# 利用sqlcmd登录mssql问题报告

## 问题概述

利用微软提供的sqlcmd工具，我们可以与后台mssql服务进行交互，从而可以进行登录，操作数据库的功能。但是目前现有文档并没有解决mssql证书认证问题，因此需要本文档进行记录解决证书问题的过程。

## Sqlcmd简介

Sqlcmd是微软提供给使用者的一套实用工具，根据官网的描写：

The sqlcmd utility lets you enter Transact-SQL statements, system procedures, and script files at the command prompt, in Query Editor in SQLCMD mode, in a Windows script file or in an operating system (Cmd.exe) job step of a SQL Server Agent job. This utility uses ODBC to execute Transact-SQL batches.

我们可以看出，sqlcmd具有普适性。

Sqcmd下载地址在于：

<https://www.microsoft.com/en-us/download/details.aspx?id=53591>

非windows系统的下载方式官网也给出了：

<https://docs.microsoft.com/en-us/sql/linux/sql-server-linux-setup-tools?view=sql-server-linux-2017>

按照文档中给出的步骤安装即可。这些文档都是正确的。

## Mssql登录模式解析

Sql server有三种加密方式：

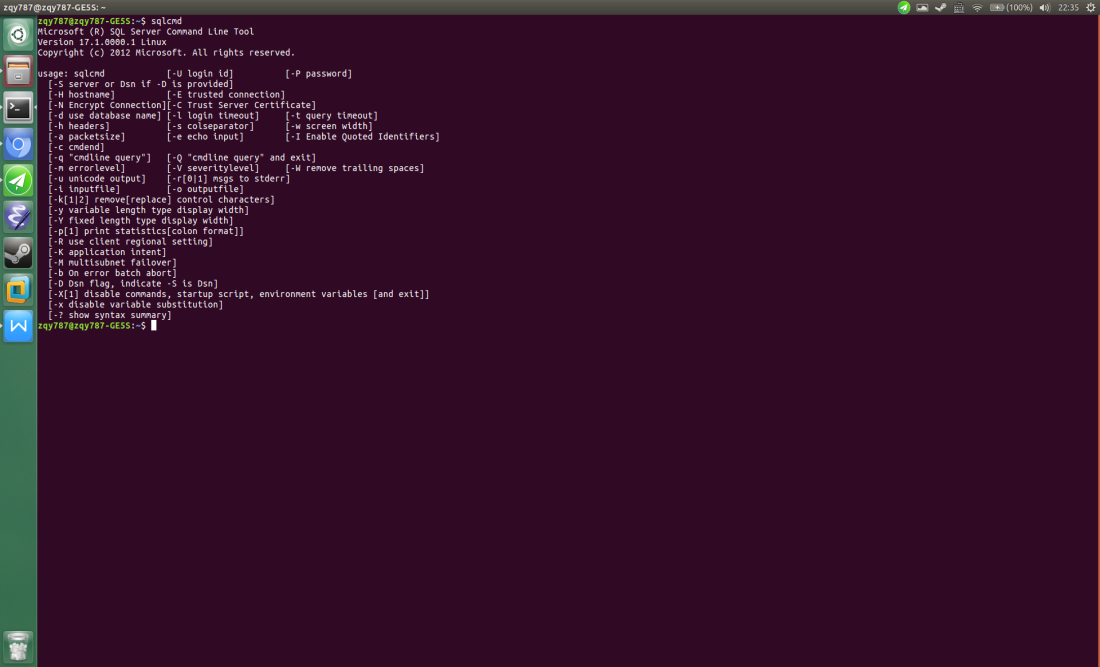
1.明文传输

2.仅加密登录过程

3.加密所有过程

默认情况下，sql server会自动采取2方案，就是仅加密登录过程。

在sqlcmd中，所有的选项列出如下：



我们可以看出，sqlcmd没有明文传输选项。因此当使用sqlcmd工具登录时候，只能采取2 3 方式登录。

2方式登录口令

sqlcmd -U <username> -P <password> -S <host ip>,<host port>

3 方式登录口令

sqlcmd -U <username> -P <password> -S <host ip>,<host port> -N

其中所需要的证书，需要在配置中预先配置好。

## 在仅加密登录方式中如何提取证书，从而提取用户名，密码

结论是：不可能。

根据有关回答，我们知道登录证书的名字是##MS\_SQLAuthenticatorCertificate##。但是我们无法提取：

物理层面上，我们发现，证书存储在master.mdf中，这说明我们无法绕开mssql进行证书提取。

根据

<https://www.mssqltips.com/sqlservertip/4271/where-does-sql-server-store-its-certificates/>

与自己的实践，我发现即使最高权限，也无法备份##MS\_SQLAuthenticatorCertificate##，因此通过备份的方式提取也是不可行的。

根据stackoverflow的有关回答：

<https://dba.stackexchange.com/questions/189594/sql-server-self-signed-cert-no-private-key>

我们知道两点：

1. 在设计中，##MS\_SQLAuthenticatorCertificate##就是不允许被外部使用的，因此并没有留出接口供外部调用。
2. 每次登录，##MS\_SQLAuthenticatorCertificate##证书都会被重新生成，因此提前备份是不可行的。

因此想要使用ssl，我们必须加密全部过程。

## 加密所有报文登录方式问题与解决

在官方文档中：

<https://docs.microsoft.com/en-us/sql/linux/sql-server-linux-encrypted-connections?view=sql-server-linux-2017>

提供了如何利用sqlcmd进行加密的方式。但是这个官方文档错误非常多。

1. 官方文档提出要把key文件放入 /etc/ssl/private/ 中，但实际上mssql用户组对于这个文件是没有访问权限的。解决方案要不然是放入普通文件夹中，要不然对于private文件增加mssql组的权限。否则会出现找不到证书的bug
2. 官方文档中对于证书给出了600权限，实际上对于组外，我们至少要给出r权限，否则就会报错。我猜测官方在写文档时候直接使用的就是mssql用户，因此对于实际情况缺乏判断。

最后的效果如图，我们发现所有的报文都被加密了，证明成功。

