Microsoft

# SQL Server Audit – Evidence Never Lies


## Patrick Keisler
Senior Premier Field Engineer


# About the Speaker

## Patrick Keisler

- Senior Premier Field Engineer
- Over 15 years of database experience
- Specialize in administration of high availability and disaster recovery environments

Email: pkeisler@microsoft.com
Blog: www.patrickkeisler.com
Twitter: @patrickkeisler

# Recent High Profile Data Breaches

- Yahoo (2016) – 1 Billion User Accounts

  Source: http://money.cnn.com/2016/12/14/technology/yahoo-breach-billion-users/index.html

- Adult Friend Finder (2016) – 400 Million Accounts

  Source: https://www.washingtonpost.com/news/the-switch/wp/2016/11/14/adult-friendfinder-hit-with-one-of-the-biggest-data-breaches-ever-report-says/

- Anthem Insurance (2015) – 80 Million User Accounts

  Source: http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/

- Target (2013) – 40 Million Credit Card Accounts

  Source: http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/

Microsoft

# Agenda

- Why Audit?
- Components
- Viewing Audit Data
- Troubleshooting & Tips
- Audit for Azure SQL Database

*** Starting with SQL Server 2016 SP1 ***
These features are available in ALL editions!!
https://blogs.msdn.microsoft.com/sqlreleaseservices/sql-server-2016-service-pack-1-sp1-released/

Microsoft

# Why Do We Need to Audit?

- Compliance Requirements
  - Sarbanes-Oxley
  - HIPAA
  - PCI
- Company Reporting
  - Who is accessing my database?
- Security Conscious DBA
  - Who changed that table over the weekend?
  - Where are all these failed login attempts coming from?

Microsoft

# Auditing in the Past

- SQL Trace – **Depreciated*
  - Easy to setup, but known performance hit
- C2 Audit Mode – **Depreciated*
  - Known performance hit, no customization, and creates large trace files
- DML Triggers
  - Difficult to setup, but extremely customizable
- Common Criteria
  - Limited audit options
- Third-Party Solutions
  - Easy to setup, but can be costly

