Rocket® software

Audit Logging for Rocket® UniVerse and Rocket® UniData®

Improve security | Assist with compliance and audits

Contents

Introduction

Every day brings a new and complex set of interactions, events, and activities within your business applications and data. But what happens when something unexpected occurs? Whether for security best practices, regulatory compliance, or passing an audit, organizations today need to understand what's happening with their data and applications.

Compliance is a key driver for introducing Audit Logging to a Rocket® UniVerse or Rocket® UniData® implementation. You must be both accurate and fast in achieving compliance. Beyond compliance, Audit Logging also assists organizations with:

- **Accountability:** Identify accounts tied to certain events, helping you make informed decisions about training or disciplinary actions.
- **Reconstruction:** Track data to the "tick" (microsecond) level, sequentially within each process, to understand what happened before and during an event.
- **Intrusion detection:** Investigate unusual or unauthorized events, such as failed logins or logins outside of designated schedules, to detect potential security breaches.
- **Problem detection:** Analyze log data to uncover issues requiring attention, such as resource usage concerns or failed jobs.
- **Customization:** Tailor audit log data to meet your unique business needs by creating custom triggers throughout your application. Leverage the User Event Logging feature's versatility to customize event logging as needed.

Back to contents

Audit Logging

With Audit Logging, organizations running Rocket UniVerse or UniData can strengthen their security posture by gaining insight into activities within their data and application environments. This proactive approach allows them to identify and address underlying issues effectively.

For example, by implementing Audit Logging, organizations can easily detect unauthorized access, such as a user viewing clients not assigned to them or accessing sensitive information like Social Security numbers. Proper logging helps auditors to pinpoint improper access and identify patterns of abuse, thereby mitigating potential security threats.

The basic principles of Audit Logging in UniVerse and UniData involve monitoring system, data, and user resources that trigger events. An audit event is an action on a database entity, which could include a user running a maintenance program that accesses files, system resources, programs, or utilities. For details on event types, please refer to Appendix A.

Audit Logging always logs:

- **System-level configuration changes**
- **Security operations**
- **Data encryption operations**
- **The starting or stopping of UniVerse or UniData background processes**

Logging database resource usage and related authentication and authorization operations can significantly cut the time needed to prepare for compliance audits and increase your chances of passing them. Whether you're preparing for HIPAA, HITECH, PCI-DSS, SOX, GDPR, the Fair Credit Reporting Act, or other regulations, Audit Logging provides you with the data you need. It also includes reporting and archiving features to help you easily demonstrate compliance.

Audit Logging: Change Data Capture

Change Data Capture (CDC) records changes at the individual field level instead of at the record level. Field-level CDC offers several benefits:

- **Define what triggers an event based on individual field changes you specify.**
- **Track exactly what data was changed, by whom, and when.**
- **Enjoy low to no performance impact since field-level CDC captures less data.**
- **Meet regulatory requirements like PCI and HIPAA with ease by capturing precise changes.**

This reduces the time, resources, and costs associated with audit data compliance.

> "Audit Logging allows users to check off numerous compliance questions during security audits."
>
> **Steve McConnell,**
> Columbia Ultimate Technical Support Supervisor

Back to contents

Improved Performance

We've enhanced performance by making Audit Logging multi-threaded and streamlining the audit architecture. This new design minimizes the number of processes interacting directly with the Audit Logging product. For example, instead of using separate processes, a single process now reads the configuration file, updates the Audit Logging environment, and manages events and user audits. You can configure up to eight audit threads to run simultaneously, each handling a large volume of logging processes.

Log Only What You Need to Log

Audit Logging now also offers simplified reporting by allowing you to log what you need.

- **Flexible:** Configure it through policies to log events selectively or collectively.
- **Easy to Configure:** Authorized users can change Audit Logging on the fly without having to stop or restart the application.
- **Customizable:** If we don't currently log it, you can add a custom event to your code, which will then be logged just like any other audit event.

One of our Rocket customers, who must adhere to the Fair Credit Reporting Act, uses Audit Logging to record user access to sensitive customer data and other events that might indicate a security breach. They create an exception report to focus on what matters most, such as unauthorized access and potential security threats. The result? Simplified reporting and reduced demand on system resources.

