MATERI SISTEM MANAJEMEN BASIS DATA 2019
Tim SMBD
Minggu ke 9

Topik

Auditing SQL Server

Tujuan

1. Menjelaskan opsi untuk auditing data access di SQL Server
2. Mengimplementasi SQL Server Audit
3. Mengelola SQL Server Audit

Pendahuluan

Auditing

Audit pada sebiah SQL Server adalah tindakan yang melibatkan pelacakan dan pencatatan setiap event yang terjadi pada Database Engine. Event yang di audit dapat ditulis pada event log atau audit file.

Ada beberapa tingakatan audit untuk SQL Server, tergantung pada syarat dari organisasi atau standar dari instalasi SQL Server anda. Audit SQL Server menyediakan toll untuk mengaktifkan, menyimpan, dan melihat audit pada berbagai server dan database objects.

Audit SQL Server dapat merekam aksi dari groups per-instance, dan grup audit database per database. Event akan tercatat setiap kali ada tindakan.

Menggunakan C2 Audit Mode

C2 adalah salah satu dari serangkaian peringkat keamanan yang diterbitkan oleh National Computer Security Center (NCSC) pada dokumen Trusted Computer System Evaluation Criteria (TCSEC). C2 mengacu pada beberapa kebijakan keamanan uang menentukan bagaimana sistem beroperasi dengan aman. Sertifiaksi berlaku untuk instalasi tertentu, Hardware, Software, dan enviroment tempat sistem beroperasi.

Kebijakan keamanan pada C2 dikenal dengan Discretionary Access Control. Pengguna Sistem:

1. Object sendiri
2. Memiliki Kontrol atas perlindungan object yang mereka miliki
3. Bertanggung jawab atas semua tindakan terkait akses.

C2 relatif mudah untuk dicapai oleh sebuah situs.

SQL server dapat dikonfigurasi untuk memnuhi persyaratan C2. Meskipun mudah dikonfigurasi, opsi ini jarang digunakan karena dampak kinerja yang kurang pada server yaitu pembuatan volume yang besar pada event information. Terkadang user yang melakukan

konfigurasi tanpa menyadari telah mengaktifkan C2 sehingga user kehabisan disk space. C2 akhirnya telah digantikan oleh Common Criteria Compliance.

Common Criteria Compliance.

SQL Server menyediakan opsi server “common criteria compliance enabled” yang dapat diatur di sp_configure pada sistem stored prcedure dan tersedia pada versi Enterprise. Ketika opsi ini diaktifkan akan ada 3 perubahan yang terjadi pada cara SQL Server beroperasi :

1. Residual Information Protection (RIP) : memori akan selalu ditimpa dengan pola bit yang dikenal sebelum digunakan kembali.
2. Kemampuan untuk melihat statistik login : audit login diakytifkan secara otomatis.
3. Kolom GRANT tidak akan mengesampingkan tabel DENY : merubah perilaku dari permission system.

Implementasi RIP akan meningkatkan keamanan tetapi berdampak negatif pada performa dari sistem.

Penggunaan Triggers pada Auditing

Triggers dapat memainkan peran penting dalam audit. Ini memungkinkan pelacakan lebih detail dan log yang masuk dan juga memungkinkan log masuk kembali berdasarkan logika bisnis dan administrasi.

Penggunaan SQL Trace pada Auditing

SQL Trance adalah sistem store prcedure yang digunakan oelh SQL Server Profiler. Digunakan untuk mengelola pelacakan menawarkan metode penelusuran yang jauh lebih ringan, terutama ketika event tersebut difilter dengan baik. SQL Trance memiliki kemampuan untuk menangkap perintah yang dikirim ke server, dapat digunakan untuk mengaudit perintah tersebut.
SQL Trance menggunakan mekanisme penelusuran server-side yang mendjamin bahwa tidak ada event yang hilang, selama ada ruang yang tersedia pada disk dan tidak ada kesalahan penulisan. Kemungkinan event yang hilang perlu dipertimbangkan ketika mengevaluasi penggunaan SQL Trance untuk tujuan audit.

Implementasi SQL Server Audit

Kita akan belajar menggunakan Extended Event. Dan kita akan menggunakan Dynamic Management View (DMV) untuk mendukung fitur audit pada SQL Server.

