Securing SQL Server: Windows Local Groups as SQL Logins

In SQL Server, you can create logins using Windows local groups as a way to manage access to the database server. This means that you can add users to a Windows local group and then create a SQL Server login using that group. The users who are members of the group will then be able to connect to the database server using the group login.

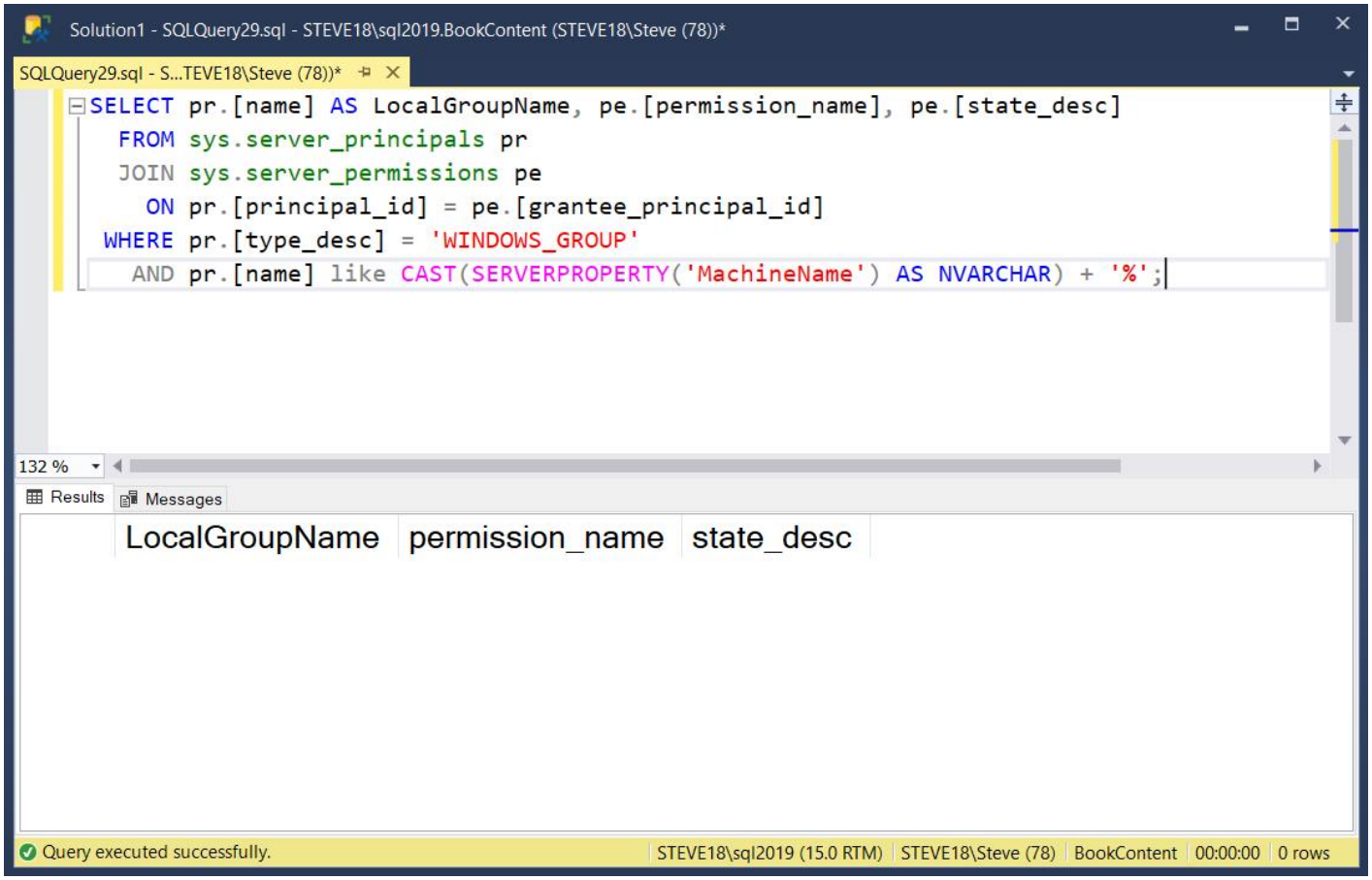
While using Windows local groups as SQL logins can be a convenient way to manage access to the database server, it can also be a security risk if not properly managed. This is because Windows local groups are not as granular as SQL Server logins, and they do not have the same level of control over the permissions of the users who are members of the group.

For example, if you create a SQL Server login using a Windows local group, all of the users who are members of the group will have the same permissions on the database server. This can be a problem if you need to grant different levels of access to different users, as you will not be able to control the permissions of individual users within the group.

You can use the following query to check to see if you have any local groups set up as SQL Logins:

```
SELECT pr.[name] AS LocalGroupName, pe.[permission_name], pe.[state_desc]
  FROM sys.server_principals pr
  JOIN sys.server_permissions pe
    ON pr.[principal_id] = pe.[grantee_principal_id]
 WHERE pr.[type_desc] = 'WINDOWS_GROUP'
   AND pr.[name] like CAST(SERVERPROPERTY('MachineName') AS NVARCHAR) + '
%';
```

The query should return no results if you are clear. If any results are returned soem investigation will be required.



In addition, Windows local groups are managed outside of SQL Server, which means that you will need to use the Windows operating system tools to manage the membership of the group. This can be a problem if you need to quickly add or remove users from the group, as it requires additional steps and may not be as efficient as using SQL Server logins.

In summary, using Windows local groups as SQL logins can be a convenient way to manage access to the database server, but it can also be a security risk if not properly managed. It is important to carefully consider the granularity of the permissions that you need to grant to your users, and to use the appropriate tools to manage the membership of the group in order to reduce the risk of security issues.

Want to learn more about securing your SQL Server, take a look at my free white paper on sever steps to help harden your SQL Server.

Securing SQL Server Whitepaper.