MySQL 認証（PC）

認証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。認証を設定して使用すると、ホストをさらに詳しく評価し、最も正確な結果を取得し、誤検出を減らすことができます。本書では、コンプライアンススキャンにおける MySQL 認証の設定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、対象のホスト上で認証スキャン用の MySQL ユーザアカウントと権限を設定します。次に、Qualys Policy Compliance を使用して次の手順を実行します。1) MySQL 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、スキャン対象の各ホストで認証が成功または失敗したかを確認します。

MySQL 資格情報

スキャンを実行する前に存在している必要があるアカウントと権限を設定するために、以下のスクリプトのセットが用意されています。これらのスクリプトには、root や Administrator などのスーパーユーザアカウントが必要です。

指定のスクリプトを表示された順序で実行してください。

1)「mysql」データベース内のユーザアカウントの作成

こ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。スクリプトを実行する前に、パスワードを指定してください。ここではスキャナから実行可能なリモートユーザを作成するため、「%」の使用は必須です。

CREATE USER ‘QUALYS_SCAN’@’%’ IDENTIFIED BY ‘[ここにパスワードを入力]’ ;

注記 - ホスト値にワイルドカードを使用するため、この方法で MySQL ユーザアカウントを作成するとある程度のリスクが生じます。これは、データベースインストールの正常なスキャンを確実に実行できる一般的な方法です。

無断複写・転載を禁じます。2015-2020 年 クォリスジャパン株式会社

この他に、より高いセキュリティを想定したユーザアカウントを作成する方法もあります。MySQL では、IP アドレスまたはそのバリエーションのいずれかを使用してユーザアカウントを作成できます。その 1 つの方法は、Qualys Scanner Appliance の IP アドレスを特定して、その IP アドレスによってユーザアカウントを作成することです。例えば、スキャナの IP アドレスが 192.168.100.1 の場合、スクリプトは次のようになります。

CREATE USER ‘QUALYS_SCAN’@’192.168.100.1’ IDENTIFIED BY ‘[ここにパスワードを入力]’ ;

データベースサーバと Qualys スキャナが同じサブネット内にある場合、サブネットを使用することもできます。ワイルドカードを使用して、ユーザアカウントをさまざまな方法で作成できます。

CREATE USER ‘QUALYS_SCAN’@’192.168.100.%’IDENTIFIED BY ‘[ここにパスワードを入力]’ ;
または
CREATE USER ‘QUALYS_SCAN’@’192.168.%.%’IDENTIFIED BY ‘[ここにパスワードを入力]’ ;

より安全な接続を提供するもう 1 つの方法は、ネットワーク層で対処することです。ファイアウォール ACL を調整することで、望ましくないアクティビティから保護できます。

SSL 認証

MySQL 認証は SSL にも対応しています。MySQL 認証レコードにサーバ SSL 証明書を設定および適用できるだけでなく、クライアント SSL 証明書によるセキュリティ強化もサポートしています。これは、QUALYS_SCAN ユーザに対して設定できます。mysql.user テーブル内で、クライアント SSL 証明書を受け入れるようにユーザを変更すると、セキュリティ強化のための複数の制限を追加できるようになります。

MySQL 認証レコードでは、オプションでクライアント SSL 証明書と秘密鍵を追加できます。

2) スキャンアカウントへの権限の付与

このスクリプトにより、スキャンに使用されるユーザアカウントに権限が付与されます。認証が正常に実行され、コンプライアンススキャンが実行されるためには、次の権限が必要です。

GRANT SELECT ON MYSQL.USER TO QUALYS_SCAN;
GRANT SELECT ON MYSQL.DB TO QUALYS_SCAN;
GRANT SELECT ON INFORMATION_SCHEMA.PLUGINS TO QUALYS_SCAN;
GRANT SELECT ON MYSQL.TABLES_PRIV TO QUALYS_SCAN;

レプリケーションを扱うコントロールをスキャンする場合、続けて以下を行います。

GRANT SELECT ON MYSQL.SLAVE_MASTER_INFO TO QUALYS_SCAN;

以上の権限付与を実行した後、権限をフラッシュしてグラントテーブルを再生成します。

FLUSH PRIVILEGES;