Extended Events

EE memungkinkan anda untuk menentukan tindakan yang harus diambil ketika event itu terjadi. Konfigurasi EE dikirim dalam file .exe atau .dll yang disebut “packages”. Packages

adalah unit deployment dan installation untuk EE. Anda tidak dapat mengubah konfigurasi internal tetapi dapat mengubah paket yang lain. EE menggunakan terminologi khusus untuk menggambarkan objek yang digunakan:

Object	Description
Events	Points of interest during the execution of code
Targets	Places that the trace details are sent to (such as files)
Actions	Responses that can be made to events (for example, one type of action captures execution plans to include in the trace)
Types	Definitions of the objects that Extended Events works with
Predicates	Dynamic filters that are applied to the event capture
Maps	Mapping of values to strings. (An example would be the mapping of codes to descriptions)

Konfigurasi SQL Server Audit

1. Creating an audit : menentukan bagaiman hasil akan diproses. Contoh ketika mengonfigurasi audit, anda harus memutuskan apa yang dilakukan jika ruang disk habis.
2. Defening the target : menentukan kemana output akan dikirim.
3. Creating an audit specification : menentukan tindakan yang akan diaudit. Tindakan ini bisa di tingkat servera tau database.
4. Enabling the audit and audit specification : Langkah dimana object akan diaktifkan, karena default audit dibuat dalam keadaan nonaktif).
5. Read the output events : berkaitan dengan detail output dari audit.

Audit Actions dan Action Groups

Actions dapat terjadi pada 3 level : Server, database dan audit.

Action Groups

Action groups digunakan untuk menghindari banyaknya individual actions. Membuat pengaturan dan pengelolaan audit lebih mudah karena menghindari kebutuhan banyaknya individual action pada audit.
Contoh action group :
• BACKUP_RESTORE_GROUP
• DATABASE_MIRRORING_LOGIN_GROUP

• DATABASE_OBJECT_ACCESS_GROUP
• DBCC_GROUP
• FAILED_LOGIN_GROUP
• LOGIN_CHANGE_PASSWORD_GROUP

Definisi Audit Target

Audit dapat dikirim ke tiga target :

1. Dikirim ke File. Ouput file memberikan performance yang tinggi dan opsi paling mudah untuk dikonfigurasi.
2. Dikirim ke Windows application events log. Hindari mengirimkan terlalu banyak detail ke log karena administrator jaringan cenderung tidak menyukai aplikasi yang meulis konten terlalu banyak ke salah satu event logs.
3. Dikirim ke Windows security event log. Security event log adalah opsi secure output tetapi mengharuskan SQL Server service ditambahakan “generate security audits” sebelum digunakan.

Creating Audits

- Creating an audit requires a number of configurations:

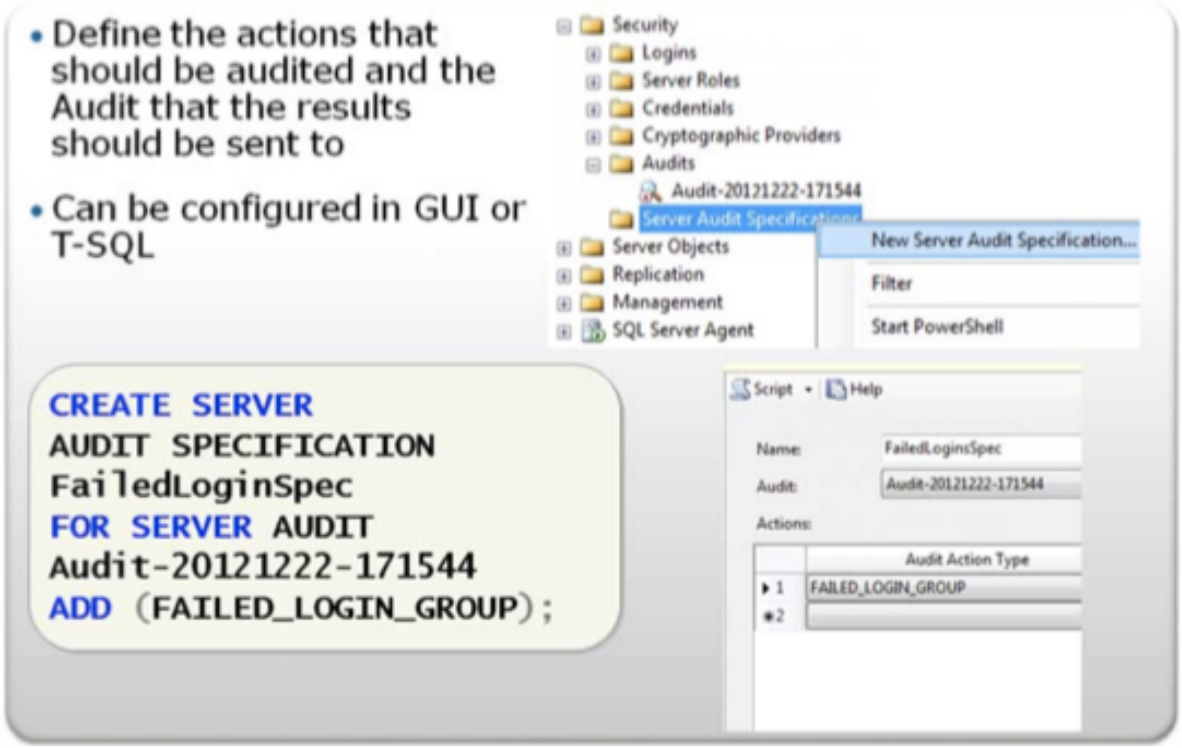
Configuration	Comment
Audit name	Name for the audit
Queue delay (in milliseconds)	Amount in time before audit actions must be processed
Shut down server on audit failure	Indicates that SQL Server cannot continue if audit is not working
Audit destination	Audit Target
Maximum rollover files	Maximum number of files to retain (only for files)
Maximum file size (MB)	Maximum size of each audit file
Reserve disk space	Indicates whether disk space for the audit files should be reserved in advance
Maximum files	Caps the number of audit files

