

Re: Trace Log – Failure to capture known SQL activity

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2007-03/msg00189.html>

- *From:* "Uri Dimant" <urid@xxxxxxxxxxxx>
 - *Date:* Wed, 28 Mar 2007 09:32:43 +0200
-

Is it SQL Server 2000 or 2005?

```
select identity(int,1,1) as traceid, a.name as [Database],
ltrim(rtrim(convert(varchar,b.spid))) as spid,
ltrim(rtrim(b.loginame)) as loginame,ltrim(rtrim(b.program_name))
as program_name,ltrim(rtrim(b.hostname))
as hostname into #audittrace from master.dbo.sysprocesses b (nolock) ,
master.dbo.sysdatabases A where
a.dbid = b.dbid and ltrim(rtrim(loginame)) not in
('DBA1','domain\systemaccount','DBA2','domain\administrator') and
ltrim(rtrim(left(program_name,8))) in ('MS SQLEM','SQL Quer')
```

"Digital Slug" <DigitalSlugospamalias@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:45767E07-9443-4867-8298-BE206EAEC034@xxxxxxxxxxxxxxxxxxxx

Hello,

I am capturing SQL Server trace log activity (daily basis) on a generic RDBMS production server. It captures ordinary user traffic just fine. However, it fails to capture certain types of known RDBMS activity.

Is it possible for an administrator to sidestep SQL Server activity logs and traces?

Can you suggest additional ?sp_trace_setevent? events that should be captured?

The problem and my basic trace log settings are listed below.

Problem:

1. SQL traffic from authorized Server/RDBMS administrators is captured in trace log.
2. Windows Server event logs captures an unauthorized administrator (database/domain admin) logging on to server and performing RDBMS

Re: Trace Log – Failure to capture known SQL activity

operations.

3. SQL Server trace log does not indicate that DB activity has occurred by unauthorized administrator.

Standard Trace Configuration:

Event 10, RPC:Completed – Occurs when a remote procedure call (RPC) has completed.

Event 11, RPC:Starting – Occurs when an RPC has started.

Event 12, SQL:BatchCompleted – Occurs when a Transact-SQL batch has completed.

Event 13, SQL:BatchStarting – Occurs when a Transact-SQL batch has started.

Event 14, Audit Login – Occurs when a user successfully logs in to Microsoft SQL Server.

Event 15, Audit Logout – Occurs when a user logs out of SQL Server.

Event 16, Attention – Occurs when attention events, such as client-interrupt requests or broken client connections, happen.

Event 17, ExistingConnection – Detects all activity by users connected to SQL Server before the trace started.

Need a little help here?..

Thanks!