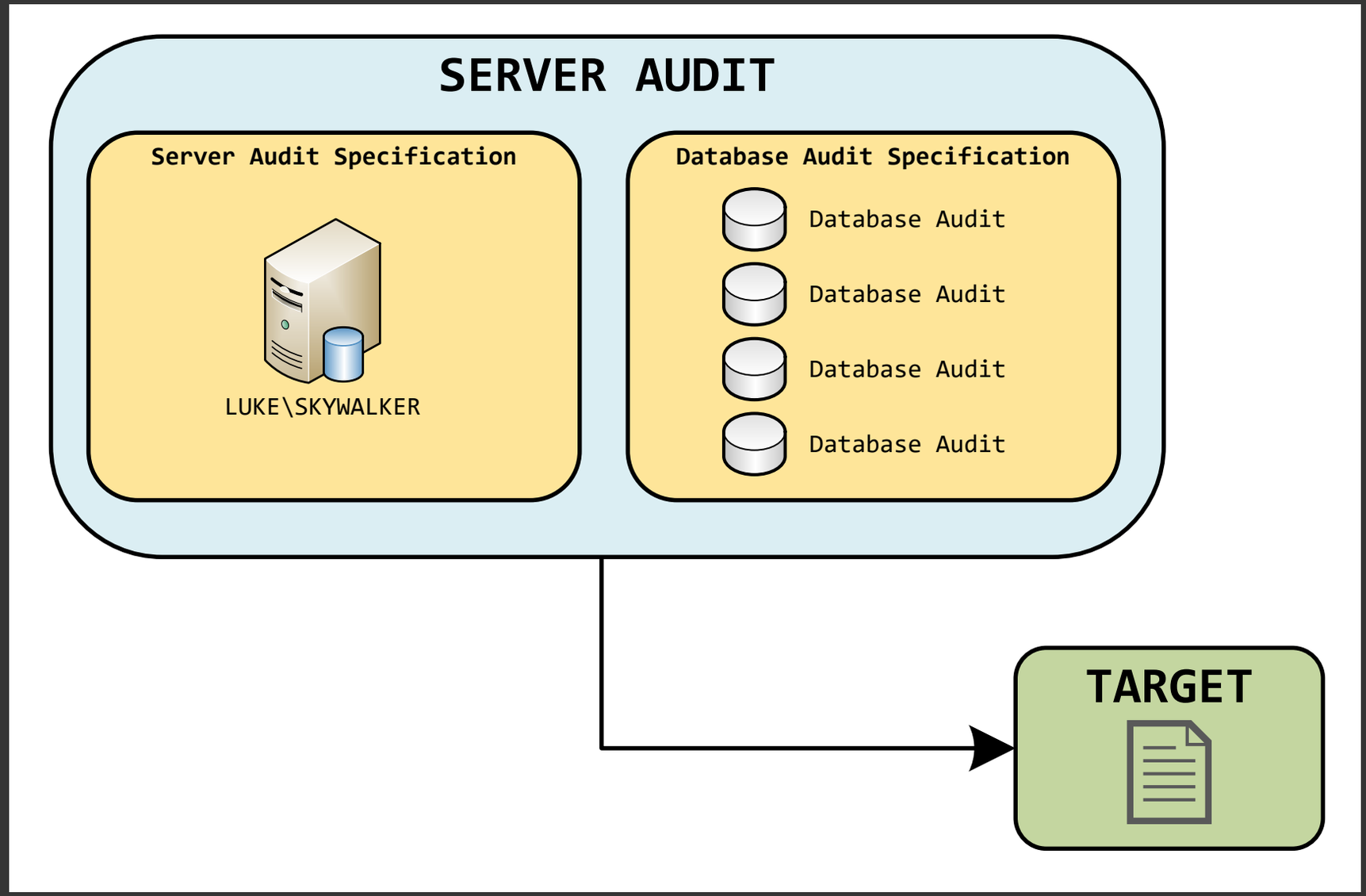
Microsoft

# SQL Audit Foundation

- Built upon Extended Events (XEvents)
  - Performance is the primary focus
- Audit is a special XEvent session
  - Visible with some XEvent DMVs but cannot be configured/altered through the XEvents GUI.

Microsoft

# Components of SQL Audit



# Server Audit & Target

- Target – where to write the audit records
  - File
  - Windows Event Log (Security or Application)
- What to do when the audit fails
  - Continue
  - Shutdown
  - Fail Operation
- How quickly to process the audit records
  - QUEUE_DELAY = 0 – Synchronous
  - QUEUE_DELAY >=1000 – Asynchronous (default)

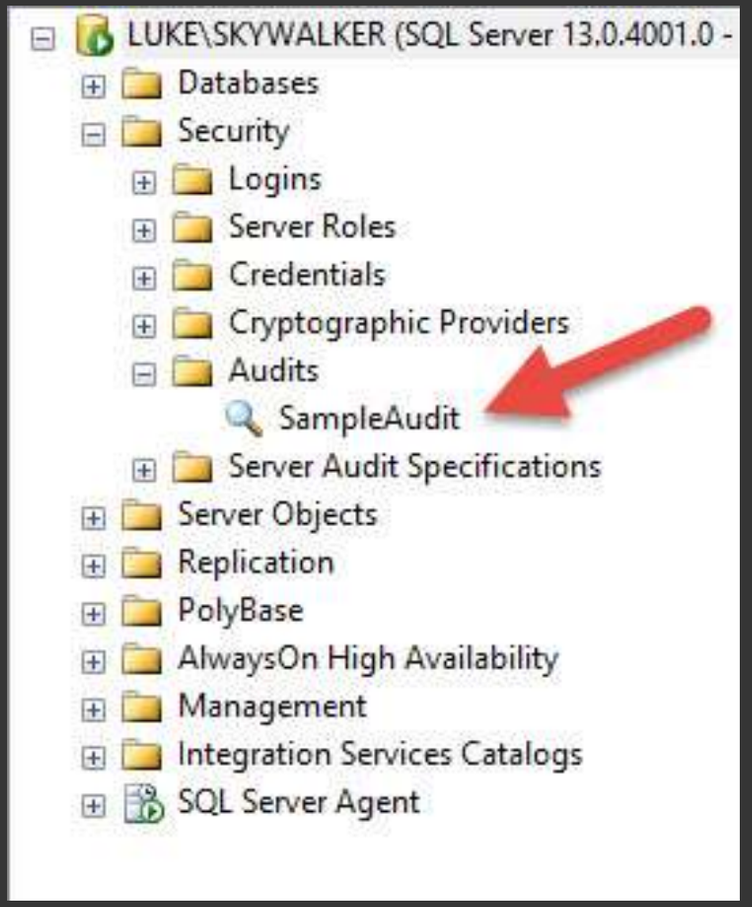
Microsoft

# Create a Server Audit & Target

```
USE master;
GO

CREATE SERVER AUDIT SampleAudit
TO FILE (FILEPATH = 'E:\Audit')
WITH (ON_FAILURE = SHUTDOWN);
GO

ALTER SERVER AUDIT SampleAudit WITH (STATE = ON);
GO
```



