Top 6 Security Events to Monitor in SQL Server

Sponsored by LOGbinder SQL

Thanks to

- Made possible by

LOGbinder SQL

http://www.logbinder.com/products/logbindersql

A Randy Franklin Smith Company

© 2013 Monterey Technology Group Inc.

Preview of Key Points

- How does SQL auditing work?
- Top 6 Events
- Getting these events into your SIEM

How SQL auditing works

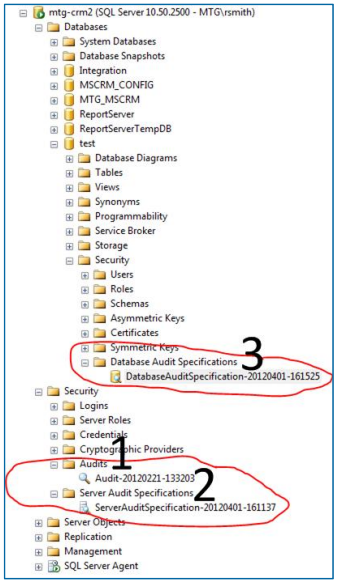
- What can you audit?

ULTIMATE WINDOWS SECURITY .COM

LOGbinder SQL

SQL Server Auditing

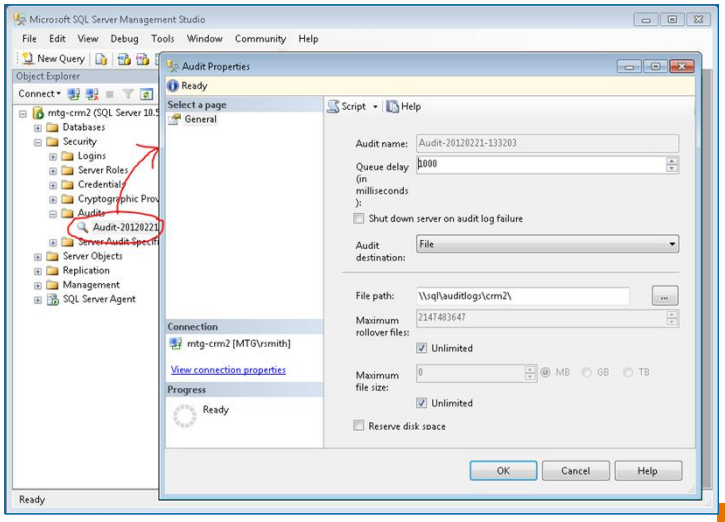
- 3 audit policy objects
  1. Server Audit
  2. Server Audit Specification
  3. Database Audit Specificaiton



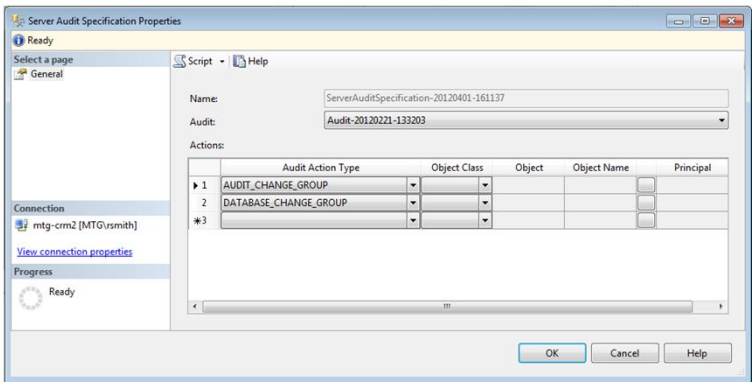
ULTIMATE WINDOWS SECURITY .COM

LOGbinder SQL

SQL Server Auditing



SQL Server Auditing



SQL Server Auditing

- Audit action groups
  - Categories of auditable activity
  - Assigned at the
    - Server level
    - Database level

SQL Audit Logs

- Windows Event Log
  - Application or Security
- Binary file
  - Readable by any edition of SQL Server
  - <audit_name>_<audit_guid>_nn_<timestamp_as_bigint>.sqlaudit
  - SELECT * FROM fn_get_audit_file('E:\SqlAudits*', default, default)
  - Over 2 dozen columns

