SQL Server 安全审核

SQL Server 审核

SQL Server 审核是指你可以在数据库或服务器实例监控事件。审核日志包含你选择捕获的事件的列表，在服务器上生成数据库和服务器对象、主体和操作的活动记录。你几乎可以捕获任何发生的事情的数据，包括成功和不成功的登录，读、更新、删除的数据，管理任务，以及更多。审核可以深入到数据库和服务器。这似乎有点奇怪存在办法回头追溯那些已经发生的事件。但审核日志往往是你用于检测攻击的第一和最佳的资源，特别是当攻击只探测数据库，但尚未成功访问数据或损坏数据。当发生这样的攻击，监管人员对你施加压力，审核日志可能会帮助你找出发生了什么，什么数据被访问，以及攻击的来源。如果没有日志，在你可以确定发生了什么之前，你必须先捕捉到攻击者，然后再回复他们。

SQL Server 审核对象

无论你是使用 T-SQL 还是 SSMS 用户接口来管理审核，你会操作下面三个对象：

->服务器审核：服务器审核对象是审核的顶级容器，你将始终使用该对象进行审核。通常，你将创建一个服务器审核汇总一个或多个用于特定目的(比如 compliance 或特定一组服务器/数据库对象)的审核规范。在这个对象你可以配置审核的名称、审核日志保存路径、审核文件最大限制、审核日志失败时的操作。你还可以定义过滤来控制事件日志的写入。

->服务器审核规范：在这个对象你可以定义服务级别的事件以捕获写入审核日志。这个规范需要与你之前创建的服务器审核关联。就是在这里定义你想记录哪些对

象上的哪些事件。

->数据库审核规范：这个对象和服务器审核规范相似，你用它来捕获单独数据库上的事件。它也要关联到服务器审核。

通常你会使用一个服务器审核，依据你想要捕获事件的类型结合一种或两种其他对象。如果所有的事件都发生在一个数据库中，使用数据库审核规范对象。否则，如果事件跨越两个或多个数据库，或是服务器级别事件，则使用服务器审核规范对象。

当你创建一个服务器审核时，审核日志有三种存储位置：文件、安全日志、应用程序日志。你应该很小心的选择审核目标(审核日志存储位置)，因为它可以很容易的包含敏感信息，如社会保险号码、信用卡号、工资、企业财务数据等。因此，你应该使用未经授权的用户不能访问的位置。这意味着，应用程序日志可能不是一个好选择，因为默认情况下用户不需要提高权限就可以查看它。但安全日志可以是一个很好的选择，因为访问需要 admin 权限。文件也可以是一个很好的选择，因为你可以使用系统内置的安全特性保护文件夹或文件夹中的文件。

创建服务器审核

你可以使用 SSMS 图形界面或 T-SQL 语句创建审核。在 SSMS 下创建是非常容易的，我们即将这样操作。打开 SSMS 连接到本地数据库实例。对象资源管理器->安全性->审核，右击审核选择"新建审核"，打开创建审核对话框。

你可以使用对话框设置服务器审核的各种属性：

->审核名称根据日期和时间自动初始化成 Audit-20150908-143152 这种格式，当然你可以自行修改为任何你喜欢的。我设置成 Sample Audit 更好识别审核。

->下一步，你可以设置队列延迟(毫秒)，默认是设置为 1 秒，代表最大等待日志

写入的时间。这个值在性能和安全性之间折衷：一个较短的时间限制将使其更可能在灾难故障前记录到关键事件，但可能会影响服务器的性能。我让服务器审核保持默认设置，这意味着，在最坏的情况下，我可能会失去一秒的条目。作为示例审核这是可以接受的！

->下一步，设置在审核日志失败时的操作，当 SQL Server 不能写入一个审核日志条件时，比如没有可用磁盘空间。默认是继续，只是在 Windows 事件日志产生一个错误，审核继续执行。这是一个严酷的选择(关闭服务器)，审核是至关重要时它是必要的。操作失败选项是介于前面两个极端之间的某个地方，让失败的事务回滚。我还是将此项保持默认。

->剩余需要你选择的是审核目标。有三个选择：文件、安全日志、应用程序日志。如果你选择后面两个 Windows 事件日志，对话框中剩余选项就都会禁用，其他选项只适用于审核目标为文件。

如果你选择了文件选项，你就得选择一个路径。本例子中我选择的是 D:\SQL2012，一个可以随时清理以腾出空间的文件夹。你可以设置任何你喜欢的路径，不同的分区或者网络磁盘。

文件审核目标的其他选项让你设置文件大小和文件数量。你可以设置最大滚动更新文件数为一个最大值或者无限制。对于最大滚动更新文件数选项，一旦文件夹下的文件数达到最大值，SQL Server 会用新文件重写最旧的文件。对于最大文件数选项，一旦达到最大值，审核日志就会写入失败。如果你选择了关联的无限制选项，那么滚动更新文件数将不受限制。你同样可以设置最大文件大小或大小无限制。对话框中最后一个选项——保留磁盘空间，告诉 SQL Server 预分配等于你指定的最大文件大小的磁盘空间，如果有，只有当最大文件大小的无限制选