# Server Audit Specification

- Define what actions are audited at the server-level
  - SUCCESSFUL_LOGIN_GROUP
  - AUDIT_CHANGE_GROUP
- Define which server audit the records are written to
- 1:1 relationship
  - One Server Audit Spec per Server Audit

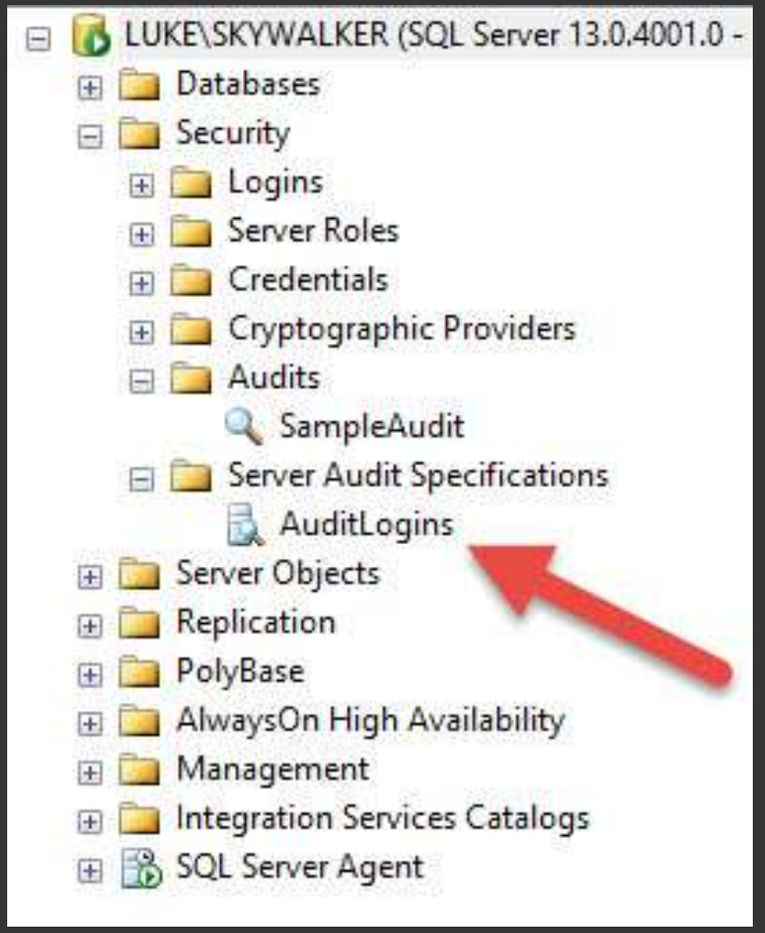
Microsoft

# Create a Server Audit Specification

```
USE master;
GO

CREATE SERVER AUDIT SPECIFICATION AuditLogins
FOR SERVER AUDIT SampleAudit
    ADD (SUCCESSFUL_LOGIN_GROUP)
   ,ADD (AUDIT_CHANGE_GROUP);
GO

ALTER SERVER AUDIT SPECIFICATION
WITH (STATE = ON);
GO
```



# Database Audit Specification

- Define what actions are audited at the database-level
  - DATABASE_OBJECT_CHANGE_GROUP
  - SCHEMA_OBJECT_CHANGE_GROUP
- Define which server audit the records are written to
- 1:1 relationship
  - 1 Database Audit Spec per DB per Server Audit
- SQL Server 2008 – 2016 RTM
  - Requires Enterprise Edition
- SQL Server 2016 SP1 going forward
  - Available in All Editions

