Configuring SQL Server Agent in a Safepeak Deployment

How to enable database clients on the SQL Server host to connect through Safepeak

Introduction

This document will describe why and how the SQL Server Agent, the SQL Server Management Studio (SSMS) or any other client installed locally on the SQL Server host need to be configured to access the database through Safepeak.

Summary

Database clients must access the SQL Server database through Safepeak, even if they run locally on the database server host.

The following are perquisites for windows authenticated connection from the SSMS or SQL Server Agent to the local SQL Server Database to succeed:

- The database alias used in the client connection string must be specified using a numeric IP address and not using a hostname (e.g. use 10.254.11.22 and not dbserver.acme.com).
- The following Window registry key must be created and set to configure Windows to allow the local authenticated connection from network source.
  Path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
  Name: DisableLoopbackCheck
  Type: DWORD
  Value: 1

If the client and Windows are not configured correctly the client will fail to connect to the database when using windows authentication[1].

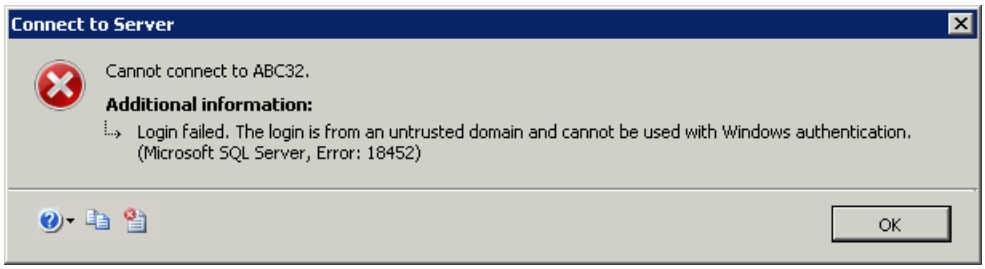
Background and Rational

Clients such as the SQL Server Agent service, the SQL Server Management Studio or SQLCMD that run locally on the SQL server host can still benefit from reduced database server CPU utilization and disk I/O by using the Safepeak cache for data access. This will also allow other clients to reuse the cached results sets from their queries.

More importantly, Safepeak constantly analyses all data access traffic and identifies data modification language (DML) queries and data definition language (DDL) queries that require stale data to be evicted from Safepeak's in-memory cache. This is why any data access to the SQL Server must be done through Safepeak. This is also true for access made by clients running locally on the SQL server.

The Windows Server operating system is by default configured not to allow local windows authenticated access from an external network source - this is exactly the case of the SQL Server Agent or SSMS accessing the local SQL Server database instance via Safepeak. Therefore the client connection and the Windows system need to be configured specifically to allow this.[1]

If the client and Windows are not configured correctly the client will fail to connect to the database; SSMS for instance will report that the connection is from an untrusted domain.



Step by Step Example

The following is a setup procedure example that will guide you through the configuration process. It assumes the following:

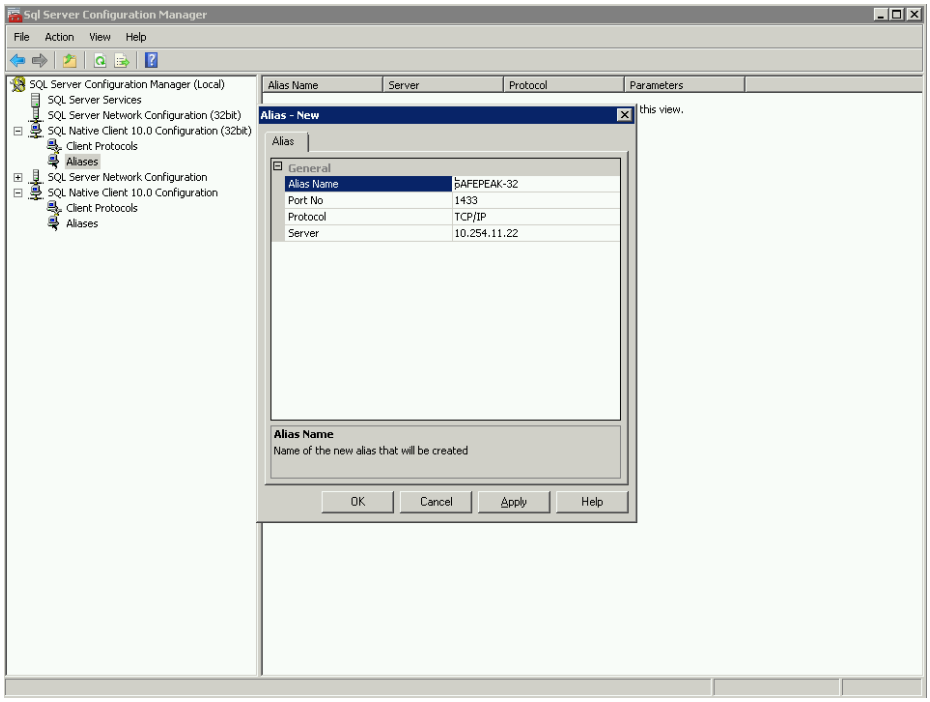
- An SQL Server 2008R2 64-bit installation.
- The Safepeak server IP address is 10.254.11.22.
- The Safepeak port is 1433.

1. Set the database connection aliases.

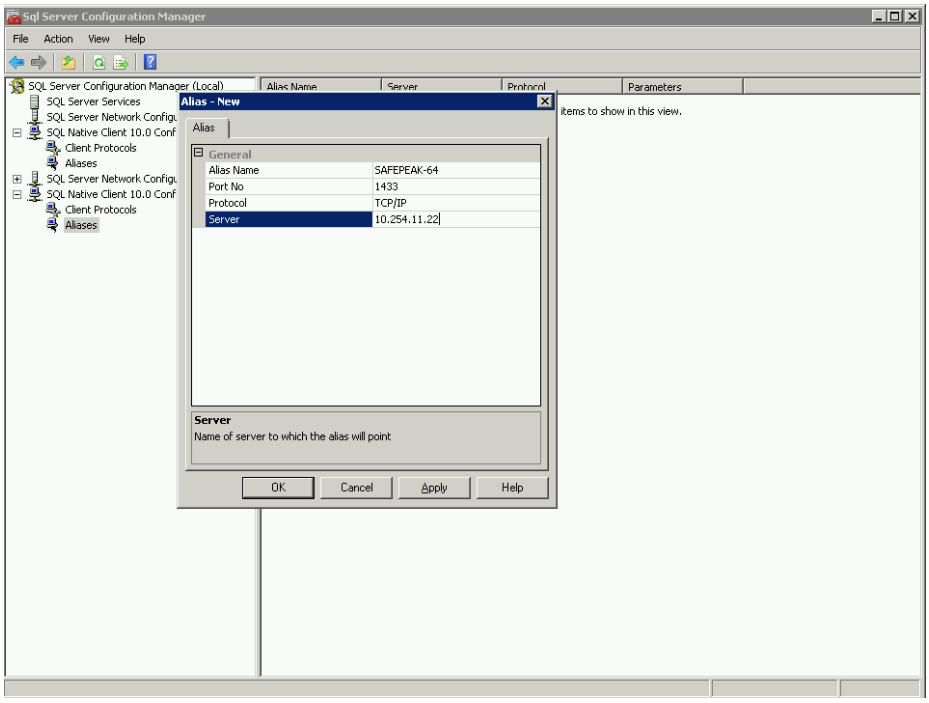
The database alias can be set using the SQL Server Configuration Management utility.

[1] This limitation does not concern SQL Server authentication. Note that beginning with SQL Server 2005, SQL Server Agent does not support SQL Server Authentication. This option is available only when you administer an earlier version of SQL Server.