项没有选中时才适用。因此，你有足够的选项来控制你的审核文件在指定的驱动器上的空间量。

图 11.1 显示我创建名叫 Sample Audit 的审核

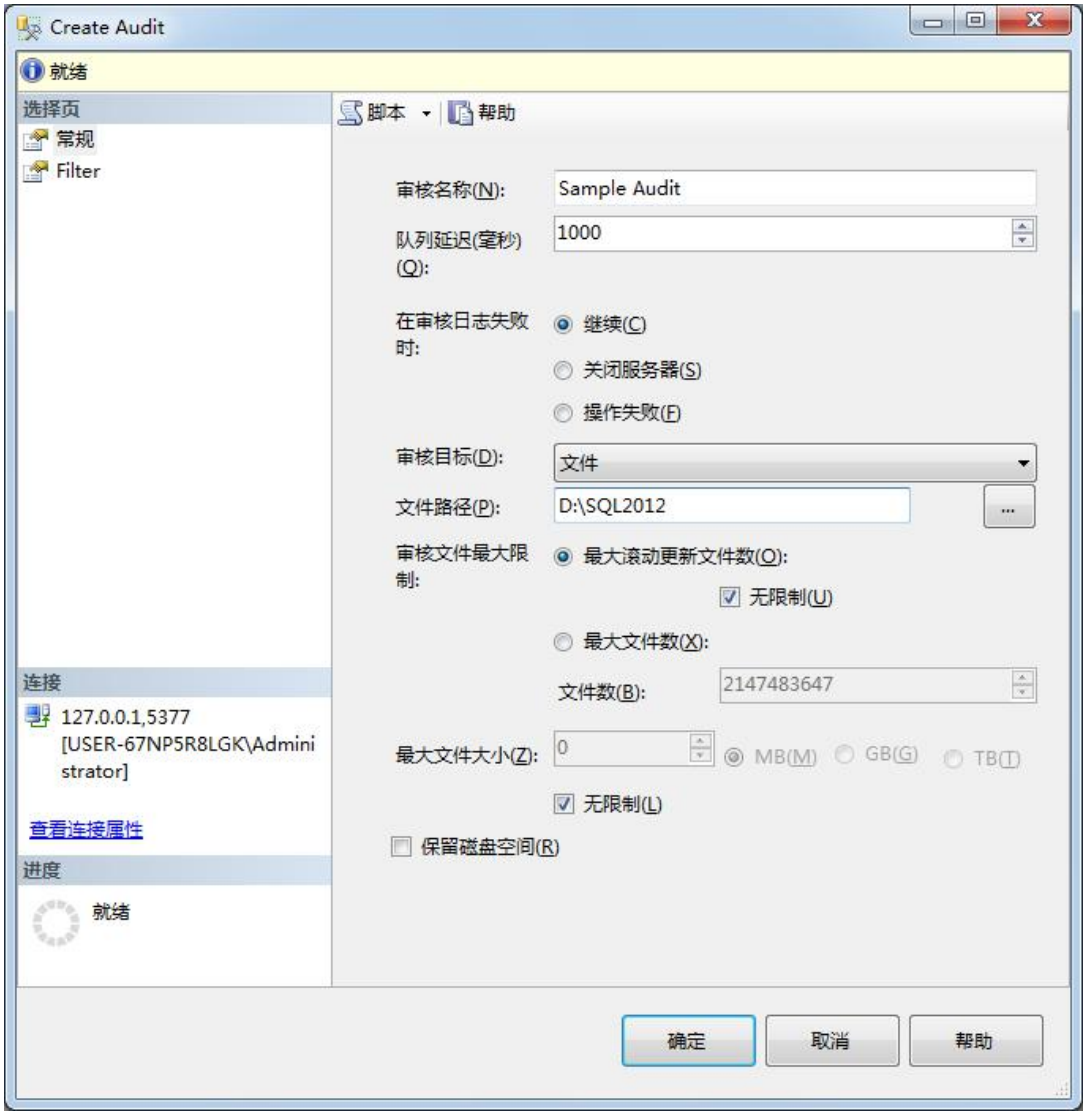

图 11.1 在 SSMS 创建服务器审核

你也可以使用 T-SQL 语句创建审核。代码 11.1 使用 CREATE SERVER AUDIT 创建相同设置的 Sample Audit.我通过创建审核对话框中的脚本按钮生成相关脚本。

```
USE master;
GO
CREATE SERVER AUDIT [Sample Audit]
```

```
    TO FILE
    (    FILEPATH = N'D:\SQL2012'
        ,MAXSIZE = 0 MB
        ,MAX_ROLLOVER_FILES = 2147483647
        ,RESERVE_DISK_SPACE = OFF
    )
    WITH
    (    QUEUE_DELAY = 1000
        ,ON_FAILURE = CONTINUE
    );
    GO
```

代码 11.1 T-SQL 代码创建 Sample Audit

代码 11.2 显示创建一个服务器审核，将日志写入到应用程序日志而不是文件。因为没有其他额外选项，所以代码比前面的要简洁。

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

代码 11.2 创建写入到应用程序日志的审核

现在在对象资源管理器->安全性->审核节点 ,你会看到有两个对象 ,如图 11.2 所示。注意，在放大镜图标上都叠加有一个红色的向下箭头图标。这表明，审核没有启用，这是创建时的默认状态。你可以通过右键单击审核对象，从弹出的菜单中选择启用审核，或者使用代码 11.3 中的 ALTER SERVER AUDIT 语句启用审核。一旦你启用了审核，红色的箭头就会消失，虽然你可能需要再次刷新对象资源管

