Pivotal Greenplum Authentication (PC)

Thank you for your interest in authenticated compliance scanning! When you use authentication, you get a more in-depth assessment of your hosts and the most accurate results. This document provides tips and best practices for authenticating to Greenplum database instances.

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? Yes, it's required for compliance scans.

Are my credentials safe?

Yes, credentials are exclusively used for READ ACCESS ONLY 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 a Greenplum user account and privileges on target hosts (we'll help you with this below). Then, using Qualys Policy Compliance, complete these steps: 1) Add Greenplum authentication records. 2) Launch a compliance scan. 3) Run the Authentication Report to view the authentication status (Passed or Failed) for each scanned host.

Greenplum Setup

Greenplum Database is based on PostgreSQL open-source technology. In order for the Qualys Compliance Scan to work properly on a Greenplum database, the following account and privileges must exist prior to running the scan. We've provided a set of scripts below to help you set up an account and grant privileges. Note – These scripts require a super-user account. For example, postgres. Please connect to a database with a super-user account and run the scripts provided, in the order shown.

1) Create a User Account on Greenplum Instance

This script creates a user account called QUALYS_SCAN.

CREATE ROLE qualys_scan WITH ENCRYPTED PASSWORD '[enter password here]' LOGIN;

Copyright 2020-2022 by Qualys, Inc. All Rights Reserved.

Note – If you want to scan all databases in the Instance, you don't need to create a user account in each database. However, you need to perform Step 2 and Step 3 (below) on each database.

2) Grant Privileges on connected database for Scan User Account (Optional)

By default, if the initial default privileges were not changed, the Scan User Account already has privileges to perform SQL statements querying (except view PG_SHADOW). You can also check privileges in Step 3 first, and then grant any missing privileges.

```
GRANT CONNECT ON DATABASE [Current database name] TO qualys_scan;
GRANT USAGE ON SCHEMA PG_CATALOG TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_SETTINGS TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_USER TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_GROUP TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_ROLES TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_SHADOW TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_CLASS TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_STAT_ACTIVITY TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_LOCKS TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_DATABASE TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_NAMESPACE TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_TABLESPACE TO qualys_scan;
GRANT SELECT ON PG_CATALOG.PG_AUTHID to qualys_scan;
```

Note – To PG_CATALOG.PG_SHADOW view, the information may be sensitive to you. It will be used in checking the empty or plain password roles detection, and we will ensure that the SQL query will never return column 'passwd' value from this view in our signatures. You can decide whether you want us to support those detections.

3) Check Privileges on the Scan Account

We provide a script 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_Greenplum_Auth_verx.x.txt. A super user should execute the script by connecting to a database to determine if all the appropriate privileges have been set up correctly. The script will generate an output listing the status of all the prerequisites.

Sample Output

```
Prerequisites                                          Status
-------------------------------------------------------  -------------------------------------------------
PostgreSQL 8.3.23 (Greenplum Database 5.16.0)          <---Current logged on database version
qualys_scan                                            <---Current logged on role name
qualys_scan                                            PASSED - account exists
postgres                                               PASSED - account can connect to current database
PG_CATALOG                                             PASSED - USAGE privilege exists
PG_CATALOG.PG_SETTINGS                                 PASSED - SELECT privilege exists
PG_CATALOG.PG_USER                                     PASSED - SELECT privilege exists
PG_CATALOG.PG_GROUP                                    PASSED - SELECT privilege exists
PG_CATALOG.PG_ROLES                                    PASSED - SELECT privilege exists
PG_CATALOG.PG_SHADOW                                   PASSED - SELECT privilege exists
PG_CATALOG.PG_CLASS                                    PASSED - SELECT privilege exists
PG_CATALOG.PG_STAT_ACTIVITY                            PASSED - SELECT privilege exists
PG_CATALOG.PG_LOCKS                                    PASSED - SELECT privilege exists
PG_CATALOG.PG_DATABASE                                 PASSED - SELECT privilege exists
PG_CATALOG.PG_NAMESPACE                                PASSED - SELECT privilege exists
PG_CATALOG.PG_TABLESPACE                               PASSED - SELECT privilege exists
```

PG_CATALOG.PG_AUTHID PASSED - SELECT privilege exists
(17 rows)

4) Configure the Client Authentication in $MASTER_DATA_DIRECTORY/pg_hba.conf file

Greenplum offers a number of different client authentication methods. The method used to authenticate a particular client connection can be selected on the basis of (client) host address, database, and user. Client authentication is controlled by a configuration file, which is traditionally named pg_hba.conf (hba stands for host-based authentication) and is stored in the database cluster's data directory. A default pg_hba.conf file is installed when the data directory ($MASTER_DATA_DIRECTORY) is initialized by initdb. It is possible to place the configuration file elsewhere.

