IBM Data and Application Risk Scanner

Version: 1.1.0

Date: 01/16/2017

Contents

Introduction

Use this document to install and configure the IBM Data and Application Risk Scanner for QRadar.

Description of the Application

Data privacy and security are the most pressing concerns that any organization must face. Previously within the European Union each country required different levels of compliance, the newly announced General Data Protection Regulation (GDPR) expands and standardizes data protection rules across the whole European Union.

Use the IBM Data and Application Risk Scanner application for QRadar to get a preview of the risk associated with applications and databases in your environment. For databases, this new QRadar application performs a lightweight scan of your Oracle databases searching for GDPR type of data. Only one data source will be scanned at a time. The new QRadar application also calculates an estimate of the vulnerability and risk distribution associated with applications and databases in your environment.

The application includes links for additional information on Guardium and IBM Application Security on Cloud, and how to fully protect your database and application assets.

Target Audience

- QRadar clients who do not have Guardium, or have limited deployment of Guardium.
- QRadar clients who have not used IBM's AppScan or Application Security on Cloud.
- The user of this application is a QRadar admin or Security Analyst with access to QRadar.

Installation and Configuration

Pre-Requisites

A functional and licensed installation of QRadar SIEM version 7.2.7 or higher is required.

Installation

1. Download the IBM Data and Application Risk Scanner from the IBM Security App Exchange Portal (https://exchange.xforce.ibmcloud.com/hub).
2. Login as an administrative user.
3. Go to the Admin tab and click Extensions Management in the System Configuration section.
4. Click Add, choose the application file downloaded and then click Add again.
5. Refresh the page to see IBM Data and Application Risk Scanner tab.

Configuration

1. The user of IBM Data and Application Risk Scanner must provide the data source details for connecting to the Oracle database they wish to scan for GDPR type of data. The data source details involve database type, user name, password, hostname/IP, port number, service name and connection property.
2. The user of IBM Data and Application Risk Scanner should create a role and grant select any table and any dictionary to this role. Then grant this role to the user that is going to execute classification.

   Example:

   Create role g_classifier;

   grant select any table to g_classifier;

   grant select any dictionary to g_classifier;

   create user g_classify_user identified by guardium;

   grant connect, g_classifier to g_classify_user;

   alter user g_classify_user default role all;

Un-installing the Application

1. Login as an administrative user.
2. Go to the Admin tab and click the Extensions Management icon in the System Configuration Section.
3. Select the IBM Data and Application Risk Scanner and click Uninstall.

Using the Application

Use the IBM Data and Application Risk Scanner application for QRadar to get a preview of the GDPR risk associated with applications and databases in your environment. For databases, this new QRadar application performs a lightweight scan of your Oracle databases searching for GDPR type of data. Only one data source will be scanned at a time. The new QRadar application also calculates an estimate of the vulnerability and risk distribution associated with applications and databases in your environment.

Types of GDPR data

The application performs a lightweight scan of the database looking for GDPR type of data using a variety of techniques including meta-data search and pre-defined regular expressions. Examples of GDPR types of data include: international and U.S. phone numbers, international passport numbers, and email addresses (@).

Risk types

For databases, the Risk types are High, Medium and Unknown.

When the Risk type is High, this is indicative of GDPR data found.

When the Risk type is Medium, this is indicative of GDPR data not found or the scan has timed-out.

When the Risk type is Unknown, this is indicative of a network error or database exception interfering with the scan or the GDPR scan has not run yet.

For applications, the Risk types are High, Medium and Low.