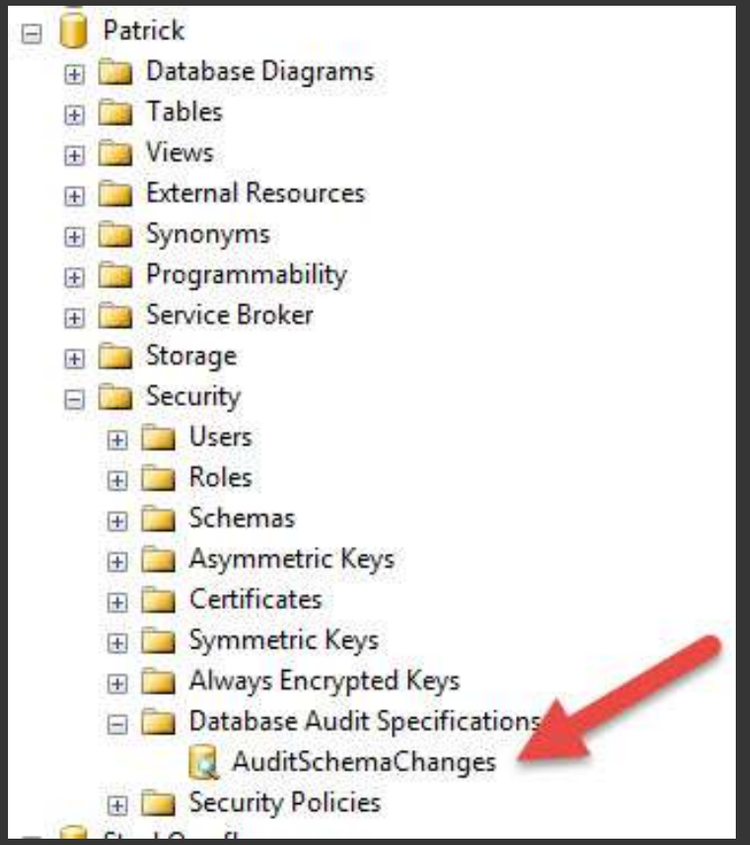
Microsoft

# Create a Database Audit Specification

```
USE Patrick;
GO

CREATE DATABASE AUDIT SPECIFICATION AuditSchemaChanges
FOR SERVER AUDIT SampleAudit
  ADD (SCHEMA_OBJECT_CHANGE_GROUP);
GO

ALTER DATABASE AUDIT SPECIFICATION AuditSchemaChanges
WITH (STATE = ON);
GO
```



# Audit Actions & Action Groups

- Actions (or events) that cause an operation to be audited
  - ALTER TABLE
  - DBCC
- Actions can be
  - Bundled as a group of events
  - Single events
- Action levels can be
  - Server-level
  - Database-level
  - Audit-level

Microsoft

# Audit Actions & Action Groups

- 42 Server-level action groups
- 24 Database-level action groups
- 7 Database-level acti
  - SELECT, INSERT, UPDATE
- 1 Audit-level action g
  - AUDIT_CHANGE_GROUP

| | |
|---|---|
| APPLICATION_ROLE_CHANGE_PASSWORD_GROUP | LOGIN_CHANGE_PASSWORD_GROUP |
| AUDIT_CHANGE_GROUP | LOGOUT_GROUP |
| BACKUP_RESTORE_GROUP | SCHEMA_OBJECT_ACCESS_GROUP |
| BROKER_LOGIN_GROUP | SCHEMA_OBJECT_CHANGE_GROUP |
| APPLICATION_ROLE_CHANGE_PASSWORD_GROUP | DATABASE_PRINCIPAL_CHANGE_GROUP |
| AUDIT_CHANGE_GROUP | DATABASE_PRINCIPAL_IMPERSONATION_GROUP |
| BACKUP_RESTORE_GROUP | DATABASE_ROLE_MEMBER_CHANGE_GROUP |
| DATABASE_CHANGE_GROUP | DBCC_GROUP |
| DATABASE_LOGOUT_GROUP | FAILED_DATABASE_AUTHENTICATION_GROUP |
| DATABASE_OBJECT_ACCESS_GROUP | SCHEMA_OBJECT_ACCESS_GROUP |
| DATABASE_OBJECT_CHANGE_GROUP | SCHEMA_OBJECT_CHANGE_GROUP |
| DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP | SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP |
| DATABASE_OBJECT_PERMISSION_CHANGE_GROUP | SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP |
| DATABASE_OPERATION_GROUP | SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP |
| DATABASE_OWNERSHIP_CHANGE_GROUP | USER_CHANGE_PASSWORD_GROUP |
| DATABASE_PERMISSION_CHANGE_GROUP | USER_DEFINED_AUDIT_GROUP |
| DBCC_GROUP | TRACE_CHANGE_GROUP |
| FAILED_DATABASE_AUTHENTICATION_GROUP | TRANSACTION_GROUP |
| FAILED_LOGIN_GROUP | USER_CHANGE_PASSWORD_GROUP |
| FULLTEXT_GROUP | USER_DEFINED_AUDIT_GROUP |