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_MySQL_Auth_verx.x.txt ファイル内にあります。このスクリプトは、適切な権限がすべて正しく設定されているかどうかを確認するためのもので、データベースのスーパーユーザが実行しなければなりません。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

```
+--------------------+-----------------------------------------+
| Prerequisites      | Status                                  |
+--------------------+-----------------------------------------+
| root@localhost     | <---Current logged on user              |
| QUALYS_SCAN        | PASSED - account exists                 |
| USER               | PASSED - SELECT privilege exists        |
| DB                 | PASSED - SELECT privilege exists        |
| PLUGINS            | PASSED - SELECT privilege exists        |
| SLAVE_MASTER_INFO  | FAILED - SELECT privilege does not exist |**
| TABLES_PRIV        | PASSED - SELECT privilege exists        |
+--------------------+-----------------------------------------+
```

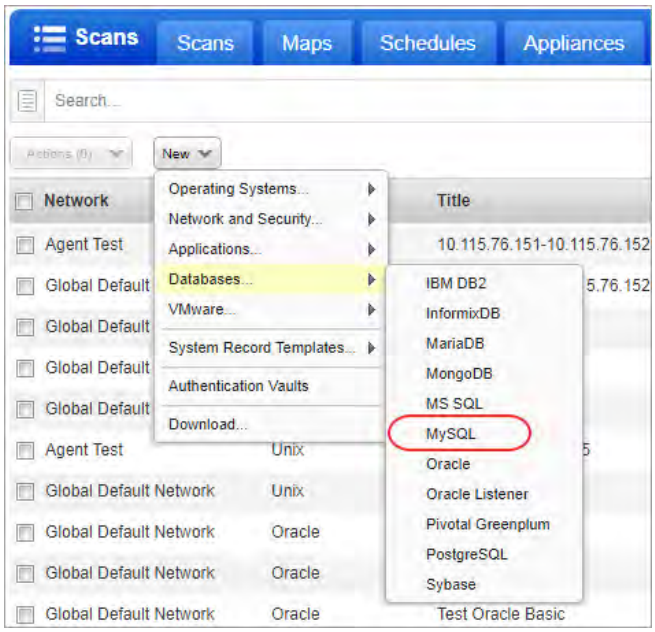
** レプリケーションがセットアップされていない場合、SLAVE_MASTER_INFO のエントリのステータスは「FAILED」になることに注意してください。その場合でも、スキャンは実行されます。

MySQL 認証レコード

スキャン対象の各 MySQL インスタンスに対して個別の認証レコードを作成する必要があります。スキャンの際、アカウントのすべての MySQL 認証レコードを使用して、1 つのホストで 1 つまたは複数の MySQL インスタンスが認証されます。