Timeout

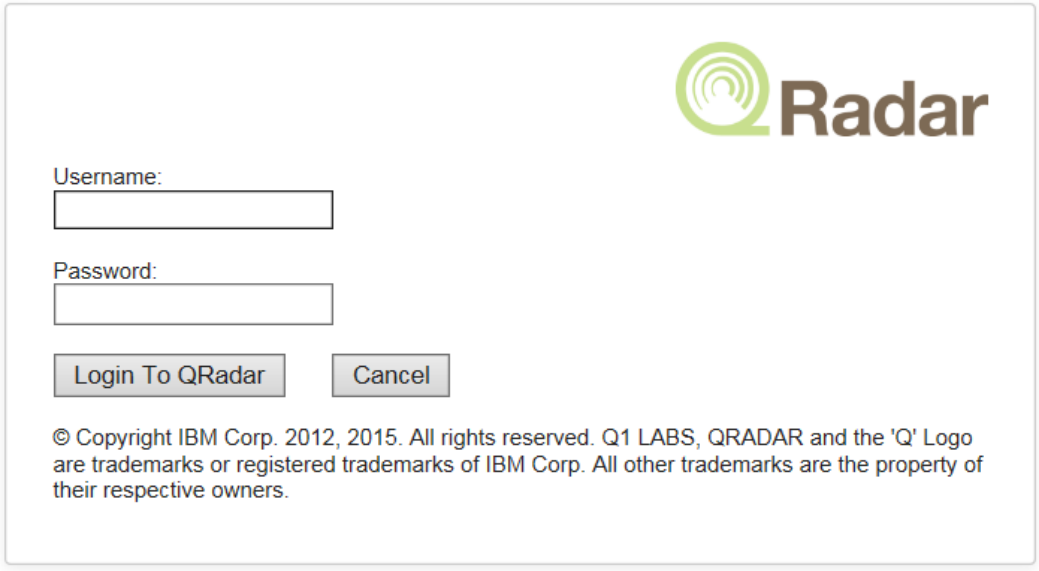
When initiating a scan of GDPR type of data for a given database, the application will only do a partial scan of that database. This means that there is an upper limit on the number of tables scanned and on the number of rows considered for each table. The scan returns immediately after the first instance of GDPR type of data has been discovered. There is also an overall upper limit of 20 minutes on the time the scan takes.

If no assets are found during the scan, a message will display: Scan completed. No asset found.

This application scans for QRadar log activities every 10 minutes looking for databases and applications that are registered with QRadar.

Log-in page

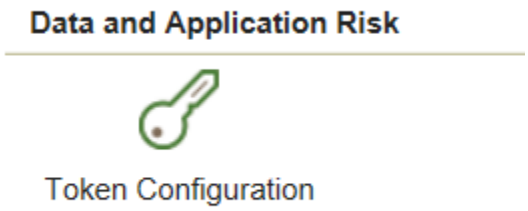
Log-in to QRadar.