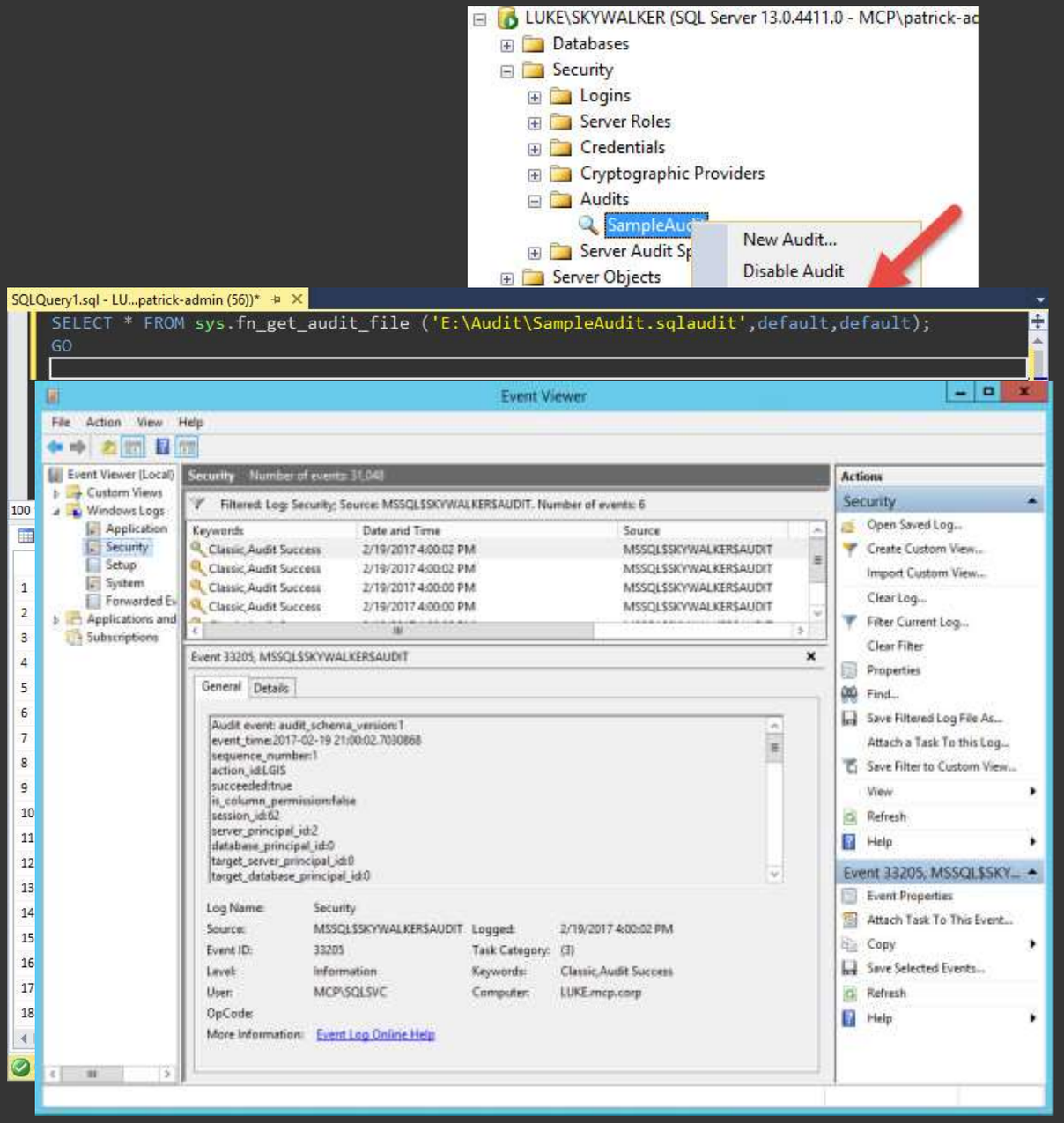
# How to Choose the Correct Group?

