IBM DB2 for z/OS Authentication (PC)

Thank you for your interest in authenticated scanning! When you configure and use authentication, you get a more in-depth assessment of your hosts, the most accurate results, and fewer false positives. This document provides tips and best practices for setting up IBM DB2 for z/OS authentication for compliance scans.

A few things to consider

Why should I use authentication?

With authentication we can remotely log in to each target system with credentials that you provide, and because we are logged in, we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? Yes, it is required for compliance scans.

Are my credentials safe?

Yes, credentials are exclusively used for READ access to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

Which technologies are supported?

For the most current list of supported authentication technologies and the versions that have been certified for VM and PC by record type, please refer to the following article:

Authentication Technologies Matrix

What are the steps?

First, set up an IBM DB2 for z/OS user account and privileges (on target hosts) for authenticated scanning. Then, using Qualys Policy Compliance, complete these steps:

1) Add an IBM DB2 authentication record.

2) Launch a compliance scan.

3) Run the Authentication Report to find out if authentication passed or failed for each scanned host.

IBM DB2 for z/OS Credentials Setup

Qualys will perform DB2 scanning by connecting to a remote port the database server is listening on. The z/OS target will need to have an external IP and the DB2 database port bound to the IP. We have provided a set of scripts below to help you set up an account and privileges which must exist prior to running scans. These scripts require an administrative account.

Please run the scripts provided, in the order shown. The role and scan account need to be created in the database you want to scan.

1) Create a user account

Please create a scan user account for successful authentication and compliance scanning. We recommend creating a user account called QUALYSSC.

2) Grant required privileges

Login to the database using the administrative account and use the script below. The script below grants the required privileges to the user created in Step 1.

```
GRANT EXECUTE ON PACKAGE NULLID.SYSSH200 to QUALYSSC;
GRANT SELECT ON SYSIBM.SYSUSERAUTH TO QUALYSSC;
GRANT SELECT ON SYSIBM.SYSSCHEMAAUTH TO QUALYSSC;
GRANT SELECT ON SYSIBM.SYSPACKAUTH TO QUALYSSC;
GRANT SELECT ON SYSIBM.SYSTABAUTH TO QUALYSSC;
GRANT SELECT ON SYSIBM.SYSDBAUTH TO QUALYSSC;
GRANT SELECT ON SYSIBM.SYSROUTINEAUTH TO QUALYSSC;
GRANT SELECT ON SYSIBM.SYSCOLAUTH TO QUALYSSC;
GRANT SELECT ON SYSIBM.SYSAUDITPOLICIES TO QUALYSSC;
```

3) Verify Privileges on the Scan Account

Verify that the scan account has the necessary privileges to login and perform assessment. You may use the sample script for reference - QG_DB2_11+ZOS_Auth_verx.x.txt

Sample Output

```
Prerequisites                                          Status
------------------------------------------------------ --------------------------------------------------
DB2 VERSION                                            11.01
NULLID.SYSSH200                                        PASSED - EXECUTE privilege is granted to User
SYSIBM.COLAUTH                                         PASSED - EXECUTE privilege is granted to User
SYSIBM.SYSAUDITPOLICIES                                PASSED - EXECUTE privilege is granted to User
SYSIBM.SYSDBAUTH                                       PASSED - SELECT privilege is granted to User
SYSIBM.SYSPACKAUTH                                     PASSED - SELECT privilege is granted to User
SYSIBM.SYSROUTINEAUTH                                  PASSED - SELECT privilege is granted to User
SYSIBM.SYSSCHEMAAUTH                                   PASSED - SELECT privilege is granted to User
SYSIBM.SYSTABAUTH                                      PASSED - SELECT privilege is granted to User
```

Did you get different results? Contact your IBM DB2 for z/OS DBA to ensure that privileges are set up correctly.

Last updated: May 27, 2022