SQL Server 数据库安全检查清单

SQL Server 对于组织来说是个敏感信息库，管理者需要确保只有授权用户才能访问到这部分敏感信息。然而，要让 SQL Server 配置安全同时还不会产生错误，这不是一件容易的事，作为 DBA 我们不得不执行一系列额外步骤来强化我们的 SQL Server 部署安全配置。本文中列出了一份微软 SQL Server 数据库安全最佳实践检查表，能够帮助 DBA 更好地保护数据库，避免来自内部和外部的攻击。

1.认证

SQL Server 支持两种模式的认证：Windows 认证和混合模式认证。根据 SQL Server 安全性最佳实践，我们建议为您的 SQL Server 部署选择 Windows 认证，除非遗留应用系统需要混合模式认证向后兼容访问。

Windows 认证比混合认证模式更安全，启用这种模式后，Windows 认证凭据(也就是 Kerberos 或者 Windows NT LAN 管理器【NTLM】认证凭据)是允许登录到 SQL Server 的。Windows 登录使用许多加密信息认证 SQL Server，密码不会在认证期间跨网络传递。此外，在 Kerberos 协议下活动目录还提供了额外的安全级别。因此，认证就更加可靠，利用基于角色的活动目录组可以减少控制访问的管理工作。相比于 Windows 认证模式，混合模式认证支持 Windows 账号和 SQL Server 专用账号登陆 SQL Server。SQL 登陆密码通过网络传递用于认证，相比起来不如 Windows 登陆安全。

2.确保 sySAdmin 账号安全

如果不修改就退出，“sySAdmin”(SA)账号是很脆弱的。潜在的 SQL Server 攻击者们都意识到了这一点，如果他们控制了这个强大的用户，数据库攻击就更容易。为了防止使用“SA”账号进行攻击，可以把“SA”账号重命名为别的账号名称。我们可以按照以下操作实现这一点：在“对象资源管理器”中展开“登录”，右键点击“SA”账号并在菜单中选择“重命名”。或者我们也可以执行以下 T-SQL 脚本重命名“SA”账号：

```
USE [master]
GO
ALTER LOGIN SA WITH NAME = []
GO
```

此外，也可以禁用 SQL Server 实例的“SA”账号。

3.为 SA 和 SQL Server 专用登录账号设置复杂密码

在使用混合认证模式时，要确保为“SA”账号和其它 SQL Server 上使用的 SQL Server 专用登录账号设置复杂密码。首先，为“SA”账号和所有其它 SQL 登录账号选中“强制密码过期”和“加强密码策略”选项。这两项可以保证所有其它 SQL Server 专用登录账号遵循底层操作系统的登录策略。除此之外，对所有新设置的 SQL 登录账号启用“MUST_CHANGE”选项。该选项确保登陆者必须在第一次登录后修改密码。

4.“sySAdmin”固定服务器角色和“CONTROL SERVER”权限资格

要谨慎选择 sySAdmin 固定服务器角色的资格，因为该角色可以在 SQL Server 上为所欲为。此外，不要明确授予“CONTROL SERVER”权限给 Windows 登录、Windows 组登录和 SQL Server 登录，因为这种权限的登录获得了对整个 SQL Server 部署的完全管理员权限。默认情况下，sySAdmin 固定服务器角色明确拥有这项权限。

5.SQL Server 管理

要避免使用“SA”，或者任何其它已授予“CONTROL SERVER”权限的 SQL 登录账号，或者 sySAdmin 固定服务器角色下辖成员管理 SQL Server 实例。相反，要为 DBA 们设置专门的 Windows 登录账号，给这些账号分配“sySAdmin”权限作为管理用途。要给用户分配权限，可以使用内建的固定服务器角色或者数据库角色，也可以创建你自己定制的服务器角色和数据库角色满足你更精细化的权限控制。

6.禁用 guest 用户访问

默认情况下，guest 用户存在于每个用户和系统数据库下，它是安全封闭环境下的潜在安全风险，因为它允许与数据库无关的用户登录访问数据库。由于这一潜在风险，我们需要在所有用户和系统数据库(除了 msdb)中禁用 guest 用户。这样才能保证公共服务器角色成员不能访问 SQL Server 实例上的用户数据库，除非用户被明确授权访问这些数据库。

7.限制对公共角色授权

由于潜在的安全风险， 我们可以使用下面的扩展存储过程取消公共角色的访问权限。

此外，不要明确分配权限给用户公共角色和对系统存储过程的访问。要列出公共角色可用的存储过程，可以执行如下查询：

```
SELECT o.[name] AS [SPName]
,u.[name] AS [Role]
FROM [master]..[sysobjects] o
INNER JOIN [master]..[sysprotects] p
ON o.[id] = p.[id]
INNER JOIN [master]..[sysusers] u
ON P.Uid = U.UID
AND p.[uid] = 0
AND o.[xtype] IN ('X','P')
```

8.减少 SQL Server Surface Area

配置 SQL Server 时应该仅安装必要的功能特性，安装后使用 SQL Server 系统的外围界面禁用不需要的功能。你还可以使用基于策略的管理功能创建系统策略为一个或多个 SQL Server 系统实施精细配置设置。

9.强化 SQL Server 端口

另一项 SQL Server 安全性最佳实践是使用 SQL Server 配置管理器修改 SQL Server 安装时的默认端口。而且，要使用专门 TCP 端口替代动态端口。此外，要确保避开常见的 TCP 端口(比如 1433 和 1434)，不要用这些端口做客户端请求和交互，因为这些端口过于为人熟知，容易成为攻击目标。

10.禁用 SQL Server 浏览器服务

要确保 SQL Server 浏览器服务只运行在多个 SQL Server 实例运行其上的单个 SQL Server 上。SQL Server 浏览器服务显示了网络环境中的 SQL Server 信息，这在安全封闭的环境中可能成为潜在安全威胁。

11.SQL Server 服务账号

我们应该创建专用低权限域账户来运行 SQL Server 服务。此外，要定期检查 SQL Server 服务账号成员，确保它们不是任何域用户组或本地用户组的成员，因为那样会使这些用户具备不必要的权限。

12.确保 SQL Server 错误日志和注册键的安全

使用 NTFS 权限确保 SQL Server 错误日志和注册键安全，因为它们可以展现关于 SQL Server 实例和安装的大量信息。