



# Who's Attacking Your Database? Monitoring Authentication and Logon Failures in SQL Server

Sponsored by



© 2016 Monterey Technology Group Inc.



Thanks to

• Made possible by



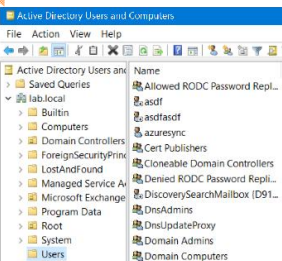
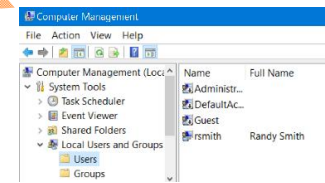
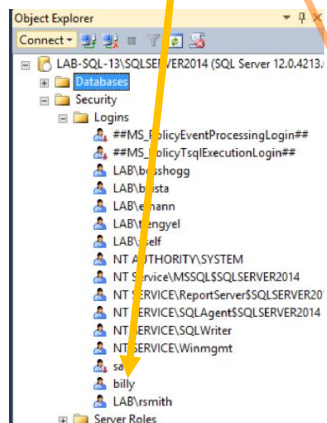
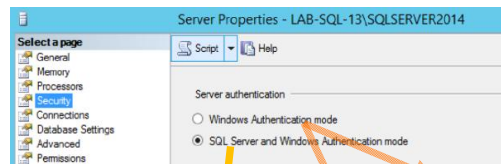
[www.logbinder.com](http://www.logbinder.com)





## Preview of Key Points

- 2 kinds of authentication
- 3 sources of logon audit events
- Logon failure scenarios
- Beyond failed logons
- LOGbinder

## 2 kinds of authentication





## 3 sources of logon audit events

*All 3 needed!*

- SQL Server
- Active Directory
- Local Server

## 3 sources of logon audit events

		Type of logon		
		SQL Authentication	Windows Authentication	
			Active Directory	Local Account
Log source	SQL Server	<ul style="list-style-type: none"> <li>Actual authentication failures (e.g. bad password)</li> <li>Problems with the account's status in SQL Server</li> </ul>	<ul style="list-style-type: none"> <li>Problems with the AD account's status/permissions within SQL Server</li> </ul>	<ul style="list-style-type: none"> <li>Problems with the local account's status/permissions within SQL Server</li> </ul>
	Active Directory	<ul style="list-style-type: none"> <li>Nothing</li> </ul>	<ul style="list-style-type: none"> <li>Actual authentication failures (e.g. bad password)</li> <li>Problems with the account's status in AD</li> </ul>	<ul style="list-style-type: none"> <li>Nothing</li> </ul>
	Local Server	<ul style="list-style-type: none"> <li>Nothing</li> </ul>	<ul style="list-style-type: none"> <li>Possibly 4625</li> </ul>	<ul style="list-style-type: none"> <li>Actual authentication failures (e.g. bad password)</li> <li>Problems with the account's status in local server</li> </ul>

ULTIMATE WIND OWS SECURITY .COM

LOBinder

### 3 sources of logon audit events

- Active Directory
  - Security Event Log
- Local Server
  - Security Event Log
- SQL Server
  - Application log
  - SQL Audit

ULTIMATE WIND OWS SECURITY .COM

LOBinder

### Security Log

- Account Logon events
  - Authentication – not logon session
    - Logged on domain controllers when account is in AD
    - Logged on SQL Server's local Windows Security Log when a local account
- Logon events
  - Not authentication – actual logon session
  - Always logged on SQL Server's local Windows Security Log when a local account
    - AD account
    - Local account

## SQL logon events

- Application log
  - Only logon events
- SQL Audit (SQL 2008+)
  - Logon events
  - Plus so much more
  - <https://www.ultimatewindowssecurity.com/sqlserver/auditpolicy/auditactiologroups/default.aspx>

## SQL Logon Events in Application Log

Server Properties - LAB-SQL-13\SQLSERVER2014

Select a page: General, Memory, Processors, Connections, Database Settings, Advanced, Permissions

Server authentication:  
 Windows Authentication mode  
 SQL Server and Windows Authentication mode


Login auditing:  
 None  
 Failed logins only  
 Successful logins only  
 Both failed and successful logins


Source	Event ID	Level	Date and Time	Source	Source ID
Event Viewer (LAB-SQL-13\SQLSERVER2014)	18456	Information	3/1/2016 7:14:19 AM	MSSQL\$SQLSERVER2014	18456
Custom Views	18456	Information	3/1/2016 7:14:14 AM	MSSQL\$SQLSERVER2014	18456
Windows Logs > Application	18456	Information	3/1/2016 7:14:13 AM	MSSQL\$SQLSERVER2014	18456
Security	18456	Information	3/1/2016 7:14:05 AM	MSSQL\$SQLSERVER2014	18456
Setup	18456	Information	3/1/2016 7:10:53 AM	MSSQL\$SQLSERVER2014	18456
System	18456	Information	3/1/2016 7:10:38 AM	MSSQL\$SQLSERVER2014	18456
Forwarded Events	18456	Information	3/1/2016 7:10:14 AM	MSSQL\$SQLSERVER2014	18456