理器。如果你是跟着 SSMS 界面操作，继续向前，启用 Sample Audit 审核，接下来我们将会使用。

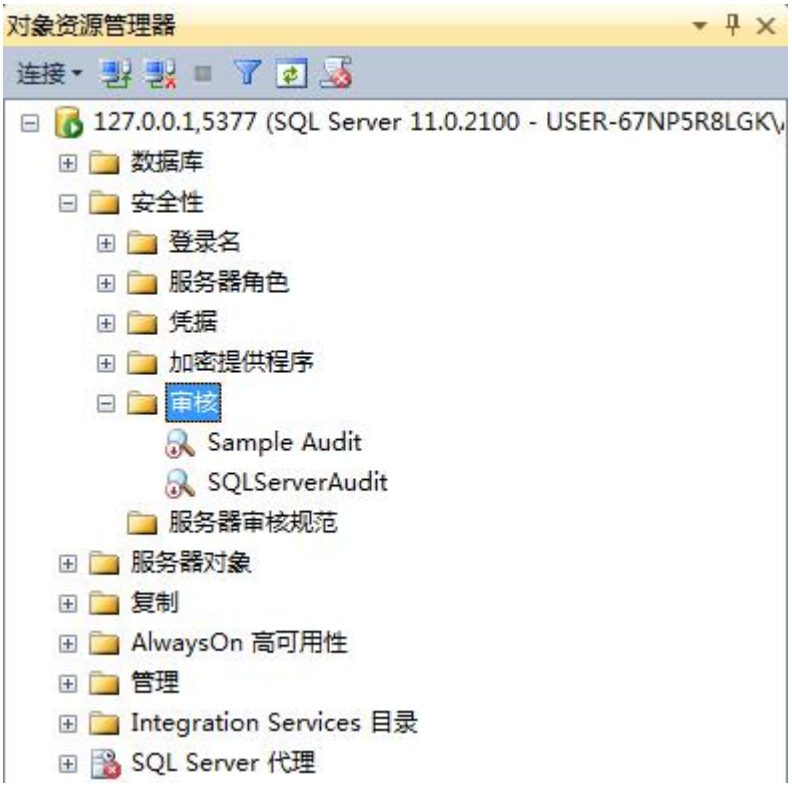

图 11.2 对象资源管理器下的服务器审核

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

代码 11.3 T-SQL 启用 SQLServerAudit 审核

创建服务器审核规范

一旦你创建了一个服务器审核，你可以定义你想写的审核事件。服务器审核本质上是审核规范的一个容器。记住，有两种类型的审核规范：服务器和数据库审核规范。

我将创建服务器审核规范用于记录 SQL Server 登录失败的信息到日志。这是一个数据库范围外的服务器级别的操作，所以我需要在服务器级别上创建一个规

范。使用 SSMS->安全性->服务器审核规范，右击服务器审核规范，选择新建服务器审核规范，打开创建服务器审核规范对话框。

你可以接受自动生成的规范名称，但我命名为 TestSQLServerAuditSpec.然后从审核下拉列表中选择服务器审核 ,列表中包含实例上所有已存在的服务器审核。本例中我选择使用 Sample Audit,意味着审核日志条目会保存到文件中。

然后，你可以使用对话框的操作部分来定义你想记录的事件或事件组。可用的操作类型列表有非常多 如图 11.3 所示。本例选择 FAILED_LOGIN_GROUP 类型。

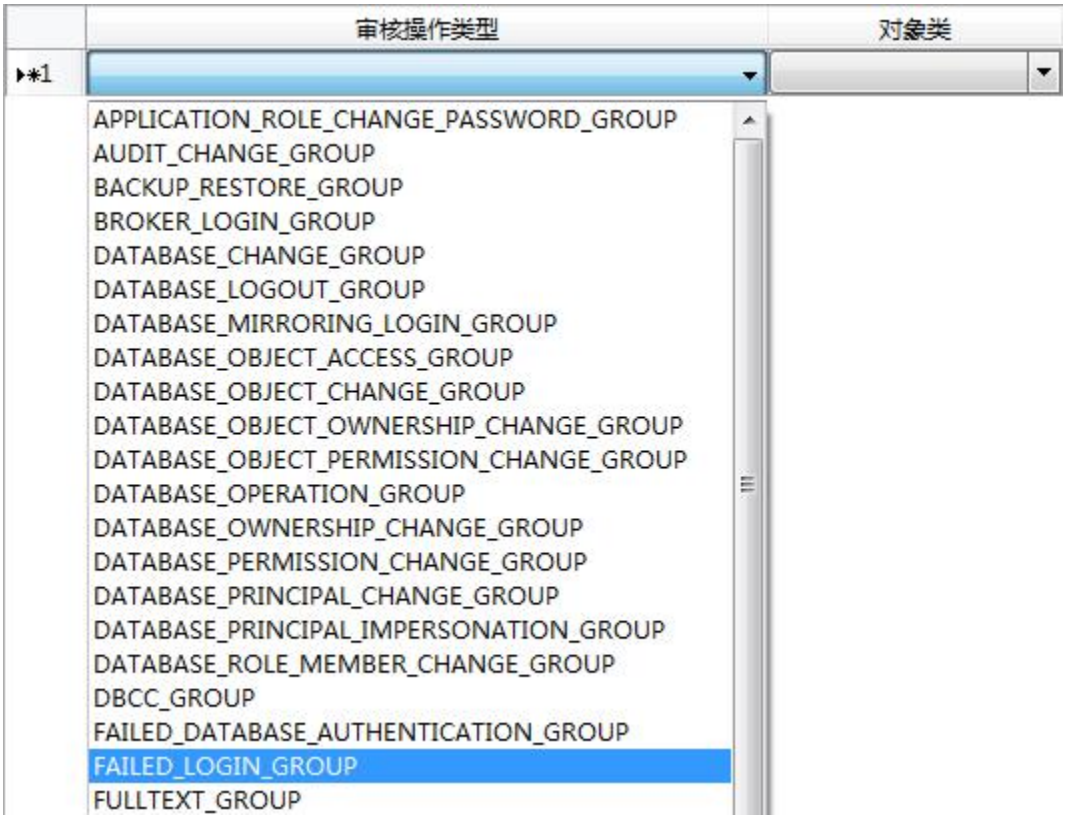

图 11.3 选择审核操作类型

FAILED_LOGIN_GROUP 操作类型的其余列是禁用的，因为该类型没有其他可用选项。但其他类型让你将操作与各种服务器对象关联起来。对话框应该看起来像图 11.4，当你单击“确定”按钮时，它将创建规范。

