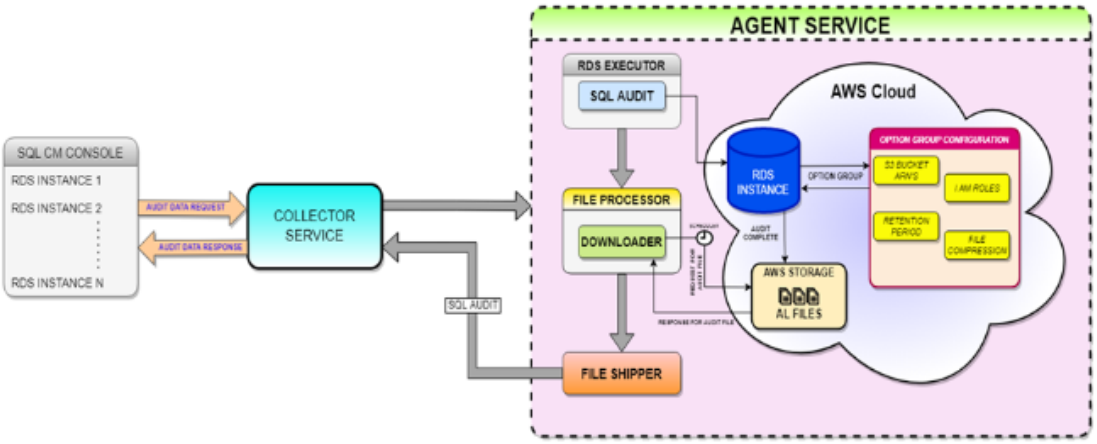
How the SQL Compliance Manager Cloud Agent works

SQL Compliance Manager offers an improved architecture that allows registering cloud instances with its new Cloud Agent Service. The SQL Compliance Manager Cloud Agent runs under the SQL Compliance Manager Agent Service account on each registered SQL Server computer that hosts the audited instances and databases inside the AWS Cloud. The Cloud Agent gathers SQL events logs from audited SQL Server on cloud instances and databases and then sends the raw data to the Collection Server.

Architecture

Once a cloud instance is registered to audit events, the Collector service receives the audit data request from your registered cloud instance and invokes the Cloud Agent Service to start auditing your cloud instance.

The audited cloud instance is based on the Option Group and S3 bucket Configuration, and after audit completion, the cloud instance transmits the audit file to the AWS S3 bucket. Then, the File processor downloads the new *.*sqlaudit* file from the AWS S3 bucket parses the file and transfers it to the File Shipper. Finally, the SQL Audited files are transferred to the Collector Service, where the files are processed, and the data is updated in the SQL Compliance repository.



Pre-Requisites

The following access and permissions are required on AWS RDS in the AWS console before registering an RDS instance through the SQL CM Console.

- Access to an AWS Account
- Permission to create a directory service for RDS (if RDS is registered using windows auth).
- Permission to create Microsoft AD Windows authentication (if RDS is registered using windows auth).
- Permission to configure and add permissions to the IAM role in RDS.
- Permission to create Option Group and lists of S3 buckets.

Create an Option Group

An *Option Group* specifies features called options that are available in your registered Amazon RDS DB instance. Options can have settings that specify how the option works. When you associate a DB instance with an Option Group, the specified options, and option settings are enabled for that DB instance.

Configure your Option Group by using the SQLcm Configuration Wizard for the Agent RDS configuration, or create an option group by using the AWS Management Console.

Create an Option Group from the AWS console

Login to your AWS account and follow the steps below:

1. In the main navigation pane, select the **Options groups** from the sidebar menu.
2. In the Create option group window, fill out the Option group details and click **Create**.
    - **Name** - the name of the option group.
    - **Description** - a brief description of the option group.
    - **Engine type** - choose the DB engine that you want.
    - **Major engine version** - choose the major version of the DB engine that you want.
3. Next, select the created Option Group and select **Add option**.
4. In the S3 destination section, fill out the required S3 Bucket information.
5. Next, choose the **Create a New Role** option, and provide a name for the IAM role.
    a. Make sure to check the permissions policies for the IAM role.
6. In the Additional configuration section, make sure to enable the **compression** and **retention** options.
7. Select the **Database** option from the sidebar menu, and in the Database options section, select the recently created option group from the Option group dropdown menu.
8. Finally, in the Manage IAM roles section, select the role for the instance.

Important notes on RDS auditing

- RDS does not support the Middle East (Bahrain) region and works only with SQL Server versions 2012 and above.
- The Max File Size for SQL Audit on the RDS instance limit is 50 MB.
- Before and After Data is not supported on the RDS instance due to the limitation of creating trusted assemblies using sql script. BAD operations are removed from the properties, reports, alerts, and summary tabs.