



Jurusan Teknologi Informasi Politeknik Negeri Malang

## **Jobsheet-8: Auditing SQL Server Enviroment**

### **Mata Kuliah Sistem Manajemen Basis Data**

Pengampu: Tim Ajar Sistem Manajemen Basis Data

Maret 2020

---

#### **Topik**

Auditing SQL Server

#### **Tujuan**

Mahasiswa memahami:

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

#### **Pendahuluan**

#### **Auditing**

Audit pada sebuah 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 tingkatan audit untuk SQL Server, tergantung pada syarat dari organisasi atau standar dari instalasi SQL Server anda. Audit SQL Server menyediakan tool 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 yang menentukan bagaimana sistem beroperasi dengan aman. Sertifikasi berlaku untuk instalasi tertentu, Hardware, Software, dan environment 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 memenuhi 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 procedure 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 diaktifkan 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 procedure 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 bagaimana 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 menulis 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 ditambahkan “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 tentang bagaimana SQL Server akan 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 detail audit, tanggal waktu atau kombinasi keduanya, setelah mengkonfigurasi nama, konfigurasi queue delay sangat penting. Queue delay menunjukkan berapa lama SQL Server dapat menyangga hasil audit sebelum dikirimkan ke target.

## Creating Server Audit Specifications

- Define the actions that should be audited and the Audit that the results should be sent to
- Can be configured in GUI or T-SQL

**CREATE SERVER  
AUDIT SPECIFICATION  
FailedLoginSpec  
FOR SERVER AUDIT  
Audit-20121222-171544  
ADD (FAILED\_LOGIN\_GROUP);**

The screenshot shows the SQL Server Enterprise Manager interface. The left pane displays the 'Security' folder expanded, showing 'Logins', 'Server Roles', 'Credentials', 'Cryptographic Providers', 'Audits', and 'Server Audit Specifications'. The 'Server Audit Specifications' folder is selected, and a context menu is open with the option 'New Server Audit Specification...'. The right pane shows the 'New Server Audit Specification' dialog box. The 'Name' field is 'FailedLoginsSpec', the 'Audit' field is 'Audit-20121222-171544', and the 'Actions' list contains 'FAILED\_LOGIN\_GROUP'.

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 menyediakan sejumlah Dynamic management Views (DMVs) dan sistem views yang dapat membantu 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

- Event log audits can be retrieved using the log viewers provided by the operating system
- File-based audits can be retrieved and queried using the sys.fn\_get\_audit\_file function

```
SELECT * FROM sys.fn_get_audit_file(
    'J:\SQLAudits\Audit\LoginLogoutLog\*',
    NULL,
    NULL);
```

untuk log yang dikirim ke file, SQL Server menyediakan fungsi yang dapat mengembalikan content log berbasis 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. Karena persyaratan ini, format record dibatasi ukurannya oleh aturan yang terkait dengan event logging systems. Karakter akan dibagi menjadi 4000 karakter dan potongan akan tersebar di sejumlah entri. Ini berarti bahwa satu peristiwa tunggal dapat menghasilkan banyak entri audit. Kolom sequence\_no disediakan untuk menunjukkan beberapa entri baris.

## Potential SQL Server Audit Issues

Ada sejumlah masalah untuk dipertimbangkan dengan audit SQL Server.

1. Setiap audit diidentifikasi oleh GUID. Ketika database di restore atau 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 sampai situasinya diperbaiki dengan menjalankan perintah CREATE SERVER AUDIT untuk menetapkan GUID 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 penulisan audit harus dipertimbangkan. Jika ruang disk terisi, SQL Server mungkin tidak mulai. Jika demikian, anda mungkin perlu memaksa entri ke dalamnya melalui satu user startup dan -f parameter startup.

## Langkah-langkah praktikum

### Praktikum 1. DML Triggers

1. Buka **Microsoft SQL Server 2012**, klik **SQL Server Management Studio**. Connect ke **Server Window**, klik **Connect**.
2. Buat database baru **tempdb**
3. Buat product table di query tabel **Marketing.Product** di database **MarketDev**.

```
SELECT ProductID, ProductName, Color, Size
INTO dbo.Product
FROM MarketDev.MarketDev.Product;
GO
```

4. Tambah **primary key constraint** pada tabel.



```
ALTER TABLE dbo.Product
ADD CONSTRAINT PK_Product PRIMARY KEY (ProductID);
GO
```

5. Buat tabel **detail produk** untuk di audit.

```
CREATE TABLE dbo.ProductColorAudit
( ProductColorAuditID int IDENTITY(1,1) PRIMARY KEY,
  ProductID int NOT NULL,
  OldColor nvarchar(16) NULL,
  NewColor nvarchar(16) NULL,
  ChangedWhen datetime2 NOT NULL DEFAULT (SYSDATETIME()),
  ChangedBy sysname NOT NULL DEFAULT (SYSTEM_USER)
);
GO
```

