

# SQL Insights Troubleshooting Guide

Last updated by | Ricardo Marques | Nov 3, 2022 at 1:44 AM PDT

---


## Contents

- Introduction
  - What does this page cover?
  - What are the support boundaries for SQL insights?
- Links to Documentation
  - Internal Documentation
  - Public Documentation
- Troubleshooting in Azure Support Center
- Viewing the error log
- Common Issues
  - Connectivity Error During Setup
  - Trying to Use SQL Insights on Unsupported Databases
- Common Customer Questions
  - What is the performance impact of SQL insights?
  - What exact queries are run to collect the data?
  - Can I write my own custom queries?
  - Can I build my own visualizations?
- Steps to enable monitoring for a SQL database
  - 1. Customer creates a SQL user that will be used to login t...
  - 2. Customer stores the credentials of this SQL user in a sec...
  - 3. Customer creates the monitoring VM (owned by Monitor)
  - 4. Customer configures networking settings to allow the m...
  - 5. Customer creates a monitoring profile (owned by Monit...
  - 6. Customer adds the monitoring VM to the monitoring pr...
  - 7. Customer is able to view the collected data

## Introduction

---

### What does this page cover?

This page is a troubleshooting guide for SQL insights. This TSG is intended for the SQL POD. You can also see the [TSG for the Azure Monitor POD](#) .

For an overview of SQL insights and for a glossary of technical terms used in this document, see the overview at [Azure Monitor for SQL \(aka SQL insights\)](#).




## What are the support boundaries for SQL insights?

See [support boundaries](#).






## Links to Documentation

---

### Internal Documentation

- [TSG for the Azure Monitor POD](#) 
- [SQL Insights Troubleshooting with ASC](#)
- [Deep dive presentation from product group - recorded March 16, 2021](#) 
- [Technical documentation from product group](#) 

### Public Documentation

- [Overview - SQL insights](#) 
- [FAQ - SQL insights](#) 
- [Enable SQL insights](#) 
- [Create alerts with SQL insights](#) 
- [Troubleshooting SQL insights](#) 

## Troubleshooting in Azure Support Center

---

ASC will provide an overview of the monitoring profiles, monitoring VMs, and monitoring settings the customer has created. See [SQL Insights Troubleshooting with ASC](#) for instructions on how to use ASC for SQL insights.

## Viewing the error log

---

The monitoring VM emits error logs that can help determine the cause of any connectivity issue. These error logs are sent to the customer's Log Analytics workspace and are easily accessible by the customer on the Azure Portal. See [Issues collecting data from SQL databases](#) for instructions on how the customer can view these error logs.

With customer permission, CSS is able to use ASC to read these error logs directly from the customer's Log Analytics workspace. See [view collection error logs](#) for instructions on how to do this. Typically, this should not be necessary; the customer can just share the error messages with you.

## Common Issues

---

### Connectivity Error During Setup

Most issues with SQL insights occur during the onboarding process. Customers may make mistakes during setup or may have unexpected configurations that pose challenges for our systems. Most issues owned by SQL will be connectivity issues: "How can get the agent in the monitoring VM to connect to my SQL database?". Treat these as standard "How To" connectivity tickets and use [Connectivity: Configuration and How To Questions](#) to assist.

ASC can be helpful to detect these issues. See the [SQL Insights tab on ASC Resource Explorer](#) or look for connectivity-related Insights on the Case Overview page. If there are no Insights, try using the "Edit & Run Again" button on the ASC Case Overview page to re-run the Insights on the database of interest.

If the setup issue is about Azure Monitor rather than SQL, review the [support boundaries](#) and transfer to Azure Monitor when appropriate.

## Trying to Use SQL Insights on Unsupported Databases

SQL insights does not support all database types. When customers try to use SQL insights to monitor unsupported databases, they may encounter seemingly unrelated error messages like "Error in plugin: Script AzureSQLDBSchedulers failed: mssql: The user does not have permission to perform this action" .

For a full list of supported and unsupported scenarios, see [Supported versions](#) ☐. For a summary:

- **Azure SQL Database elastic pools:** SQL insights will not work for databases inside elastic pools. This is because permissions work differently for these databases. Specifically, the `VIEW DATABASE STATE` permission is not supported.
  - We have seen customers successfully setup SQL insights for a database, then move that database into an elastic pool. In this case, SQL insights will begin to display the above permission error until it's moved out of the elastic pool
  - We are working to support elastic pools - hopefully sometime in 2022.
- **Azure SQL Database low service tiers:** SQL insights will not work for databases on Basic, S0, S1, and S2 [service tiers](#). Similar to elastic pools, the above permission error will be shown for low service tier databases.
  - A new server role coming in T61 (late 2021 or early 2022) will add support for these low service tiers

## Common Customer Questions

---

### What is the performance impact of SQL insights?

Internal testing suggests that the performance impact of SQL insights is extremely low: approximately 1-2% of total CPU and memory capacity. The product team ran these tests across numerous tiers of SQL DB, SQL MI, and SQL Server. These tests used query frequencies ranging from 15 seconds to 180 seconds.


### What exact queries are run to collect the data?

See [Data collected by SQL insights](#) ☐ for an overview on all the data sets available in SQL insights. The exact query text can be found in the open source [Telegraf](#) ☐ repo on GitHub. Queries for SQL DB and MI are found in [azuresqlqueries.go](#) ☐, and queries for SQL Server and SQL VM are found in [sqlserverqueries.go](#) ☐.