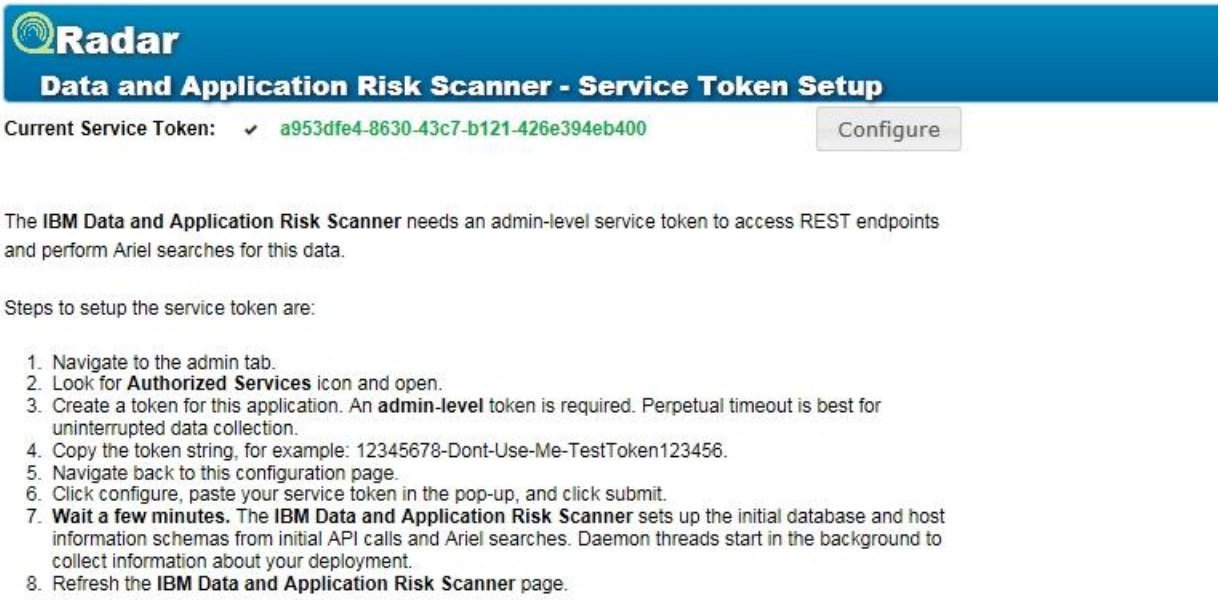


Then select the Data and Applications Risk (Data/App Risk) tab.

If this is the first use of the IBM Data and Application Risk Scanner application, then the Service Token Setup screen below will appear. The IBM Data and Application Risk Scanner needs an admin-level service token to access REST endpoints and perform Ariel searches for this data. Print out the screen below which makes it easier to follow the steps to setup the service token.

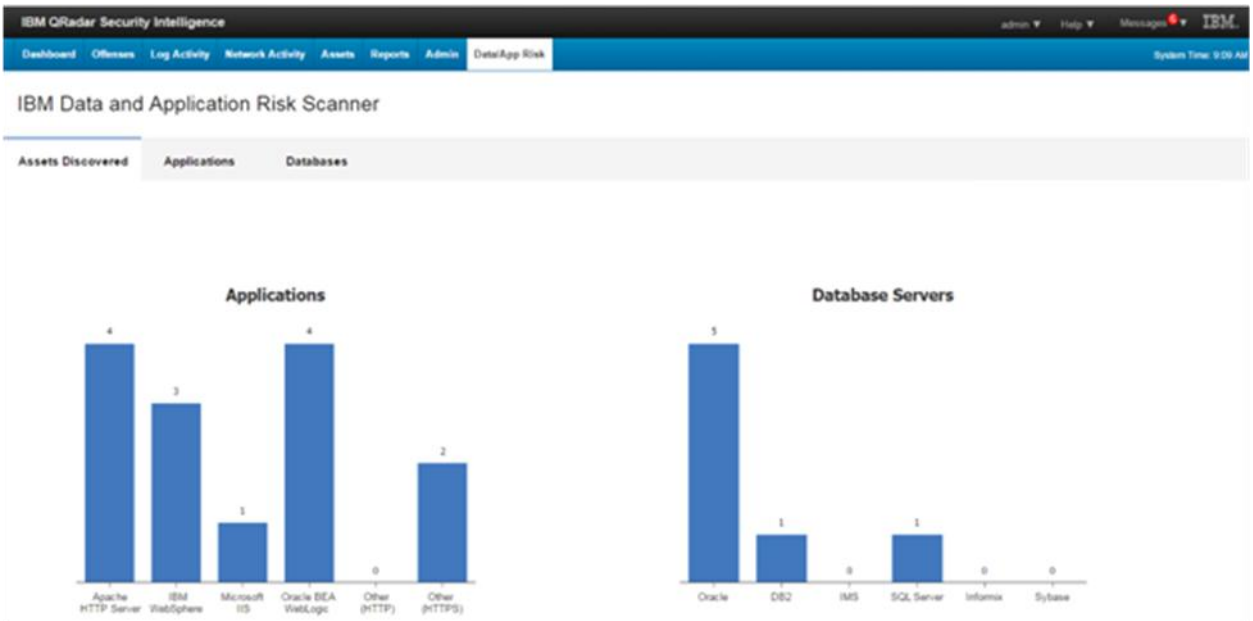
The Service Token Setup screen can also be retrieved from the Admin tab, Plug-ins, Data and Applications Risk, Token Configuration.





