DB2 Authentication

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 DB2 authentication.

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're logged in we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? It's required for compliance scans and recommended for vulnerability 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 user account and privileges (on target hosts) for authenticated scanning. Then, using Qualys, complete these steps: 1) Add a DB2 authentication record to associate credentials with hosts (IPs). 2) Launch a scan using an option profile with authentication enabled (it's always enabled in compliance profiles). 3) Run the Authentication Report to find out if authentication passed or failed for each scanned host.

IBM DB2 Credentials

We've provided a set of scripts below to help you set up a DB2 account and privileges which must exist prior to running scans. These scripts require a super-user account, such as the instance owner. Please run the scripts provided, in the order shown.

1) Create a User Account

Because DB2 uses the user accounts that are inherent to the OS, we recommend creating a user account named QUALYSSC for the purpose of scanning the data environment. Due to the fact that DB2 only allows user accounts with a max length of 8 characters to access its databases, configuring the user account within these boundaries is an important step.

Go to Step 2a if you are running a version of DB2 prior to v9.5. Go to step 2b if you are on v9.5+.

Copyright 2012-2024 by Qualys, Inc. All Rights Reserved.

2a) Grant Permissions to the Scan Account (DB2 v9.1-v9.3)

This script will grant the appropriate permissions to the table objects needed to successfully scan a DB2 host. Note – An administrator will need to add these permissions.

```
CONNECT TO [db-name];
GRANT CONNECT ON DATABASE TO USER QUALYSSC;
GRANT SELECT ON SYSIBMADM.DBCFG TO USER QUALYSSC;
GRANT SELECT ON SYSIBMADM.DBMCFG TO USER QUALYSSC;
GRANT SELECT ON SYSIBM.SYSTABAUTH TO USER QUALYSSC;
GRANT SELECT ON SYSCAT.DBAUTH TO USER QUALYSSC;
GRANT SELECT ON SYSCAT.SCHEMATA TO USER QUALYSSC;
GRANT SELECT ON SYSCAT.TABLES TO USER QUALYSSC;
GRANT SELECT ON SYSIBM.SYSVERSIONS TO USER QUALYSSC;
```

Please continue to Step 4.

2b) Grant Permissions to the Scan Account (DB2 v9.5+)

This script will create a role and grant the appropriate permissions to the table objects needed to successfully scan a DB2 host. Note – An administrator will need to create this role and add permissions. We recommend a role called QUALYSROLE.

```
CONNECT TO [db-name];
CREATE ROLE QUALYSROLE;
GRANT CONNECT ON DATABASE TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBMADM.DBCFG TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBMADM.DBMCFG TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBM.SYSTABAUTH TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.DBAUTH TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.SCHEMATA TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.TABLES TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBM.SYSVERSIONS TO ROLE QUALYSROLE;
```

Privilege to execute function SYSPROC.ENV_GET_INST_INFO and package NULLID.SYSSH200 is granted to PUBLIC by default. If errors are encountered by the scan account executing the below statement, grant the next privilege as well.

```
SELECT SERVICE_LEVEL, FIXPACK_NUM, BLD_LEVEL FROM TABLE
(SYSPROC.ENV_GET_INST_INFO());
GRANT EXECUTE ON FUNCTION SYSPROC.ENV_GET_INST_INFO TO ROLE QUALYSROLE;
GRANT EXECUTE ON PACKAGE NULLID.SYSSH200 TO ROLE QUALYSROLE;
```

If you wish to scan control 10179, please grant the following privileges

```
GRANT SELECT ON SYSIBMADM.CONTAINER_UTILIZATION TO ROLE QUALYSROLE;
```

Add scan account QUALYSSC to the OS group defined by SYSMON_GROUP

2c) Grant Permissions to the Scan Account (DB2 v10+)

GRANT EXECUTE ON FUNCTION SYSPROC.ENV_GET_REG_VARIABLES TO ROLE QUALYSROLE;

2d) Restrictive databases

If your databases are restrictive, you will need to grant these privileges as well:

For versions 9.5 and above:

GRANT SELECT ON SYSCAT.COLUMNS TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.CONTEXTS TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.ROLEAUTH TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.ROLES TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.SECURITYLABELCOMPONENTS TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.SECURITYLABELS TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.SECURITYPOLICIES TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.SECURITYPOLICYEXEMPTIONS TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.TABLES TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBMADM.CONTAINER_UTILIZATION TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBMADM.ENV_INST_INFO TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBMADM.PRIVILEGES TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBMADM.REG_VARIABLES TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBM.SYSAUDITPOLICIES TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBM.SYSDUMMY1 TO ROLE QUALYSROLE;
GRANT EXECUTE ON FUNCTION SYSPROC.ENV_GET_INST_INFO TO ROLE QUALYSROLE;
GRANT USAGE ON WORKLOAD SYSDEFAULTUSERWORKLOAD TO ROLE QUALYSROLE;
GRANT EXECUTE ON PACKAGE NULLID.SYSSH200 TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.AUDITUSE TO ROLE QUALYSROLE;

Additional privileges for versions 10.x and above:
GRANT SELECT ON SYSCAT.PACKAGEAUTH TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.ROUTINEAUTH TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.SCHEMAAUTH TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.WRAPPERS TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBMADM.AUTHORIZATIONIDS TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBM.SYSTBSPACEAUTH TO ROLE QUALYSROLE;
GRANT SELECT ON SYSCAT.CONTROLS TO ROLE QUALYSROLE;
GRANT EXECUTE ON FUNCTION SYSPROC.ENV_GET_REG_VARIABLES TO ROLE QUALYSROLE;
GRANT SELECT ON SYSIBMADM.DB_HISTORY TO ROLE QUALYSROLE;

If your version is of a different minor version, you may need to grant the execute privilege on a different package below. Please grant the privilege on specific package as needed.

Additional privilege for versions DB2 9.5:
GRANT EXECUTE ON PACKAGE NULLID.SQLC2G13 TO ROLE QUALYSROLE;

Additional privilege for versions DB2 9.7:
GRANT EXECUTE ON PACKAGE NULLID.SQLC2H20 TO ROLE QUALYSROLE;

Additional privilege for versions DB2 10.5:
GRANT EXECUTE ON PACKAGE NULLID.SQLC2K26 TO ROLE QUALYSROLE;

Additional privilege for versions DB2 11.1:
GRANT EXECUTE ON PACKAGE NULLID.SQLC2O26 TO ROLE QUALYSROLE;

Additional privilege for versions DB2 11.5:
GRANT EXECUTE ON PACKAGE NULLID.SQLC2O29 TO ROLE QUALYSROLE;

3) Allow Scan Account to be a part of Scan Role

This snippet allows the scan account to be a part of the scan role that was created in Step 2b.

```
GRANT ROLE QUALYSROLE TO USER QUALYSSC;
```

4) Check Privileges on the Scan Account

We provide 2 scripts in the zip archive to help you identify missing privileges from the user account to be used for scanning. These scripts are in the files QG_DB2_Auth_verx.x.txt and QG_DB29.5+_Auth_verx.x.txt. The script should be executed by a super-user against a database to determine if all the appropriate privileges have been setup correctly. The script will generate an output listing the status of all the prerequisites.

Sample output:

Prerequisites	Status
Current User	DB2INST
DB2 VERSION	DB2 v11.1.0.0
NULLID.SYSSH200	PASSED - EXECUTE privilege is granted to role
QUALYSROLE	PASSED - role exists
QUALYSROLE MEMBER	PASSED – role is granted to user
QUALYSSC	PASSED – user exists
SYSCAT.DBAUTH	PASSED - SELECT privilege is granted to role
SYSCAT.SCHEMATA	PASSED - SELECT privilege is granted to role
SYSCAT.TABLES	PASSED - SELECT privilege is granted to role
SYSIBM.SYSTABAUTH	PASSED - SELECT privilege is granted to role
SYSIBM.SYSVERSIONS	PASSED - SELECT privilege is granted to role
SYSIBMADM.CONTAINER_UTILIZATION	PASSED - SELECT privilege is granted to role
SYSIBMADM.DBCFG	PASSED - SELECT privilege is granted to role
SYSIBMADM.DBMCFG	PASSED - SELECT privilege is granted to role
SYSPROC.ENV_GET_INST_INFO	PASSED - EXECUTE privilege is granted to role

Did you get different results? Contact your SQL Server DBA to ensure that privileges are set up correctly.