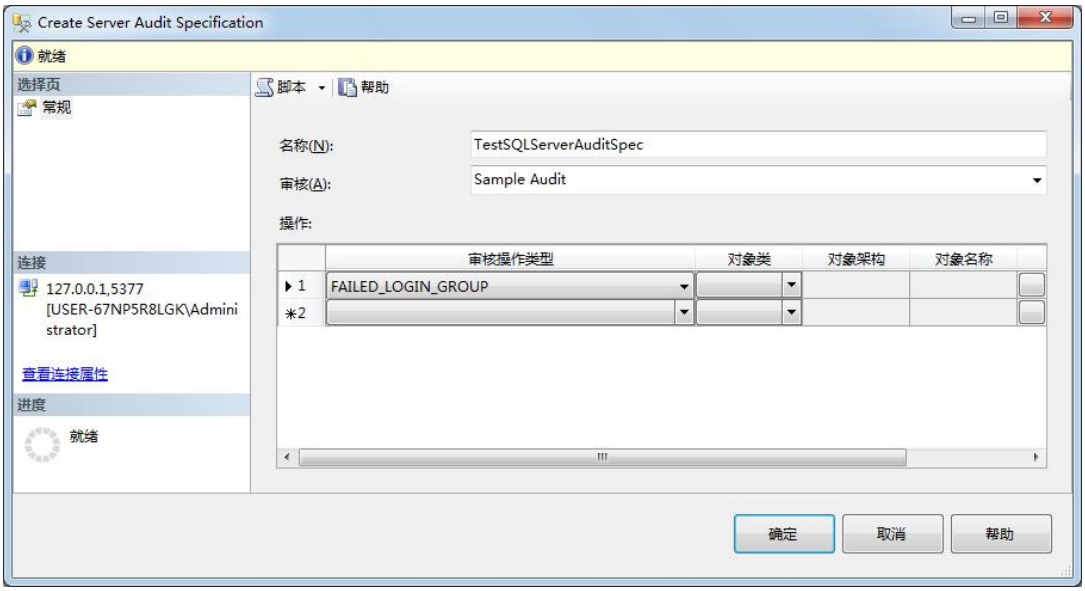

图 11.4 定义一个新的服务器审核规范

在对象资源管理器下的服务器审核规范节点会出现新创建的服务器审核规范，默认是禁用的。你可以右击规范，然后选择启用服务器审核规范。

你也可以使用代码 11.4 中的 T-SQL 语句来创建新的服务器审核规范。代码使用一个 WITH 子句选项来接收状态参数——启用或禁用规范。如果你省略这个子句，状态会默认设置为 OFF.

```
    CREATE SERVER AUDIT SPECIFICATION TestSQLServerAuditSpe
c

        FOR SERVER AUDIT [Sample Audit] ADD (FAILED_LOGIN_GR
OUP)

        WITH (STATE = ON);

    GO
```

代码 11.4 T-SQL 创建服务器审核规范

为了测试审核，连接到 SQL Server 实例，然后尝试用一个错误的密码登录数据库。你可以另外打开一个 SSMS 或者使用对象资源管理器下的连接按钮来操作。

然后右击 Sample Audit，选择查看审核日志，打开日志文件查看器对话框。

它可能需要点时间来从磁盘文件加载到的日志条目列表，但最终你会看到如图 11.5 所示的登录失败信息。每一行包含了相当多的有关事件的信息，使其向右滚动查看所有数据变得笨重。但当你选择一行时，该数据会出现在窗口下方以便于阅读。但不幸的是，如你在图中所看到的各列没有很好的格式。