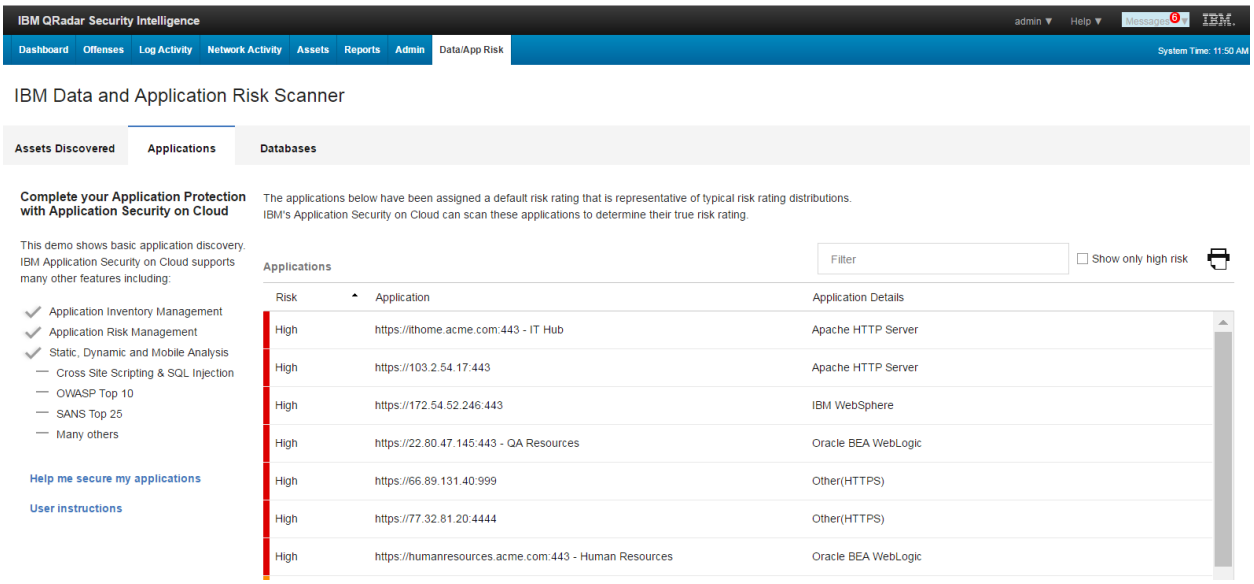
Assets Discovered tab

This shows the Assets discovered - applications and database servers - in the scan.



