SQL Server Detective: Investigating Logs and Traces

Taiob Ali

CASSUG
Capital Area SQL Server User Group

Taiob Ali

Database Solutions Manager @ GMO | Microsoft MVP | Global Data Solutions Leader | Cloud & AI Advocate

Let's connect and collaborate:

- linkedin.com/in/sqlworldwide
- sqlworldwide.com
- taiob@sqlworldwide.com
- @sqlworldwide.bsky.social

Agenda

Default Trace

Understanding SQL Server's built-in lightweight trace feature feature

SQL Error Log

Examining critical server events and error messages

SQL Agent Error Log

Investigating job-related issues and failures

System Health

Analyzing extended events for performance monitoring monitoring

Always On Health

Monitoring availability group health and status

Telemetry xEvents (Demo only)

Capturing important events for high-level SQL Server monitoring

Default Trace

Overview

Built-in lightweight tracing mechanism

History

Introduced with SQL Server 2005

Configuration

Enabled by default, limited customization options

Default Trace Configuration

Enabled by Default

Automatically starts with SQL Server instance

File Location

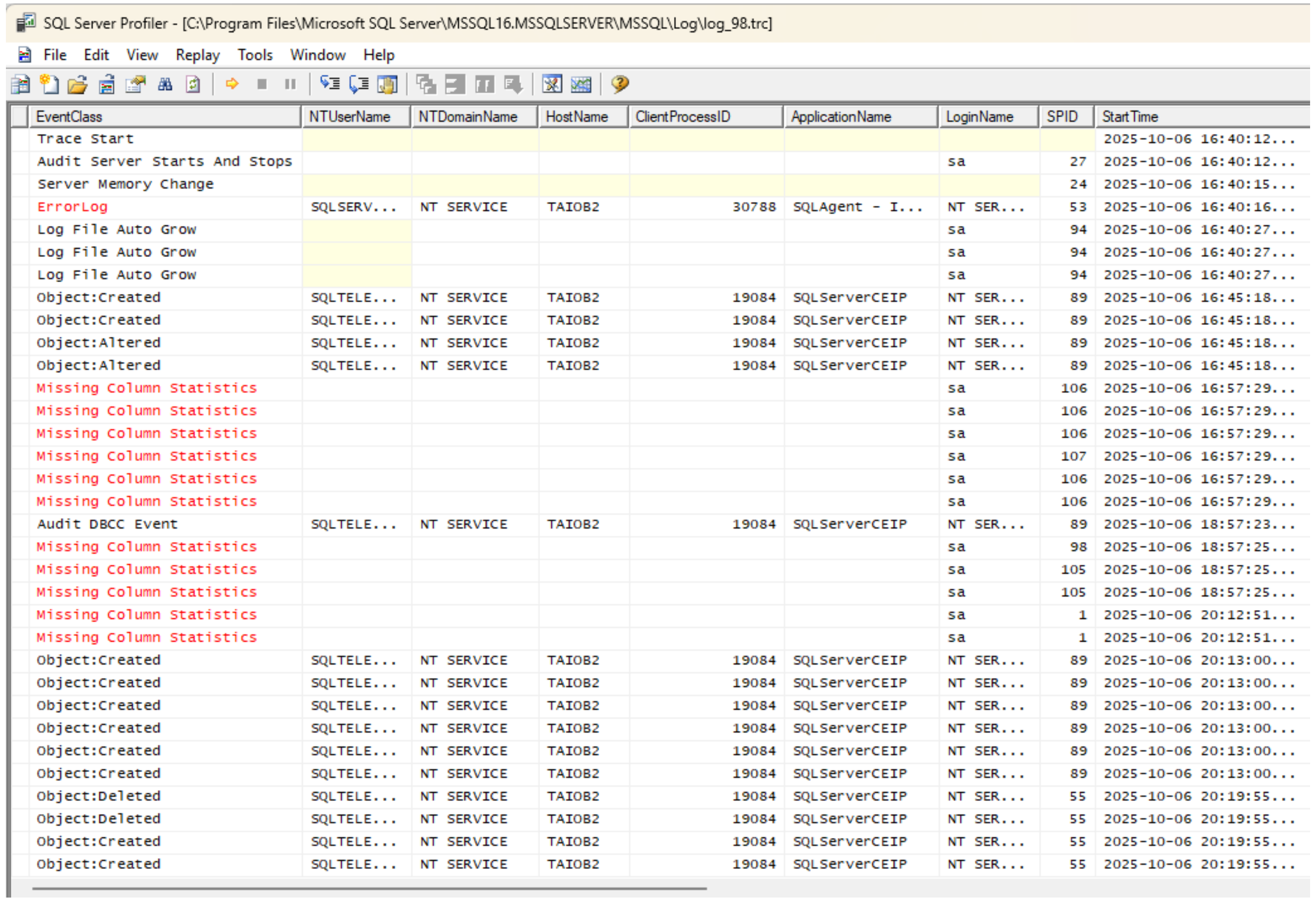
\Program Files\Microsoft SQL Server\MSSQLxx.MSSQLSERVER\MSSQL\LOG

File Configuration

Five 20 MB files, rolling over when full

Customization

Limited configuration options are available



SQL Server Profiler - [C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\Log\log_98.trc]

File Edit View Replay Tools Window Help

EventClass	NTUserName	NTDomainName	HostName	ClientProcessID	ApplicationName	LoginName	SPID	StartTime
Trace Start								2025-10-06 16:40:12...
Audit Server Starts And Stops						sa	27	2025-10-06 16:40:12...
Server Memory Change							24	2025-10-06 16:40:15...
ErrorLog	SQLSERV...	NT SERVICE	TAIOB2	30788	SQLAgent - I...	NT SER...	53	2025-10-06 16:40:16...
Log File Auto Grow						sa	94	2025-10-06 16:40:27...
Log File Auto Grow						sa	94	2025-10-06 16:40:27...
Log File Auto Grow						sa	94	2025-10-06 16:40:27...
Object:Created	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 16:45:18...
Object:Created	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 16:45:18...
Object:Altered	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 16:45:18...
Object:Altered	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 16:45:18...
Missing Column Statistics						sa	106	2025-10-06 16:57:29...
Missing Column Statistics						sa	106	2025-10-06 16:57:29...
Missing Column Statistics						sa	106	2025-10-06 16:57:29...
Missing Column Statistics						sa	107	2025-10-06 16:57:29...
Missing Column Statistics						sa	106	2025-10-06 16:57:29...
Missing Column Statistics						sa	106	2025-10-06 16:57:29...
Audit DBCC Event	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 18:57:23...
Missing Column Statistics						sa	98	2025-10-06 18:57:25...
Missing Column Statistics						sa	105	2025-10-06 18:57:25...
Missing Column Statistics						sa	105	2025-10-06 18:57:25...
Missing Column Statistics						sa	1	2025-10-06 20:12:51...
Missing Column Statistics						sa	1	2025-10-06 20:12:51...
Object:Created	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 20:13:00...
Object:Created	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 20:13:00...
Object:Created	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 20:13:00...
Object:Created	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 20:13:00...
Object:Created	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 20:13:00...
Object:Created	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	89	2025-10-06 20:13:00...
Object:Deleted	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	55	2025-10-06 20:19:55...
Object:Deleted	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	55	2025-10-06 20:19:55...
Object:Created	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	55	2025-10-06 20:19:55...
Object:Created	SQLTELE...	NT SERVICE	TAIOB2	19084	SQLServerCEIP	NT SER...	55	2025-10-06 20:19:55...