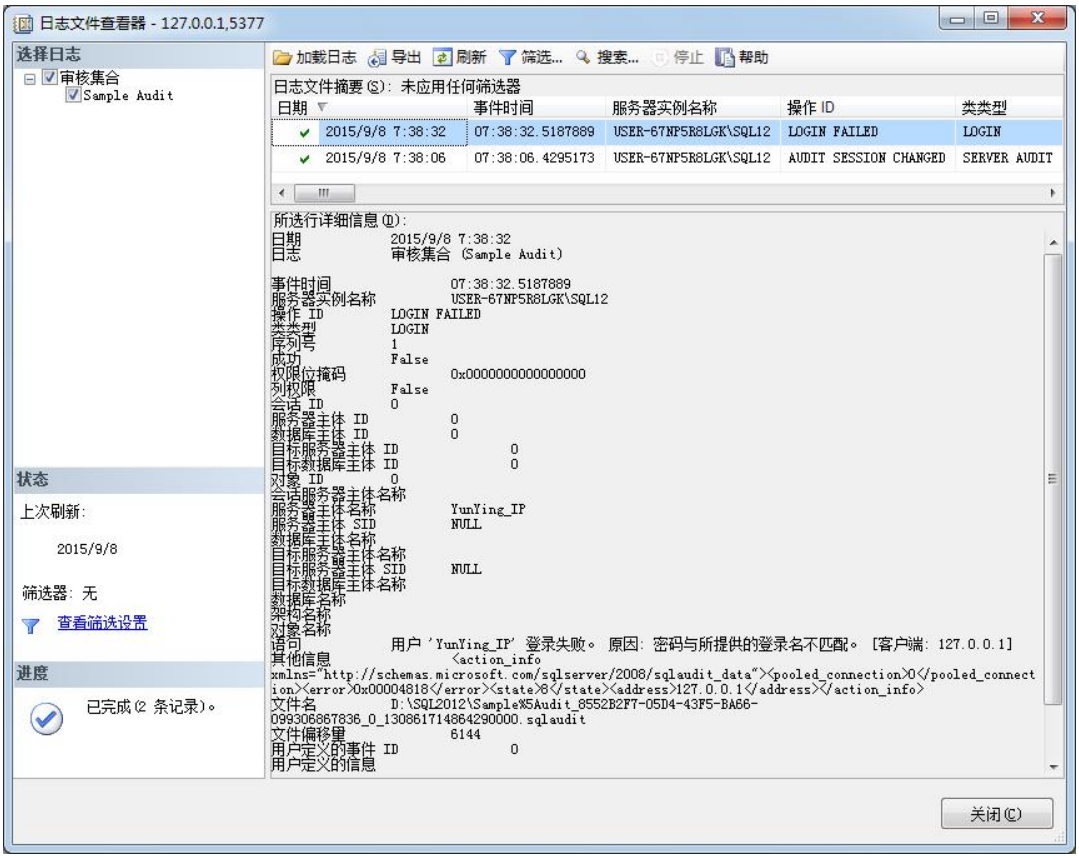

图 11.5 查看服务器审核日志

注意服务器审核自动捕获修改审核事件，在启用服务器审核时。图中是捕获的第二行信息。

创建数据库审核规范

创建数据库审核规范和创建服务器审核规范非常相似。主要不同是能够捕获到日志的事件范围。数据库审核规范能够捕获发生在单一数据库内的事件，比如通过 T-SQL 语句访问数据，修改结构或数据库对象的权限，或者执行存储过程。另一重要的区别是，你在数据库下创建数据库审核规范，而不是在安全性节点。

如果你想创建一个审核记录任何用户或程序执行一个 SELECT 语句从 AdventureWorks2012.Person.Person 表中获取数据。展开 对象资源管理器->数据库->AdventureWorks2012->安全性，右击数据库审核规范节点，选择新建数据库审核规范，打开创建数据库审核规范对话框，同样它会自动生成名称，你可以随意修改。

图 11.6 显示了在 Person.Person 表上的 SELECT 审核操作类型，关联到之前创建的审核 Sample Audit.本例中你要选择 OBJECTS 对象类(另外的选项是 DATABASE 和 SCHEMA),Person 架构，Person 表名，以及主体名称。不幸的是，你不能直接键入对象和主体名称。你必须点击旁边的省略按钮，会打开选择对象对话框。

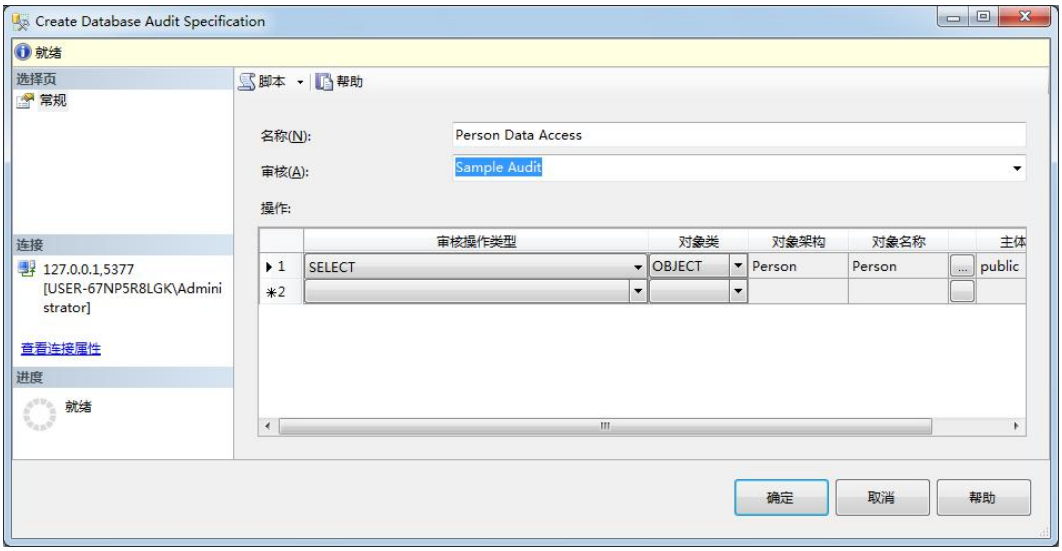

图 11.6 创建数据库审核规范

你可以将主体名称设置为任何数据库用户或角色，包括 Public 数据库角色以覆盖所有访问数据库的用户。类似服务器审核规范，你可以增加任何喜欢的操作到规范。

一旦创建了规范，记得启用它。

你也可以使用代码 11.5 中的 T-SQL 语句创建这个规范，带上 WITH 子句选项启用规范。

```
    USE AdventureWorks2012;
    GO
    CREATE DATABASE AUDIT SPECIFICATION [Person Data Acces
s]
        FOR SERVER AUDIT [Sample Audit]
        ADD (SELECT ON OBJECT::Person.Person BY public)
        WITH (STATE = ON);
    GO
```

代码 11.5 T-SQL 代码创建数据库审核规范

然后你可以通过执行表上的一个 SELECT 语句测试审核规范。一旦你做了此操作，刷新日志文件查看器，如图 11.7。正如你所看到的，日志中包含一个非常完整的事件信息，包括引起它的 SQL 语句。