Applications tab

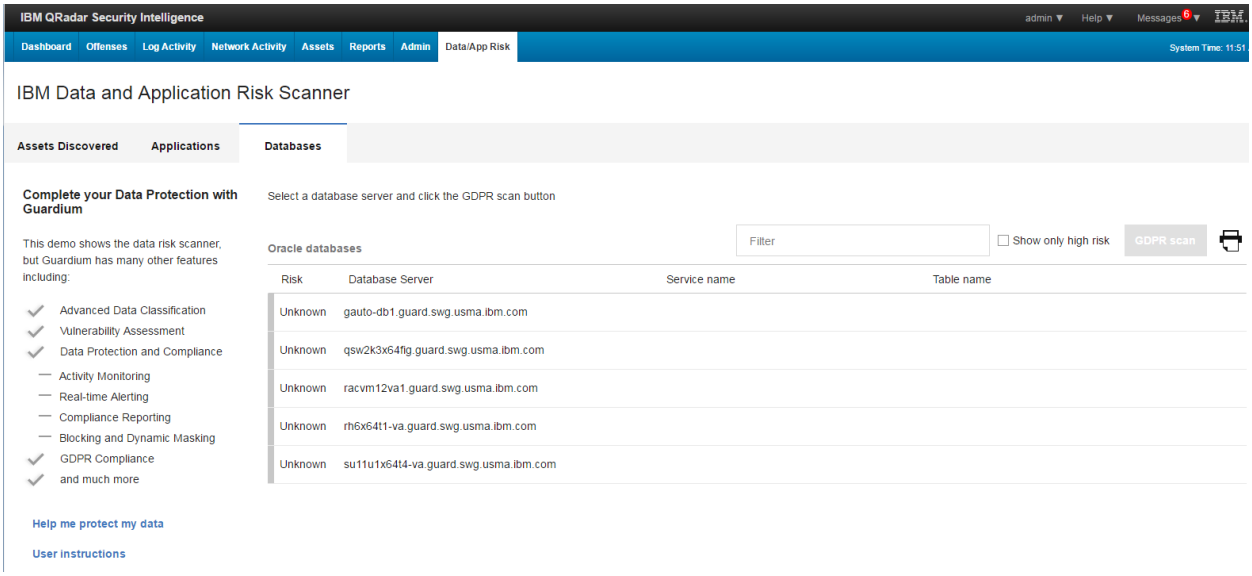
From the Applications tab, review the discovered application assets. The applications have been assigned a default risk rating that is representative of typical risk rating distributions. IBM's Application Security on Cloud can be used to scan these applications to determine their true risk rating.



Databases tab

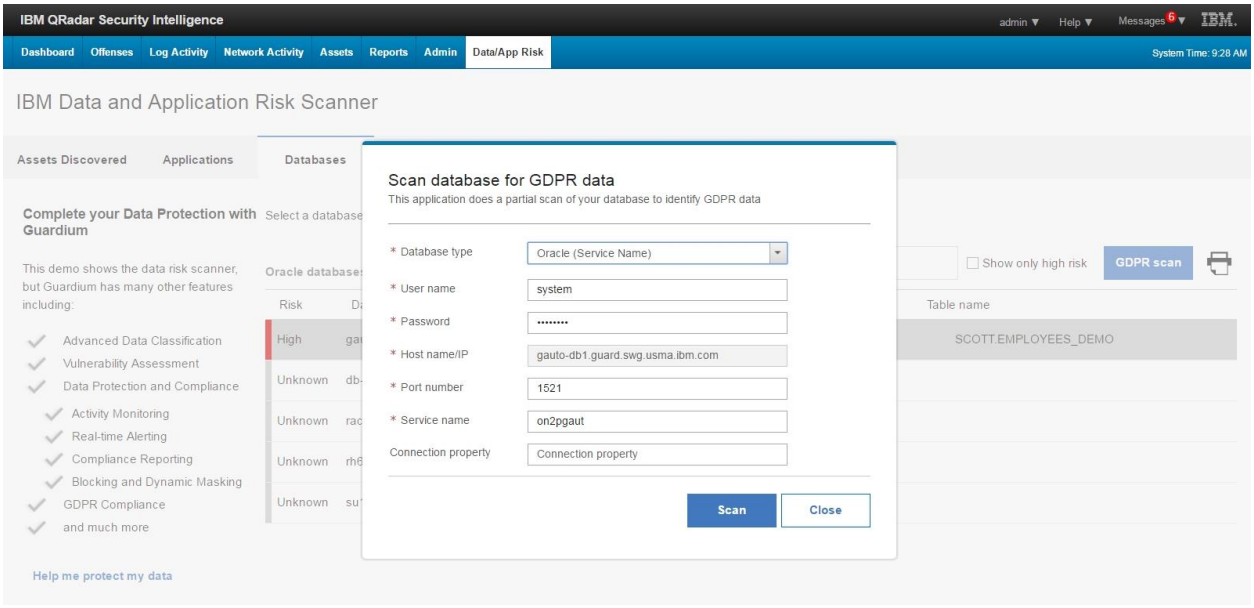
Go to the Databases tab.

