress.

Solution

Working with IBM and Information Technology Company, LLC, GAO's e*Security Lab uses System z to fully replicate diverse government agency enterprise computing environments and to audit complex applications involving massive databases comprising hundreds of millions of records.

Key Benefits

Cost-effective scalable/reliable architecture supports increasing major security audit workload. Sensitive data — often containing citizens' personally identifiable information — is held safe from disclosure or tampering, complying with multiple rigorous requirements for data protection. Flexibly partitioned virtualization supports multiple simultaneous production/test/migration environments.

GAO's vital work is done at the request of congressional committees or subcommittees, or is mandated by public laws or committee reports. It also undertakes research under authority of the Comptroller General; it supports congressional oversight by:

- auditing agency operations to determine whether federal funds are being spent efficiently and effectively;
- investigating allegations of illegal and improper activities;
- reporting on how well government programs and policies are meeting their objectives;
- performing policy analysis and outlining options for congressional consideration;
- and issuing legal decisions and opinions, such as bid protest rulings and reports on agency rules.

In addition, GAO advises Congress and the heads of executive agencies about ways to make government more efficient, effective, ethical, equitable, and responsive. Its work leads to laws and acts that improve government operations, saving the government and taxpayers billions of dollars.

Keeping Government Computing Secure

GAO frequently makes news, often with headlines such as "Last Year's IRS e-Filing Hacker Friendly", "EPA Closes Web Site", and "Too Many Weaknesses in FAA Information Systems".

GAO
U.S. Government Accountability Office

Evaluations such as these are done by GAO's e*Security Lab, part of the Center for Technology & Engineering in the Applied Research & Methods organization. This System Z based lab evaluates government agency security in areas such as safeguarding data and detecting internal/external threats, reviews include physical and logical testing, and intensively audits real data such as IRS accounts receivable.

The lab's Senior Assistant Director, 35-year government employee Edward M. Glagola, Jr., explains, though, that agencies don't receive a pass/fail grade. Instead, problem are reported via two reports: a public version summarizing results, and a restricted version describing specific issues.

Security audits involve selecting key IT control points, conducting thorough test and evaluation using manual and automated tools and techniques, and analyzing results in the context of agency missions, business activities, and network connectivity. This can be as simple as assessing network router settings and configuration, or as inclusive as reviewing all network management access methods (SSH, etc.).

Typical weaknesses encountered include applications, DBMS, and operating systems missing security patches; unnecessary and vulnerable services running; use of default or easily guessed passwords; application input not effectively validated; and ineffective system monitoring and logging. Audits also review software status; products too old, or off vendor support, are flagged as major-finding security risks.

Protecting agency data and sensitive information from corruption or tampering is a paramount obligation. Glagola notes that complying with FISMA, HIPAA, OMB, and NIST requirements for data security can be difficult. "GAO gets audited also," he continues, "so our data center must comply with the same standards and practices that we impose on other agencies." The greatest opportunity he sees is showing audited agencies that data center security can be achieved without hindering their operation or support functions.

Congress mandates annual audits for major federal agencies. Audits begin with scope definition; then systems to be included are identified and an appropriate team of specialists is assembled. Planning meetings determine system-specific scope, evaluation criteria, and tools to be used.

Initial on-site work consists mostly of data collection, with review and analysis performed at GAO. Regardless of size or manufacturer, complete data is gathered for all systems, including application and system files and full hardware/software configurations. Relatively large mainframes are common at federal sites; it's not unusual to find a 15-way IBM System z9 sporting several thousand MIPS with ultra-large and complex file structures. Fortunately, GAO-developed tools make data collection almost automatic. Data is processed through several software tools to identify risks and anomalies, but much analysis still requires skilled staff reviewing material such as hardware configuration definitions.

The e*Security Lab began in 1994 using a single R/390 (Risc/AIX system with a P/390 expansion card) running OS/390 and CICS. Falls Church, Virginia-based Information Technology Company, LLC (ITC) was engaged in 1997 to support the R/390 and provide expertise to configure and install the z800. GAO defined lab objectives and ITC created and implemented the design. ITC provides day-to-day systems administration, monitoring, management, and help desk support. Lab and ITC staff share operations support duties.

IBM supplied all mainframe hardware, including ancillary servers, workstations, and printers. Networking equipment is branded Juniper, CyberGuard and Pix.

ITC president Stan H. King notes that audits sometimes involve delving into computer history, encountering devices such 9-track tape drives and IBM Series/1 computers at IRS, or Patent and Trademark's huge Sony optical drives using two-foot diameter platters to hold patent documents -- dating back to 1789 --- in image format, connected to an Amdahl-hosted MVS environment.

Partitioned Virtualization Supports Production, Test, Migration

One z800 logical partition (LPAR) supports production work under z/OS Version 1.8, processing data for all audit work. The variety of environments audited is reflected in the three test LPARs running z/OS Version 1.9, each with a different security manager: RACF, CA-ACF2, and CA-Top Secret. These LPARs test security controls observed in the field for security risks. Another LPAR runs z/OS Version 1.10 for testing. Eventually, the new z/OS will become the production LPAR image and the next release will begin testing. The lab uses even-numbered operating system versions/releases for production, while odd-numbered

systems are used in test LPARs. Finally, a VM/Linux LPAR hosts future workload evaluation and test, with virtual Linux servers provisioned as needed using consultant-built VM tools. All resources are VM-owned and allocated to guest Linux machines based on requirements.