SQL Audit Logs

event_time:2010-09-16 12:35:30.0787755
sequence_number:1
action_id:APRL
succeeded:true
permission_bitmask:0
is_column_permission:false
session_id:54
server_principal_id:260
database_principal_id:1
target_server_principal_id:0
target_database_principal_id:0
object_id:7
class_type:RL
session_server_principal_name: ACMESP\Administrator
server_principal_name: ACMESP\Administrator
server_principal_sid:0
database_principal_name: dbo
target_server_principal_name: ACMESP\Administrator
target_server_principal_sid: 0
target_database_principal_name: John Smith
server_instance_name: SPDEV\SQL08ENT
database_name: AuditTest
schema_name:
object_name: Human Resources
statement: EXEC sp_addrolemember N'Human Resources', N'John Smith'

At 12:35AM on 9/16/2010, ACMESP\Administrator added John Smith to the Human Resources role in the AuditTest database on SQL Server SPDEV\SQL08ENT

SQL Audit Logs

- For best performance and security
  - Generate binary audit logs
  - Can target a remote shared folder
  - But how do you get that to your SIEM?
    - Stand by…

Top 6 Events to Monitor

1. Admin authority changes
2. Permission changes
3. Role membership changes
4. Failed logons
5. Data exports by privileged users
6. New logins/principals

#1

Admin authority changes

- Changes to built-in roles at the server and database level
- Add to Server Audit Specification
  - SERVER_ROLE_MEMBER_CHANGE_GROUP
  - DATABASE_ROLE_MEMBER_CHANGE_GROUP
- Monitor for
  - action_id = APRL
  - object_name =

Server roles

- bulkadmin
- dbcreator
- diskadmin
- processadmin
- public
- securityadmin
- serveradmin
- setupadmin
- sysadmin

Database roles

- db_accessadmin
- db_backupoperator
- db_datareader
- db_datawriter
- db_ddladmin
- db_denydatareader
- db_denydatawriter
- db_owner
- db_securityadmin
- public

- Who got or lost permissions
  - target_server_principal_name
  - target_database_principal_name
- Database (if applicable) = database_name
- Who did it = server_principal_name

#2

Permission and owner changes

- Add to Server Audit Specification
  - SERVER_OBJECT_PERMISSION_CHANGE_GROUP, SERVER_PERMISSION_CHANGE_GROUP, DATABASE_PERMISSION_CHANGE_GROUP, SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP, DATABASE_OBJECT_PERMISSION_CHANGE_GROUP, DATABASE_OWNERSHIP_CHANGE_GROUP, SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP, DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP, SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP

Permission changes

- Monitor for
  - action_id =G,GWG,R,RWG,RWC
- Who got or lost permissions
  - target_server_principal_name
  - target_database_principal_name
- Object whose permissions changed = object_name
  - Database (if applicable) = database_name
  - Schema (if applicable) = schema_name
- Who did it = server_principal_name
- Which permissions = statement

Owner changes

- Monitor for
  - action_id =TO
- Who got ownership
  - target_server_principal_name
  - target_database_principal_name
- Object whose ownership changed = object_name
  - Database (if applicable) = database_name
  - Schema (if applicable) = schema_name
- Who did it = server_principal_name

#3 Role membership changes

- Changes to built-in roles at the server and database level
- Add to Server Audit Specification
  - SERVER_ROLE_MEMBER_CHANGE_GROUP
  - DATABASE_ROLE_MEMBER_CHANGE_GROUP
- Monitor for
  - action_id = APRL
- Who got or lost permissions
  - target_server_principal_name
  - target_database_principal_name
- Database (if applicable) = database_name
- Who did it = server_principal_name

#4 Failed logons

- Add to Server Audit Specification
  - SERVER_ROLE_MEMBER_CHANGE_GROUP
  - DATABASE_ROLE_MEMBER_CHANGE_GROUP
- Monitor for
  - action_id = LGIF
- User name attempted = server_principal_name
- Reason = statement

#5
Database backed up privileged users

- Add to Server Audit Specification
  - BACKUP_RESTORE_GROUP
- Monitor for
  - action_id = BA
- Who did it = server_principal_name
  - Filter out backups by backup applications
- Are there more operations?

