بسم الله الرحمن الرحیم

آموزشگاه تحلیل داده

تخصصی ترین مرکز برنامه نویسی و دیتابیس در ایران

آموزش رهگیری در SQL Server

مدرس : مهندس افشین رفوآ

رمز فایل :tahlildadeh.com

SQL server، ویژگی هایی را در اختیار می گذارد که می توانید برای رهگیری (auditing) فعالیت ها و تغییراتی که روی سیستم روی می دهد استفاده کنید.

این مقاله لینک هایی را در اختیار شما می گذارد که بشما کمک می کنند اطلاعاتی را که برای رهگیری در موتور بانک اطلاعاتی SQL Server نیاز دارید، پیدا کنید.

مقدمه ای بر رهگیری SQL Server

رهگیری نمونه ای از SQL Server یا بانک اطلاعاتیSQL Server ، مستلزم trackingو logging کردن رویدادهایی است که در سیستم روی می دهند. می توانید از چندین متد رهگیری برای SQL Server استفاده کنید. هنگام شروع کار با ۲۰۰۸Enterprise SQL Server ، می توانید رهگیری اتوماتیک را با استفاده ازSQL Server Auditتنظیم کنید.

رهگیری در SQL Server چندین سطح (level) دارد، بستگی به مقررات و استانداردهای لازم نصب دارد SQL . Server Audit، ابزارها و فرآیندهایی را در اختیار می گذارد که باید برای فعال کردن، ذخیره، مشاهدهaudit ها در سرورهای مختلف و اشیاء بانک اطلاعاتی در اختیار داشته باشید.

می توانید گروه های server audit action برای هر نمونه، و چه گروه های database audit action، یا database audit actionsبرای هر بانک اطلاعاتی را رکورد کنید. رویدادaudit ، هر بار که اقدامی قابل رهگیری انجام می شود، روی می دهد.

اجزای SQL Server Audit

audit، ترکیبی از چند عنصر درون بسته ای واحد برای گروهی از اکشن های سرور یا بانک اطلاعاتی است. اجزای SQL Server Audit، برای ایجاد خروج ای که auditنامیده می شود، ترکیب می شوند، درست مثل تعریف گزارش ترکیب شده با گرفیک ها عنصرهای داده که گزارشی را ایجاد می کند.

SQL Server Auditاز Extended Events برای کمک به ایجاد audit استفاده می کنند.

SQL Server Audit

شیSQL Server Audit ، نمونه ای واحد از سرور یا اکشن های در سطح بانک اطلاعاتی و گروهای اکشن ها را جمع آوری می کند تا مانیتور کند audit . در سطح نمونه SQL Server است. می توانید برای هر نمونه SQL Serverچندین audit داشته باشید.

وقتی یک audit تعریف می کنید، در واقع موقعیت خروجی نتایج را تعیین می کنید. این، مقصد audit نامیده می شود audit . در حالت *disabled* ایجاد می شود، و بطور اتوماتیک هیچ اکشنی را رهگیری نمی کند. بعد از اینکه auditفعال می شود، مقصد اودیت (audit destination) داده ها را از audit دریافت می کند.

Server Audit Specification

شیServer Audit Specification ، متعلق به audit است. می توانید برای هر audit، یک server auditspecificationایجاد کنید، زیرا هر دو در اسکوپ نمونه SQL Server ایجاد می شوند.

server audit specification، گروه های اکشن در سطح سرور زیادی را جمع آوری می کند. می توانید گروه های اکشن را در server audit specification شامل کنید. گروه هایAudit action ، گروه هایی از پیش تعریف شده اند که رویدادهایی اتمی (atomic events) هستند که در Database Engineاتفاق می افتند. این اکشن ها به audit ارسال می شوند، که آنها را در target رکورد می کند.

Database Audit Specification

شی Database Audit Specification نیز متعلق به SQL Server audit است. می توانید یک database audit specificationبرای هر SQL Server database برای هر audit ایجاد کنید.

Database Audit Specification، اکشن های audit در سطح بانک اطلاعاتی را جمع آوری می کند. می توانید یا گروه های audit action یا رویدادهای audit را به database audit specification اضافه کنید. رویدادهایAudit ، اکشن هایی اتمی هستند که می توان توسط موتور SQL Server رهگیری کرد. گروه های اکشنaudit ، گروهی از اکشن های از پیش تعریف شده هستند. هردو در اسکوپ بانک اطلاعاتی SQL Server هستند. این اکشن ها به audit فرستاده می شوند، که آنها را روی target رکورد می کنند.

Target

نتایج audit به target ارسال می شوند، که می تواند یک فایل، logرویداد Windows Security، یا log رویداد Windows Application باشدlog . ها باید بطور دوره ای مرور و آرشیو شوند تا مطمئن شویم کهtarget ، فضای کافی برای نوشتن رکوردهای اضافی دارد.

مهم

رویداد log . را بخواند یا روی آن بنویسد Windows Application رویداد log هر کاربر تایید شده ای می تواند Windows رویداد log نیاز دارد و از Windows Security رویداد logکمتری از permission به application Security کمتر امن است.

برای نوشتن رویlog Windows Security ، نیاز است که SQL Server service account به سیاست Generate security auditsاضافه شود. بطور پیش فرض، Local System، Local Service، وNetwork Serviceبخشی از سیاست هستند. این تنظیمات را می توان با استفاده از سیاست امنیتی snap-inیا (secpol.msc)پیکربندی کرد.