Saat anda membuat audit, anda akan membuat keputusan teantang bagaimana SQL Server akakn memproses hasil yang dikirim ke audit target. Audit dapat dibuat menggunakan GUI di SSMS atau melalui perintah CREATE SERVER AUDIT di T-SQL.

Audit Configuration Options

Nama pada audit sering berkaitan dengan dengan detail audit, tanggal waktu atau kombinasi keduanya, setelah mengkonfigurasi nama, konfigurasi queue delay sangat penting. Queue delay menunjukan berapa lama SQL Server dapat menyangga hasil audit sebelum dikirimkan ke target.

Creating Server Audit Specifications



membuat spesifikasi Server audit dapat dilakukan dengan GUI atau T-SQL. Spesifikasi server audit dibuat dalam keadaan dinonaktifkan secara default. Audit Object, termasuk spesifikasi audit, biasanya dinonaktifkan sampai audit objects telah dibuat.

Server audit specification merinci tindakan yang akan diaudit. Anda dapat memilih action group atau individual action dan object. Nama specification adalah FailedLoginSpec dan data dikumpulkan dari spesifikasi akan dikirim ke audit 20121222-171544 audit. Action group yang akan di audit adalah FAILED_LOGIN_GROUP.

Audit-related DMVs dan System Views

- SQL Server provides a set of DMVs and system views for managing SQL Server Audit

Audit-related DMVs
sys.dm_server_audit_status
sys.dm_audit_actions
sys.dm_audit_class_type_map

Audit-related System Views
sys.server_audits
sys.server_file_audits
sys.server_audit_specifications
sys.server_audit_specification_details
sys.database_audit_specifications
sys.database_audit_specification_details

SQL server menydiakan selumlah Dynamic management Views (DMVs) dan sistem views yang dapat membanty anda mengelola SQL Server Audit.
DMVs dan sistem view yang tersedia :

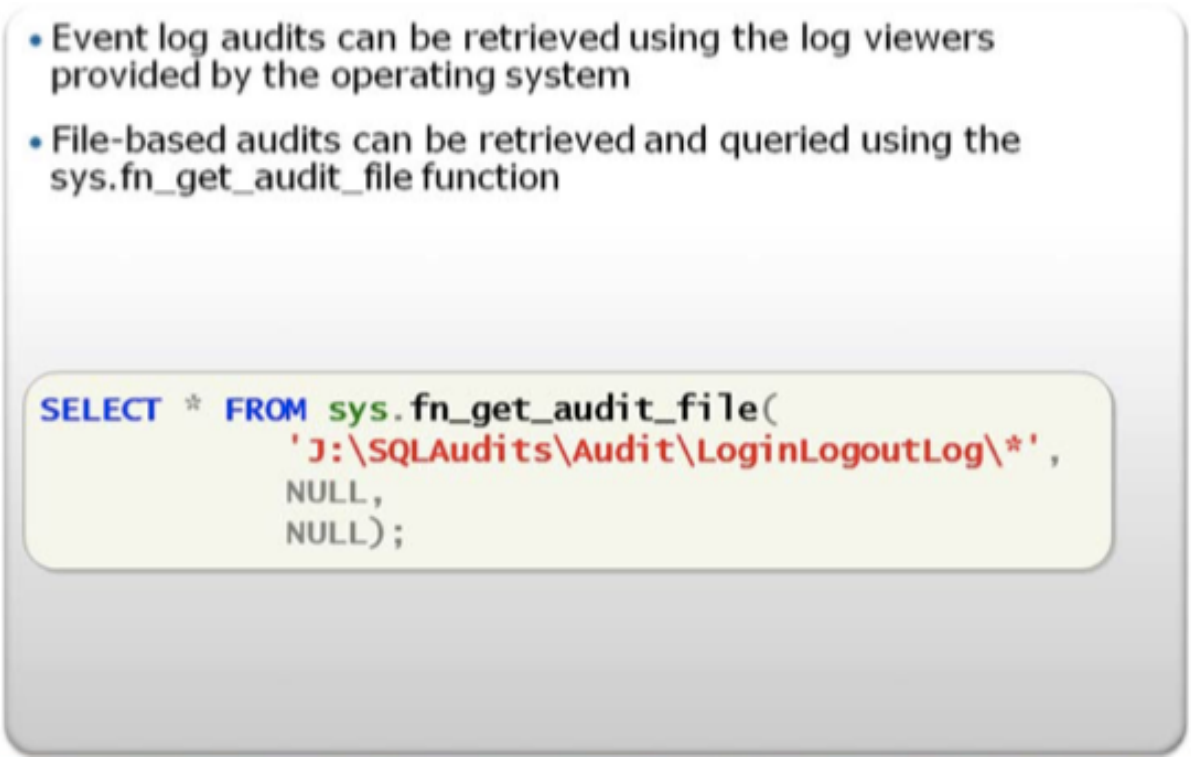
DMV/View	Description
sys.dm_server_audit_status	Returns a row for each server audit indicating the current state of the audit
sys.dm_audit_actions	Returns a row for every audit action that can be reported in the audit log and every action group that can be configured as part of an audit
sys.dm_audit_class_type_map	Returns a table that maps the class types to class descriptions
sys.server_audits	Contains one row for each SQL Server audit in a server instance
sys.server_file_audits	Contains extended information about the file audit type in a SQL Server audit
sys.server_audit_specifications	Contains information about the server audit specifications in a SQL Server audit

