Audit serveru MS SQL

Má-li být SQL server auditován prostřednictvím LOGmanageru, je nutné auditování na straně SQL serveru nastavit buď pomocí SQL Server Management Studio nebo pomocí transact SQL.

Funkce auditování SQL Serveru zahrnuje tři hlavní součásti:

- Audit serveru (Server Audit)
- Specifikace auditu serveru (Server Audit Specification)
- Specifikace databázového auditu (Database Audit Specification)

Audit serveru určuje, jakým způsobem a kam budou události zapisovány. Audit serveru musí být nakonfigurován v každém případě.

Dále je potřeba nakonfigurovat Specifikaci auditu serveru nebo Specifikaci databázového auditu nebo obě specifikace.

Specifikace auditu serveru bude zapisovat obecné události serveru a obecnější události ze všech databází, např. vypnutí serveru nebo přihlášení uživatelů.

Specifikace databázového auditu bude zapisovat události spojené s konkrétní databází a je zde možnost podrobnější definice auditovaných akcí, např. audit příkazů INSERT, DELETE atd.

V případě menších databázových prostředí bude pravděpodobně stačit definovat Specifikaci auditu serveru. Naopak v případě větších prostředí je možné definovat audit pouze konkrétních akcí a na důležitých databázích, čímž se ušetří systémové prostředky.

Podrobnější informace jsou dostupné na: https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-databaseengine?view=sql-server-ver15

Audit serveru (Server Audit)

Audit serveru je nadřazenou součástí auditu SQL Serveru a může obsahovat specifikace auditu serveru a/nebo specifikace auditu databáze.

Audit serveru lze vytvořit buď pomocí SQL Server Management Studio nebo pomocí transact SQL.

Při konfiguraci pomocí SQL Server Management Studio je Audit serveru umístěn v hlavní databázi. Používá se k definování cíle, kde budou informace o auditu uloženy. Nový audit serveru je možné vytvořit kliknutím pravým tlačítkem myši na složku Security/Audits a volbou New Audit.



V konfiguraci auditu serveru je třeba nastavit název auditu (Audit name) např. Audit-LOGM a přepnout cíl auditu (Audit destination) na Application Log.

Události z Application Log jsou automaticky odesílány na LOGmanager pomocí Windows Event Sender agenta (WES) nebo Beats agenta.

🔀 Create Audit		_						
🕕 Ready								
Select a page & General & Filter	🗊 Script 👻 😯 Help							
	Audit name:	Audit-LOGM						
	Queue delay (in milliseconds):	1000	-					
	On Audit Log Failure:	Continue Eail operation						
		Shut down server						
	Audit destination:	Application Log	~					
	Path:							
	Audit File Maximum Limit:	 Maximum rollover files: Unlimited 						
Connection		O Maximum files:						
q₩ SQL2017 [LAB∖vlastofka]	Maximum file size:	Number of files: 2147483647	►					
View connection properties	Reserve disk	Space						
Progress								
Ready								
		OK Cancel	Help					

Nový audit serveru je ve výchozím nastavení vypnutý a je třeba ho zapnout kliknutím pravým tlačítkem myši a volbou Enable Audit.

🖃 📕 Audits	
Server A	New Audit Enable Audit
Beh/Base	View Audit Logs
Always On I	Script Audit as
⊞ Manageme ⊡ Integration □	Policies Facets
 	Start PowerShell

Audit je také možné nastavit a zároveň i zapnout pomocí transact SQL:

USE [master] GO CREATE SERVER AUDIT [Audit-LOGM] TO APPLICATION_LOG WITH (QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE) ALTER SERVER AUDIT [Audit-LOGM] WITH (STATE = ON) GO

Specifikace auditu serveru (Server Audit Specification)

Při konfiguraci pomocí SQL Server Management Studio je Specifikace auditu serveru umístěna v hlavní databázi. Používá se k definování toho, co je třeba auditovat na úrovni serveru.

Novou specifikaci auditu serveru je možné vytvořit kliknutím pravým tlačítkem myši na složku Security/Server Audit Specifications a volbou New Server Audit Specification...



V konfiguraci Specifikace auditu serveru je třeba nastavit název nové specifikace, např. ServerAuditSpec-LOGM a vybrat název Auditu serveru, který byl nakonfigurován v předchozím kroku.

Dále je třeba vybrat typy auditních akcí (Actions), které by měly být auditovány. Seznam nastavených akcí se bude lišit podle konkrétních potřeb uživatele. Zde je k dispozici úplný seznam možností:

https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-action-groups-andactions?view=sql-server-ver15

💀 Server Audit Specification Properties							×
🕕 Ready							
Select a page	🗊 Script 👻 😮 Help						
	Name:						
	Audit:		Audit-LOGM	~			
	Actions						
			Audit Action Type		Object	^	
Connection	▶ 01	BACKUP_RES	TORE_GROUP	~		~	
y ₩ SQL2017 [LAB∖vlastofka]	02	AUDIT_CHAN	GE_GROUP	~		~	
	03	DBCC_GROUP	2	~		~	
	04	SERVER_OBJ	ECT_PERMISSION_CHANGE_GROUP	~		~	
View connection properties	05	SERVER_PER	MISSION_CHANGE_GROUP	~		~	-
Programe	06	DATABASE_P	RINCIPAL_IMPERSONATION_GROUP	~		~	-
Produ	07	SERVER_PRI		~			
Ready	< ^^	EALER LOOP			>	*	
			ОК	Can	cel	Help	