Default Trace Content (Partial list)

Database Operations

- Object creation events
- Object deletion events
- Schema changes

Performance Issues

- Hash warnings
- Sort warnings
- Missing column statistics statistics

Security Events

- Login failures
- Security audit events

System Events

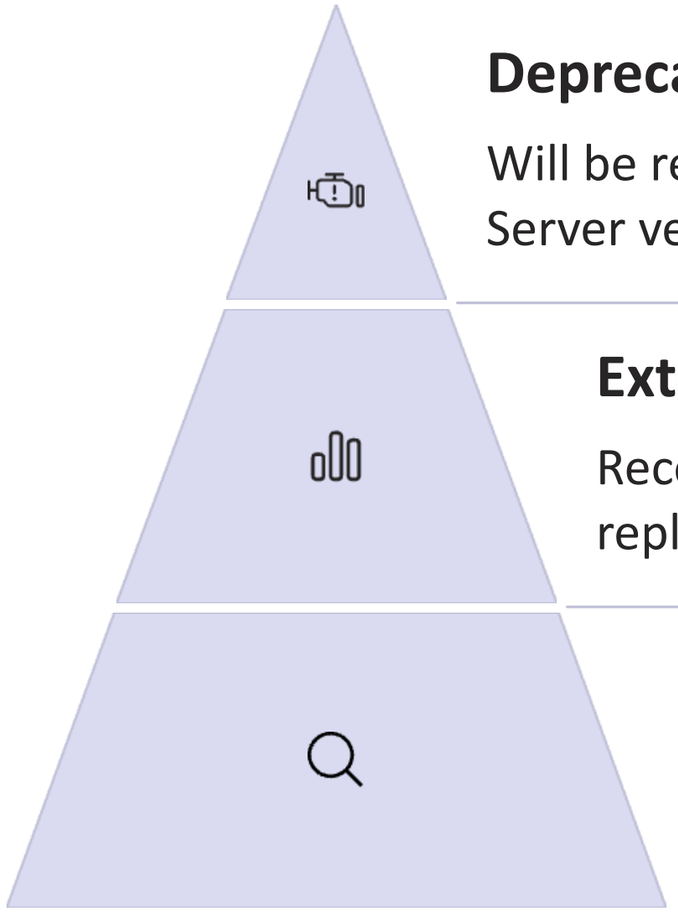
- Memory changes
- Full-Text crawl start/stop

SQL SERVER DEFAULT TRACE

The default trace is a feature in SQL Server that automatically captures a range of events for diagnostic and auditing purposes.

- **Errors and warnings** Error occurrences and warnings in the server
- **Object changes** Creation, modification, or deletion of objects
- **Audit events** Login events and security changes
- **Server configuration** Alterations to server settings

Default Trace Future Status



Deprecation Notice

Will be removed in a future SQL Server version

Extended Events

Recommended replacement replacement technology

Migration Plan

Avoid using this feature in new development work and plan to modify existing applications that currently use it.

SQL Server Error Log

Primary Diagnostic Tool

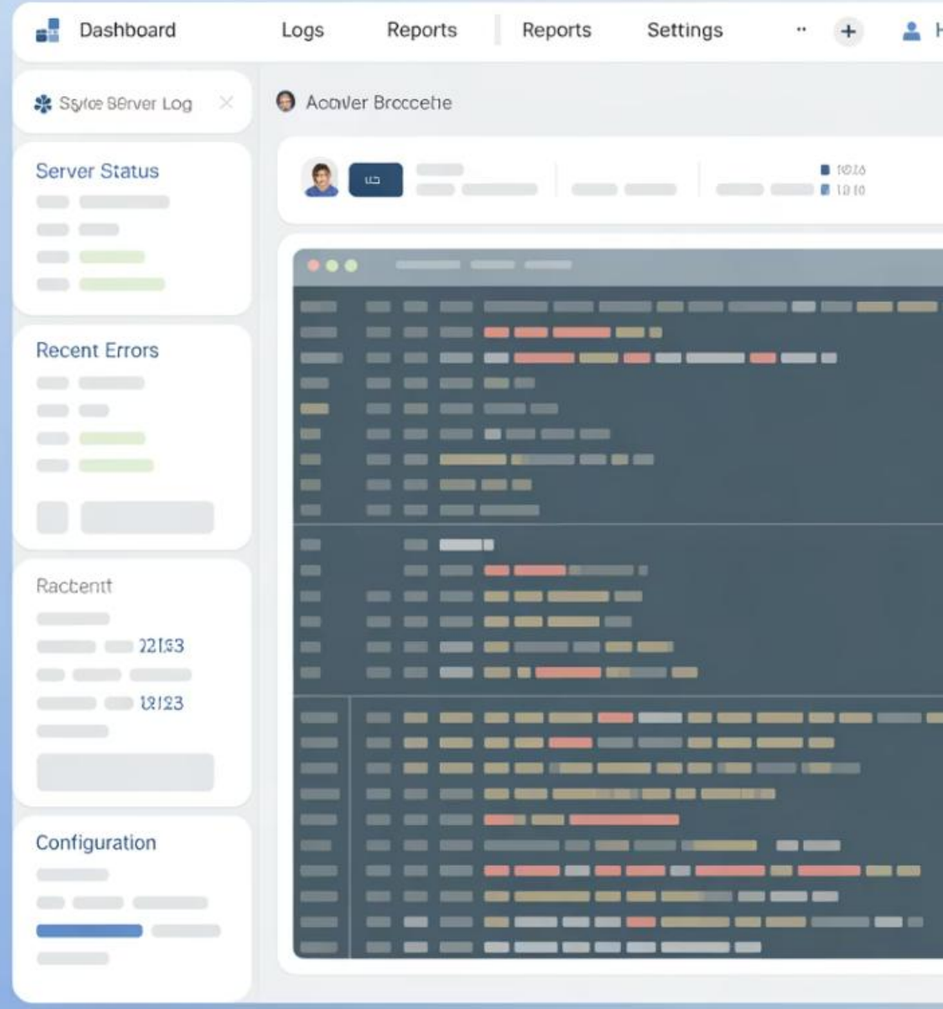
Critical initial resource for SQL SQL Server troubleshooting g and monitoring monitoring

Event Recording

Captures system events, errors, and informational messages

Historical Analysis

Enables post-incident investigation and root cause analysis



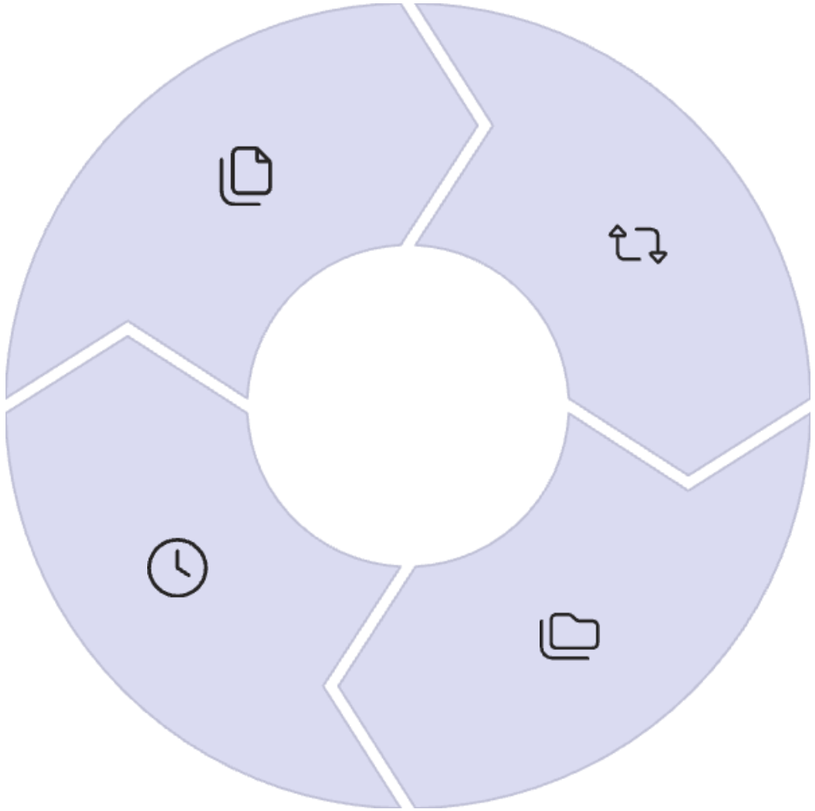
SQL Server Error Log Configuration

File Creation

A new file is generated with with each SQL Server startup, startup, or the Maximum size is size is reached