Check out these sample configurations for the $MASTER_DATA_DIRECTORY/pg_hba.conf file for client authentication. For "databases" , you can provide multiple database names separated by commas. For "address", provide an IPV4 or IPV6 address range for your scanner(s).

Password Authentication with plain or SSL-encrypted TCP/IP socket

Provide the password in the authentication record.

```
host        [databases]   qualys_scan   [address]   md5
or
host        all           qualys_scan   [address]   md5
```

Password Authentication with SSL-encrypted TCP/IP socket

Provide the password in the authentication record.

```
hostssl     [databases]   qualys_scan   [address]   md5
or
hostssl     all           qualys_scan   [address]   md5
```

Password Authentication with SSL-encrypted TCP/IP socket and client certificate will be requested during SSL connection startup

Provide the password, client certificate and private key in the authentication record.

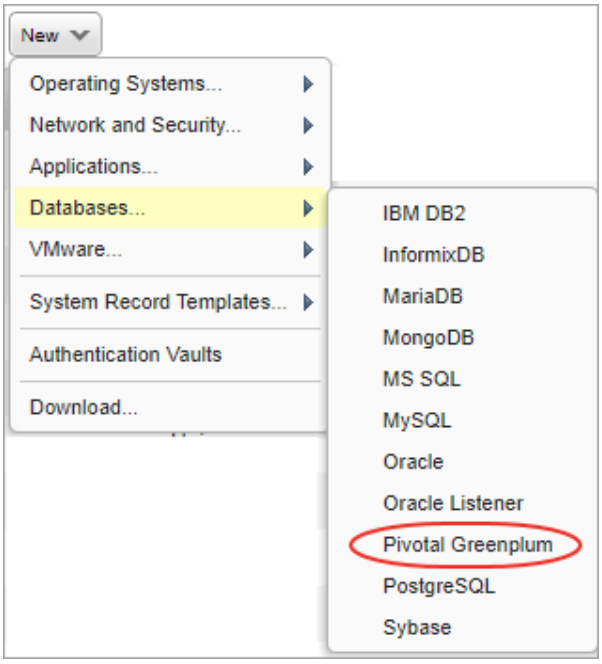
```
hostssl     [databases]   qualys_scan   [address]   md5 clientcert=1
or
hostssl     all           qualys_scan   [address]   md5 clientcert=1
```

Certificate Authentication

Provide the client certificate and private key in the authentication record.

```
hostssl     [databases]   qualys_scan   [address]   cert
or
hostssl     all           qualys_scan   [address]   cert
```

Greenplum Authentication Records



Create a Pivotal Greenplum record for each database instance you want to scan for compliance. Unix authentication is required so you'll also need a Unix record for the host running the database.

How do I get started?

Go to Scans > Authentication > New > Databases > Pivotal Greenplum Record. (Only available in accounts with Qualys PC.)

