“The certificate chain was issued by an authority that is not trusted” when connecting DB in VM Role from Azure website

Asked 7 years, 3 months ago Active 4 months ago Viewed 263k times

203

24

I am experiencing error when connecting MY DB which is in VM Role(I have SQL VM Role) from Azure Website. Both VM Role and Azure Website are in West zone. I am facing following issue:

> SqlException (0x80131904): A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not trusted.)]

I am able to connect to my DB using SSMS. 1433 port is open on my VM role. What is wrong with my connection?

azure-web-roles azure-vm-role

edited Nov 25 '18 at 17:59
Andrea
9,820 14 53 58

asked Jul 12 '13 at 12:46
ZafarYousafi
4,264 5 25 36

8 Answers

Active | Oldest | Votes

383

You likely don't have a CA signed certificate installed in your SQL VM's trusted root store.

If you have `Encrypt=True` in the connection string, either set that to off (not recommended), or add the following in the connection string:

```
TrustServerCertificate=True
```

SQL Server will create a self-signed certificate if you don't install one for it to use, but it won't be trusted by the caller since it's not CA-signed, unless you tell the connection string to trust any server cert by default.

Long term, I'd recommend leveraging Let's Encrypt to get a CA signed certificate from a known trusted CA for free, and install it on the VM. Don't forget to set it up to automatically refresh. You can read more on this topic in SQL Server books online under the topic of "Encryption Hierarchy", and "Using Encryption Without Validation".

edited Jul 15 '19 at 22:06
Dale K

answered Jul 15 '13 at 16:11
Thiago Silva

1 sorry my bad, TTrusted_Connection=False was set in connection string. setting it true works for me. Thanx anyway – ZafarYousafi Jul 24 '13 at 8:59

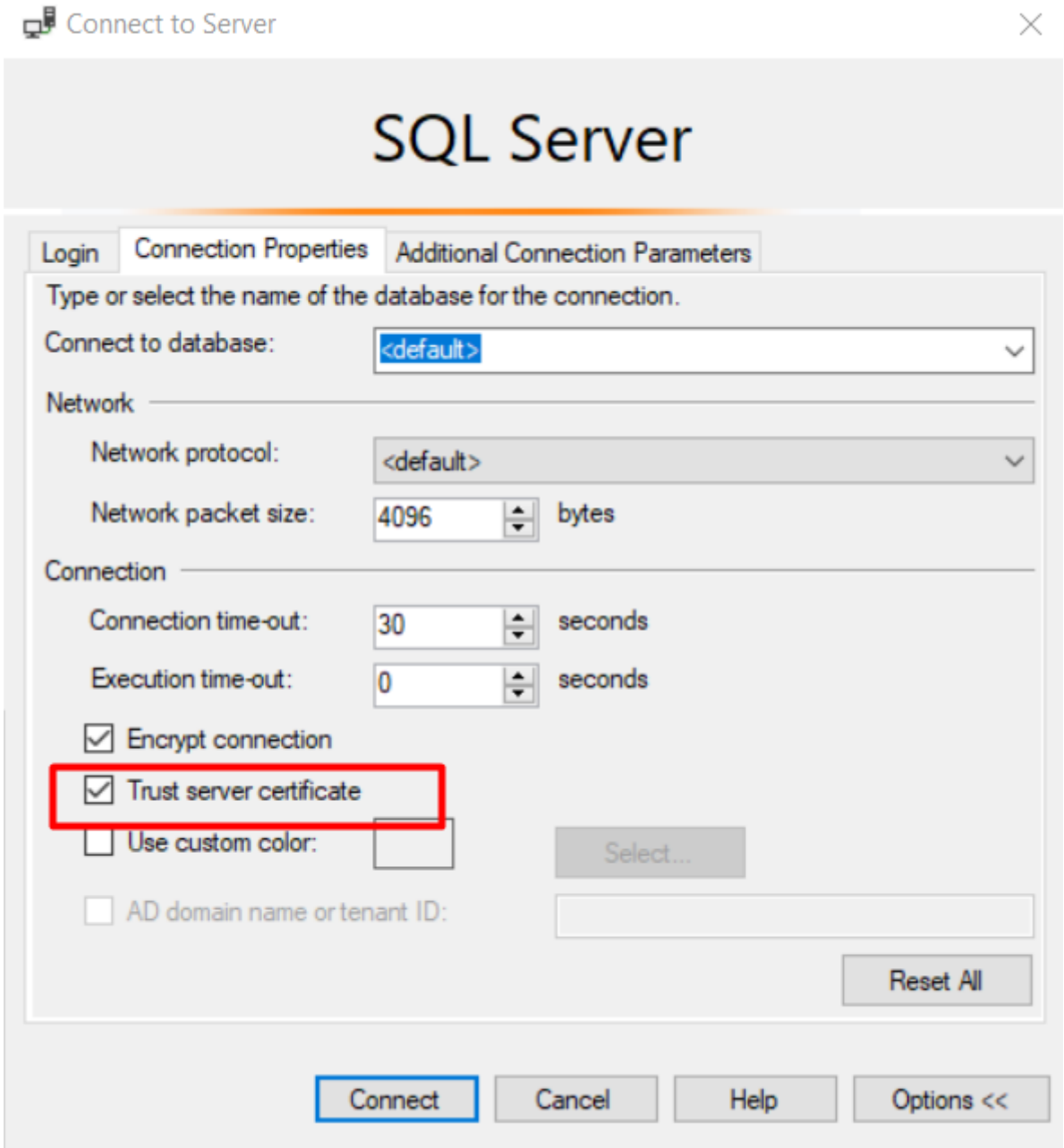
1 @ZafarYousafi you should mark this answer as correct. – Termato Jul 21 '14 at 14:51