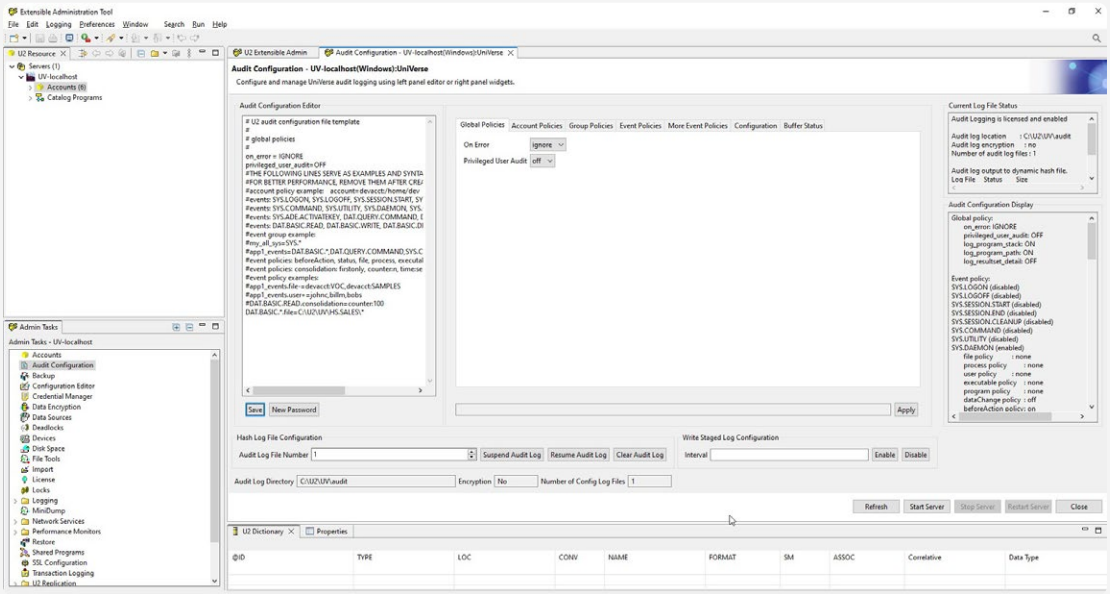

Figure 1: If you're in IT and responsible for supporting a department dealing with compliance and audits, you need to be able to easily manage UniVerse and UniData Audit Logging. UniVerse and UniData offer a graphical user interface (GUI) through XAdmin or a command-line interface, to monitor and maintain your audit environment.

Back to contents

Automatic Audit Compression

Automatic Audit Compression helps manage data size and reduces the need for extra storage capacity, since audit log files can become massive. Alternatively, you can use the non-compression function for a more granular view of the changes in your data.

Simplified Reporting

During an audit, you need to demonstrate your company's compliance, and Audit Logging can help do it. By creating reports from the audit log, you can quickly and accurately answer common audit questions, such as:

- Who updated, deleted, or changed an account?
- When did a specific user log in or out of an account?
- Which users have accessed specific data, and when?

Audit Logging provides three configurable file types for reporting:

- **Hashed file:** Offers the ability to use the native query language of the UniVerse or UniData database.
- **Sequential file:** Compatible with popular reporting tools and significantly improves performance.
- **UNIX syslog and Linux rsyslog:** Can be directed to another system for "offload" reporting.

Stronger Security

We've made Audit Logging more secure than ever. Now, only authorized users can modify the encrypted Config file, which can also be password protected. Additionally, you have the option to encrypt the Audit Log file.

Upgrade your UniVerse and UniData and Harness the Power of Audit Logging

Whether for audits, compliance, security, or resource-problem detection, Audit Logging provides a comprehensive, flexible, and easy-to-configure solution for monitoring your UniVerse and UniData databases and application activities.

Contact Rocket Software or your application provider today to schedule a demo.

Request a demo

Back to contents

Appendix A:

UniVerse and UniData Audit Logging classifies the following events as:

UniVerse and UniData system events

- SYS.LOGON: A user logon request through one of the UniVerse or UniData servers
- SYS.LOGOFF: A user logs off from a UniVerse or UniData server
- SYS.SESSION.START: A UniVerse or UniData session is initiated
- SYS.SESSION.END: A UniVerse or UniData session ended
- SYS.ADE.ACTIVATEKEY: Automatic Data Encryption key activation and deactivation
- SYS.COMMAND: A TCL (ECL in UniData) command has been run, other than query commands
- SYS.UTILITY: Running of any UniVerse or UniData utilities

NOTE: SYS.COMMAND and SYS.UTILITY can be restricted to a subset of TCL (ECL in UniData) commands or utilities

System configuration events

- SYS.CONFIG.CHANGE A system-level configuration changed, such as a uvconfig, audit configuration, or replication configuration change
- SYS.SECURITY SQL GRANT, REVOKE, future security operations
- SYS.ADE Automatic Data Encryption operations: master key, key store, key creation, key deletion, file encryption, index encryption, password related operations
- SYS.DAEMON Starting or stopping of UniVerse or UniData background processes, such as U2Rep services

Data events

- DAT.QUERY.COMMAND LIST, SORT, SELECT, SUM, REFORMAT, COUNT, TLOAD, TDUMP, CVIEW SQL SELECT
- DAT.QUERY.RESULTSET LIST, SORT, SELECT, SUM, REFORMAT, COUNT, TLOAD, TDUMP, CVIEW SQL SELECT
- DAT.BASIC.READ BASIC READ, READV, MATREAD, SELECT, SELECTINDEX, READSEQ, READBLK, BSCAN
- DAT.BASIC.WRITE BASIC WRITE, WRITEV, MATWRITE, WRITEBLK, WRITESEQ, WEOFSEQ
- DAT.BASIC.DELETE BASIC DELETE, CLEARFILE
- DAT.SQL.COMMAND SQL commands, except SELECT, GRANT, and REVOKE
- DAT.CLIENT.DELETE Client delete operations on the server, including CLEARFILE, DELETE, DELETESET
- DAT.CLIENT.READ Client read operations on the server, including READ, READBLK, READSEQ, READV, READSET, READSETFIELDS
- DAT.CLIENT.WRITE Client write operations to the server, including WRITE, WRITEBLK, WRITESEQ, WRITEV, WRITESET, WRITESETFIELDS

NOTE: DAT.*.WRITE and DAT.*.DELETE events will also capture the before/after data associated with the Change Data Capture capabilities of UniVerse and UniData Audit

User event

- USR.EVENT User-defined audit event through the new UniVerse and UniData BASIC AuditLog() function

About Rocket Software

Rocket Software is the global technology leader in modernization and partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,000 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located around the world. Rocket Software is a portfolio company of Bain Capital Private Equity. Follow Rocket Software on **LinkedIn** and X (formerly Twitter) or visit **RocketSoftware.com** to learn more.

Modernization. Without Disruption.™

Visit RocketSoftware.com ›

Rocket software

MAR-10998_UniVerseAuditLogging_Whitepaper_v2