وقتی اطلاعات log را روی فایلی ذخیره می کنید، بر ای جلوگیری از دسترسی غیرمجاز به فایل، می توانید دسترسی به موقعیت فایل را به روش های زیر محدود کنید:

- SQL Server Service Accountباید پرمیشن Read و Write داشته باشد .
- مدیران audit معمولا به پرمیشن های بالا نیاز دارند. این بدین معناست که مدیرانaudit ، اکانت های ویندوز برای مدیریت فایل های audit می باشند، از قبیل: کپی کردن آنها بهshare های مختلف، گرفتن فایل backup از آنها، و غیره .
- Audit Readerهایی که مجاز به خواندن فایل های audit هستند، باید پرمیشن Read داشته باشند .

حتی موقع نوشتن روی فایل، اگر کاربران دیگر ویندوز هم پرمیشن Read را داشته باشند، می توانند فایل auditرا بخوانند. موتور بانک اطلاعاتی روی عملیات های خواندن قفل نمی گذارد.

از آنجاییکه موتور بانک اطلاعاتی به فایل دسترسی دارد، loginهای SQL Server که پرمیشن CONTROL SERVER دارند می توانند از موتور بانک اطلاعاتی برای دسترسی به فایل های audit استفاده کنند. برای رکورد کردن هر کاربری که فایل audit را می خواند، باید یک audit روی فایل master.sys.fn_get_audit_file تعریف کنید. این کار، loginها را با پرمیشن CONTROL SERVER که از طریق SQL Server به فایل audit دسترسی پیدا کرده اند، رکورد می کند.

اگر مدیرaudit ، فایلی را به جایی دیگر کپی کند، ACLها در جای جدید با به پرمیشن های زیر کاهش پیدا کنند:

- مدیر audit – Read و Write
- خواننده audit – Read

توصیه می شود گزارش های audit از نمونه ای مستقل ازSQL Server ، از قبیل نمونه ای از SQL Server Express، ایجاد کنیم. با استفاده از نمونه ای از موتور بانک اطلاعاتی برای گزارش گیری، می توانید کاربرها را از دسترسی غیرمجاز به رکورد audit باز دارید.

می توانید با رمزگذاری پوشه ای که فایل audit در آن ذخیره شده است، با استفاده از Windows BitLocker Drive Encryption یا Windows Encrypting File System سد محکمتری در مقابل دسترسی غیر مجاز ایجاد کنید.

مروری بر استفاده از SQL Server Audit

می توانید از SQL Server Management Studio یا Transact-SQL برای تعریف auditاستفاده کنید. بعد از اینکه audit ایجاد و فعال شد، تارگت، entryها را دریافت خواهد کرد.

می توانیدlog های رویداد ویندوز را با استفاده از یوتیلیتی Event Viewer در ویندوز، بخوانید. برای تارگت های فایل، می توانید یا از Log File Viewer در SQL Server Management Studioیا از تابع fn_get_audit_fileبرای خواندن فایل تارگت استفاده کنید.

فرآیند کلی ایجاد و استفاده از audit به شرح زیر است:

۱. یک audit ایجاد و تارگت را تعریف کنید .
۲. یک server audit specification یا database audit specification ایجاد کنید که به audit مپ شود audit specification . را فعال کنید .
۳. auditرا فعال کنید .
٤. رویدادها را با استفاده ازWindows Event Viewer ، Log File Viewer، یا تابع fn_get_audit_fileبخوانید .

ملاحظات

در صورت بروز مشکلی در شروع audit ، سرور شروع بکار نخواهد کرد. در این صورت، می توان سرور را با استفاده از آپشن f– در command line راه انداخت.

از آنجاییکه ON_FAILURE=SHUTDOWN برای audit تعیین شده است، وقتی مشکل ایجاد شده در audit باعث خاموش شدن یا عدم کارکردن سرور شود، رویداد MSG_AUDIT_FORCED_SHUTDOWN، در log نوشته می شود. از آنجاییکه خاموش شدن سرور هنگام اولین رویارویی با این تنظیم روی می دهد، این رویداد فقط یکبار نوشته می شود. این رویداد بعد از پیام مشکل audit که باعث خاموش شدن می شود، نوشته می شود. مدیر می تواند این خاموش شدن را با باز کردن SQL Server در مد Single User و با استفاده از m– flag رفع کند. اگر SQL Server در این مد باز شود، باید هر audit را که ON_FAILURE=SHUTDOWN در آن تعیین شده، downgrade کنید. وقتی SQL Server با استفاده از m– flag باز می شود، پیام MSG_AUDIT_SHUTDOWN_BYPASSED در error log نوشته می شود.

Database Mirroring و SQL Server Audit

بانک اطلاعاتی ای که دارای database audit specification تعریف شده ای می باشد، و از database mirroring استفاده می کند، database audit specification را شامل خواهد شد. برای درست کارکردن روی نمونه SQL منعکس شده (mirrored SQL instance) ، آیتم های زیر باید پیکر بندی شود:

- mirror server باید دارای یک audit با همان GUID باشد تا database audit specification را برای نوشتن رکوردهای audit فعال کند. این را می توان با استفاده از فرمان CREATE AUDIT WITH GUID= پیکربندی کرد .

- برای تارگت های فایل باینری، mirror server service account باید دارای پرمیشن های مناسب با جایی باشد که

audit trail در آنجا وشته می شود.

- در تارگت های log رویداد ویندوز، سیاست امنیت که mirror server در آن قرارگرفته، باید به service account اجازه دسترسی به log رویداد امنیت یا اپلیکیشن را بدهد .