- SQL Server Security Blog
  - https://blogs.msdn.microsoft.com/sqlsecurity/2009/05/09/how-to-choose-audit-action-group-when-using-auditing-in-sql-server-2008/
- Books Online
  - https://msdn.microsoft.com/en-us/library/cc280663.aspx

# Demo 1: Create an Audit

# Viewing Audit Logs

- Management Studio
- T-SQL
  - sys.fn_get_audit_file()
- Windows Event Viewer
  - Application Log
  - Security Log




Microsoft

# Permissions to View Audit Logs

- SQL Server
  - Member of SysAdmin server role
  - Grant CONTROL SERVER
- Windows Event Log
  - Application Log visible to all users
  - Security Log can be locked down
- Audit log files are NOT encrypted!!!
  - Set file & folder permissions to prevent unauthorized access
  - Use NTFS file encryption to protect the data

Microsoft

# Demo 2: View Audit Logs

# More Granular Audits

- Audits can be created using filters
  - Specific objects
  - Specific DML actions
  - Specific rows
- Examples:
  - WHERE predicate can be used at the Server Audit
    - Filtered to a specific object or login
    - Any field from sys.fn_get_audit_file()
  - SELECT, INSERT, UPDATE, DELETE can be used at the database-level
    - Filtered to a specific object, user, or group

Microsoft

# Demo 3: Granular Audits

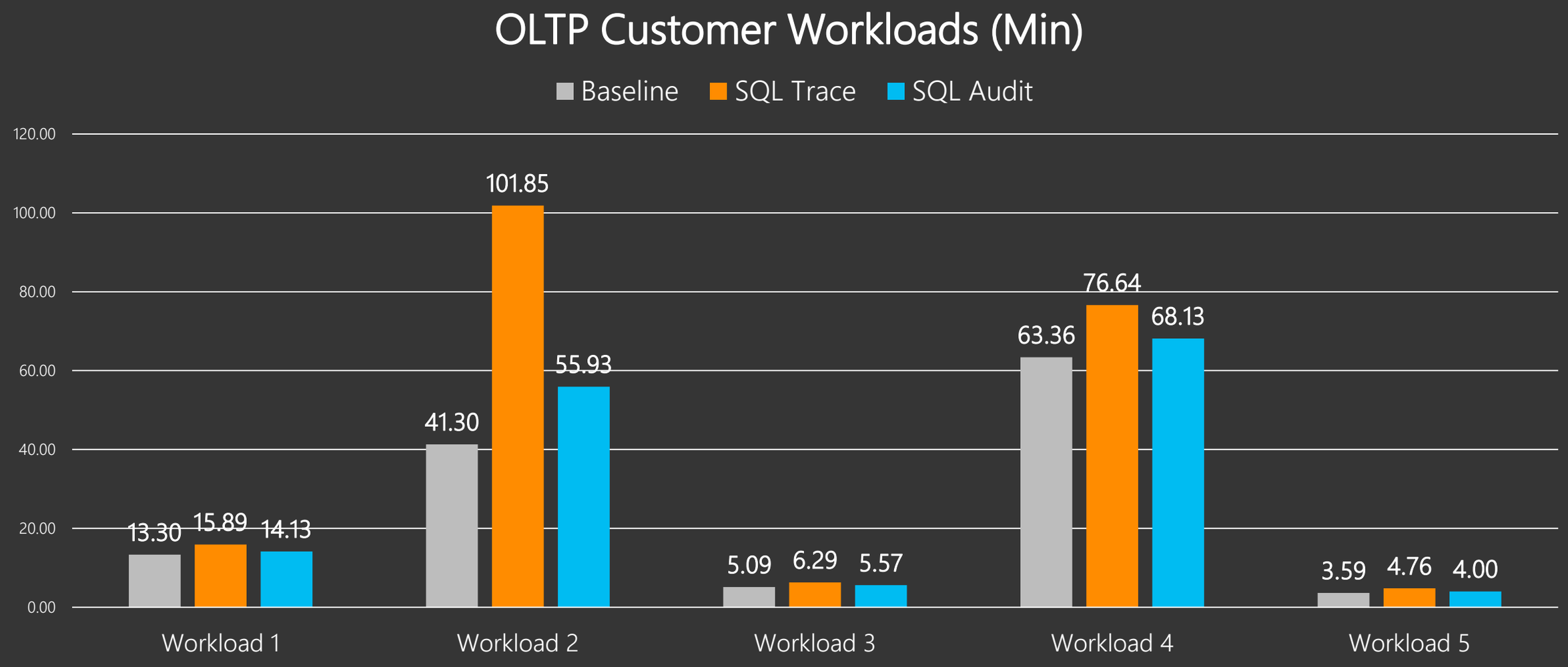
# What is the Performance Impact?

