PostgreSQL（PC）

認証コンプライアンススキャンに関心をお寄せいただきありがとうございます。認証を使用すると、ホストをさらに詳しく評価し、最も正確な結果を取得することができます。本書では、PostgreSQL データベースインスタンスの認証に関するヒントとベストプラクティスについて説明します。

考慮すべき事項

認証を使用する理由

認証を使用すると、提供された資格情報で対象の各システムにリモートからログインすることができます。ログインすることで、テスト中に更に多くのことが行えるようになります。そのため、各システムのセキュリティ状態について、より適切に可視化することができます。認証は、コンプライアンススキャンでは必須です。

資格情報の安全性について

資格情報は、読み取り専用としてシステムへのアクセスに使用されます。デバイス上で資格情報を修正したり、何かを書き込んだりするということは、決してありません。資格情報は安全性を確保した状態で扱われ、スキャンの実行中にのみ使用されます。

操作手順

まず、対象のホスト上で PostgreSQL ユーザアカウントと権限を設定します（下記で説明）。次に、Qualys Policy Compliance を使用して次の手順を実行します。1) PostgreSQL 認証レコードを追加します。2) コンプライアンススキャンを開始します。3) 認証レポートを実行して、スキャン済みの各ホストの認証ステータス（「Passed」または「Failed」）を表示します。

PostgreSQL の設定

PostgreSQL データベースで Qualys コンプライアンススキャンを正常に機能させるには、スキャンを実行する前に、次のアカウントと権限が存在している必要があります。アカウントを設定し、権限を付与するために、以下のスクリプトのセットが用意されています。注記 - これらのスクリプトでは、postgres などのスーパーユーザアカウントが必要になります。スーパーユーザアカウントでデータベースに接続し、次の順番でスクリプトを実行してください。

1) PostgreSQL インスタンスでのユーザアカウントの作成

次のスクリプトにより QUALYS_SCAN という名前のユーザアカウントが作成されます。

CREATE ROLE qualys_scan WITH ENCRYPTED PASSWORD ‘[ここにパスワードを入力]’ LOGIN;

注記 - インスタンスのすべてのデータベースをスキャンする場合、データベースごとにユーザアカウントを作成する必要はありません。ただし、各データベースで以下に示す手順 2 と手順 3 を行う必要があります。

2) 接続データベースでのスキャンユーザアカウントに対する権限の付与（オプション）

デフォルトでは、初期設定時のデフォルトの権限が変更されていなければ、スキャンユーザアカウントには既に SQL 文でクエリ（PG_SHADOW ビューは除く）を実行するための権限があります。また、まず手順 3 で権限を確認した後、不足している権限を付与することもできます。

```
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;
```

注記 - PG_CATALOG.PG_SHADOW ビューでは、機密情報が含まれる可能性があります。これは空のパスワードやプレーンテキストのパスワードのロール検出をチェックする場合に使用されます。SQL クエリでは、このビューからの‘ passwd ’カラムの値をシグネチャ内に返さないように保証します。このような検出のサポートを求めるかどうか決定することができます。

3) スキャンアカウントの権限の確認

スキャンに使用されるユーザアカウントで不足している権限の特定に利用できるスクリプトを zip アーカイブ内に用意しています。これらのスクリプトは、QG_PostgreSQL_Auth_verx.x.txt ファイル内にあります。適切な権限が正しく設定されているかどうかを判断するために、スーパーユーザが、データベースに接続することでスクリプトを実行します。このスクリプトにより、すべての必須項目の状態を表示する出力が生成されます。

