






CREATE SERVER AUDIT (Transact-SQL)

DIESES THEMA GILT FÜR:  SQL Server (ab 2008)  Azure SQL-Datenbank  Azure SQL Data Warehouse  Parallel Data Warehouse

Erstellt mit SQL Server-Überwachung ein Serverüberwachungsobjekt. Weitere Informationen finden Sie unter SQL Server Audit (Datenbankmodul) (<https://msdn.microsoft.com/de-at/library/cc280386.aspx>).

 Transact-SQL-Syntaxkonventionen (<https://msdn.microsoft.com/de-at/library/ms177563.aspx>)

Syntax

```
CREATE SERVER AUDIT audit_name
{
    TO { [ FILE (<file_options> [ , ...n ] ) ] | APPLICATION_LOG | SECURITY_LOG }
    [ WITH ( <audit_options> [ , ...n ] ) ]
    [ WHERE <predicate_expression> ]
}
[ ; ]

<file_options>::=
{
    FILEPATH = 'os_file_path'
    [ , MAXSIZE = { max_size { MB | GB | TB } | UNLIMITED } ]
    [ , { MAX_ROLLOVER_FILES = { integer | UNLIMITED } } | { MAX_FILES = integer } ]

    [ , RESERVE_DISK_SPACE = { ON | OFF } ]
}

<audit_options>::=
{
    [ QUEUE_DELAY = integer ]
    [ , ON_FAILURE = { CONTINUE | SHUTDOWN | FAIL_OPERATION } ]
    [ , AUDIT_GUID = uniqueidentifier ]
}

<predicate_expression>::=
{
    [NOT ] <predicate_factor>
    [ { AND | OR } [NOT ] { <predicate_factor> } ]
    [ , ...n ]
}

<predicate_factor>::=
event_field_name { = | < > | ! = | > | > = | < | < = } { number | ' string ' }
```

Argumente

TO { DATEI | ANWENDUNGSPROTOKOLL | SICHERHEITSPROTOKOLL }

Legt den Speicherort des Überwachungsziels fest. Die Optionen sind eine Binärdatei, das Windows-Anwendungsprotokoll oder das Windows-Sicherheitsprotokoll an. SQL Server kann nicht in das Windows-Sicherheitsprotokoll schreiben, ohne Konfigurieren zusätzlicher Einstellungen in Windows. Weitere Informationen finden Sie unter Schreiben von SQL-Serverüberwachungsereignissen in das Sicherheitsprotokoll (<https://msdn.microsoft.com/de-at/library/cc645889.aspx>).

FILEPATH = "Os_file_path"

Der Pfad des Überwachungsprotokolls. Der Dateiname wird auf der Grundlage des Überwachungsnamens und des Überwachungs-GUID generiert.

MAXSIZE = { Max_size }

Gibt die maximale Größe an, die die Überwachungsdatei annehmen kann. Die *Max_size* Wert muss eine ganze Zahl, gefolgt von MB, GB, TB oder UNLIMITED sein. Die minimale Größe, die Sie angeben können *Max_size* ist 2 MB und der Höchstwert beträgt 2.147.483.647 TB. Wird UNLIMITED angegeben, kann die Größe der Datei so lange zunehmen, bis auf dem Datenträger kein Speicherplatz mehr verfügbar ist. (0 steht ebenfalls für UNLIMITED.) Die Angabe eines Werts kleiner als 2 MB löst den Fehler MSG_MAXSIZE_TOO_SMALL aus. Der Standardwert ist UNLIMITED.