*It depends

- Your workload
- Number of events being audited
- Location of the audit log
  - Writing to a file is faster than writing to the Security Log
  - Writing to a local drive is faster than writing to share drive

Microsoft

# SQL Audit vs SQL Trace




Source: https://technet.microsoft.com/en-us/library/dd392015.aspx

# Troubleshooting

- SQL Server shuts down or fails to startup
  - Start SQL Server in single user mode (-m) then disable the audit
  - Audit is still running, but the shutdown logic is disabled

```
USE master;
GO
ALTER SERVER AUDIT SampleAudit WITH (STATE = OFF);
GO
```

Microsoft

# Troubleshooting

Wait types:

- XE_BUFFERMGR_FREEBUF_EVENT
  - Memory buffers are full
  - Potential disk bottleneck where audit log is written
- XE_SERVICES_RWLOCK
  - QUEUE_DELAY = 0 (synchronous)
  - Change QUEUE_DELAY to 1000 or higher
- PREEMPTIVE_XE_DISPATCHER
  - Potential disk bottleneck where audit log is written

# Additional Tips About Audits

- When first created, audits are disabled by default
- Audits cannot be filtered at the column-level
- Use same GUID for Server Audit if using:
  - Availability Groups
  - Database Mirroring
- Parameterized query values are not captured
- Database Audit Specifications can be created in model
  - All new databases will automatically have this when created
  - Be very aware…this includes tempdb!!!

Microsoft

# Audit for Azure SQL Database

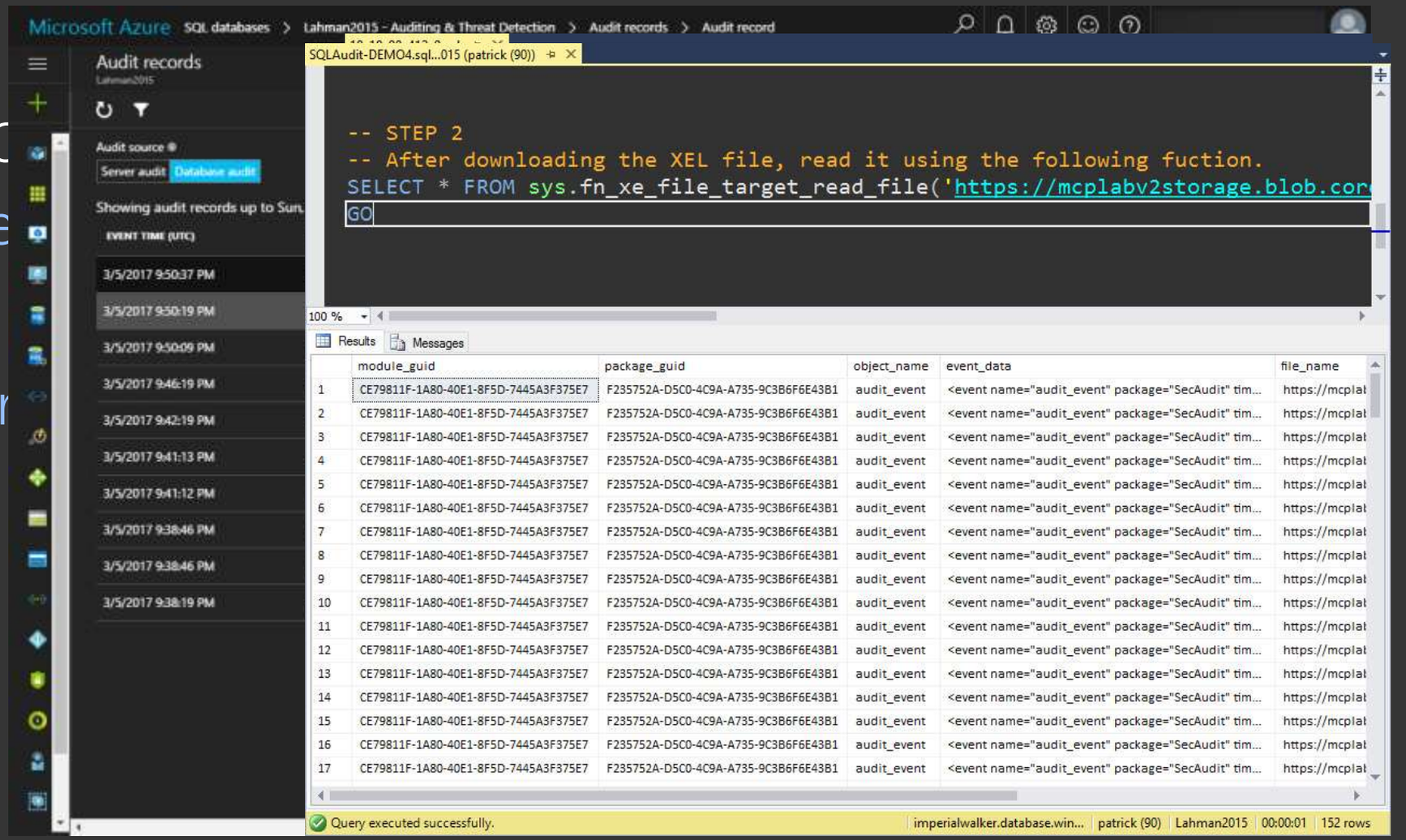
- Granularity
  - Server-level audits
  - Database-level audits

