

SQL Server Data Classification with SQL Server 2019 and Azure SQL Database

Steve Hughes

Director of Consulting

June 2020

About Steve



- Director of Consulting
- 20+ Years with SQL Server, Microsoft BI, and Azure
- <https://www.linkedin.com/in/dataonwheels/>
- steve@dataonwheels.com
- Blog: www.dataonwheels.com – Look for deck and follow up here



Beyond the Database

- Current protections in SQL Server to protect the database
 - Encryption
 - Row Level Security (RLS)
 - Active Directory
- Focus on data at rest or in motion



Microsoft®
SQL Server®



Data Classification & Labeling

- Data Classification has multiple purposes
 - Classify to identify sensitive data
 - Classify to organize data
- Labeling
 - Classification labeling makes sensitive data visible
- SQL Server Can Help!
 - SQL Server Management Studio 17.5 or later – Data Discovery & Classification
 - SQL Server 2012 and later supports classification labeling in the database

Today's Demos Use

- SQL Server Management Studio 18.5
 - 18.4+ Allows you to manage the information protection policy
- SQL Server 2019 (Developer Edition)
 - `sys.sensitivity_classifications` system catalog view

SQL Server 2012, 2014, 2016, 2017 use Extended Properties to support labeling

- `sys_information_type_name`
- `sys_sensitivity_label_name`



Let's classify, label, report

The screenshot shows the SQL Server Enterprise Manager interface. The Object Explorer on the left displays the server hierarchy for 'STEVEH-YOGA\DOWSQL2019 (SQL Server 15.0.207)'. The 'WideWorldImportance' database is selected, and a context menu is open over it. The 'Tasks' menu item is highlighted in yellow. A secondary menu is open over 'Tasks', with 'Data Discovery and Classification' highlighted in yellow. A third menu is open over 'Data Discovery and Classification', with 'Classify Data...' highlighted in yellow. Other options in the 'Data Discovery and Classification' menu include 'Generate Report...', 'Set Information Protection Policy File...', 'Export Information Protection Policy...', and 'Reset Information Protection Policy to Default'. The 'passm' logo is visible in the bottom left corner.

Object Explorer

Connect

STEVEH-YOGA\DOWSQL2019 (SQL Server 15.0.207)

- Databases
 - System Databases
 - Database Snapshots
 - WideWorldImportance
 - WideWorldImportanceDW
- Security
- Server Objects
- Replication
- PolyBase
- Always On High Availability
- Management
- Integration Services
- SQL Server Agent (Service)
- XEvent Profiler

Context Menu:

- New Database...
- New Query
- Script Database as
- Tasks
- Policies
- Facets
- Start PowerShell
- Azure Data Studio
- Reports
- Rename
- Delete
- Refresh
- Properties

Tasks Sub-Menu:

- Detach...
- Take Offline
- Bring Online
- Stretch
- Encrypt Columns...
- Data Discovery and Classification
- Vulnerability Assessment
- Shrink
- Back Up...
- Restore
- Mirror...
- Launch Database Mirroring Monitor...
- Ship Transaction Logs...
- Generate Scripts...
- Generate In-Memory OLTP Migration Checklists

Data Discovery and Classification Sub-Menu:

- Classify Data...
- Generate Report...
- Set Information Protection Policy File...
- Export Information Protection Policy...
- Reset Information Protection Policy to Default

Steps in SSMS

1. Choose the database to discover data on
2. Use the Classify Data ... tool
3. Review results by clicking results bar
 1. Columns discovered
 2. Information Type
 3. Sensitivity Label
4. Accept Selected Recommendations
5. Add Classification
6. Save
7. View Report

Be Aware

- Your mileage will vary when not using English
- Additional GPDR types may not be identified yet
- Expect ongoing improvements
 - The tool is delivered with SSMS not SQL Server



Built In Information Types

- Networking
- Contact Info
- Credentials
- Credit Card
- Banking
- Financial
- Other
- Name
- National ID
- SSN
- Health
- Data of Birth
- n/a

Built In Sensitivity Labels

- Public
- General
- Confidential
- Confidential – GPDR
- Highly Confidential
- Highly Confidential – GPDR
- [n/a]

Data Classification in Azure

- Part of the Advanced Data Security with SQL Database, SQL Managed Instance, and Synapse (in preview)
 - Advanced Data Security incurs an additional cost - \$15/server/month
 - Azure supports access logging with classified data
-
- Let's check out Azure now

Data Is Classified, Now What?

- Let's look at Information Protection Policies in SQL Server
 - You can customize this to match what you need
- Microsoft is looking at more improvements and capabilities
 - Look for new capabilities as part of SSMS
- Azure SQL Database has auditing available built in to support IP policies, SQL Server does not have this capability built in yet
 - Triggers potentially can be used in SQL Server if Audit of these are required, but still a manual process

We have a great start here and improvements will continue to come in SSMS.

Have Any Questions?



www.dataonwheels.com – Look for deck and follow up here