### Can I write my own custom queries?


Only the preset queries shown [here](#) ☐ are supported by SQL insights right now. This is a common customer request. We are considering different strategies to accomplish this that comply with our PII and security guidelines. We currently aren't publically promising this capability, and we do not yet have an ETA.

### Can I build my own visualizations?

Yes. Customers can follow the documentation for [Azure Monitor Workbooks](#)  to create their own visualizations on top of the data gathered by SQL insights.


## Steps to enable monitoring for a SQL database

---

Below are all the steps needed to enable monitoring a SQL database. See [Enable SQL insights](#)  for more details about each step.

1. Customer creates a SQL user that will be used to login to the database and run DMVs (owned by SQL)
2. Customer stores the credentials of this SQL user in a secret in an Azure Key Vault
3. Customer creates the monitoring VM (an Azure VM) that will be used to perform the monitoring
4. Customer configures networking settings to allow the VM from step 3 to connect to the SQL database (owned by SQL)
5. Customer creates a monitoring profile and specifies what data they want to collect and how frequently they want to collect it
6. Customer adds the monitoring VM to the monitoring profile, and provides a connection string specifying the database/username from step 1 and the secret name from step 2
7. Customer is able to view the collected data in Azure Monitor workbooks

### 1. Customer creates a SQL user that will be used to login to the database and run DMVs (owned by SQL)

The monitoring user is used to login to the customer's SQL database and run queries to gather monitoring data. On each database the customer wants to monitor, there must be a user that will perform the monitoring. Each database can utilize a different monitoring user and password. This user only needs a minimal set of permissions. [Refer to our documentation](#)  for instructions. There are different instructions for each flavor of SQL Azure.

The SQL POD's responsibility here is to assist customers with creating the user with the appropriate permissions.

To assist with customers with this, see the internal [Logins and users](#) docs.

### 2. Customer stores the credentials of this SQL user in a secret in an Azure Key Vault (owned by Monitor)

Issues with this should mostly be handled by the Azure Monitor CSS POD. See Azure Monitor's [Store secrets in Key Vault](#) TSG, review the [support boundaries](#), and transfer to Azure Monitor when appropriate.


This step (saving credentials on Azure Key Vault) is mandatory, and we do not recommend to use credentials in plain text on the config.

Anyway, if the customer do not wish to use AKV, he can workaround by giving an empty KV and still enter plain text password in the config as there is no validation on config to stop the user from doing so. **As a guideline and recommendation, we ask customers not to hardcode password but instead store it in KV.**

### 3. Customer creates the monitoring VM (owned by Monitor)

Issues with this should mostly be handled by the Azure Monitor CSS POD. See the [Azure Monitor](#) TSG, review the [support boundaries](#), and transfer to Azure Monitor when appropriate.

#### 4. Customer configures networking settings to allow the monitoring VM to connect to the SQL database (owned by SQL)

Customers will likely need to configure their networking settings to allow connections from new places (from the monitoring VMs). [Refer to our documentation](#)  for instructions. There are different instructions for each flavor of SQL Azure.

The SQL POD's responsibility here is to assist customers with allowing the monitoring VM to access the SQL database. Customers may have unique networking, firewall, or security configurations that can prevent successful connections.

To assist with customers with this, see the internal [Connectivity: Configuration and How To Questions](#) docs.

#### 5. Customer creates a monitoring profile (owned by Monitor)

Monitoring profiles are how customers specify what data they want to collect and how frequently they want to collect it. Within a single profile, customers can select different sets of queries for SQL DB, SQL MI, and SQL VM. However, within a single profile customers can choose only 1 collection frequency.

Issues with this should mostly be handled by the Azure Monitor CSS POD. See Azure Monitor's [Issues creating a monitoring profile](#) TSG, review the [support boundaries](#), and transfer to Azure Monitor when appropriate.

#### 6. Customer adds the monitoring VM to the monitoring profile (owned by Monitor)

Issues with this should mostly be handled by the Azure Monitor CSS POD. See the [Azure Monitor](#) TSG, review the [support boundaries](#), and transfer to Azure Monitor when appropriate.

In this step, customers provide the connection strings specifying the databases/usernames from step 1 and the secret names from step 2.

Sometimes, customers only need to monitor one flavor of SQL, and thus only populate one of the 3 connection string lists ( `sqlManagedInstanceConnections` , `sqlAzureConnections` , and `sqlVmConnections` ). For example, in the screenshot below, only the `sqlManagedInstanceConnections` list is populated. In this case, the customer still needs to keep the 2 other (highlighted) lists, even though they are empty. If one of the lists is deleted, the Azure Monitor agent may crash.

```
secrets: {  
  "DemoPassword": {  
    "name": "DemoPassword",  
    "keyvault": "https://masree-telegraf-vault.vault.azure.net/"  
  }  
},  
"version": 1,  
"parameters": {  
  "sqlManagedInstanceConnections": [  
    "sqlserver://MonitoringUser:$DemoPassword@mymanagedinstance.public.72c37a30b974.database.windows.net",  
    "sqlAzureConnections": [],  
    "sqlVmConnections": []  
  ]  
}
```

## 7. Customer is able to view the collected data

Customers can visualize the data in [Azure Monitor Workbooks](#) or can query the data directly in Log Analytics.

**How good have you found this content?**