#6
New logins and users

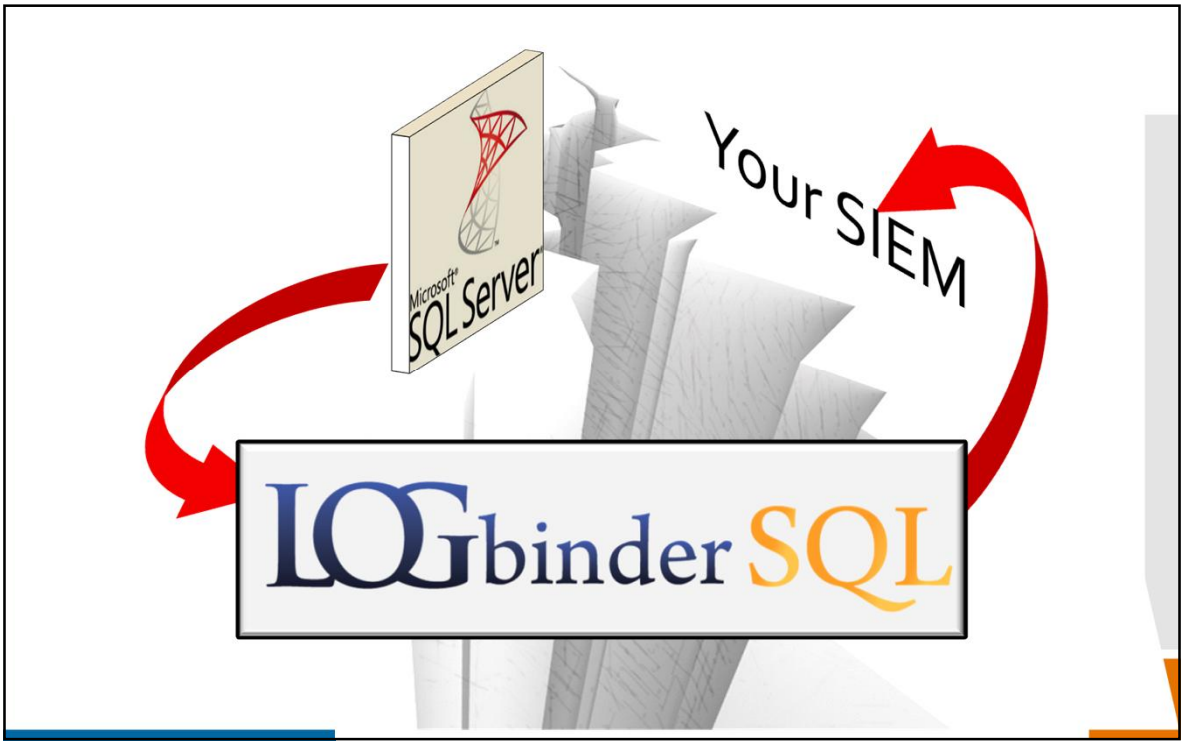
- Add to Server Audit Specification
  - SERVER_PRINCIPAL_GROUP
  - DATABASE_PRINCIPAL_GROUP
- Monitor for
  - action_id = CR
  - class=

class_type	class_type_desc	securable_class_desc
US	USER	USER
LX	LOGIN	LOGIN
AU	ASYMMETRIC KEY USER	USER
CU	CERTIFICATE USER	USER
GU	GROUP USER	USER
SU	SQL USER	USER
WU	WINDOWS USER	USER
AL	ASYMMETRIC KEY LOGIN	LOGIN
CL	CERTIFICATE LOGIN	LOGIN
SL	SQL LOGIN	LOGIN
WG	WINDOWS GROUP	LOGIN
WL	WINDOWS LOGIN	LOGIN

  - Who did it = server_principal_name
  - New login/user = object_name

Bottom Line

- Awesome audit logging
  - Comprehensive, consistent, flexible
- Log management and security issues
  - To be consumed by SIEM solutions directly
    - Must use lower performance Windows event log
    - Usually agent required = push back by db admins
  - Binary logs preferable for performance, security and db admin acceptance
  - Either way you have 349 different audit events reflected in one message structure
    - Cryptic and complicated to interpret



Bridge the gap

- LOGbinder SQL
  - No agent on your SQL Servers
  - Higher performance binary log format
  - Translates cryptic, raw audit data into easy-to-understand audit messages
  - Resolves cryptic Action IDs
  - Outputs to
    - Windows Security Log
    - Syslog
    - Common Event Format (for ArcSight)

LOGbinder SQL

www.logbinder.com

Bridge the Gap Between Exchange and Your SIEM