



Monitoring Privileged Access on SQL Server

Sponsored by



© 2015 Monterey Technology Group Inc.



Thanks to

• Made possible by



www.logbinder.com

© 2015 Monterey Technology Group Inc.



Preview of Key Points

- Privileged access in SQL Server
 - Authority model
 - Types of activities
- Auditing in SQL Server
- Auditing privileged access
 - Server operations
 - Database operations
 - Data access
 - Delegation
- Getting SQL audit data to your SIEM
- LOGbinder for SQL Server



Privileged access in SQL Server

- Roles
- Permissions

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Privileged access in SQL Server

- Roles
 - Like groups in Windows
 - Types
 - Server
 - Assigned server level permissions
 - Members
 - Logins
 - Server roles
 - Database
 - Assigned permissions to Database, Schema, Schema objects
 - Members
 - Database users
 - Database roles

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

Privileged access in SQL Server

- Permissions
 - Much like permissions on files in Windows
 - Granted at levels
 - Server
 - Database
 - Schema

Privileged roles and permissions

- Fixed server and database roles
- <http://social.technet.microsoft.com/wiki/contents/articles/2024.database-engine-fixed-server-and-fixed-database-roles.aspx>

Auditing in SQL Server

- Define audit policy
 - Server level
 - From SQL Server 2012 onwards, available in all editions
 - Database level
 - Only available in Enterprise editions
- Audit specification
 - Action group
 - Object
 - Principal

Auditing privileged access

- Not about auditing
 - Application
 - End-user
- About auditing DB admins and other privileged users
- How not to audit everything
 - Audit infrequent privileged operations performed by all
 - Backup database
 - Manage DB encryption
 - Audit other significant actions performed by known admins
 - Direct queries or updates to important tables
 - Monitor delegation of privileged access
 - Permission changes
 - Role membership changes
 - Ownership changes

Server level operations

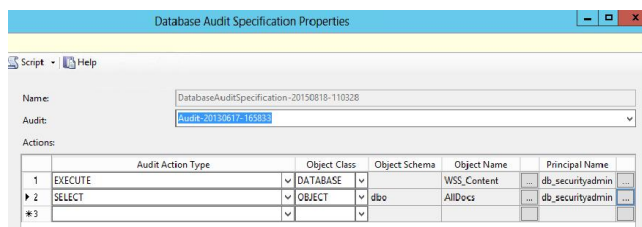
- Server level action groups to audit
 - APPLICATION_ROLE_CHANGE_PASSWORD_GROUP
 - AUDIT_CHANGE_GROUP
 - BACKUP_RESTORE_GROUP
 - LOGIN_CHANGE_PASSWORD_GROUP
 - SERVER_OBJECT_CHANGE_GROUP
 - SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP
 - SERVER_OBJECT_PERMISSION_CHANGE_GROUP
 - SERVER_OPERATION_GROUP
 - SERVER_PERMISSION_CHANGE_GROUP
 - SERVER_PRINCIPAL_CHANGE_GROUP
 - SERVER_PRINCIPAL_IMPERSONATION_GROUP
 - SERVER_ROLE_MEMBER_CHANGE_GROUP
 - SERVER_STATE_CHANGE_GROUP
 - TRACE_CHANGE_GROUP
 - <https://www.ultimatewindowssecurity.com/sqlserver/auditpolicy/auditactiongroups/default.aspx>
- Audit for public role

Database level operations

- Database level action groups to audit
 - DATABASE_OBJECT_CHANGE_GROUP
 - DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP
 - DATABASE_OBJECT_PERMISSION_CHANGE_GROUP
 - DATABASE_OPERATION_GROUP
 - DATABASE_OWNERSHIP_CHANGE_GROUP
 - DATABASE_PERMISSION_CHANGE_GROUP
 - DATABASE_PRINCIPAL_CHANGE_GROUP
 - DATABASE_PRINCIPAL_IMPERSONATION_GROUP
 - DATABASE_ROLE_MEMBER_CHANGE_GROUP
 - SCHEMA_OBJECT_CHANGE_GROUP
 - SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP
 - SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP
 - <https://www.ultimatewindowssecurity.com/sqlserver/auditpolicy/auditactiongroups/default.aspx>
- Audit for public role

Audit other significant actions performed by known admins

- Direct queries or updates to important tables
- Select, update, delete on important tables by privileged user
- Execution of stored procedures
- Understand
 - Application authority model and architecture
 - Which tables are important
 - Confidentiality
 - Integrity
- How



ULTIMATE WINDOWS SECURITY .COM

LOGbinder

SQL Server

Privileged user activity

Next step

Your SIEM

logpoint solarwinds LogRhythm
EventTracker GFI McAfee
IBM RSA
ArcSight splunk

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

SQL Audit

- Output – 2 different formats available
 - Windows event log
 - binary file format readable through a stored procedure