Retention

Six archived files with an unlimited size by default, configurable



Log Cycling

Use sp_cycle_errorlog to create new files

Storage Location

\Program Files\Microsoft SQLServer\MSSQLxx.MSSQLSERVER\MSSQL\LOG\ERORRLOG.xx

SQL Server Error Log Access Methods

Management Studio

Access through SSMS Object Explorer under Management node

sp_readerrorlog

Stored procedure with parameters for file selection

- @p1: 0=current, 1=previous
- @p2: 1=SQL Error log, 2=SQL 2=SQL Agent log (default is is NULL SQL Error log)

xp_readerrorlog

Extended stored procedure with additional parameters

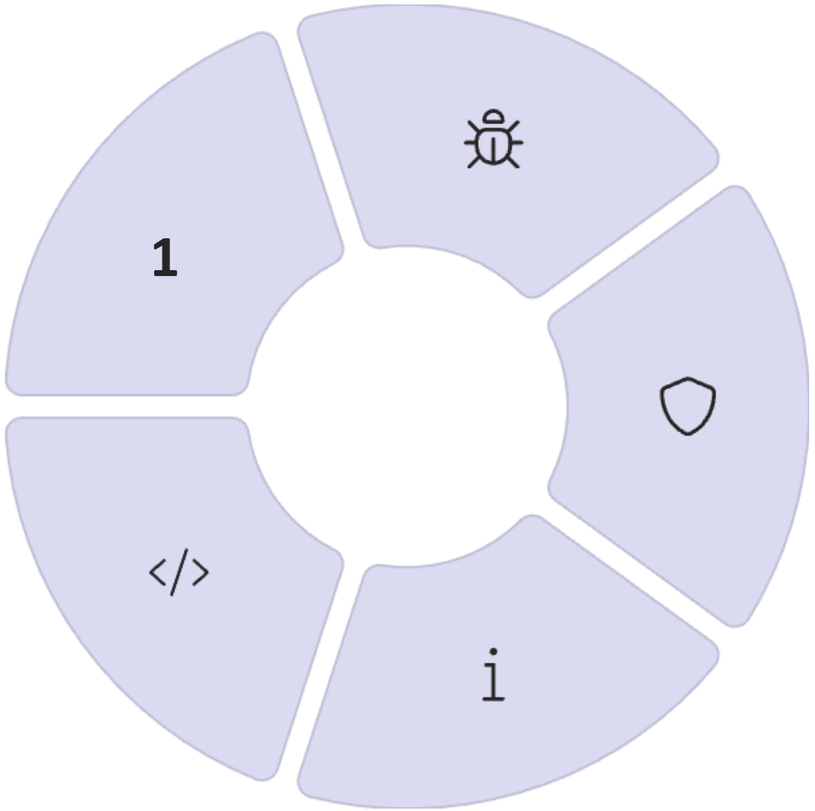
- @p5: Filter by start time
- @p6: Filter by end time
- @p7: Sort order options

```
/*
Use the three additional parameters (start time, end time, sort order filter via
 execution order).
*/
DECLARE @logFileType SMALLINT= 2;
DECLARE @start DATETIME;
DECLARE @end DATETIME;
DECLARE @logno INT= 0;
SET @start = dateadd(dd,-3,getdate());
SET @end = GETDATE()
DECLARE @searchString1 NVARCHAR(256)= 'SQLServerAgent';
DECLARE @searchString2 NVARCHAR(256)= 'startup service account';
EXEC master.dbo.xp_readerrorlog
  @logno,
  @logFileType,
  @searchString1,
  @searchString2,
  @start,
  @end;
```

SQL Server Error Log Content (Partial List)

System Events
SQL Server startup and shutdown sequences

User-Defined Events
Custom messages from applications and stored procedures



Error Messages

Authentication failures (18456), file access issues (5120)