IBM DB2 Authentication Records

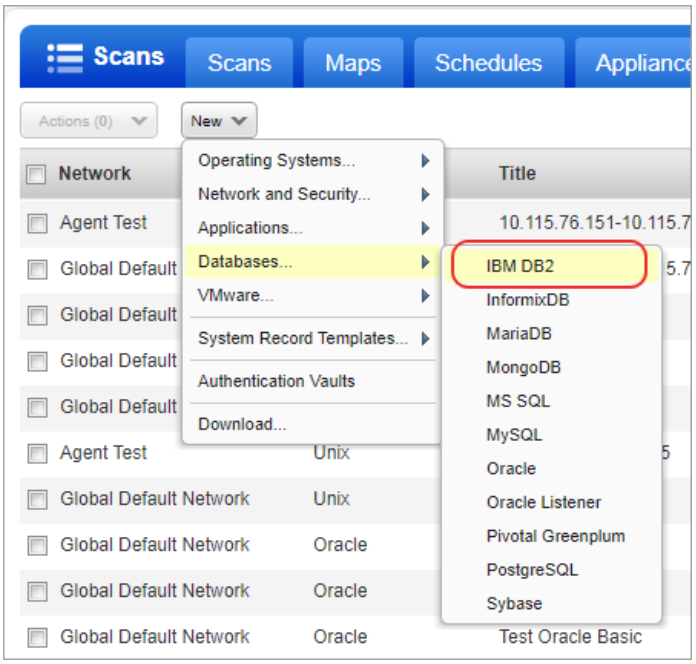
You'll create DB2 authentication records in Qualys to associate credentials to hosts (IPs). You'll need to supply a user name and password, the database name you want to authenticate to and the port the database is on.

Where do I create records?

Go to Scans > Authentication > New > Databases > IBM DB2 Record.

Can I have multiple DB2 records?

Yes. When there are multiple DB2 instances on a host, you need to create a separate authentication record for each instance.

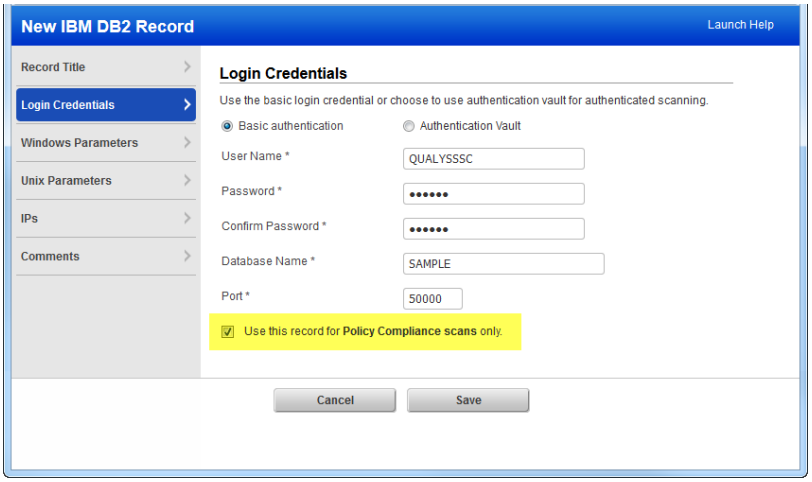


What defines a DB2 instance?

For a vulnerability scan, an instance is defined uniquely by an IP address and port. For a compliance scan, an instance is defined uniquely by an IP address, port and database name.

Will the same record be used for VM and PC scans?

By default, DB2 records will be used for both vulnerability and compliance scans. You can choose to have a record only used for PC scans. Select the check box "Use this record for Policy Compliance scans only" in the authentication record.



Show me an example of multiple DB2 records

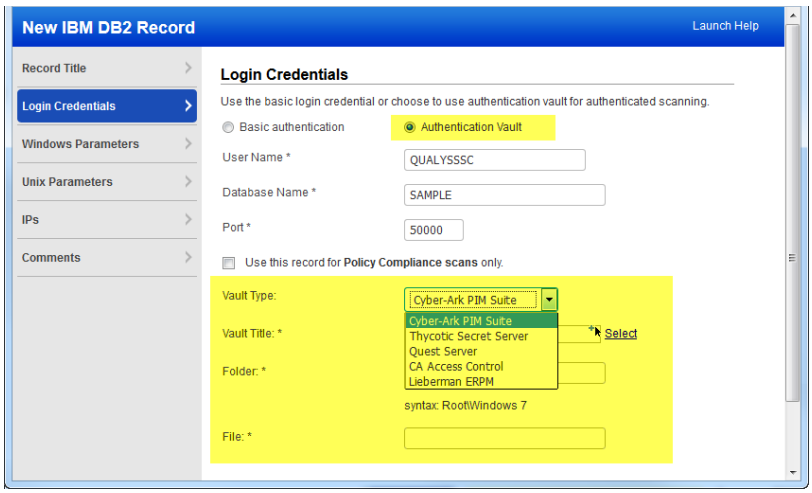
Let's say you want to define these DB2 records in your account. In the table below, PC Only=Yes indicates that the check box "Use this record for Policy Compliance scans only" is selected in the record.