MAX_ROLLOVER_FILES = {Ganzzahl | UNBEGRENZTE}

Gibt die maximale Anzahl der Dateien an, die im Dateisystem zusätzlich zur aktuellen Datei beibehalten werden. Die *MAX_ROLLOVER_FILES* Wert muss eine ganze Zahl oder UNLIMITED sein. Der Standardwert ist UNLIMITED. Dieser Parameter wird ausgewertet, sobald die Überwachung neu gestartet wird (der möglich, wenn der Instanz von der Datenbankmodul neu gestartet wird oder wenn die Überwachung aktiviert ist deaktiviert, und klicken Sie dann auf erneut) oder wenn eine neue Datei benötigt wird, da MAXSIZE erreicht wurde. Wenn *MAX_ROLLOVER_FILES* ausgewertet wird, wenn die Anzahl der Dateien überschreitet das *MAX_ROLLOVER_FILES* festlegen, wird die älteste Datei gelöscht. Daher, wenn die Einstellung der *MAX_ROLLOVER_FILES* ist 0, die eine neue Datei jedes Mal erstellt die *MAX_ROLLOVER_FILES* -Einstellung ausgewertet wird. Nur eine Datei wird automatisch gelöscht, sobald *MAX_ROLLOVER_FILES* -Einstellung ausgewertet wird daher der Wert der *MAX_ROLLOVER_FILES* wird verringert, die Anzahl der Dateien nicht möglich ist, es sei denn, alte Dateien manuell gelöscht werden. Der Maximalwert für die Anzahl der Dateien beträgt 2.147.483.647.

MAX_FILES = ganze Zahl

Gilt für: SQL Server 2012 bis SQL Server 2016.

Gibt die maximale Anzahl von Überwachungsdateien an, die erstellt werden können. Führt kein Rollover zur ersten Datei aus, wenn die Grenze erreicht wird. Wenn die MAX_FILES-Grenze erreicht wird, schlägt jede Aktion, die zusätzliche Überwachungsereignisse nach sich zieht, fehl.

RESERVE_DISK_SPACE = { ON | OFF }

Diese Option ordnet der Datei auf dem Datenträger den MAXSIZE-Wert zu. Sie gilt nur, wenn MAXSIZE nicht gleich UNLIMITED ist. Der Standardwert ist OFF.

QUEUE_DELAY = ganze Zahl

Bestimmt die Zeit in Millisekunden, die verstreichen kann, bevor die Verarbeitung von Überwachungsaktionen erzwungen werden. Der Wert 0 steht für eine synchrone Übermittlung. Der minimale festlegbare Abfrageverzögerungswert ist 1000 (1 Sekunde), was auch der Standardwert ist. Der maximale Wert beträgt 2.147.483.647 (2.147.483,647 Sekunden oder 24 Tage, 20 Stunden, 31 Minuten und 23,647 Sekunden). Die Angabe eines ungültigen Werts löst den Fehler MSG_INVALID_QUEUE_DELAY aus.

ON_FAILURE = {WEITERHIN | HERUNTERFAHREN | FAIL_OPERATION}

Gibt an, ob die an das Ziel ausgebende Instanz SQL Server fehlschlagen lassen, fortsetzen oder beenden soll, wenn das Ziel keine Daten in das Überwachungsprotokoll schreiben kann. Der Standardwert ist CONTINUE.

CONTINUE

SQL Server-Vorgänge werden fortgesetzt. Überwachungsdatensätze werden nicht beibehalten. Die Überwachung versucht weiterhin, Ereignisse zu protokollieren und wird fortgesetzt, wenn die Fehlerbedingung aufgelöst wurde. Durch Auswählen der continue-Option können unter Umständen unüberwachte Aktivitäten ausgeführt werden, die gegen Ihre Sicherheitsrichtlinien verstoßen. Verwenden Sie diese Option, wenn die weitere Verwendung von Datenbankmodul wichtiger als die Beibehaltung einer vollständigen Überwachung ist.

SHUTDOWN

Erzwingt, dass ein Server heruntergefahren wird, wenn die Serverinstanz, die in das Ziel schreiben soll, keine Daten in das Überwachungsziel schreiben kann. Die Anmeldung, die dies ausgibt, muss über die **SHUTDOWN** -Berechtigung verfügen. Wenn die Anmeldung nicht über diese Berechtigung verfügt, schlägt diese Funktion fehl, und es wird eine Fehlermeldung ausgegeben. Es treten keine überwachten Ereignisse auf. Verwenden Sie die Option, wenn ein Überwachungsfehler die Sicherheit oder die Integrität des Systems beeinträchtigen konnte.