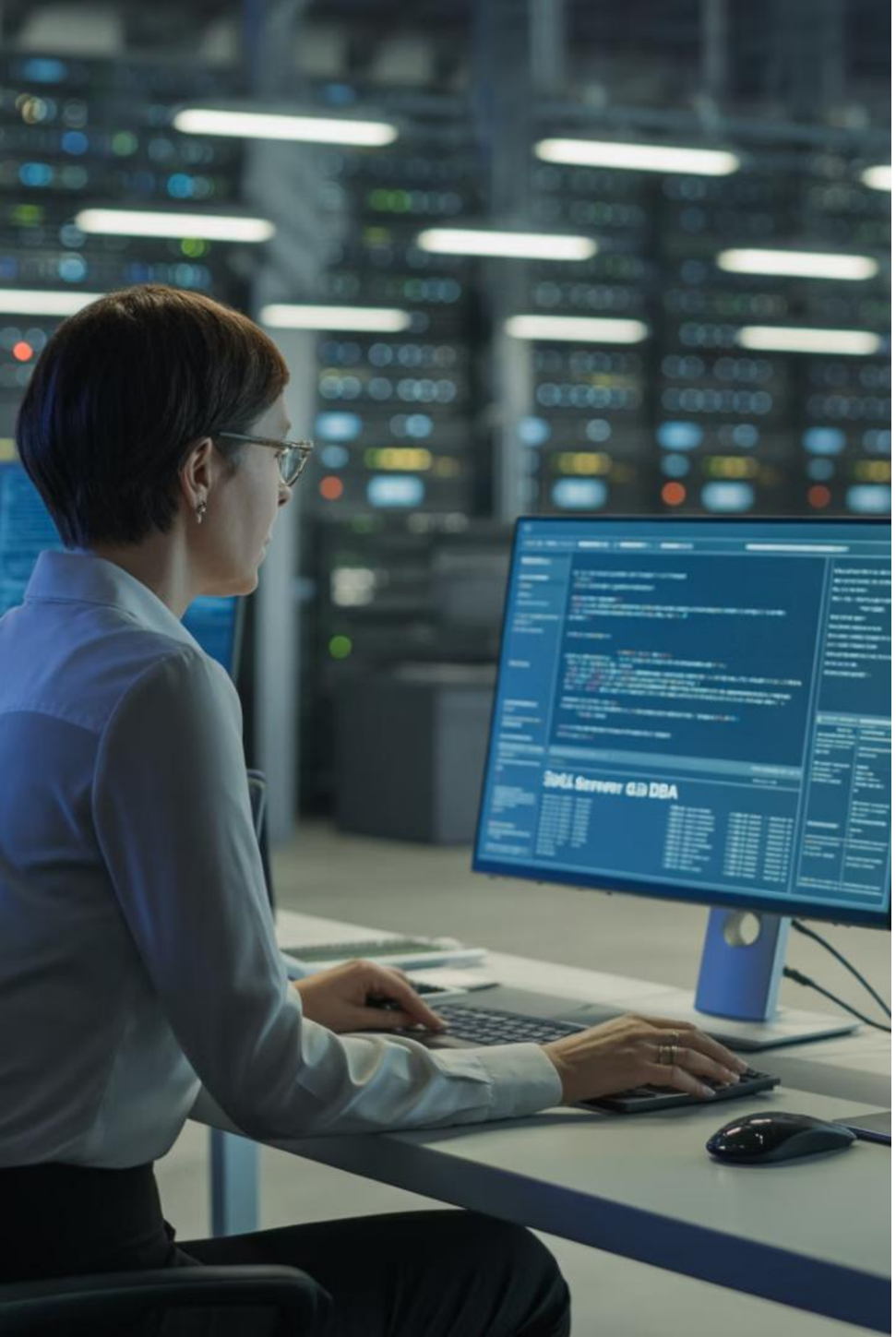
Security Events

Login attempts, Permission changes, Security policy changes

Information Messages

Configuration changes, backup/restore operations

SQL Server Agent Error Log



Agent Error Log Configuration

File Creation

A new log is generated at each SQL Server startup

Archive Files

Default retention of nine historical log files

File Size

Unlimited size by default, no size restriction

Log Cycling

Use sp_cycle_agent_errorlorlog to create new files

Storage Location

\Program Files\Microsoft SQL Server\MSSQLxx.MSSQLSERVER\MSSQL\LOG\SQLAGENT.1

Agent Error Log Access Methods

Management Studio

Access through SSMS Object Explorer under the SQL Server Server Agent node

sp_readerrorlog

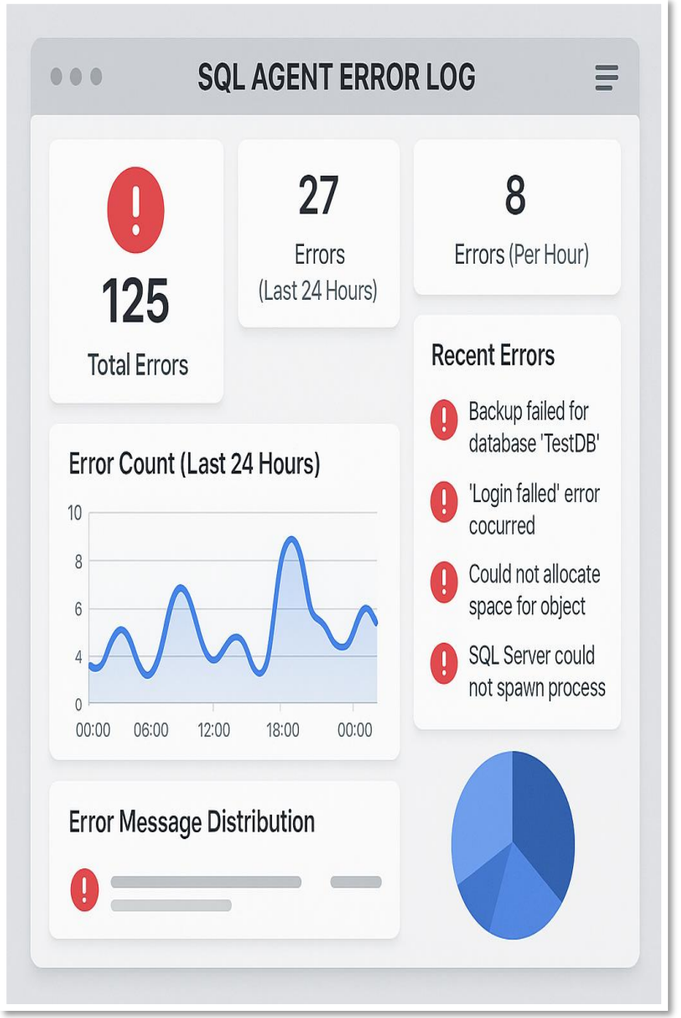
Stored procedure with parameters for file selection

- @p1: 0=current, 1=previous, etc.
- @p2: 1=SQL Error log, 2=SQL 2=SQL Agent log (default is is NULL SQL Error log)

xp_readerrorlog

Extended stored procedure with additional parameters

- @p5: Filter by start time
- @p6: Filter by end time
- @p7: Sort order options



Agent Error Log Content (Partial List)

Three Level

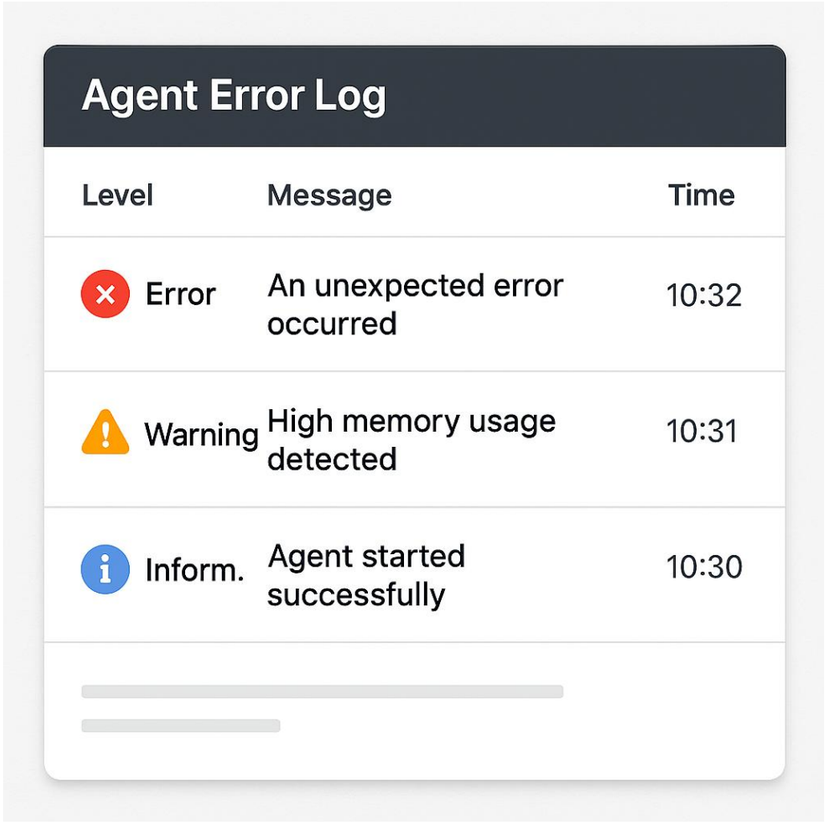
- Error: [516] Step 2 for job 0xB694DFA54D46EF409E7CD7BFAF23C199 failed with SQL error number 50000, severity 18
- Warning: [474] Unable to refresh Database Mail Profile
- Information