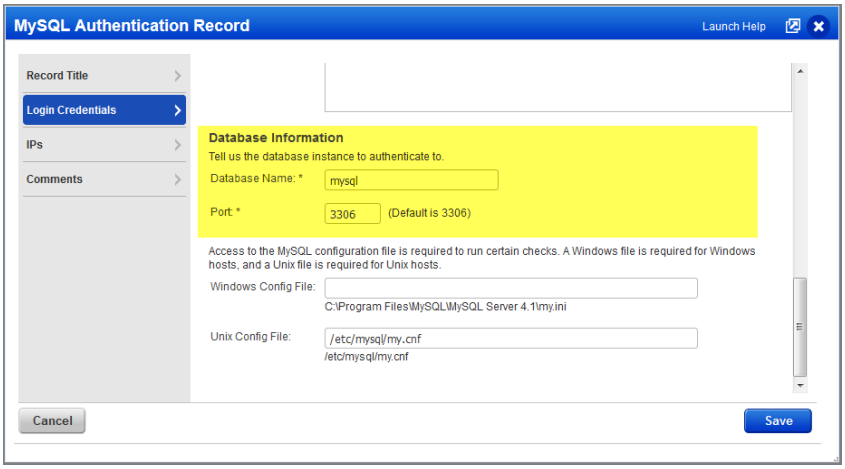
レコードを作成する場所

「Scans」→「Authentication」→「New」→「Databases」→「MySQL Record」に移動します。



必要なデータベース情報

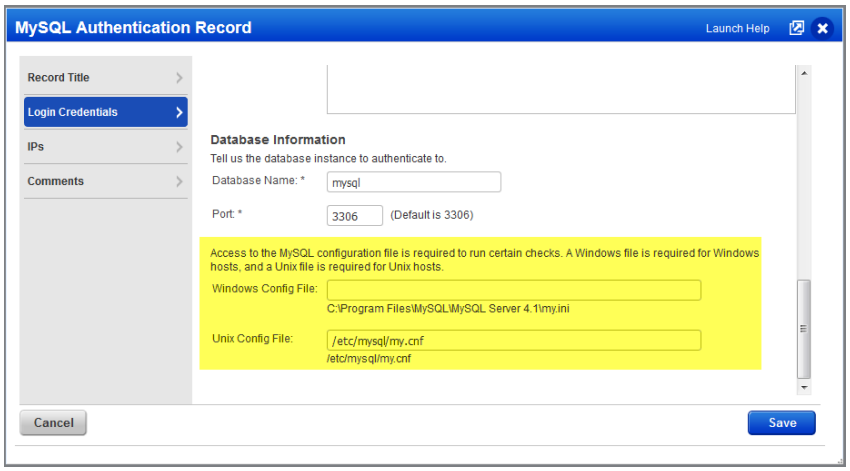
認証するデータベース名とデータベースが実行されているポートを指定します（または、デフォルトのデータベース名とポートを使用します）。



ヒント - MySQL 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することに注意してください。正常にログインを完了することなく MySQL 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「mysqladmin flush-hosts」コマンドを発行してカウンタをリセットし、カウンタ値が低すぎる値に設定されていないか調べて、値を大きくすることが推奨されます。

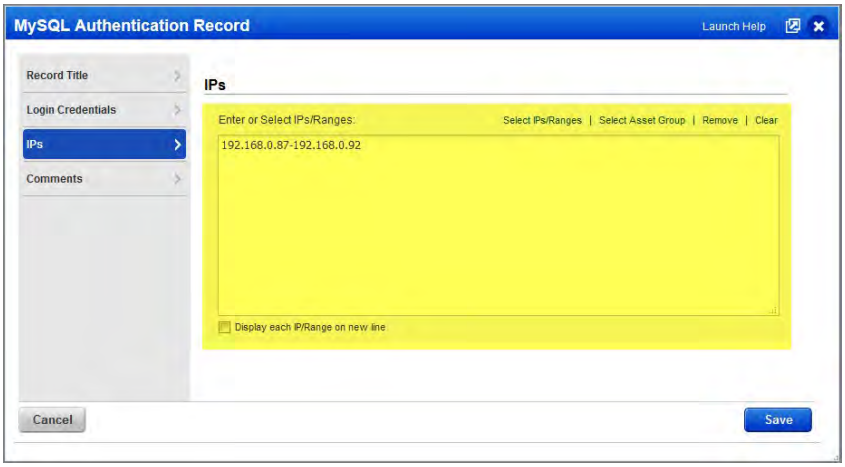
MySQL 構成ファイル

必須ではありませんが、重要なのは、認証レコード内に MySQL 構成ファイルの場所を指定することです。このファイルは、特定のチェックで必要になります。Unix と Windows の場合、このファイルは探している情報を入力するうえで必要な情報の収集に役立ちます。



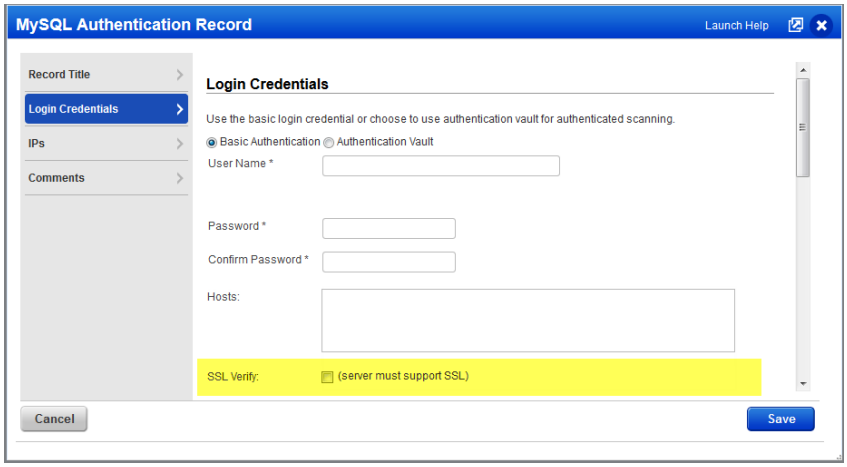
レコードに IP を追加する

入力された資格情報を使用してスキャンエンジンがログインする必要がある MySQL データベースの IP アドレスを選択します。



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。



最終更新日: 2020 年 6 月 19 日