6 It is not good to advise setting `TrustServerCertificate` to `true` --this disables certificate checking. That's no better than just setting `Encrypt` to `false` ! – Matt Thomas Mar 30 '17 at 19:34

6 The advice given "TrustServerCertificate=True" in this answer might make the problem go away, but it's terrible advice. Fix the cause, NOT the symptoms. The other part of the answer suggesting installing a CA signed cert is the way to go. – Mitch Wheat Oct 1 '18 at 10:53

1 In newer versions of SSMS you find a little option called "Trust server certificate" in the "Connection Properties" Tab. Checking this boy has the same effect as the commands listed above. – verfluecht Dec 18 '18 at 7:58

96



If you're using SQL Management Studio, please goto connection properties and click on "Trust server certificated"


1,157 7 4

18 It is not a bad advice per se. I would say that you can use it when you need to connect to a development server and do your job, such as coding. As a software developer I constantly struggle with DevOps who don't have time to fix things quickly and I can't afford to waste precious time against deadlines. Weighing data exposure turning off this option depends a lot of your environment, if it's local or remote, how admins set it up, IP restrictions and it can be easily mitigated with other workarounds. You can't say it's a bad advice without having a bit of information about your infrastructure. – OrizG Dec 29 '18 at 1:29

1 You just saved my day. Thanks @ct.tan – Milinda Wickramasinghe Dec 9 '19 at 7:22

1 @OrizG I have a SQL Server installed on a local machine, and I use it for personal projects. At the moment, I don't want to spend a penny with it, so I got myself a free host and tried to configure the server in a way that I Ca-sign the certificates, and exchange them between the server and clients I'll be using to access it. However, because of the free host, I didn't manage to do that with Let's Encrypt. What exactly are the disadvantages of this solution, in comparison with properly doing the certificate exchange, with trusted CA signed certificates? – ccoutinho Feb 20 at 23:29

32

If you're seeing this error message when attempting to connect using SSMS, add `TrustServerCertificate=True` to the Additional Connection Parameters.

edited Jul 15 '19 at 22:08


Dale K
11.5k 8 32 59

answered May 1 '17 at 5:01


vmanne
379 4 5

23 Mitch, you made this same comment on three answers to this question. It might be helpful to other readers if you provided some substantive information or link as to why this is "really, really bad advice." – Shoeless Oct 2 '18 at 15:26

1 @Shoeless Several comments on the accepted answer explain. – Tom Blodget Dec 5 '18 at 22:05

@Shoeless the same reason it's bad in any other certificate scenario -- it enables MITM attacks -- though with SQL Server, you're doing some infrastructure centric setup anyway, so MITM can be mitigated in other ways (i.e. restricting IP access and ensuring that the two machines are directly connected on the same network, etc.) -- Still, it's a bit cringe, but hey, Apple shipped MITM enabled devices for a couple of years before bothering to fix anything? -- So, it's probably fine. 😆 – BrainSlugs83 Aug 19 at 21:43

5

If You are trying to access it through Data Connections in Visual Studio 2015, and getting the above Error, Then Go to Advanced and set `TrustServerCertificate=True` for error to go away.

answered Aug 10 '16 at 1:50


Bhavjot
466 5 15

9 It is not a bad advice per se. I would say that you can use it when you need to connect to a development server and do your job, such as coding. As a software developer I constantly struggle with DevOps who don't have time to fix things quickly and I can't afford to waste precious time against deadlines. Weighing data exposure turning off this option depends a lot of your environment, if it's local or remote, how admins set it up, IP restrictions and it can be easily mitigated with other workarounds. You can't say it's a bad advice without having a bit of information about your infrastructure. – OrizG Dec

1

I got this Issue while importing Excel data into SQLDatabase through SSMS. The solution is to set `TrustServerCertificate = True` in the security section

edited Jul 15 '19 at 22:06

Dale K
11.5k 8 32 59

answered Dec 9 '18 at 8:53

Kanna Reddy
59 5

1

I ran into this error trying to run the profiler, even though my connection had Trust server certificate checked and I added `TrustServerCertificate=True` in the Advanced Section. I changed to an instance of SSMS running as administrator and the profiler started with no problem. (I previously had found that when my connections even to local took a long time to connect, running as administrator helped).

edited Jul 15 '19 at 22:07

Dale K
11.5k 8 32 59

answered Jun 28 '18 at 15:24

Bill
11 2

1

Got hit by the same issue while accessing SQLServer from IIS. Adding TrustServerCertificate=True didnot help.

Could see a comment in MS docs: **Make sure the SQLServer service account has access to the TLS Certificate you are using. (NT Service\MSSQLSERVER)**

Open personal store and right click on the certificate -> manage private keys -> Add the SQL service account and give full control.

Restart the SQL service. It worked.

answered Jun 17 at 10:54

Kaavya T
11 1

0

The same can be achieved from ssms client itself. Just open the ssms, insert the server name and then from options under heading connection properties make sure Trust server certificate is checked.

edited May 10 '18 at 9:34

Zoe
22.1k 13 91 122

answered May 10 '18 at 9:32

Manas
1