Warnings and Errors

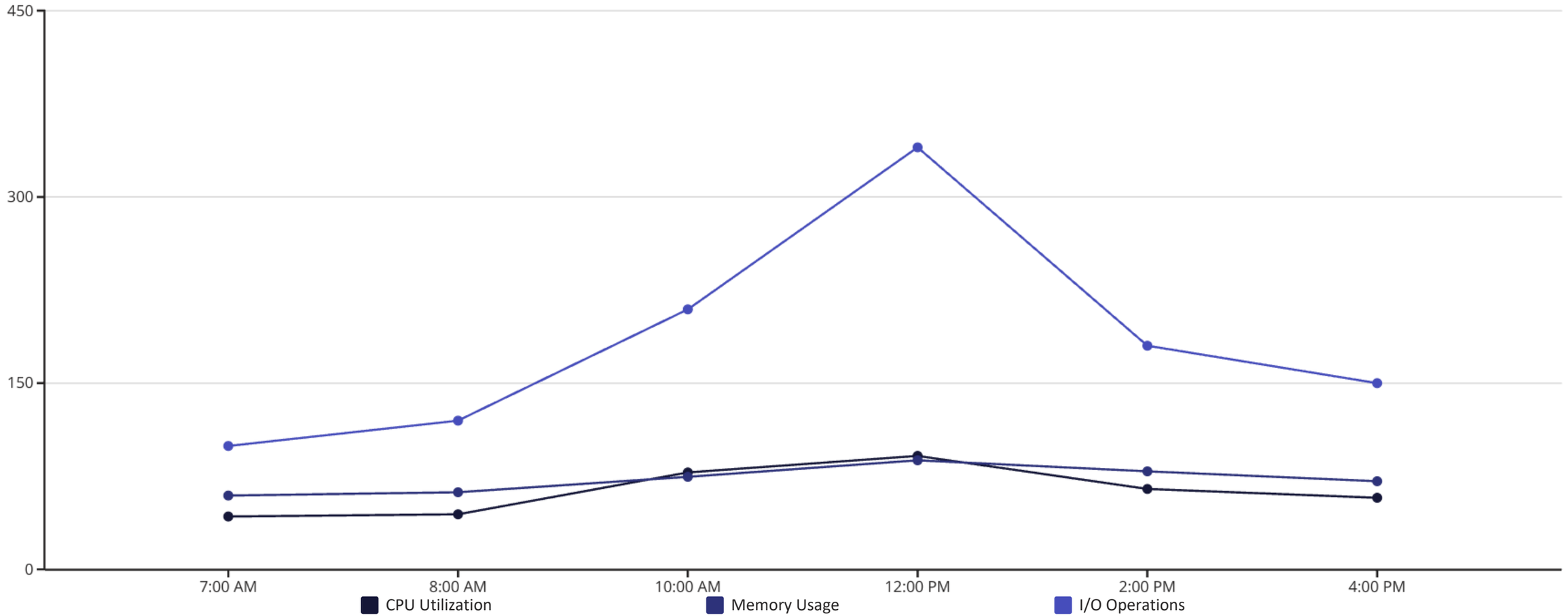
- Job <job_name> was deleted while it was running
- Unable to start mail session

Execution Trace Messages (will demo)

- Detailed job execution steps steps and outcomes



System_health Extended Event Trace



The system_health session tracks server resource utilization throughout the day, with peak usage occurring around noon. CPU and Memory usage patterns correlate with fluctuations in the database workload, while I/O operations exhibit more dramatic variation.

System_health XE Configuration

Introduction

Default Extended Events session since SQL Server 2008

Startup Behavior

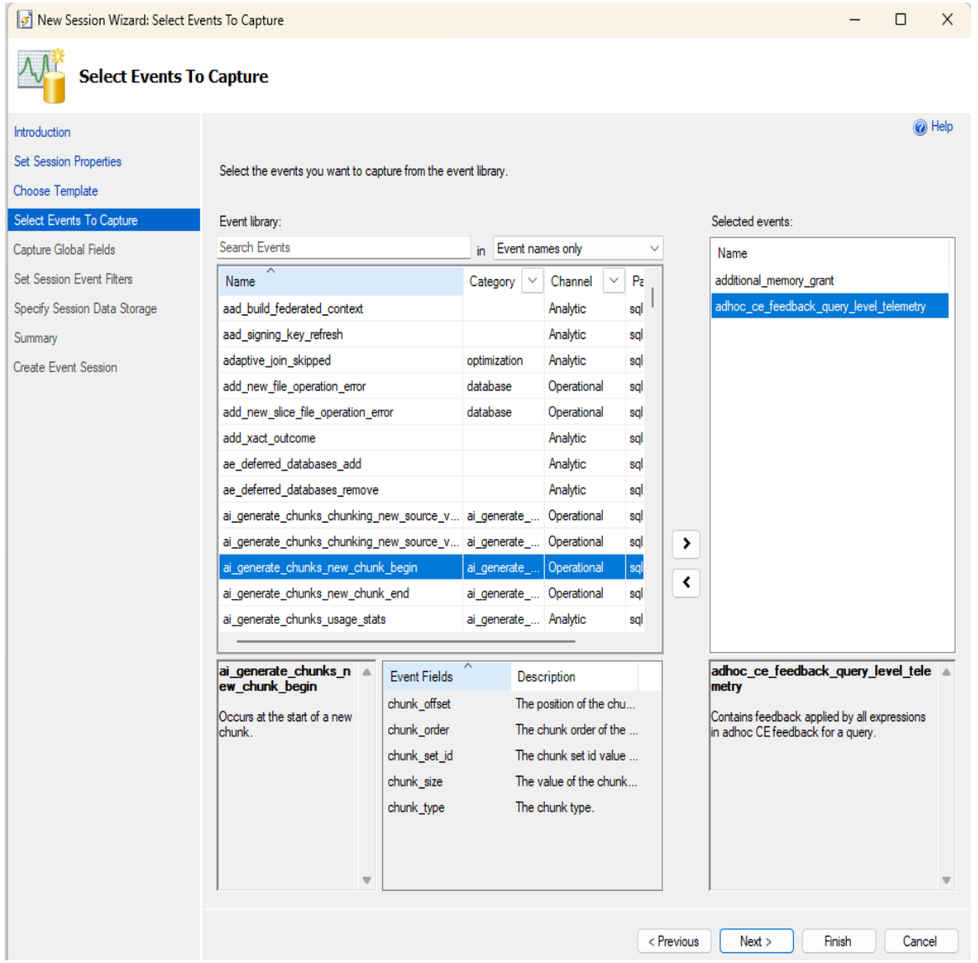
Automatically begins at SQL Server startup

File Location

\Program Files\Microsoft SQL Server\MSSQLxx.MSSQLSERVER\MSSQL\LOG\system_health_0_*.xel

File Management

Nine archived files, created at each server restart. restart. Unlimited size. Configurable but not recommended.



System_health XE Access Methods

SSMS XEvent Viewer

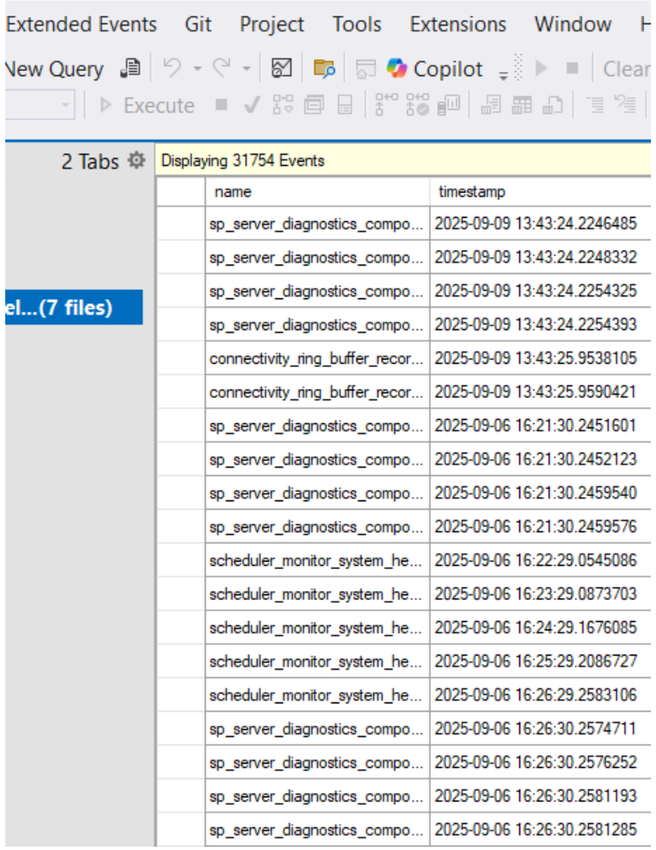
Use "Merge Extended Event Files" option to analyze trace data