出力例

```
必須項目                                                    状態
---------------------------------------------------------- ------------------------------------------------
PostgreSQL 9.5.4                                           <---現在ログオンしているデータベースバージョン
postgres                                                   <---現在ログオンしているロール名
qualys_scan                                                PASSED - account exists
testing_db                                                 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) $PGDATA/pg_hba.conf ファイルでのクライアント認証の設定

PostgreSQL では、さまざまなクライアント認証方法が提供されています。特定のクライアント接続を認証するための方法は、(クライアント)ホストのアドレス、データベース、およびユーザに基づき選択できます。クライアント認証は構成ファイルによって制御されます。この構成ファイルは、通常 pg_hba.conf(hba は host-based authentication(ホストベースの認証)の略)という名前で、データベースクラスタのデータディレクトリに保存されます。initdb によってデータディレクトリ($PGDATA)が初期化されると、デフォルトの pg_hba.conf ファイルがインストールされます。構成ファイルを他の場所に保存することもできます。

クライアント認証の $PGDATA/pg_hba.conf file ファイルについて、以下のサンプル設定を参照してください。“ databases ”には、複数のデータベース名をカンマで区切って入力できます。“ address ”には、スキャナの IPV4 または IPV6 アドレス範囲を入力できます。

プレーンテキストまたは SSL で暗号化された TCP/IP ソケットでのパスワード認証

認証レコードのパスワードを入力します。

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

SSL で暗号化された TCP/IP ソケットでのパスワード認証

認証レコードのパスワードを入力します。

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

SSL で暗号化された TCP/IP ソケットおよびクライアント証明書でのパスワード認証は、SSL 接続の開始時に要求されます

認証レコードのパスワード、クライアント証明書、および秘密鍵を入力します。

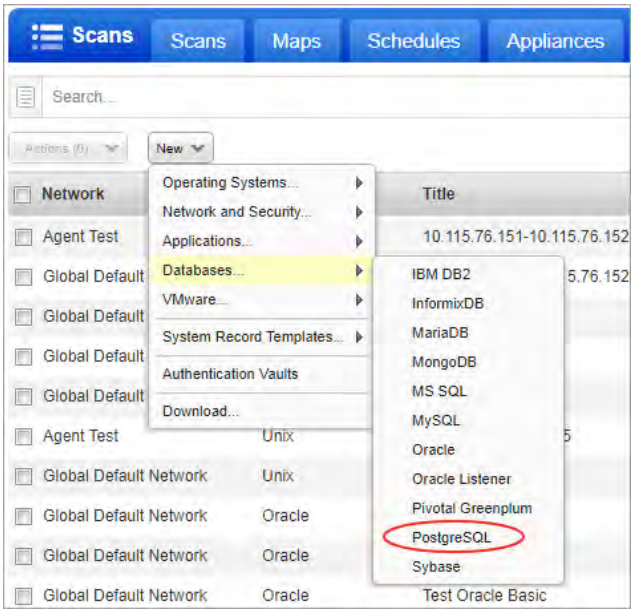
```
hostssl     [databases]   qualys_scan   [address]   md5 clientcert=1
or