Event 18456, MSSQL\$SQLSERVER2014

General Details

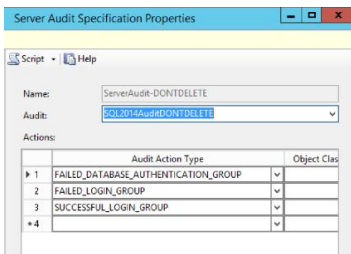
[Login failed for user 'LAB\smith'. Reason: Could not find a login matching the name provided. [CLIENT: 10.42.1.246]]

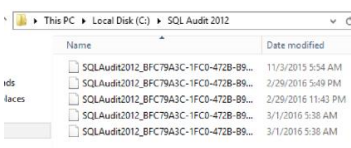





SQL Audit

- Real audit solution
  - Blows away C2 and SQL TRACE
  - Logon events just the tip of the iceberg
  - Lowest performance hit
  - Zero touch for SIEM and log management
    - with LOGbinder







Logon failure scenarios

		Applicati on Event ID	LOGbinder Event ID	Key text
Windows only	AD/Windows account has no corresponding login in SQL	18456	24003	Could not find a login matching the name provide
Windows and SQL	Login disabled in SQL	18470		The account is disabled
	Login has no access to DB	18456		Failed to open the explicitly specified database
	Login has no permission to connect to database engine			Token-based server access validation failed with an infrastructure error
SQL only	SQL Authentication not enabled			An attempt to login using SQL authentication failed. Server is configured for Windows authentication only
	Bad password			An error occurred while evaluating the password
	Locked out			Login failed for user 'john'. Reason: Password did not match that for the user provided. [D The account is currently locked out. The system administrator can unlock it

ULTIMATE WINDOWS SECURITY .COM

Logbinder

# SQL Audit

- Beyond logon auditing
- What happens once some is in?
- SQL Audit is the only way to track
  - Security changes
    - Logins, roles, permissions
  - Privileged operations
    - Backing up databases
    - Bulk selects
    - Manual modifications to tables
  - Direct access by end users
  - ...

ULTIMATE WINDOWS SECURITY .COM

Logbinder

# SQL Audit

- SQL Audit
  - Local event log
  - Binary file
- 5 reasons why you SQL Audit – Binary format is the best way
  - Performance
  - Security
  - Stability
  - Hard to understand
  - DB admin push back

# 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 for SQL Server

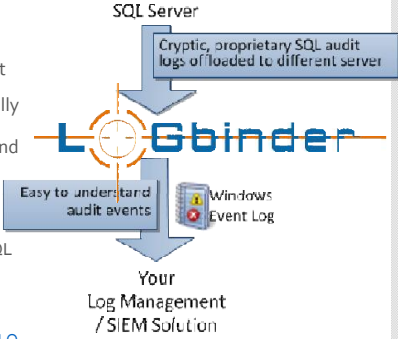




LOGbinder

- 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.
  - 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, Qradar, McAfee, Event Tracker, LogRhythm, LogPoint, SolarWinds, Splunk and many, many more



SQL Server



Cryptic, proprietary SQL audit logs of loaded to different server

LOGbinder

Easy to understand audit events

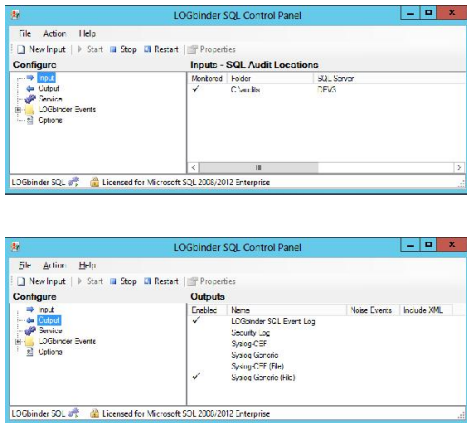
Windows Event Log

Your Log Management / SIEM Solution






LOGbinder

- 5 minute setup



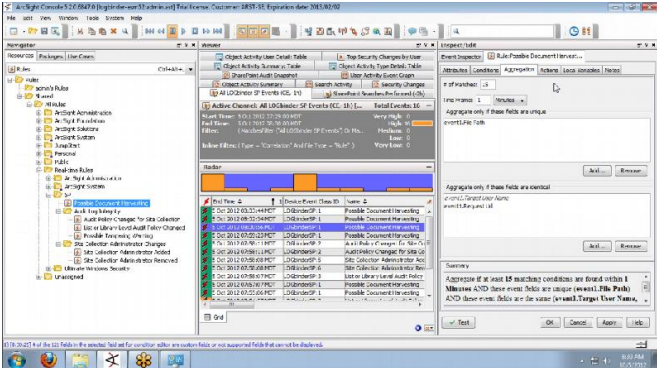
The screenshot shows two windows of the LOGbinder SQL Control Panel. The top window displays the 'Inputs - SQL Audit Locations' configuration, with a table showing a monitored folder 'C:\msdlog' for 'SQL Server' on 'RPU0'. The bottom window displays the 'Outputs' configuration, with a table listing various output destinations like 'LOGbinder SQL Event Log', 'Security Log', 'Syslog C IP', 'Syslog UDP', 'Syslog C IP (File)', and 'Syslog UDP (File)', all of which are checked as enabled.







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

- People can attack SQL server and break into
  - You'll never know if you are only watching Windows security log
- SQL Logon auditing is only the beginning
  - What happens when they do break in?
- SQL Audit is the answer
  - LOGbinder delivers SQL Audit events to your SIEM with zero touch