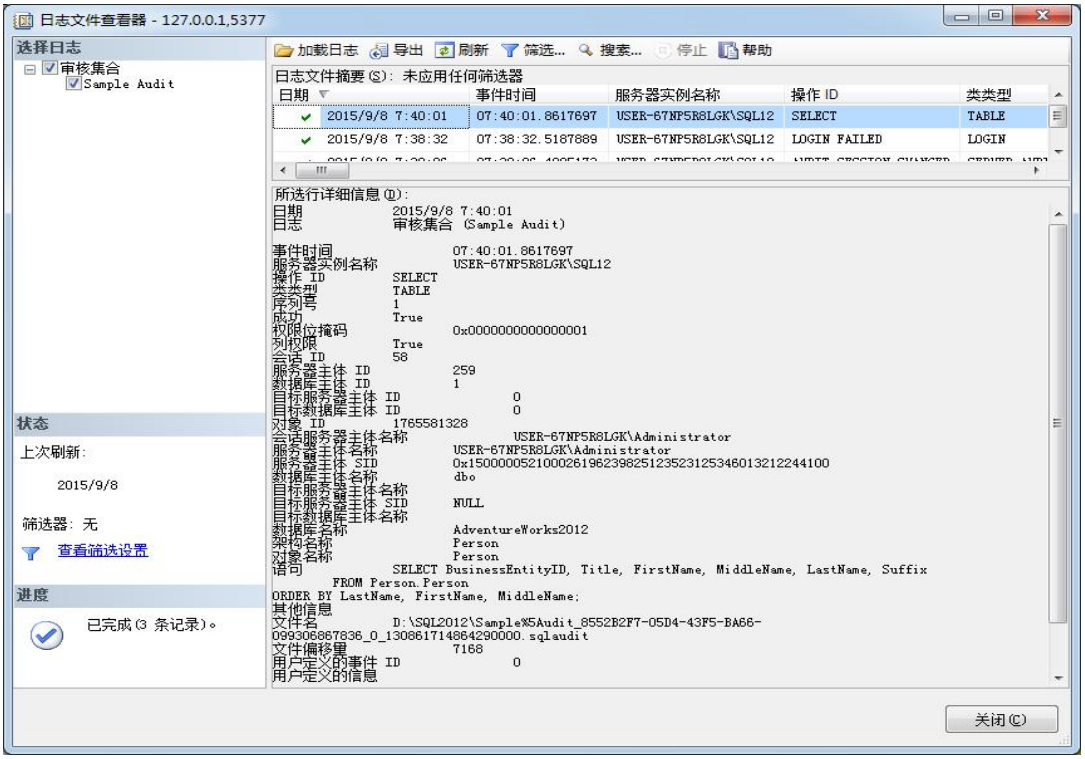

图 11.7 查询 Person.Person 后的审核日志

也可以用 T-SQL 方式查看审核记录

```
    select * from fn_get_audit_file('D:\SQL2012\Sample%5Au
dit_8552B2F7-05D4-43F5-BA66-099306867836_0_130861714864290
0000.sqlaudit', default, default)
```

注意图片中的其他信息列没有任何内容，这是因为产生事件直接是 SELECT 语句。但是当 SELECT 语句是在存储过程或其他代码模块下执行，其他信息会包含 T-SQL 堆栈信息的 XML 代码块。这可以用于区分查询是以查询语句还是代码模块执行的。

我们创建一个名叫 tempPerson 的存储过程，包含图片中语句列的 SELECT 语句。在你执行过存储过程后，你会得到了图 11.8 所示的结果，同样出现因为有人在 Person.Person 表上执行了 SELECT 语句。但是这次注意其他信息列。