ULTIMATE WINDOWS SECURITY .COM

LOGbinder

SQL Audit


- Event log obvious choice?
- 5 reasons why you shouldn't use the event log
 - Performance
 - Security
 - Stability
 - Hard to understand
 - DB admin push back


ULTIMATE WINDOWS SECURITY .COM

LOGbinder

SQL Audit


- Binary audit log
 - Output to any folder on network
 - SIEM connector can then read it with zero-touch to production DB server
 - Hands off!
 - Fast, fast, fast
 - Binary file I/O is the fastest there is
 - No context changes flipping in and out of Windows API
 - Both directions







SQL Audit

- But how do you get the binary audit log into your SIEM?
 - LOGbinder SQL

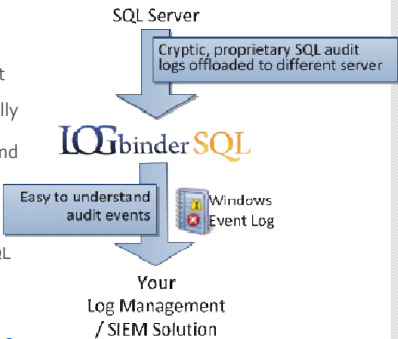






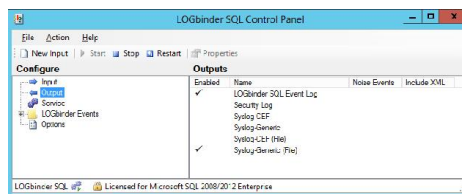
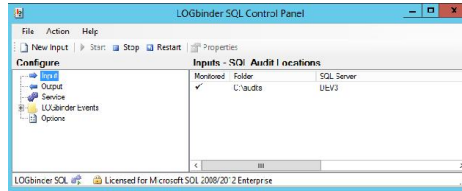
LOGbinder

- Small efficient Windows service that runs on any Windows server on your network
- One instance of LOGbinder SQL can process logs from many SQL Servers
- LOGbinder SQL can coexist with other LOGbinder products like LOGbinder EX for Exchange and LOGbinder SP for SharePoint
- Simply configure each SQL Server (optionally with our free [SQL Server Audit Wizard](#)) to write its audit events to a specified folder and then provide those folders to LOGbinder SQL.
- LOGbinder SQL
 - 1. Processes events as they appear in SQL Server binary audit log files
 - 2. Translates them into easy-to-read events
 - <http://www.logbinder.com/Products/LOGbinderSql/EventsGenerated>
 - 3. Forwards to your SIEM solution in its native format
 - ArcSight, Oradar, McAfee, EventTracker, LogRhythm, LogPoint, SolarWinds, Splunk and many, many more



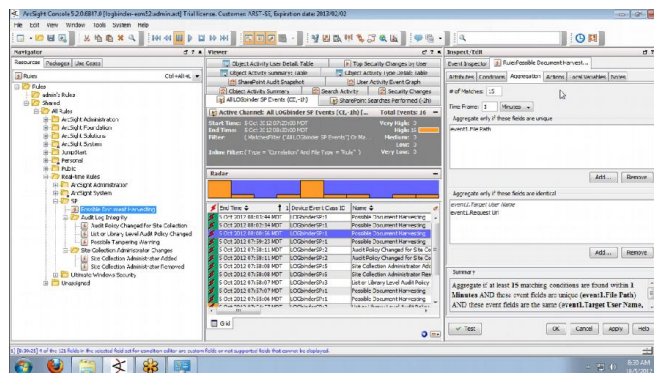
LOGbinder



- 5 minute setup



LOGbinder



- SQL Events showing up in your SIEM within seconds



LOGbinder

- Benefits
 - Application security intelligence for SQL Server
 - Fill the audit gap in your compliance efforts
 - Catch APTs that have penetrated upstream defenses
 - Less push back from database admins
 - Zero Impact
 - Use SQL Server's fastest, most efficient audit log output method and thereby offload all subsequent log processing from busy database servers to a server of your choice.
 - No agent required. LOGbinder SQL does not require an agent to be installed on your SQL Servers. In fact, LOGbinder SQL doesn't even need to send a single packet to your database servers.
 - Know what's happening inside of SQL Server including
 - Security operations involving logins, roles and permissions
 - Maintenance of tables, stored procedures and any other object
 - Database operations like backup and restore
 - Transact SQL table commands like insert, delete, update and select
 - Correlate SQL Server security activity with related events from the rest of your environment
 - No data silos or additional consoles to monitor

Bottom line

- SQL Server is where your data is
 - Not monitoring it with your SIEM is risky and non-compliant
- LOGbinder bridges the gap between SQL Server and your SIEM
- Now your SIEM can detect database intrusions within seconds
 - Without impacting your DB
- Download a free trial at
 - www.logbinder.com
- Free whitepaper
 - **Comparison: SQL Server Audit and SQL Trace**
 - <http://1drv.ms/1w96eNw>