Lock Outs In Sql Server Essay, Research Paper

Lock Outs in SQL Server

If you lock yourself out of SQL Server without being able to log on with a sysadmin login, you don’t have to reinstall SQL Server. To access SQL Server, you need to use the registry key for SQL Server 2000 and SQL Server 7.0 that determines the authentication mode of SQL Server.

In SQL Server 7.0, the key is:

HKEY\_LOCAL\_MACHINESOFTWAREMicrosoft MSSQLServerMSSQLServerLoginMode

In SQL Server 2000, the key is:

HKEY\_LOCAL\_MACHINESOFTWAREMicrosoft

MicrosoftSQLServerMSSQLServerLoginMode

The value of LoginMode is 0 for Windows Authentication only, and 1 for Mixed Mode. After locking yourself out, you can change the value of LoginMode to 0, restart SQL Server, and log in as the system administrator (sa), provided you know the sa password.

The following information about SQL Server role memberships might help you understand how you locked yourself out. When you install SQL Server 2000 or 7.0, the installation process automatically creates a login for BUILTINAdministrators with sysadmin server role membership. The BUILTINAdministrators login stands for the Administrators local group in your Microsoft Windows 2000 or Microsoft Windows NT server. The Windows 2000 or Windows NT Administrator account is a member of the Administrators local group by default. Also, if your server is a member of a domain (both in Windows 2000 and in Windows NT 4.0), the global group Domain Admins becomes a member of the local Administrators group, too. This means that all members of the Administrators local group automatically gain sysadmin rights in your SQL Server.

To tighten security for your SQL Server, you might prefer to create your own group and map it to a login with sysadmin rights to your SQL Server computer and remove the BUILTINAdministrators login, or at least remove it from the sysadmin server role. This way, you’ll have better control of who gains sysadmin rights in your SQL Server. This approach also breaks the relationship between SQL Server administrators and Windows 2000 or Windows NT administrators, who usually have different tasks and need different rights. As another step in tightening security, you might want to configure your SQL Server to support only Windows Authentication. However, keep in mind that this configuration will disable your sa account. (This method is probably the only way to disable the sa account because you can’t delete the sa account.) If you implement these security measures in the wrong order, you won’t be able to log on to SQL Server as a sysadmin without using the key I described. The correct order is:

1. Create the Windows 2000 or Windows NT group and assign members to it. For example, call this group “SQLAdmins”.

2. Map SQLAdmins to a Windows Authenticated login in your SQL Server and assign this login to the sysadmin server role.

3. Delete the BUILTINAdministrators login or remove it from the sysadmin server role.

4. Change your SQL Server authentication mode to Windows Authentication only.

5. Restart SQL Server to reflect the changed authentication mode.

Note: If you implement these security steps in the wrong order-by deleting the BUILTINAdministrators login, changing your SQL Server authentication mode to Windows Authentication only, then restarting SQL Server, you will have disabled the sa account and you will have no other Windows Authenticated login defined in your SQL Server. Thus, you are locked out. To avoid this situation, implement the security measures in the correct order.