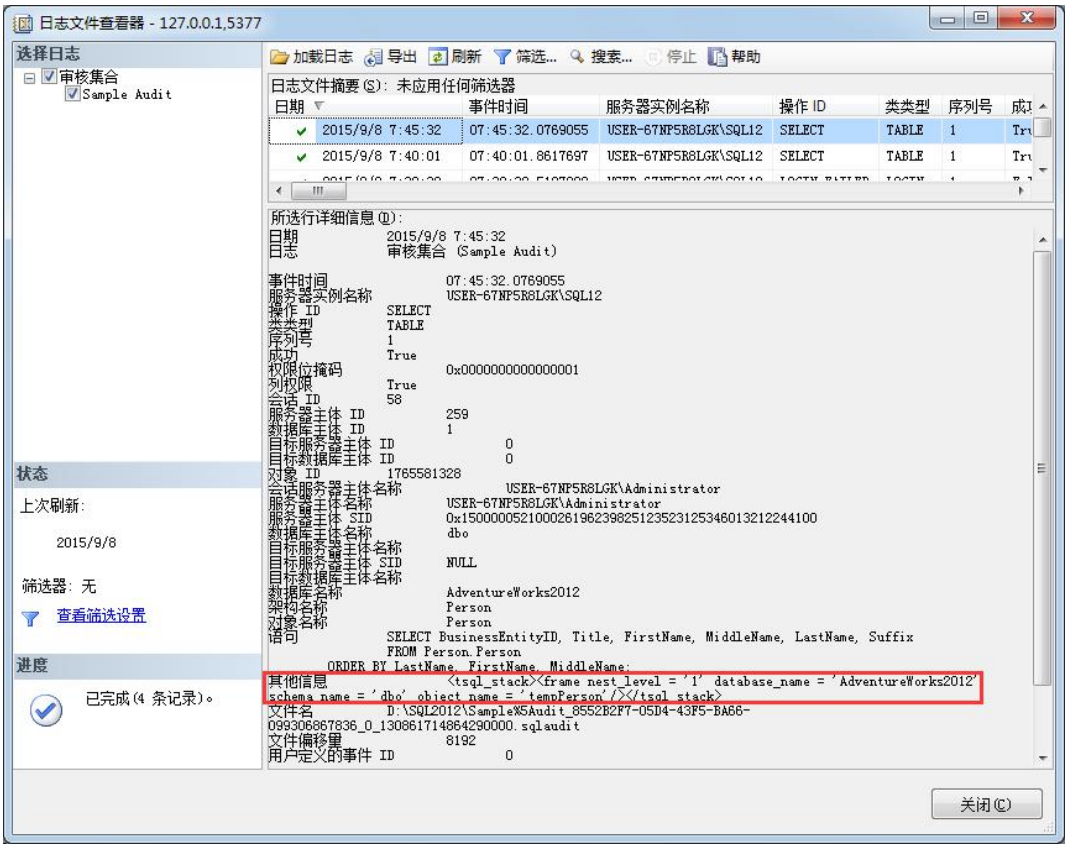

图 11.8 执行封装 SELECT 语句的存储过程

其他信息列包含 XML 代码，包括一些引起审核日志的代码信息，最重要的

是存储过程的架构和名称。

编写自定义审核信息

你不局限于仅捕获每个事件的默认信息。你还可以创建用户自定义的审核事件，它允许你将任何你希望的日志写入到审核日志。代码 11.6 中演示了如何实现这个。只有当审核规范(不管是服务器还是数据库)被禁用时，才能修改它，所以代码首先禁用规范。然后添加 USER_DEFINED_AUDIT_GROUP 操作类型到 TestSQLServerAuditSpec 规范，并立刻启用它。最后一行代码使用 sp_audit_write 系统存储过程往审核日志中写入一些有趣东西。

```
    USE master;
    GO
    ALTER SERVER AUDIT SPECIFICATION TestSQLServerAuditSpec
        WITH (STATE = OFF);
    GO
    ALTER SERVER AUDIT SPECIFICATION TestSQLServerAuditSpec
        ADD (USER_DEFINED_AUDIT_GROUP)
        WITH (STATE = ON);
    GO
    -- Write some custom audit information
    EXEC sp_audit_write 9999, 1, N'Something in SQL Server
succeeded!'
```

代码 11.6 编写自定义审核信息

当然，你也可以通过 SSMS 图形界面修改服务器审核规范。

如果你执行代码 11.6，然后查看审核日志，你会看到条目出现在图 11.9 的顶部。你仍然能得到很多审核事件的背景信息，包括事件的 T-SQL 语句，但是你

会发现在底部的用户定义的信息项是我们定义内容。

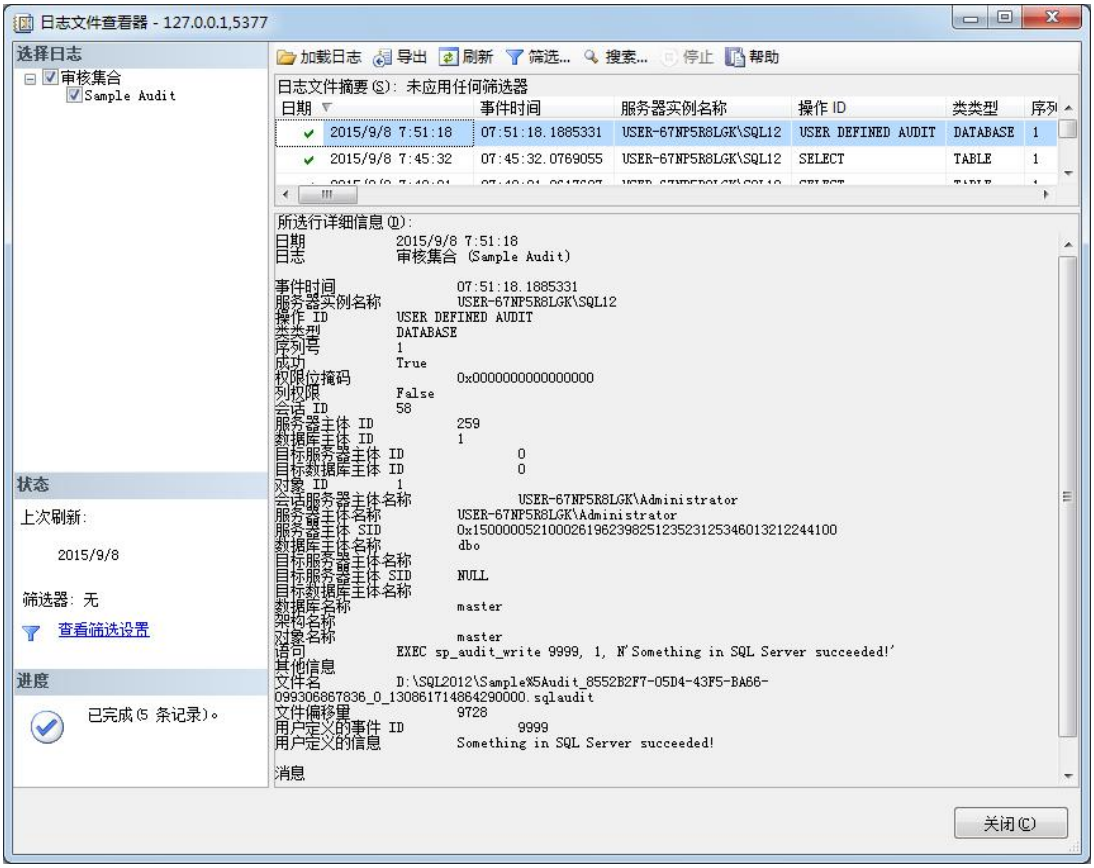

图 11.9 审核日志包含用户定义的信息

提示：如果 USER_DEFINED_AUDIT_GROUP 服务器审核规范禁用，数据库会忽略 sp_audit_write.