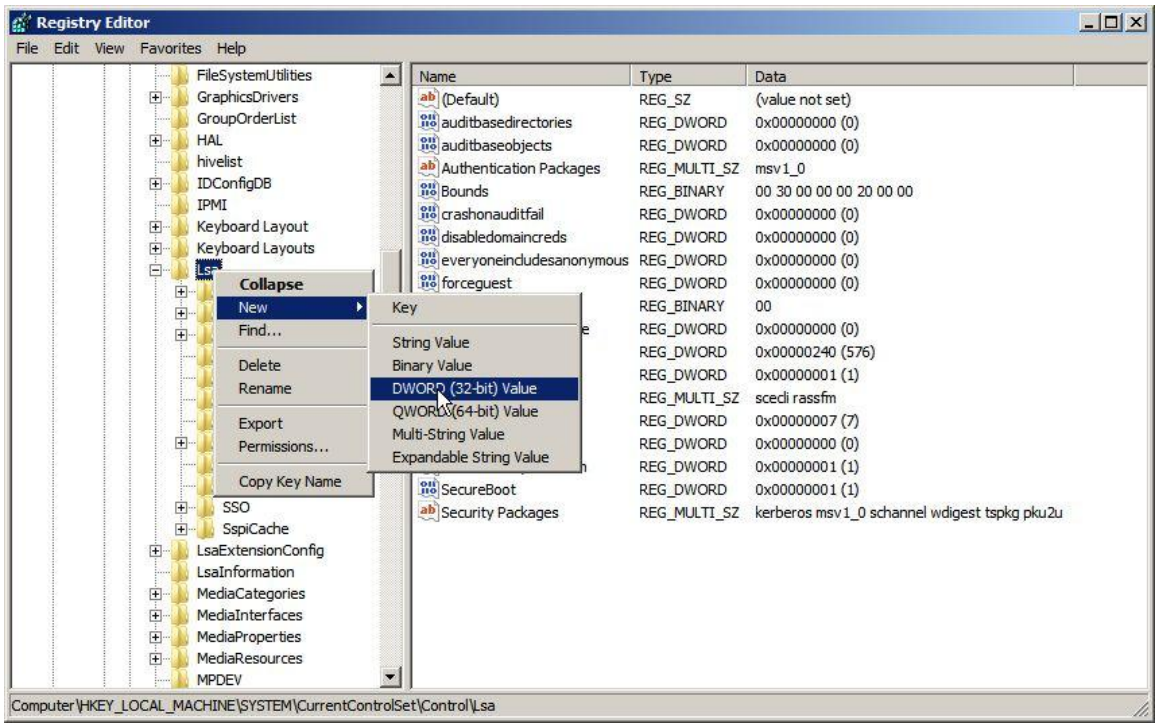
1.1. Set the 32-bit alias for SSMS



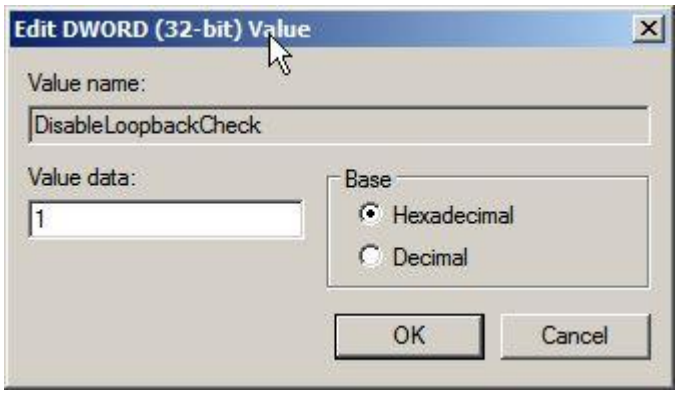
1.2. Set the 64-bit alias for SQL Agent installations on 64-bit hosts



2. Configure the registry.
   The registry can be configured using the windows registry editor (regedit.exe).
   2.1. Create a new DWORD value under the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa path named “DisableLoopbackCheck”



   2.2. Double-click the value name to set it to 1



Alternatively the following Windows PowerShell command can be used:

```
New-ItemProperty HKLM:\System\CurrentControlSet\Control\Lsa –Name “DisableLoopbackCheck"
 -value "1" -PropertyType dword
```

3. Connect SSMS using the 32-bit alias.

4. Set the connection alias for the SQL Server Agent.