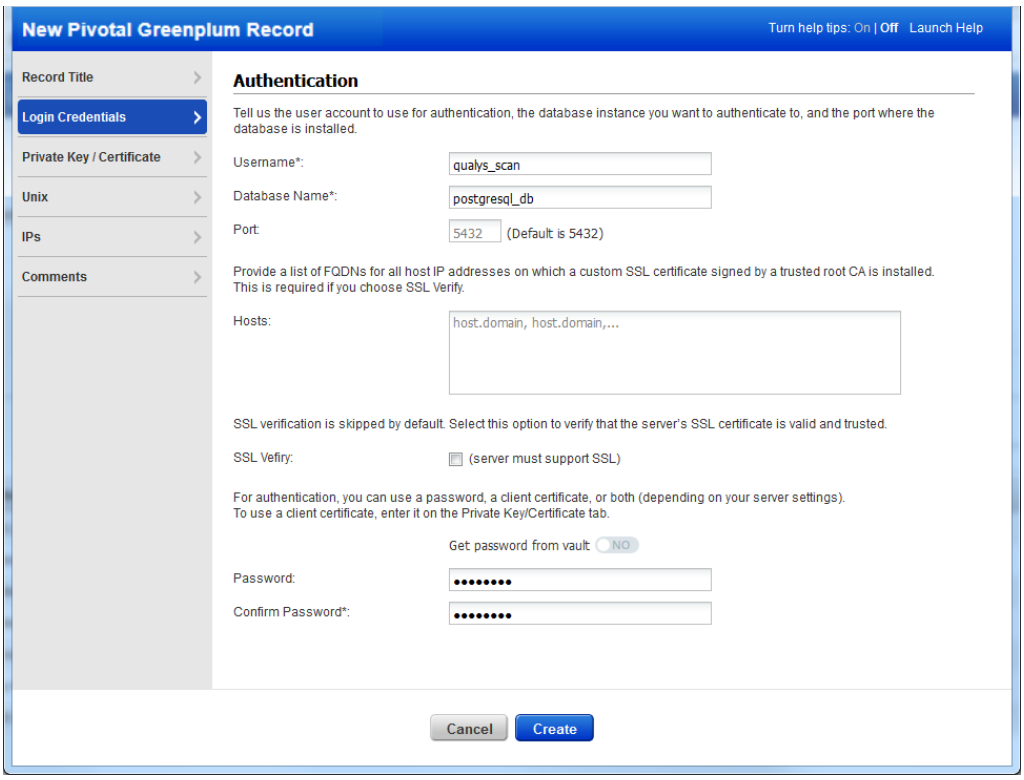
What information is required?

You'll need to tell us the user account to be used for authentication, the database instance to authenticate to, and the port where the database is installed (default is 5432).

The authentication method you use depends on your server settings.

You can provide:

- a password (enter on the Login Credentials tab or get from a vault),
- a client certificate (enter on the Private Key / Certificate tab),
- a password AND client certificate (enter values on both tabs).



Should I use SSL?

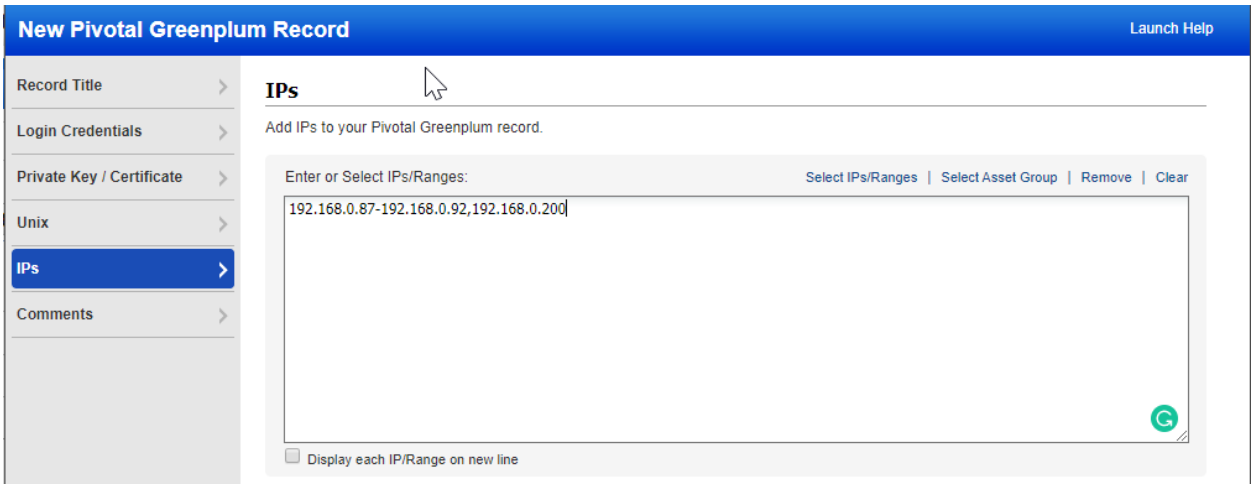
Using SSL provides a secure connection to your database. By selecting “SSL Verify”, and if your database server supports SSL, you will be requesting a SSL secured link. The server SSL certificate verification is also enforced. By default, this option is set to false.

Your Greenplum configuration file

On the Unix tab, tell us the full path to the Greenplum configuration file on your Unix hosts (IP addresses). The file must be in the same location on all IPs in this record (listed on the IPs tab).

Which IPs should I add to the record?

Select the IPs for the Greenplum databases that the scanner should log into using the provided credentials. Unix authentication is required so you’ll also need Unix records for these same IPs.



Last updated: May 27, 2022