DMV/View	Description
sys.server_audit_specification_details	Contains information about the server audit specification details (actions) in a SQL Server audit
Sys.database_audit_specifications	Contains information about the database audit specifications in a SQL Server audit
Sys.database_audit_specification_details	Contains information about the database audit specifications in a SQL Server audit

Managing SQL Server Audit

Tujuan dari manage SQL server audit adalah mengambil audit, bekerja dengan audit record structure, dan identifikasi potensi masalah dari Audit SQL Server.

Retrieving Audits



untuk log yang dikirim ke file, SQL Server menyediakan fungsi yang dapat mengembalikan content log bebasis file sebagai tabel yang bisa di query dengan T-SQL. Folder yang berisi audit log sering berisi beberapa audit file. Fungsi sys.fn_get_audit_file digunakan untuk mengambil file tersebut. Dibutuhkan 3 parameter: file_pattern, initial_file_name, dan audit_record_offset. File_pattern yang disediakan bisa dalam salah satu dari 3 format:

Format	Description
<path>*	Collects all audit files in the specified location
<path>\LoginsAudit_{GUID}	Collect all audit files that have the specified name and GUID pair
<path>\LoginsAudit_{GUID}_00_29384.sqlaudit	Collect a specific audit file

Working with the Audit Record Structure

Audit record structure adalah detail dalam Books Online dengan topik “sys.fn_get_audit_file (T-SQL)”. Audit record harus dapat disimpan dalam sistem event log dan ke dalam file. Karean persyaratan ini, format record dibatasi ukurannya oleh aturan yang terkait dengan event logging systems. Karakter akan dibagi menjadi 4000 karakter dan potongan akan tersbar di sejumlah entri. Ini berarti bahawa satu peristiwa runggal dapat menghasilkan banyak entri audit. Kolom sequence_no disediakan untuk menunjukan bebrapa entri baris.

Potential SQL Server Audit Issues

Ada sejumlah masalah untuk dipertimbang kan dengan audit SQL Server.

1. Setiap audit diidentifiaksi oelh GUID. Ketiak database di restore arau dilampirkan pada server, upaya dilakukan untuk mencocokkan GUID dalam database dengan GUID audit di server. Jika tidak ada kecocokan yang terjadi, audit tidak akan berfungsi samapi situasinya diperbaiki dengan menjalankan perintah CREATE SERVER AUDIT untuk menetapkanGUID yang sesuai.
2. Jika database dilampirkan ke edisi SQL Server yang tidak mendukung tingkat kemampuan audit yang sama, maka lampiran akan berfungsi tetapi audit diabaikan.
3. Mirror server memperkenalkan masalah serupa ke GUID yang tidak cocok. Mirror partner harus memiliki audit server dengan GUID yang sama. Anda dapat membuat dengan menggunakan perintah CREATE SERVER AUDIT dan memberikan nilai GUID untuk mencocokkan nilai pada server utama.
4. Secara umum, dampak kinerja penuliasan audit harus dipertimbangkan. Jika ruang disk terisi, SQL Server mungkin tidak mulai. Jika demikian, anda mungkin perlu memaksa entri ke dalamnya melalu satu user startup dan –f parameter stratup.