Live Data Monitoring

Use "Watch Live Data" in in SSMS for real-time session monitoring

T-SQL Analysis

Query with fn_xe_file_target_read_file function for programmatic access



name	timestamp
sp_server_diagnostics_compo...	2025-09-09 13:43:24.2246485
sp_server_diagnostics_compo...	2025-09-09 13:43:24.2248332
sp_server_diagnostics_compo...	2025-09-09 13:43:24.2254325
sp_server_diagnostics_compo...	2025-09-09 13:43:24.2254393
connectivity_ring_buffer_recor...	2025-09-09 13:43:25.9538105
connectivity_ring_buffer_recor...	2025-09-09 13:43:25.9590421
sp_server_diagnostics_compo...	2025-09-06 16:21:30.2451601
sp_server_diagnostics_compo...	2025-09-06 16:21:30.2452123
sp_server_diagnostics_compo...	2025-09-06 16:21:30.2459540
sp_server_diagnostics_compo...	2025-09-06 16:21:30.2459576
scheduler_monitor_system_he...	2025-09-06 16:22:29.0545086
scheduler_monitor_system_he...	2025-09-06 16:23:29.0873703
scheduler_monitor_system_he...	2025-09-06 16:24:29.1676085
scheduler_monitor_system_he...	2025-09-06 16:25:29.2086727
scheduler_monitor_system_he...	2025-09-06 16:26:29.2583106
sp_server_diagnostics_compo...	2025-09-06 16:26:30.2574711
sp_server_diagnostics_compo...	2025-09-06 16:26:30.2576252
sp_server_diagnostics_compo...	2025-09-06 16:26:30.2581193
sp_server_diagnostics_compo...	2025-09-06 16:26:30.2581285

System_health XE Content (Partial List)

Wait Statistics

- Non-Preemptive waits >30 secs
- Preemptive waits >5 secs

Ring Buffer Data

- Deadlock
- Security errors
- Connection close – such as login failure
- Non-yielding condition

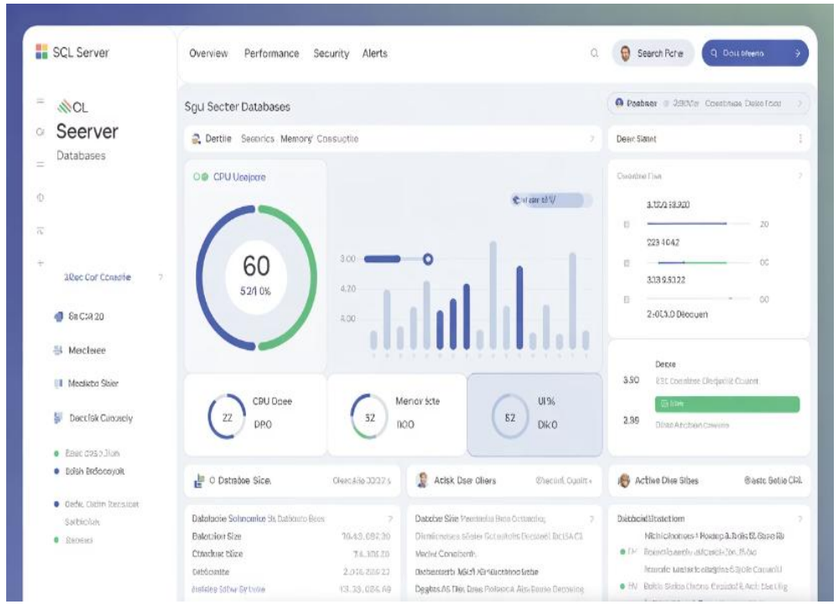
Memory Events

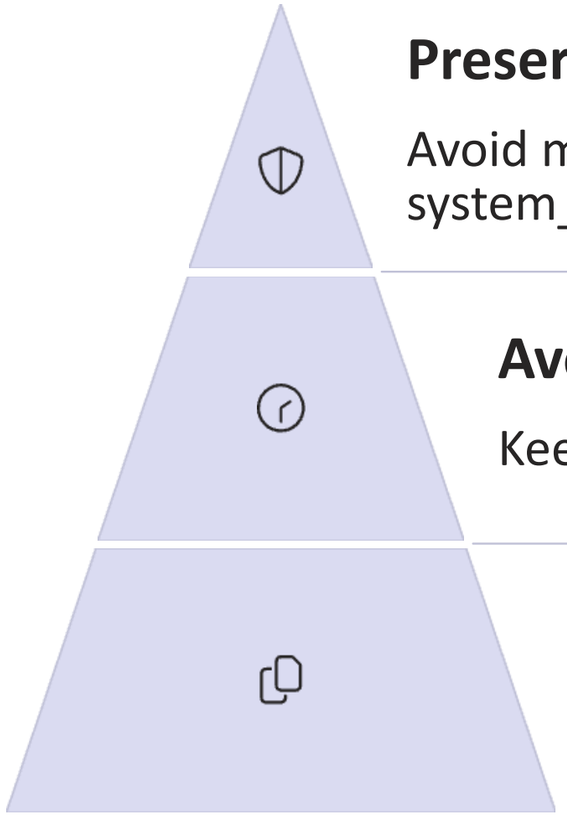
- Out of memory reports
- Memory allocation failures
- Memory pressure indicators

Error Events

- 14 specific error codes (41309 is one example)
- Severity level 20+ errors
- Resource errors

System_health XE Best Practices





Preserve Default Configuration

Avoid modifying the system_health session

Avoid Stopping or Pausing

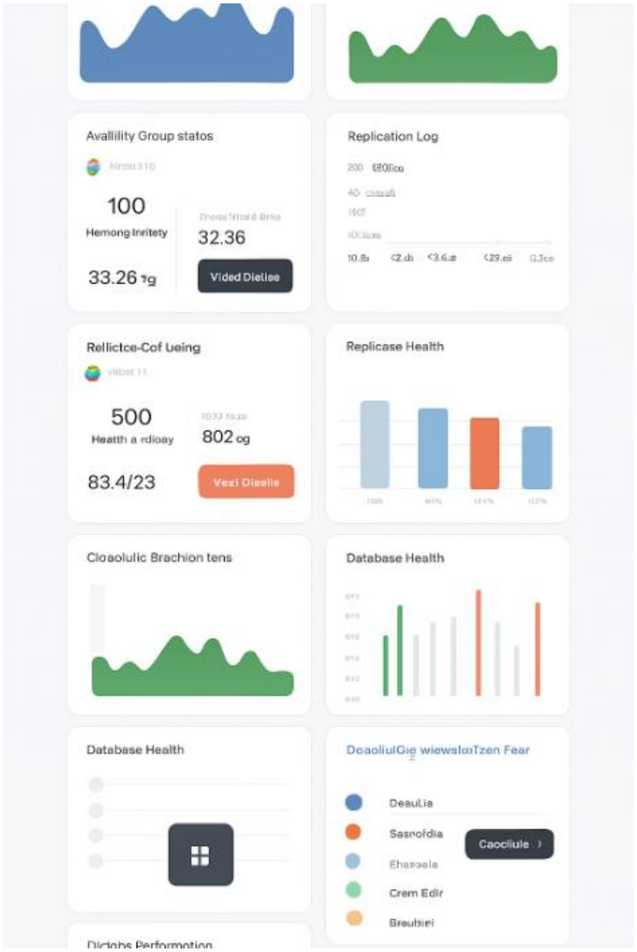
Keep session running continuously

Use Cloned Sessions

Create separate sessions for custom monitoring

Microsoft strongly recommends against stopping, altering, or deleting the system_health session. Future product updates may overwrite any customizations. If you need additional data collection, create a new Extended Events session with your specific requirements.