Select a database server and click the GDPR scan button to scan the database server.



After clicking the GDPR scan button

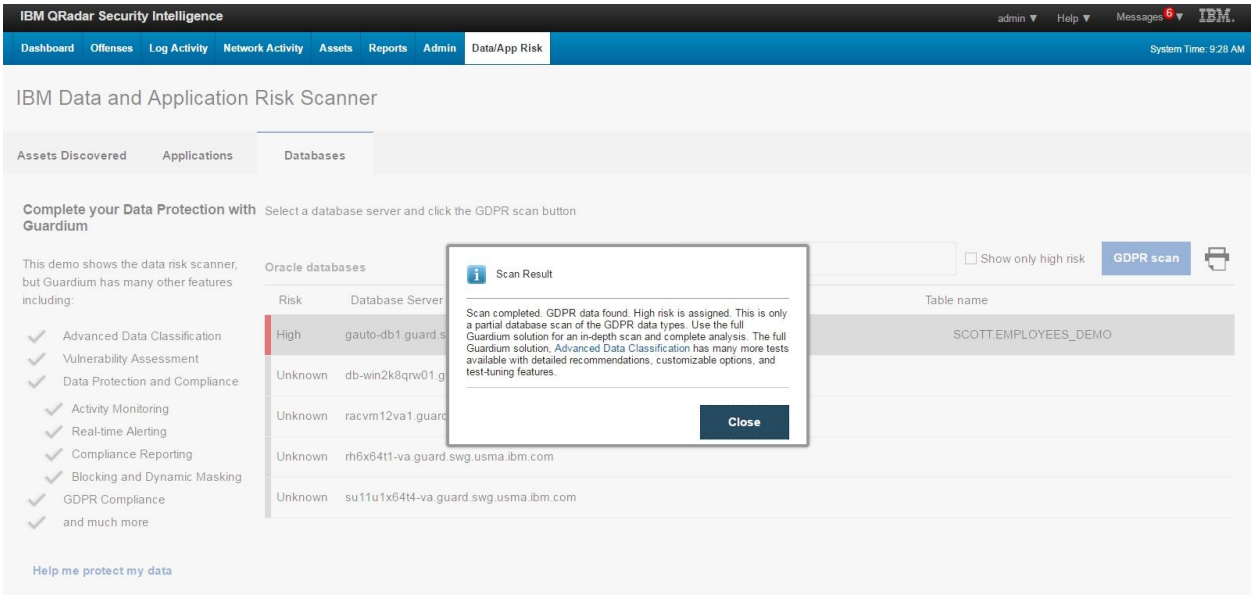
Fill in the database connection parameters: user name; password; port number; service name; and, then click GDPR scan.



Results after scan has run

When the Risk type is High, this is indicative of GDPR data found.

Click the Print button to print the scan results.



The results shown are only a highly-focused sample of Data and Application Risk in the databases scanned.

The full product (see link at Advanced Data Classification) has many more tests available with detailed recommendations, customizable options, and test-tuning features.

Additional information

Advanced Data Classification

https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=sw-infomgt&S_PKG=500010163&S_TACT=C406001W&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US

Vulnerability Assessment

http://www-03.ibm.com/software/products/en/security-guardium-vulnerability-assessment

Data Protection and Compliance

http://www-03.ibm.com/software/products/en/guardium-data-protection-for-databases

Activity monitoring; Real-time alerting; Compliance reporting; Blocking and dynamic masking

GDPR compliance

https://event.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&referrer=&eventid=1245241&sessionid=1&key=E604B82C5D87DD5BC6293F300D87F0DD&regTag=&sourcepage=register

https://event.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&partnerref=secintel&eventid=1241814&sessionid=1&key=D96E412ACA19C50680E7684760C70FFA&regTag=&sourcepage=register

Data security and protection

http://www-03.ibm.com/software/products/en/category/data-security