**数据库的审核功能**

SQL Server 2008之前的版本只能是通过触发器或SQL 跟踪来实现审核，没有专门的管理工具来管理审核。到了SQL Server 2008的时候，新增了数据库审核功能，相比较于触发器，数据库审核不需要编写语句，并且不依赖与具体的表或数据库，而是独立存在的。利用SQL Server所提供的全面的数据审核功能，可以帮助企业不论是在[服务器](http://product.it168.com/list/b/0402_1.shtml)级别还是在数据库级别都可以监控所有的事件。

SQL Server 2012的 审核功能，可以对[服务器](http://product.pcpop.com/Server/10734_1.html)级别和数据库级别的事件组或者是单个事件进行审核。SQL Server 审核可以是一组操作，例如 Server\_Object\_Change\_Group，也可以是单个操作，例如对表的 SELECT 操作。Server\_Object\_Change\_Group 包括对任何服务器对象的 CREATE、ALTER 和 DROP 操作。通过 SQL Server 审核，用户可以创建针对服务器级别的审核规范和针对数据库级别事件的数据库审核规范。

经过审核的事件以及结果将发送到目标，目标可以是文件、Windows 安全事件日志或 Windows 应用程序事件日志。必须定期查看和归档这些日志，以确保目标具有足够的空间来写入更多记录。这些记录项包括：触发可审核操作的日期时间、操作会话ID、相关权限、发生审核的实体对象、当前登录名及用户名等信息。但是需要注意的是任何经过身份验证的用户都可以读取和写入Windows 应用程序事件日志。因此，在将审核信息保存到某一文件时，为了避免信息被篡改，用户可以考虑限制对文件位置的访问，并对SQL Server帐户设置适当的权限，例如审核管理员将目标进行存档时，新目标路径的权限一般定义为审核管理员具有读写权限，一般的审核读取者具有读权限。

建立审核的过程是：创建审核并且定义目标文件、创建服务器审核规范和数据库审核规范、将创建好的审核规范映射到审核、启用审核。经过以上简单几步，在创建并启用审核功能后，目标文件将接收各项的输出。

**实验：**

**创建审核**

首先在安全性—审核中创建一个默认的审核规范，此审核规范目的是将审核的结果输出到Windows应用程序事件日志。操作方法是，在对象资源管理器中，打开“安全性”节点下的“审核”，右键即可新建审核，选择将结果输出到Windows应用程序事件日志中后就不能定义审核文件的个数以及审核文件的最大大小，如下图所示：





接下来需要创建服务器审核规范并映射到刚才创建的默认审核上，创建服务器审核规范的方法是：在对象资源管理器中，右键单击“服务器审核规范”，然后单击“新建服务器审核规范”。这将打开“创建服务器审核规范”页。





在名称中使用默认设置，用户可以根据需要进行更改，审核项中选择刚才新建的默认审核名。“审核操作类型”选项，根据需要选择相应的操作组，在此选取 FAILED\_LOGIN\_GROUP。指的是主体尝试登录到 SQL Server，但是失败。此类中的事件由新连接引发或由连接池中重用的连接引发。说简单点就是记录尝试登录到 Microsoft SQL Server的失败信息。

审核创建完成后，默认为禁用状态，接下来就分别启用服务器审核规范和审核，如下图所示：





**测试**

下面来测试刚才创建的审核能否生效，我们使用SA用户，故意使其登录失败。如下图所示：



**查看审核日志**
　　用户可以使用 Windows 中的“事件查看器”实用工具来读取 Windows 事件。对于文件目标，可以使用 SQL Server Management Studio 中的“日志文件查看器”或使用 fn\_get\_audit\_file 函数来读取目标文件。如下图所示：







下面再针对select查询做一个审核。来记录针对NorthwindCS数据库中表的Select操作。

首先还是创建审核，操作方法同上面相同，审核名为：查询审核。在这里选择审核目标为文件，然后将文件存放在C:\审核日志这个文件夹下面，在启动审核之后，可以看到文件夹里增加了一个文件，这个就是审核日志。





再针对数据库创建数据库审核规范，操作方法是：在指定数据库上找到“安全性”选项卡，在其中的“数据库审核规范”上，点击右键，弹出“新建数据库审核规范”，如下图所示：



这里对应选择刚才新建的查询审核规范，审核操作类型选择select，对象类型选择Object



可以看到，对象名称这里可以选择要审核的对象类型，可以是表、视图、存储过程等。还可以具体到对应的哪一张表、哪一个视图等。



在主体名称中，可以选择审核对应的数据库角色或者某个用户



创建好之后全部启用，然后随便查询两个，不过查询的范围必须在刚才定义的对象名称和主体名称之内，否则无法审核到



查看审核结果如下：



除了右键审核查看审核日志以外，还可以用SQL语句进行查询：

SELECT \* FROM sys.fn\_get\_audit\_file (

'C:\审核日志\查询审核\_E59B8169-454B-49DC-9E17-1239B1CFD7F2\_0\_130964552067760000.sqlaudit'

,default,default)

 where database\_name = 'NorthwindCS'

GO