Doporučené auditní akce:

SUCCESSFUL_LOGIN_GROUP - Uživatel se úspěšně přihlásil k SQL Serveru FAILED_LOGIN_GROUP - Neúspěšný pokus o přihlášení k SQL Serveru LOGOUT_GROUP - Uživatel se odhlásil z SQL Serveru AUDIT_CHANGE_GROUP - Audit vytvoření, úpravy nebo odstranění specifikace auditu BACKUP_RESTORE_GROUP - Audit zálohovaní nebo obnovení ze zálohy DBCC_GROUP - Audit příkazů DBCC (Microsoft SQL Server Database Console Commands) SERVER_OPERATION_GROUP - Audit změn zabezpečení (např. externí přístupy nebo autorizace) SERVER_STATE_CHANGE_GROUP - Audit změn stavu SQL serveru (spuštění nebo zastavení) SERVER_PRINCIPAL_IMPERSONATION_GROUP - Audit zosobnění pověření v rámci serveru DATABASE_PRINCIPAL_IMPERSONATION_GROUP - Audit zosobnění v rámci databáze SERVER_PERMISSION_CHANGE_GROUP - Audit změn oprávnění GRANT, REVOKE nebo DENY v rámci serveru

Nová Specifikace auditu serveru je ve výchozím nastavení vypnutá a je třeba ji zapnout kliknutím pravým tlačítkem myši a volbou Enable Server Audit Specification...



Specifikaci auditu serveru je také možné nastavit a zároveň i zapnout pomocí transact SQL:

```
USE [master]

GO

CREATE SERVER AUDIT SPECIFICATION [ServerAuditSpec-LOGM]

FOR SERVER AUDIT [Audit-LOGM]

ADD (BACKUP_RESTORE_GROUP),

ADD (AUDIT_CHANGE_GROUP),

ADD (DBCC_GROUP),

ADD (DBCC_GROUP),

ADD (SERVER_PERMISSION_CHANGE_GROUP),

ADD (DATABASE_PRINCIPAL_IMPERSONATION_GROUP),

ADD (SERVER_PRINCIPAL_IMPERSONATION_GROUP),

ADD (FAILED_LOGIN_GROUP),

ADD (SUCCESSFUL_LOGIN_GROUP),
```

```
ADD (LOGOUT_GROUP),
ADD (SERVER_OPERATION_GROUP),
ADD (SERVER_STATE_CHANGE_GROUP)
WITH (STATE = ON)
GO
```

Specifikace databázového auditu (Database Audit Specification)

Specifikace databázového auditu kontroluje události na úrovni databáze a konfiguruje se podobně jako Specifikace auditu serveru.

Hlavní rozdíl je v tom, že Specifikaci databázového auditu je potřeba konfigurovat pro každou databázi samostatně kliknutím pravým tlačítkem myši na složku NazevDB/Security/Database Audit Specifications a volbou New Database Audit Specification...



V konfiguraci Specifikace databázového auditu je třeba nastavit název nové specifikace, např. DBAuditSpec-LOGM a vybrat název Auditu serveru, který byl nakonfigurován v prvním kroku (Audit-LOGM).

Dále je třeba vybrat typy auditních akcí (Actions), které by měly být auditovány.

Seznam nastavených akcí se bude lišit podle konkrétních potřeb uživatele. Zde je k dispozici úplný seznam možností:

 $\label{eq:https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15$

V případě Specifikace databázového auditu není doporučené nastavení, protože každé prostředí bude vyžadovat audit jiných akcí.

🔉 Database Audit Specification Pr	operties									- 0	×
🕦 Ready											
Select a page	Script	t 👻 🕜 Help									
	Name	e: DBAuditSpec-LOGM									
	Audit	Audit: Audit-LOGM									~
	Action	Actions:									
			Audit Action Type			Object Class Object Schen		Object Name		Principal Name	
Connection	▶1	DELETE		· · · · · · · · · · · · · · · · · · ·		DATABASE 🗸 🗸		TestDB		testuser	
q ₩ SQL2017 [LAB∖vlastofka]	*2				/	~					
View connection properties											
Progress											
Ready											
								OK	С	ancel He	lp

Nová Specifikace databázového auditu je ve výchozím nastavení vypnutá a je třeba ji zapnout kliknutím pravým tlačítkem myši a volbou Enable Database Audit Specification...



Specifikace databázového auditu je také možné nastavit a zároveň i zapnout pomocí transact SQL:

```
USE [TestDB]
GO
CREATE DATABASE AUDIT SPECIFICATION [DBAuditSpec-LOGM]
FOR SERVER AUDIT [Audit-LOGM]
ADD (DELETE ON DATABASE::[TestDB] BY [testuser])
WITH (STATE = ON)
GO
```