- Targets
  - Blog storage (went live Feb 2017)
  - Table storage

Microsoft

# Viewing Audit Data for Azure SQL DB

- Azure Portal
- Management Stud
  - After dowloading the
- T-SQL
  - sys.fn_xe_file_target_r




Microsoft

# Audit Action Groups for Azure SQL DB

- Same groups for server & database level
- Must use PowerShell configure

- BATCH_STARTED_GROUP
- BATCH_COMPLETED_GROUP
- APPLICATION_ROLE_CHANGE_PASSWORD_GROUP
- AUDIT_CHANGE_GROUP
- BACKUP_RESTORE_GROUP
- DATABASE_LOGOUT_GROUP
- DATABASE_OBJECT_CHANGE_GROUP
- DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP
- DATABASE_OBJECT_PERMISSION_CHANGE_GROUP
- DATABASE_OPERATION_GROUP
- DATABASE_PERMISSION_CHANGE_GROUP
- DATABASE_PRINCIPAL_CHANGE_GROUP
- DATABASE_PRINCIPAL_IMPERSONATION_GROUP
- DATABASE_ROLE_MEMBER_CHANGE_GROUP
- FAILED_DATABASE_AUTHENTICATION_GROUP
- SCHEMA_OBJECT_ACCESS_GROUP
- SCHEMA_OBJECT_CHANGE_GROUP
- SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP
- SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP
- SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP
- USER_CHANGE_PASSWORD_GROUP

Microsoft

# Granular Audits in Azure SQL DB

- Must use blob storage
- Must use PowerShell or REST API to configure

```
no functions in script (click icon on left hand side to create one)
1  Set-AzureRmSqlDatabaseAuditingPolicy `
2    -ServerName 'imperialwalker' `
3    -DatabaseName 'Lahman2015' `
4    -ResourceGroupName 'MCPLABv2' `
5    -AuditAction 'SELECT ON SCHEMA::dbo BY public' `
6    -AuditActionGroup 'SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP',`
7                      'FAILED_DATABASE_AUTHENTICATION_GROUP'
8
```

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing#a-idsubheading-7aautomation-powershell--rest-api

https://msdn.microsoft.com/en-US/library/mt695939(Azure.100).aspx

Microsoft

# Demo 4: Auditing in Azure SQL Database

# Other Resources

- SQL Server 2008 Audit White Paper
  - https://msdn.microsoft.com/en-us/library/dd392015.aspx
- SQL Server Audit
  - https://msdn.microsoft.com/en-us/library/cc280386.aspx
- SQL Server Security Blog
  - https://blogs.msdn.microsoft.com/sqlsecurity/
- Audit for Azure SQL Database
  - https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing-get-started

Microsoft