hostssl     all           qualys_scan   [address]   md5 clientcert=1
```

Certificate Authentication

認証レコードのクライアント証明書と秘密鍵を入力します。

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

PostgreSQL 認証レコード



コンプライアンススキャンを実行する PostgreSQL データベースインスタンスごとに PostgreSQL レコードを作成します。Unix 認証が必要であるため、PostgreSQL データベースを実行しているホストの Unix レコードも必要になります。

操作手順

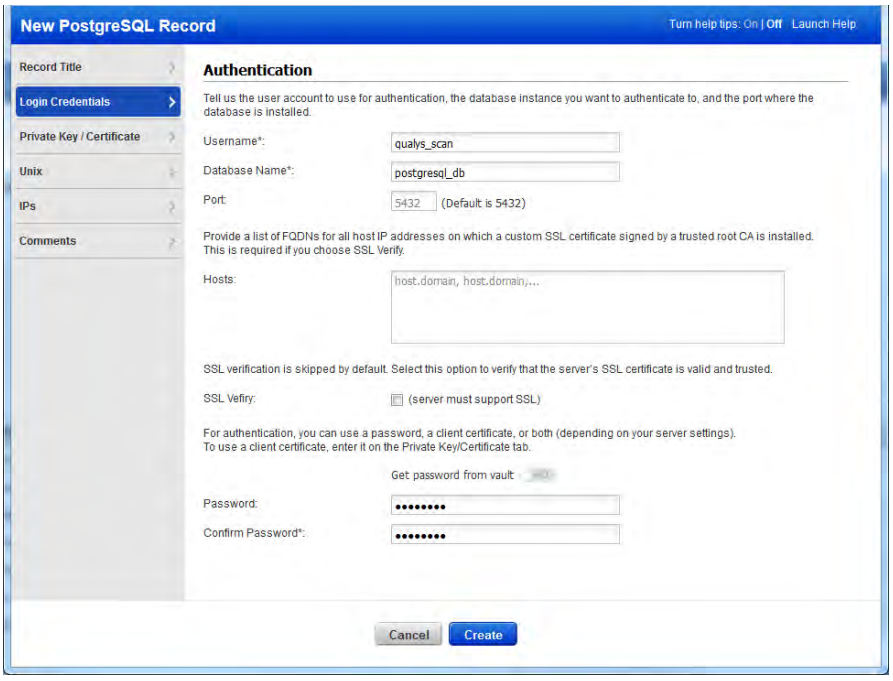
「 Scans 」→「 Authentication 」→「 New 」→「 Databases 」→「PostgreSQL」を選択します（Qualys PC が有効なアカウントでのみ使用できます）。

必要な情報

認証に使用するユーザアカウント、認証を行うデータベースインスタンス、データベースがインストールされているポート（デフォルトは 5432）を指定します。

使用する認証方法は、サーバの設定によって異なります。

次のような指定方法があります。
- パスワード（「Login Credentials」タブで入力するか、Vault から取得します）。
- クライアント証明書（「Private Key / Certificate」タブで入力します）。
- パスワードおよびクライアント証明書（両方のタブで値を入力します）。



SSL の必要性

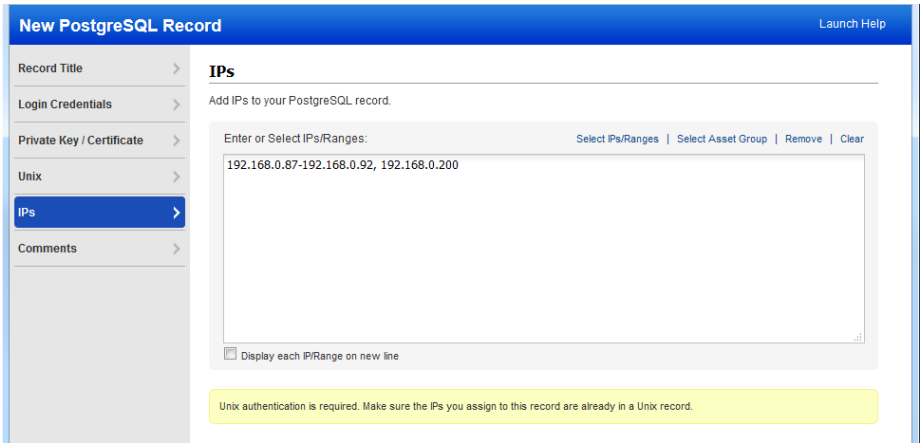
SSL を使用すると、データベースに安全に接続できます。データベースサーバが SSL に対応している場合、「SSL Verify」を選択すれば、SSL で保護されたリンクをリクエストすることになります。サーバの SSL 証明書の検証も実施されます。デフォルトでは、このオプションは false に設定されています。

PostgreSQL 構成ファイル

「Unix」タブで、Unix ホスト(IP アドレス)上の PostgreSQL 設定ファイルへの完全パスを指定します。(「IPs」タブに表示されている)このレコードのすべての IP のファイルは、同じ場所にある必要があります。

レコードに追加する IP

入力された資格情報を使用してスキャナがログインする必要がある PostgreSQL データベースの IP を選択します。Unix 認証が必要であるため、同じ IP の Unix レコードも必要になります。



役立つヒント - ログインカウンタのヒント

PostgreSQL は、ログイン失敗カウンタを維持することにより、ポートスキャンからの保護を積極的に実行します。正常にログインを完了することなく PostgreSQL のポートに接続を試みると、このカウンタがインクリメントします。これを意識しておくことは管理者にとって必要です。最終的に、サーバがデータベースへの TCP 接続の受け入れを停止するためです。

管理者は「PostgreSQLadmin flush-hosts」コマンドを発行してカウンタをリセットし、低すぎる値に設定されている可能性があるカウンタ値を大きくすることが推奨されます。

最終更新日: 2020 年 6 月 19 日