

Locking SQL Server to a specific application on a web server

Asked 16 years, 1 month ago Modified 16 years, 1 month ago

Viewed 312 times



1



I'm curious, is there a way to tell the SQL Server that a specific group has access to the database only from a single location/application. I have an SQL Server and a Web Server. Our applications use stored procedures and access for each stored procedure is based on the role that is allowed to access it. Then user groups are assigned roles based on the functions they'll perform. As an added layer of security I would like to specify the web application that these users can access the database from.

I suppose this is overkill. The stored procedure names are hidden from users at all times (all errors are hidden, with generic "sorry this isn't working" displayed to the user). Users only have access to the stored procedures they are allowed to execute. It would just be a nice additional piece of security so should a table accidentally grant everyone full access, the database would only allow full access from one location.

sql-server

security

web-applications

Share

Improve this question

Follow

asked Nov 17, 2008 at 15:15



[user108418](#)

13 ● 2

3 Answers

Sorted by:

Highest score (default)



0



In the connection string, you can set `Application Name=MyAppName` - this is not real security, but you can check this in your SPs (`sysprocesses` - in the `program_name` column) and through `sp_who` .

There's nothing you can do about tables - which is why I recommend that **nobody** be in **any** role which is allowed access to tables at all (`SELECT` , `INSERT` , `UPDATE` , or `DELETE`).

You can audit this on a regular basis with some automated T-SQL to ensure that no one has done anything stupid.

I'm not advocating this in any way, but you can do something like this for views (comparing the SPID of the current process and `program_name`):

```
CREATE VIEW YourViewNameHere
AS
SELECT *
FROM YourTableNameHere
WHERE EXISTS (
    SELECT spid, program_name
    FROM sys.sysprocesses
    WHERE program_name = 'YourProgramNameHere'
```

```
AND spid = @@SPID  
)
```

Share Improve this answer

edited Nov 17, 2008 at 18:32

Follow

answered Nov 17, 2008 at 15:45



Cade Roux

89.6k ● 40 ● 184 ● 266

What about with View's? This question stems from the idea of using Linq to Sql and rather than having separate stored procedures for each level of access implement views which enforce the access for each table and are used by the Linq to SQL. – [user108418](#) Nov 17, 2008 at 18:15



0



I suggest run the application/app pool as a service account which has permission on the procedures, but don't grant any permissions to the users themselves. This entails not implementing user security at the database level, but instead at the app level..



Share Improve this answer

answered Nov 17, 2008 at 15:37



Follow



ScottK

126 ● 1 ● 7

The only problem with this is varying the levels of access for a application. Many applications have both an administrator level and a basic user level. To have varying levels this method would need X pools and X applications for X levels.

– [user108418](#) Nov 17, 2008 at 18:13



0



The easiest way is to just lock it down on the user-level. You can run your win/web application under a specific security context that you have the needed rights configured for.

This gives the benefit of forcing users to run your app to interact with SQL and can't just open Enterprise Manager or whatever.

Share Improve this answer

Follow

answered Nov 17, 2008 at 17:03



[Kevin Fairchild](#)

10.9k ● 6 ● 34 ● 52
