Microsoft SQL Server

The IBM® Security QRadar® DSM for Microsoft SQL Server collect SQL events by using the syslog, WinCollect Microsoft SQL, or JDBC protocol.

The following table identifies the specifications for the Microsoft SQL Server DSM:

Table 1. Microsoft SQL Server DSM

Specification	Value
Manufacturer	Microsoft
DSM name	SQL Server
RPM file name	DSM-MicrosoftSQL-*QRadar-version-Build_number*.noarch.rpm
Supported versions	2008, 2012, and 2014 (Enterprise editions only)
Event format	syslog, JDBC, WinCollect
QRadar recorded event types	SQL error log events
Automatically discovered?	Yes
Includes identity?	Yes
More information	Microsoft website (http://www.microsoft.com/en-us/server-cloud/products/sql-server/)

You can integrate Microsoft SQL Server with QRadar by using one of the following methods:

JDBC Microsoft SQL Server Enterprise can capture audit events by using the JDBC protocol. The audit events are stored in a table view. Audit events are only available in Microsoft SQL Server 2008, 2012, and 2014 Enterprise.

WinCollect
You can integrate Microsoft SQL Server 2000, 2005, 2008, 2012, and 2014 with QRadar by using WinCollect to collect ERRORLOG messages from the databases that are managed by your Microsoft SQL Server. For more information, see your WinCollect documentation.

To integrate the Microsoft SQL Server DSM with QRadar, use the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the Microsoft SQL Server RPM on your QRadar Console.
2. For each instance of Microsoft SQL Server, configure your Microsoft SQL Server appliance to enable communication with QRadar.
3. If QRadar does not automatically discover the Microsoft SQL Server log source, create a log source for each instance of Microsoft SQL Server on your network.

Microsoft SQL Server preparation for communication with QRadar

To prepare Microsoft SQL Server for communication with QRadar, you must create an audit object, audit specification, and database view.

Creating a Microsoft SQL Server auditing object

Create an auditing object to store audit events.

Procedure

1. Log in to your Microsoft SQL Server Management Studio.
2. From the navigation menu, select **Security** > **Audits**.
3. Right-click **Audits** and select **New Audit**.
4. In the **Audit name** field, type a name for the new audit file.
5. From the **Audit destination** list, select **File**.
6. From the **File path** field, type the directory path for your Microsoft SQL Server audit file.
7. Click **OK**.
8. Right-click your audit object and select **Enable Audit**.

Creating a Microsoft SQL Server audit specification

Create an audit specification to define the level of auditing events that are written to an audit file.

Before you begin

You must create an audit object. See "Creating a Microsoft SQL Server auditing object."

About this task

You can create an audit specification at the server level or at the database level. Depending on your requirements, you might require both a server and database audit specification.

Procedure

1. From the Microsoft SQL Server Management Studio navigation menu, select one of the following options:
   - **Security** > **Server Audit Specifications**
   - **<Database>** > **Security** > `Database Audit Specifications`
2. Right-click **Server Audit Specifications**, and then select one of the following options:
   - **New Server Audit Specifications**
   - **New Database Audit Specifications**
3. In the **Name** field, type a name for the new audit file.
4. From the **Audit** list, select the audit object that you created.
5. In the **Actions** pane, add actions and objects to the server audit.
6. Click **OK**.
7. Right-click your server audit specification and select one of the following options:
   - **Enable Server Audit Specification**
   - **Enable Database Audit Specification**

Creating a Microsoft SQL Server database view

Create the dbo.AuditData database view to allow QRadar to poll for audit events from a database table by using the JDBC protocol. The database view contains the audit events from your server audit specification and database audit specification.

Procedure

1. From the Microsoft SQL Server Management Studio toolbar, click **New Query**.
2. Type the following Transact-SQL statement:

```
create view dbo.AuditData as
     SELECT * FROM sys.fn_get_audit_file
     ('<Audit File Path and Name>',default,default);
     GOa
```

   For example:

```
create view dbo.AuditData as
     SELECT * FROM sys.fn_get_audit_file
     ('C:\inetpub\logs\SQLAudits*',default,default);
     GO
```

3. From the Standard toolbar, click **Execute**.

Configuring a Microsoft SQL Server log source

Use this procedure if your QRadar Console did not automatically discover the Microsoft Windows Security Event Log log source.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **Log Sources** icon.
4. From the **Log Source Type** list, select **Microsoft SQL Server**.
5. From the **Protocol Configuration** list, select a protocol to use.
6. Configure the remaining parameters.
7. Click **Save**.
8. On the **Admin** tab, click **Deploy Changes**.