AlwaysOn_health Extended Event Trace

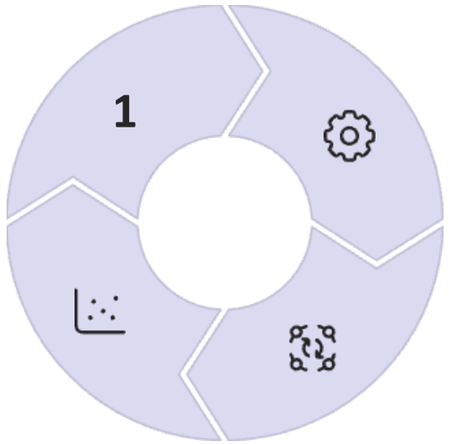


Availability Groups

Dedicated monitoring for Always On AG components

Performance

Tracks availability group efficiency metrics

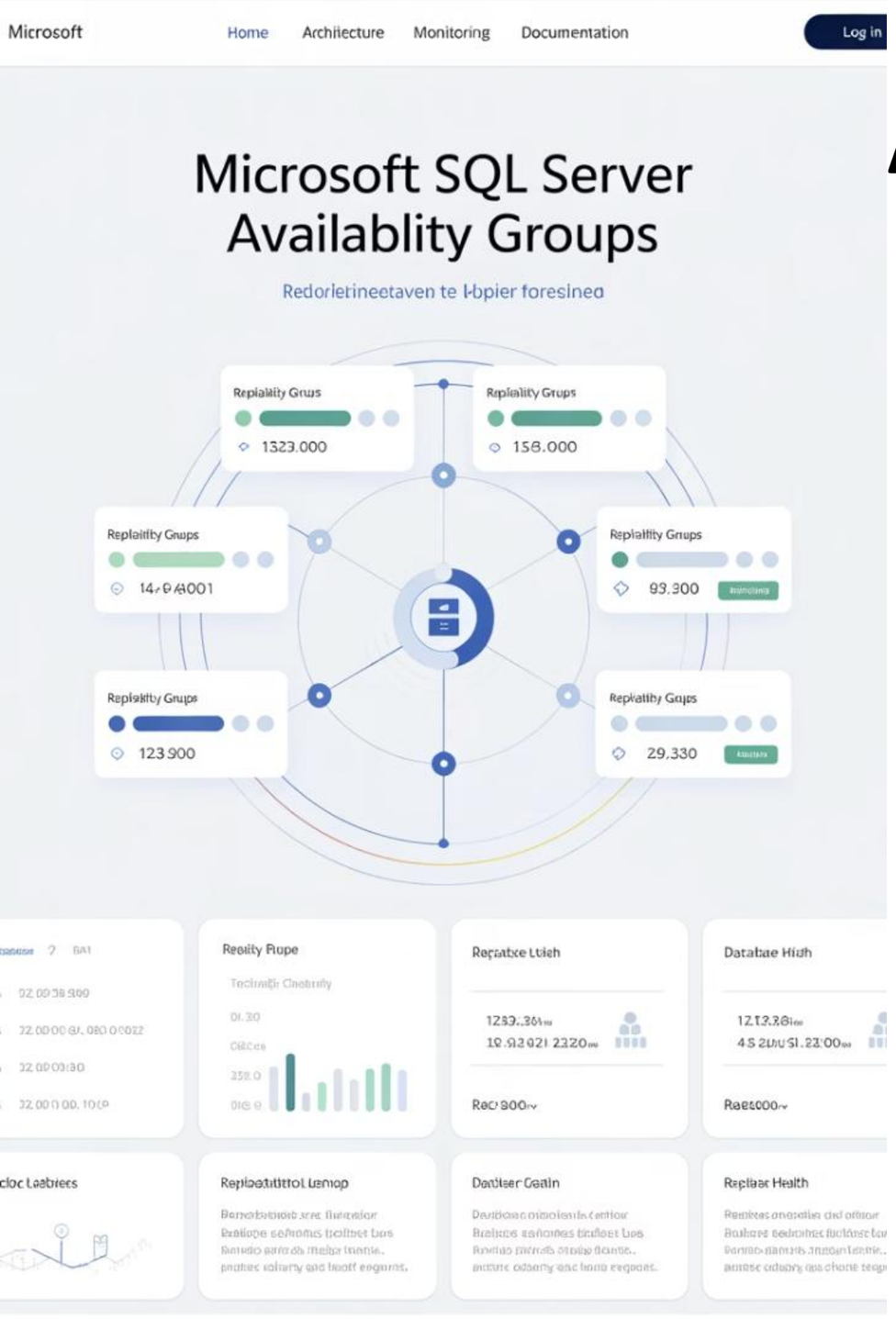


Diagnostics

Critical for troubleshooting AG AG issues

Replica Health

Monitors synchronization and failover events



AlwaysOn_health XE Configuration

Replica Coverage

Automatically starts the the session on every participating availability availability replica

Automatic Creation

Created automatically when an Availability Group is configured

File Location

\Program Files\Microsoft SQL Server\MSSQLxx.MSSQLSERVER\MSSQL\LOG\AlwaysOn_health_0_*.xel

Nine archived files with unlimited size

Configurable

AlwaysOn_health XE Access Methods

SSMS File Merge

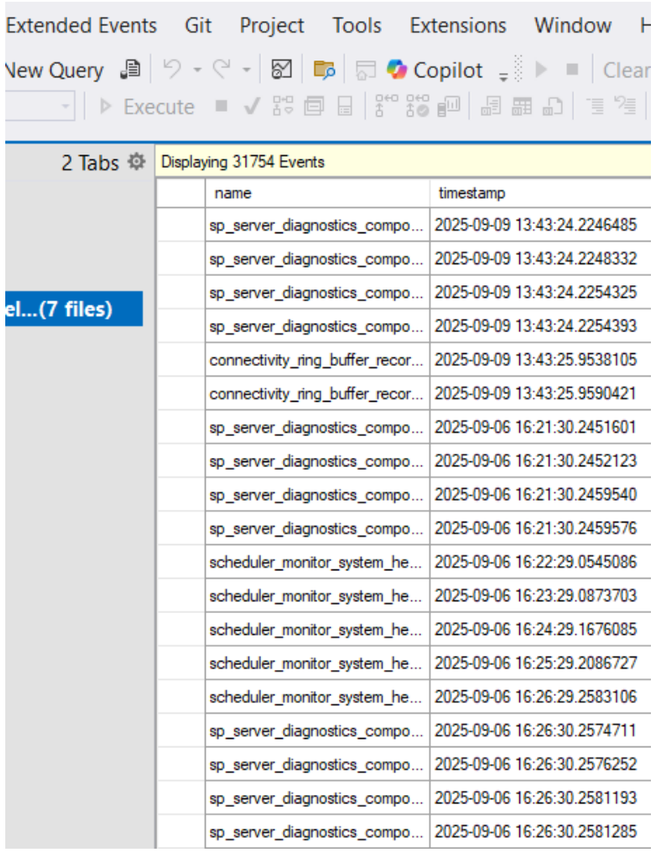
Use "Merge Extended Event Files" option to analyze trace data