6. Buat trigger untuk audit mengubah product colors.

```
CREATE TRIGGER TR_Product_Color_UPDATE
ON dbo.Product
FOR UPDATE
AS
BEGIN
    SET NOCOUNT ON;

    IF UPDATE(Color) BEGIN
        INSERT dbo.ProductColorAudit (ProductID, OldColor, NewColor)
        SELECT i.ProductID, d.Color, i.Color
        FROM inserted AS i
        INNER JOIN deleted AS d
        ON i.ProductID = d.ProductID;
    END;
END;
GO
```

7. Update product colors.

```
UPDATE dbo.Product
SET Color = 'None' WHERE Color IS NULL;
GO
```

8. Cek audit tabel

```
SELECT * FROM dbo.ProductColorAudit ORDER BY ProductColorAuditID;
GO
```

9. Update color.

```
UPDATE dbo.Product
SET Color = 'Mixed' WHERE Color = N'Multi';
GO
```

10. Cek audit tabel

```
SELECT * FROM dbo.ProductColorAudit ORDER BY ProductColorAuditID;
GO
```

## Praktikum 2. Penggunaan SQL Server Audit

1. Ikuti langkah 1-2 praktikum 1.
2. Buat database baru **master**.
3. Buat **SQL Server Audit** dan definisikan target ke **Windows application Log**

```

CREATE SERVER AUDIT MarketDevLog
  TO APPLICATION_LOG
  WITH ( QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE);
GO

```

4. Pindah ke database **MarketDev**

5. Buat database **audit specification** dengan **SELECT** pada marketing schema.

```

CREATE DATABASE AUDIT SPECIFICATION MarketingSelectSpec
  FOR SERVER AUDIT MarketDevLog
  ADD (SELECT ON SCHEMA::Marketing BY public);
GO

```

6. Tampilkan query **sys.server\_audits system view**, lalu perhatikan kolom **is\_state\_enabled**.

```

SELECT * FROM sys.server_audits;
GO

```

7. Kembali ke database **master**

8. Aktifkan server audit.

```

ALTER SERVER AUDIT MarketDevLog WITH (STATE = ON);
GO

```

9. Pindah ke database **MarketDev**

10. Aktifkan **MarketingSelectSpec audit specification**.

```

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

```

11. Query **sys.database\_audit\_specifications** dan **sys.database\_audit\_specification\_details system views**.

```

SELECT * FROM sys.server_audits;
SELECT * FROM sys.database_audit_specifications;
SELECT * FROM sys.database_audit_specification_details;
GO

```

12. Generate audit event dengan query tabel di marketing schema. Jalankan juga query yang tidak di audit.

```

SELECT * FROM Marketing.PostalCode;
GO
SELECT * FROM DirectMarketing.City;
GO

```

13. Periksa isi **Application log** dengan cara klik **my Computer**, lalu klik manage. Kemudian Klik **diagnostics, event viewer**, dan **Windows Logs** lalu klik **Application**. Klik pada setiap event pada panel diatas. Klik tab detail di panel bawah dan review isinya. Kemudian tutup **server management window**.

14. Pindah ke database **master**.

15. Matikan server audit

```

ALTER SERVER AUDIT MarketDevLog WITH (STATE = OFF);
GO

```

16. Pindah ke database **MarketDev**.

17. Matikan **MarketingSelectSpec audit specification**.

```

ALTER DATABASE AUDIT SPECIFICATION MarketingSelectSpec
  WITH (STATE = OFF);
GO

```

### Praktikum 3.Melihat hasil dari File-based Audit

1. Ikuti langkah 1-2 praktikum 1.
2. Buat database baru **master**.
3. Buka **windows Explorer** dan buat folder baru **L:\SQLAudit\AuditLog**
4. Buat **SQL Server Audit** dan definisikan tujuan ke folder yang dibuat.

```
CREATE SERVER AUDIT MarketDevLogToFile  
    TO FILE (FILEPATH = 'L:\SQLAudit\AuditLog');  
GO
```

5. Aktifkan server audit

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

6. Pindah ke database **MarketDev**
7. Buat database audit specification dengan **SELECT** activity di DirectMarketing schema

```
CREATE DATABASE AUDIT SPECIFICATION DirectMarketingSelectSpec  
    FOR SERVER AUDIT MarketDevLogToFile  
    ADD (SELECT ON SCHEMA::DirectMarketing BY public);  
GO
```

8. Aktifkan **DirectMarketingSelectSpec** audit specification

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

9. Generate audit event dengan query tabel di **DirectMarketing** schema. Jalankan juga query yang tidak di audit.

```
SELECT * FROM DirectMarketing.City;  
GO  
SELECT * FROM Marketing.PostalCode;  
GO
```

10. Query content audit file

```
SELECT * FROM  
    sys.fn_get_audit_file('L:\SQLAudit\AuditLog\*',  
        NULL,NULL);  
GO
```

11. Pindah ke database **master**
12. Matikan server audit

```
ALTER SERVER AUDIT MarketDevLogToFile WITH (STATE = OFF);  
GO
```

13. Rubah ke database **MarketDev**

14. Matikan **MarketingSelectSpec** audit specification

```
ALTER DATABASE AUDIT SPECIFICATION DirectMarketingSelectSpec  
    WITH (STATE = OFF);  
GO
```

*-- Selamat Mengerjakan --*