FAIL_OPERATION

Datenbankaktionen schlagen fehl, wenn sie überwachte Ereignisse verursachen. Aktionen, die keine überwachten Ereignisse verursachen, können fortgesetzt werden, aber es können keine überwachten Ereignisse auftreten. Die Überwachung versucht weiterhin, Ereignisse zu protokollieren und wird fortgesetzt, wenn die Fehlerbedingung aufgelöst wurde. Verwenden Sie diese Option, wenn die Beibehaltung einer vollständigen Überwachung wichtiger als der Vollzugriff auf Datenbankmodul ist.

AUDIT_GUID = "uniqueidentifier"

Um Szenarien, wie beispielsweise Datenbankspiegelung unterstützen zu können, benötigt eine Überwachung einen bestimmten GUID, der dem GUID in der gespiegelten Datenbank entspricht. Der GUID kann, nachdem die Überwachung erstellt wurde, nicht mehr geändert werden.

predicate_expression

Gilt für: SQL Server 2012 bis SQL Server 2016.

Gibt den Prädikatausdruck an, mit dessen Hilfe bestimmt wird, ob ein Ereignis verarbeitet werden muss. Die Länge von Prädikatausdrücken ist auf 3000 Zeichen beschränkt, wodurch die Länge von Zeichenfolgenargumenten eingeschränkt wird.

event_field_name

Gilt für: SQL Server 2012 bis SQL Server 2016.

Ist der Name des Ereignisfelds, das die Prädikatquelle identifiziert. Überwachungsfelder werden in beschrieben Sys. fn_get_audit_file (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280765.aspx>). Mit Ausnahme von file_name und audit_file_offset können alle Felder überwacht werden.

number

Gilt für: SQL Server 2012 bis SQL Server 2016.

Alle numerischen Typen umfassen **decimal**. Einschränkungen stellen der verfügbare physische Speicher oder eine Zahl dar, die zu groß ist, um als 64-Bit-Ganzzahl dargestellt werden zu können.

' string '

Gilt für: SQL Server 2012 bis SQL Server 2016.

Entweder eine ANSI- oder Unicode-Zeichenfolge, die vom Prädikatvergleich verlangt wird. Für die Prädikatvergleichsfunktionen wird keine implizite Zeichenfolgentypkonvertierung ausgeführt. Die Übergabe des falschen Typs führt zu einem Fehler.

REMARKS

Wenn eine Serverüberwachung erstellt wird, befindet sie sich im deaktivierten Zustand.

Die CREATE SERVER AUDIT-Anweisung liegt im Bereich einer Transaktion. Wird ein Rollback für die Transaktion ausgeführt, so wird auch für die Anweisung ein Rollback durchgeführt.

Berechtigungen

Um eine Serverüberwachung zu erstellen, zu ändern oder zu löschen, benötigen Prinzipale die ALTER ANY SERVER AUDIT-Berechtigung oder die CONTROL SERVER-Berechtigung.

Schränken Sie beim Speichern von Überwachungsinformationen in einer Datei den Zugriff auf deren Speicherort ein, um eine Manipulation zu verhindern.

Beispiele

A. Erstellen einer Serverüberwachung mit einem Dateiziel

Im folgenden Beispiel wird eine Serverüberwachung namens HIPAA_Audit mit einer Binärdatei als Ziel und ohne weitere Optionen erstellt.

```
CREATE SERVER AUDIT HIPAA_Audit  
TO FILE ( FILEPATH = '\\SQLPROD_1\Audit\' );
```

B. Erstellen einer Serverüberwachung mit einem Windows-Anwendungsprotokollziel und Optionen

Im folgenden Beispiel wird eine Serverüberwachung namens HIPAA_Audit mit dem Windows-Ereignisprotokoll als Ziel erstellt. Die Warteschlange wird jede Sekunde geschrieben und fährt bei einem Fehler das SQL Server-Modul herunter.

```
CREATE SERVER AUDIT HIPAA_Audit  
TO APPLICATION_LOG  
WITH ( QUEUE_DELAY = 1000, ON_FAILURE = SHUTDOWN);
```