Migrating z/OS releases uses a cookie cutter approach with common libraries and system files providing standardized configuration settings to put new images into service quickly — relying heavily, Glagola notes, on internal documentation and extremely detailed functional specifications serving as blueprint for all activity. They know so much about z/OS internals and inner workings of their various hardware components that they can quickly focus on specific features for analysis and tighter configuration controls.

Gene Stevens/Data Clarity

> "I doubt that such a large data structure could have been processed on anything less than a mainframe."
>
> *– Edward Glagola*

Network management is simple and straightforward. The production LPAR has two dedicated OSAs, for primary LAN attachment and for auto-failover and recovery. Networks are front-ended by multiple firewall products for security control. Activity on the production LPAR network is monitored by Network Security staff, and remote access for telecomputing is secured through VPN (virtual private network) technology and RSA SecurID two-factor authentication.

Production LPAR processing activity is monitored around the clock. Vanguard Security software products automatically notify operations and system administration staff of processing or network rules violations. Weekly reviews of system event and security logs provide additional visibility for processing activity; internally developed tools and utilities audit the system for anomalies needing investigation.

Because of the Lab's unique mission — replicating government agency environments and analyzing their real-world data -- system utilization varies with tasks at hand. TSO utilization is light; test LPARs see only two or three users daily and production TSO involves about eight users per day.

Batch work dominates. Overall processor utilization is about 40% most days when audit jobs are not running. But when audit data is being processed, CPU usage pegs 100% for 48 hours or longer, because data structures tend to be very large and jobs routinely process 200 million records through SAS for one analysis. Frequently, several batch jobs run simultaneously, with each processing hundreds of millions of records.

Auditing Into the Future

The venerable z800 and associated peripherals are due for a technology refresh. ITC's King observes that capacity planning for such a variable workload is challenging. "We looked at SMF and RMF records to evaluate peak processing and resource allocations," he says, "seeing large intervals with minimal processing and the machine nearly idle. Then when an audit runs or we receive a request from a congressional subcommittee for investigative research, we're at peak utilization."

Most heavy workloads are batch SAS jobs processing massive data structures with multiple hundreds of millions of records, so I/O performance is critical. From past experience, Glagola notes, starting with a small system configuration and planning future expansion was problematic because of budget cycle difficulties. So new system acquisitions are now configured with all features expected to be needed during the first two years after initial order.

In September 2009, the z800 was replaced by a larger z10 BC with more memory, more FICON channels, and additional OSA capability. The Enterprise Storage Server (SHARK) was upgraded to a new, larger DS8700 DASD subsystem. The tape library was enhanced and expanded to include newer tape drives, while retaining existing 3590 and 3592 drives.

An open issue is the Virtual Tape Server, which Glagola calls, "the most trouble free peripheral subsystem we ever bought." He continues, "It worked right out of the box, almost 100% plug and play, and has provided problem-free

processing ever since." He likes the completely hardware-based implementation but notes that they may switch to the newer software solution.

Users include GAO e*Security Laboratory auditors performing physical IT security audits of federal agency mainframes and GAO auditors conducting operational audits. GAO Auditors are not necessarily limited to the area of IT Security audits; they also respond to congressional requests for investigation or information. IT auditors -- such as those from the lab -- only perform the mainframe portion of security audits.

Glagola feels that the System z based e*Security Lab provides stellar data processing service to GAO. He recalls that during one congressional investigation, analysis of records over a 10-year period was required; he doubts that such a large data structure could have been processed on anything less than a mainframe. "We retrieved classified data for millions of individuals." he says, "You can't imagine the strain that hundreds of millions of records can place on a system. Everything was passed through DFSORT and SAS several times to create required reports. It was a masterpiece of processing done on time and under budget. You gotta love it."

GAO's Glagola and ITC's King agree that costs are a determining factor in selecting system architecture and see great potential for improved application performance and serviceability if moved from a VMware Windows/Intel environment to the mainframe.

As federal operation grows and becomes more complex, GAO's e*Security Lab accommodates challenges of auditing rapidly evolving technology to fulfill its stewardship mission of monitoring government-wide spending and operation. System z's traditional"ities" (scalability, operability, manageability security, availability, reliability, serviceability, and flexibility), well-trained and motivated staff, and just a bit of paranoia serve to keep agency data processing secure and honest.

Solution Components

Hardware

IBM System z10-BC
IBM Enterprise Storage Server
IBM MagStar Tape Library Subsystem
IBM MagStar External Tape Subsystem
IBM Virtual Tape Server

Software

z/OS 1.10 and 1.12
JES2
Security Server
DFSMS/DSS-RMM-HSM
Communications Server
SDSF
DFSORT
Encryption Facility
Vanguard Security Software Suite
SAS/Foundation Base
MXG
CA-Examine
DYL-Vision Results
DYL-Audit
CA-ACF2
CA-TOPS

7389 Lee Highway Suite 210
Falls Church VA 22042
800-994-9441 Fax 703-237-0223
www.p390.com