过滤审核事件

SQL Server 还包括过滤事件写入审核日志的能力，它使用和扩展事件相同的过滤机制。过滤为你提供细粒度的控制什么会被 SQL Server 写入审核日志。但重要的是，服务器仍然会为你在规范中定义的事件生成所有的日志条目，然后使用过滤来决定是否将事件写入日志。所以，即使条目没有写入日志，生成事件条目还是需要开销。这意味着，创建特定对象的审核事件通常比过滤要好。

你想创建一个审核，记录一个特定类型的所有事件，除了特定登录名的信息。代码 11.7 的第一部分创建 carol 登录名并映射到 AdventureWorks2012 数据库。然

后使用 SUSER_ID 方法检索新用户的主体 ID(我这是 288)。然后，第二部分创建一个带 WHERE 子句过滤掉主体 ID 为 288 的服务器审核，并启用服务器审核。

```
    -- Part 1: Create the login and database user
    USE AdventureWorks2012;
    GO
    CREATE LOGIN carol WITH PASSWORD = 'GEP2zYDt+5Cqw';
    CREATE USER carol FOR LOGIN carol;
    SELECT SUSER_ID('carol');


    -- Part 2: Create the server audit
    -- Change principal id from 288 based on SUSER_ID from p
revious statement
    USE master;
    GO
    CREATE SERVER AUDIT FilterAudit
        TO APPLICATION_LOG
    WITH
    (    QUEUE_DELAY = 1000
        ,ON_FAILURE = CONTINUE
    )
    WHERE server_principal_id <> 288;
    ALTER SERVER AUDIT FilterAudit WITH (STATE = ON);
    GO
```

代码 11.7 创建一个登录，然后创建一个排除此用户的审核

你也可以使用“审核属性”对话框来过滤服务器审核事件，右键单击服务器审核选择属性。选择“过滤”页，如图 11.10 所示。注意，文本框只包含用于创建服

务器审核语句中的 WHERE 子句谓词 ,括在括号中。没有必要包含 WHERE 关键字。

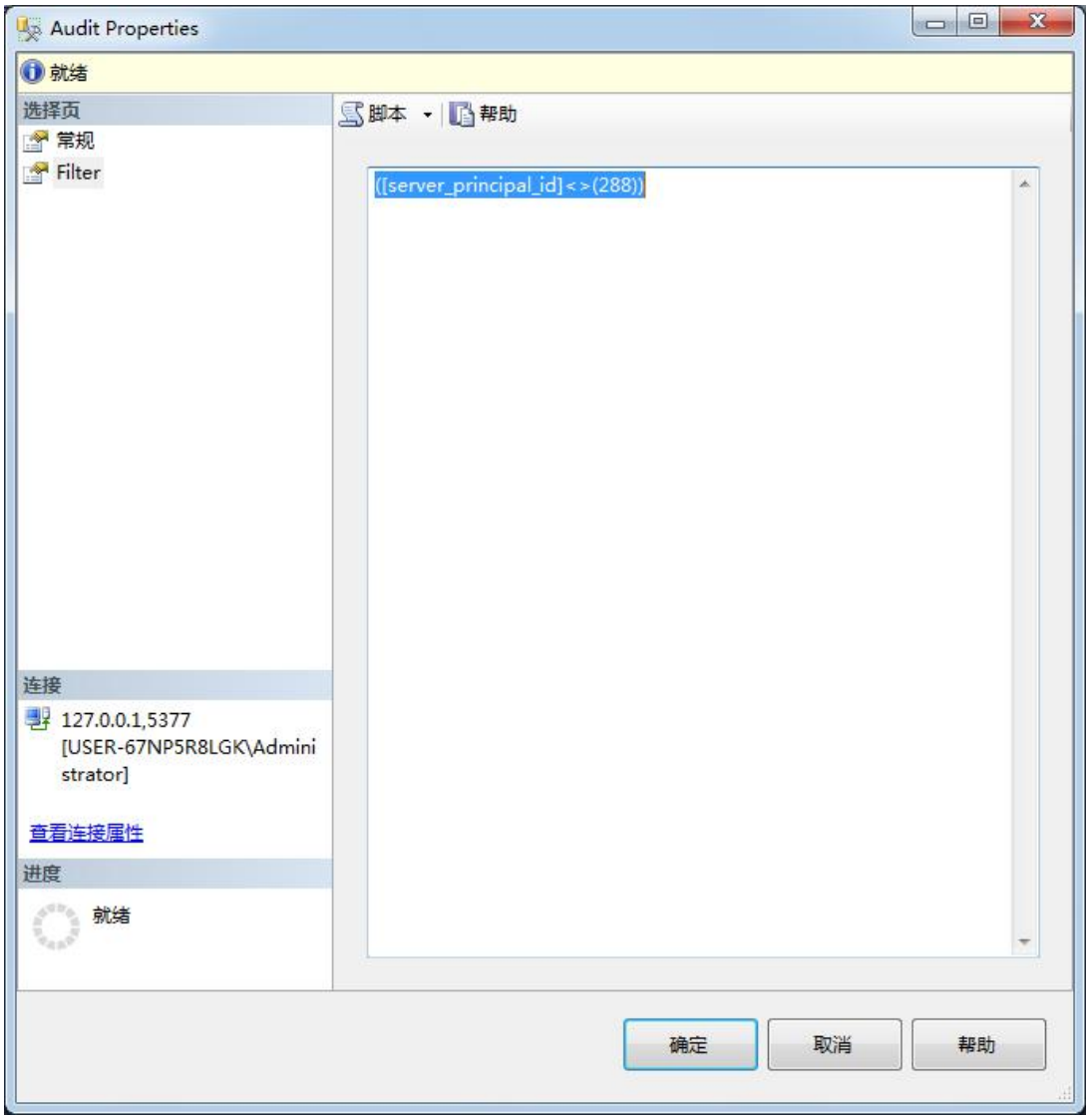

图 11.10 用审核属性添加过滤