C. Erstellen einer Serverüberwachung, die eine WHERE-Klausel enthält

Im folgenden Beispiel werden eine Datenbank, ein Schema und zwei Tabellen für das Beispiel erstellt. Die Tabelle mit dem Namen `DataSchema.SensitiveData` enthält vertrauliche Daten, und der Zugriff auf die Tabelle muss in der Überwachung aufgezeichnet werden. Die Tabelle `DataSchema.GeneralData` beinhaltet keine vertraulichen Daten. Die Datenbank-Überwachungsspezifikation überwacht den Zugriff auf alle Objekte im `DataSchema` -Schema. Die Serverüberwachung wird mit einer WHERE-Klausel erstellt, die die Serverüberwachung ausschließlich auf die `SensitiveData` -Tabelle beschränkt. Die serverüberwachung wird vorausgesetzt, ein Audit-Ordner vorhanden ist, am `C:\SQLAudit` .

Transact-SQL

```
CREATE DATABASE TestDB;
GO
USE TestDB;
GO
CREATE SCHEMA DataSchema;
GO
CREATE TABLE DataSchema.GeneralData (ID int PRIMARY KEY, DataField varchar(50) NOT NULL);
GO
CREATE TABLE DataSchema.SensitiveData (ID int PRIMARY KEY, DataField varchar(50) NOT NULL);
GO
-- Create the server audit in the master database
USE master;
GO
CREATE SERVER AUDIT AuditDataAccess
    TO FILE ( FILEPATH = 'C:\SQLAudit\' )
    WHERE object_name = 'SensitiveData' ;
GO
ALTER SERVER AUDIT AuditDataAccess WITH (STATE = ON);
GO
-- Create the database audit specification in the TestDB database
USE TestDB;
GO
CREATE DATABASE AUDIT SPECIFICATION [FilterForSensitiveData]
FOR SERVER AUDIT [AuditDataAccess]
ADD (SELECT ON SCHEMA::[DataSchema] BY [public])
WITH (STATE = ON);
GO
-- Trigger the audit event by selecting from tables
SELECT ID, DataField FROM DataSchema.GeneralData;
SELECT ID, DataField FROM DataSchema.SensitiveData;
GO
-- Check the audit for the filtered content
SELECT * FROM fn_get_audit_file('C:\SQLAudit\AuditDataAccess_*.sqlaudit',default,default);
GO
```

Siehe auch

ALTER SERVER AUDIT (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280563.aspx>)

DROP SERVER AUDIT (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280899.aspx>)

Erstellen der SERVERÜBERWACHUNGSSPEZIFIKATION (Transact-SQL) (<https://msdn.microsoft.com/de->

[at/library/cc280767.aspx](https://msdn.microsoft.com/de-at/library/cc280767.aspx))

ALTER SERVER AUDIT SPECIFICATION (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280682.aspx>)

DROP SERVER AUDIT SPECIFICATION (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280603.aspx>)

Erstellen von Datenbank-ÜBERWACHUNGSSPEZIFIKATION (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280404.aspx>)

ALTER DATABASE AUDIT SPECIFICATION (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280645.aspx>)

DROP DATABASE AUDIT SPECIFICATION (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280479.aspx>)

ALTER AUTHORIZATION (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/ms187359.aspx>)

Sys. fn_get_audit_file (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280765.aspx>)

Sys. server_audits (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280727.aspx>)

Sys. server_file_audits (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280544.aspx>)

server_audit_specifications (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280898.aspx>)

server_audit_specification_details (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280606.aspx>)

database_audit_specifications (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280726.aspx>)

database_audit_specification_details (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280403.aspx>)

dm_server_audit_status (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280524.aspx>)

dm_audit_actions (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280725.aspx>)

dm_audit_class_type_map (Transact-SQL) (<https://msdn.microsoft.com/de-at/library/cc280820.aspx>)

Erstellen einer Serverüberwachung und einer Serverüberwachungsspezifikation (<https://msdn.microsoft.com/de-at/library/cc280525.aspx>)

Community-Beiträge (<https://msdn.microsoft.com/de-at/library/community/add/cc280448.aspx>)