	IP Address	Port	Database Name	PC Only
Record 1	10.10.31.178	50000	SAMPLE	No
Record 2	10.10.30.159	50000	TOOLS	No
Record 3	10.10.30.159	50000	SAMPLE	Yes

Record 1 and Record 2 will be used for both vulnerability scans and compliance scans. Record 3 will be used for compliance scans only. You'll notice that Record 2 and Record 3 have the same IP address and port but different database names – this is allowed because Record 3 is used for compliance scans only.

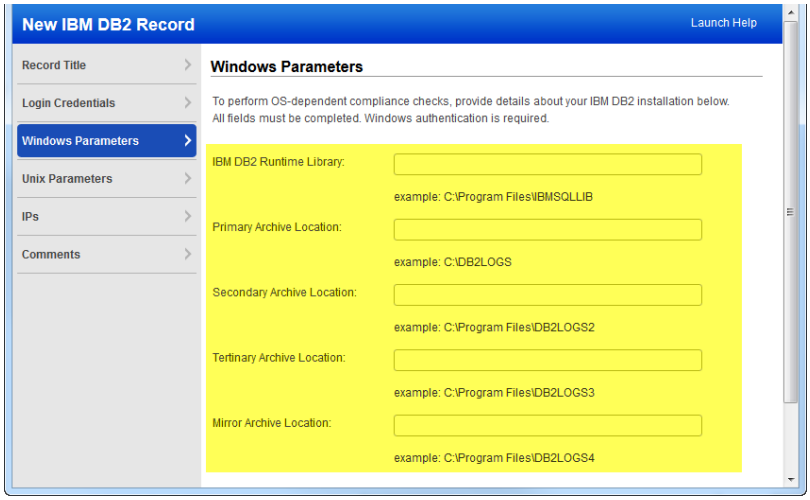
Can I access a password in a vault?

Yes. We support integration with multiple third party password vaults. Go to Scans > Authentication > New > Authentication Vaults and tell us about your vault system. Then choose "Authentication Vault" in your record and select your vault name. At scan time, we'll authenticate to hosts using the account name in your record and the password we find in your vault.



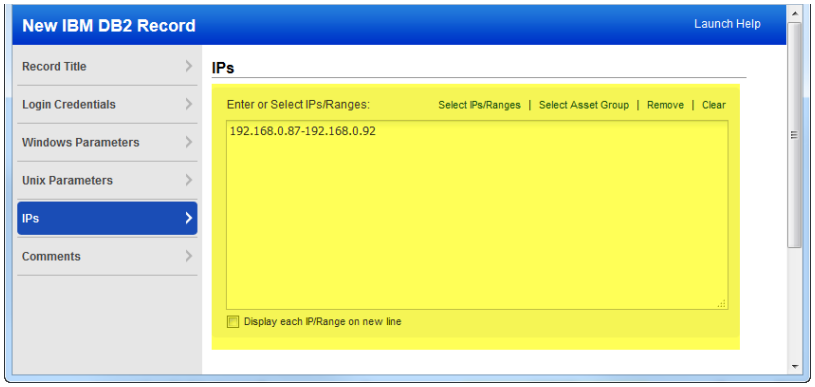
Provide details about installation

If you plan to run compliance scans, you'll also need to provide details about your IBM DB2 installation. This allows us to gather DB2 compliance data at the Windows or Unix operating system level. You'll enter Windows and Unix parameters (like the installation directory and archive locations) in the record. For a Windows installation, make sure you also have a Windows record defined with the same hosts as the DB2 record. For a Unix installation, make sure you also have a Unix record defined with the same hosts as the DB2 record.



Add IPs to the record

Select the target hosts (IPs) to authenticate to.



Last updated: March 14, 2024