Live Monitoring

"Watch Live Data" for real-time event observation

T-SQL Access

Query with fn_xe_file_target_read_file function



name	timestamp
sp_server_diagnostics_compo...	2025-09-09 13:43:24.2246485
sp_server_diagnostics_compo...	2025-09-09 13:43:24.2248332
sp_server_diagnostics_compo...	2025-09-09 13:43:24.2254325
sp_server_diagnostics_compo...	2025-09-09 13:43:24.2254393
connectivity_ring_buffer_recor...	2025-09-09 13:43:25.9538105
connectivity_ring_buffer_recor...	2025-09-09 13:43:25.9590421
sp_server_diagnostics_compo...	2025-09-06 16:21:30.2451601
sp_server_diagnostics_compo...	2025-09-06 16:21:30.2452123
sp_server_diagnostics_compo...	2025-09-06 16:21:30.2459540
sp_server_diagnostics_compo...	2025-09-06 16:21:30.2459576
scheduler_monitor_system_he...	2025-09-06 16:22:29.0545086
scheduler_monitor_system_he...	2025-09-06 16:23:29.0873703
scheduler_monitor_system_he...	2025-09-06 16:24:29.1676085
scheduler_monitor_system_he...	2025-09-06 16:25:29.2086727
scheduler_monitor_system_he...	2025-09-06 16:26:29.2583106
sp_server_diagnostics_compo...	2025-09-06 16:26:30.2574711
sp_server_diagnostics_compo...	2025-09-06 16:26:30.2576252
sp_server_diagnostics_compo...	2025-09-06 16:26:30.2581193
sp_server_diagnostics_compo...	2025-09-06 16:26:30.2581285

AlwaysOn_health XE Content (Partial List)

DDL Operations

CREATE, ALTER, DROP events events related to availability availability groups

State Changes

Replica role changes and availability mode transitions transitions

Data Movement

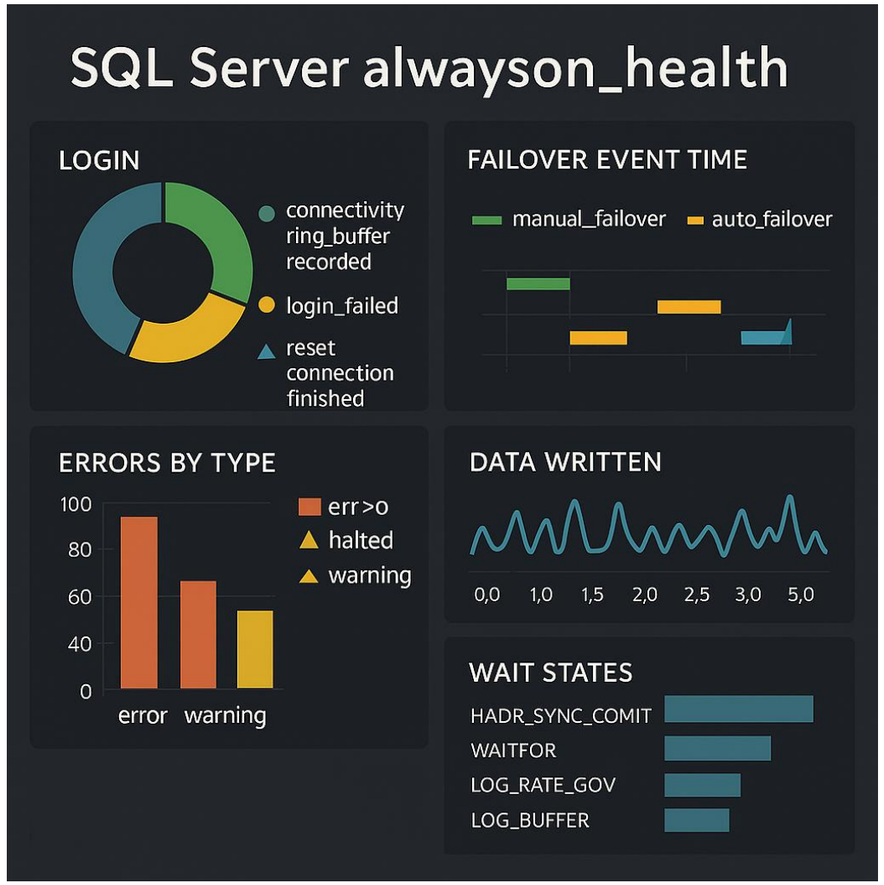
If data movement is suspended suspended or resumed

Lease Management

Lease expiration events and and timeout monitoring

Error Events

Specific AG-related error codes (35201, 35202, etc.)



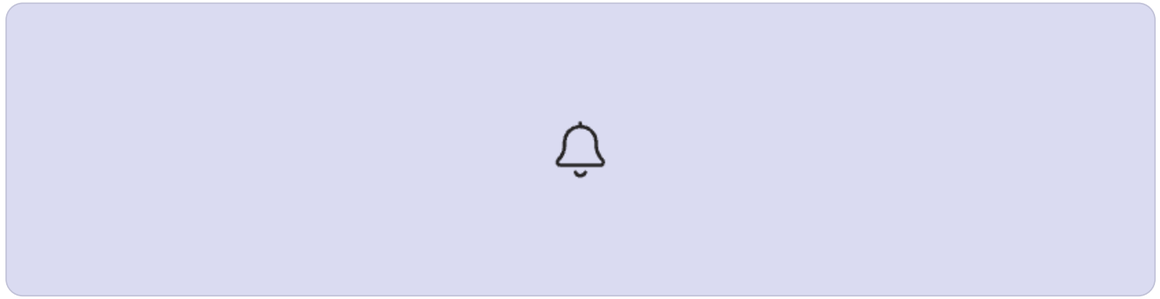
AlwaysOn_health XE Best Practices

Verify Session Status

Confirm the session is running on all replicas

Use XE for proactive monitoring

Track events before they escalate



Customize alerts for failovers

Configure custom XE-based alerts to notify you notify you only once per failover

If the availability group **was not created using the New Availability Group Wizard**, the AlwaysOn_health session might not start automatically. This prevents critical event capture during failures. Always verify the session status and manually configure it to start automatically by setting appropriate session properties.

Demo Environment Details

2022

SQL Server

SQL Server 2022 with Cumulative Update 21

21.5.14

Management Studio

SSMS version 21.5.14

26100

Microsoft Windows 11 Pro

10.0.26100 Build 26100

All demonstrations and examples in this presentation were performed using the software the software versions listed above. Some features may vary slightly in older or newer newer versions of SQL Server and related tools.


Empowering Ideas,

Contact Information

LinkedIn

linkedin.com/in/sqlworldwide

Website

sqlworldwide.com

Email

taiob@sqlworldwide.com

Bluesky

@sqlworldwide.bsky.social

GitHub

github.com/sqlworldwide

Thank You!

Download Resources

Access presentation slides and demo scripts from https://github.com/sqlworldwide/Presentations

Provide Feedback

Share your thoughts and suggestions to help improve improve future sessions

Stay Connected

Follow on LinkedIn and Bluesky