



## 第 9 章 脆弱性評価デバイスの設定

VA (脆弱性評価) デバイスは MARS に、攻撃や脅威の対象となりうる多数のターゲットについての重要な情報を提供します。また、フォールス ポジティブを正確に評価するために役立つ情報も提供します。この情報は、ホストで稼働している OS (オペレーティングシステム)、OS のパッチ レベル、ホストで稼働しているアプリケーションのタイプ、およびホストで発生しているアクティビティの詳細ログなどです。

この章では、次に示す VA デバイスをブートストラップして、MARS に追加する方法を示します。

- ・ Foundstone FoundScan 3.0
- ・ eEye REM 1.0
- ・ Qualys QualysGuard デバイス

### Foundstone FoundScan 3.0

FoundScan からデータをプルするように MARS を設定するには、次の 3 つのタスクを実行する必要があります。

- ・ 必要なデータを相関付けるように Foundstone FoundScan を設定して、データを最新状態に保ちます。
- ・ HTML インターフェイスを使用して、MARS に Foundstone FoundScan サーバを追加します。
- ・ MARS が Foundstone FoundScan サーバ データをプルするインターバルをスケジュールします。

ここで説明する内容は、次のとおりです。

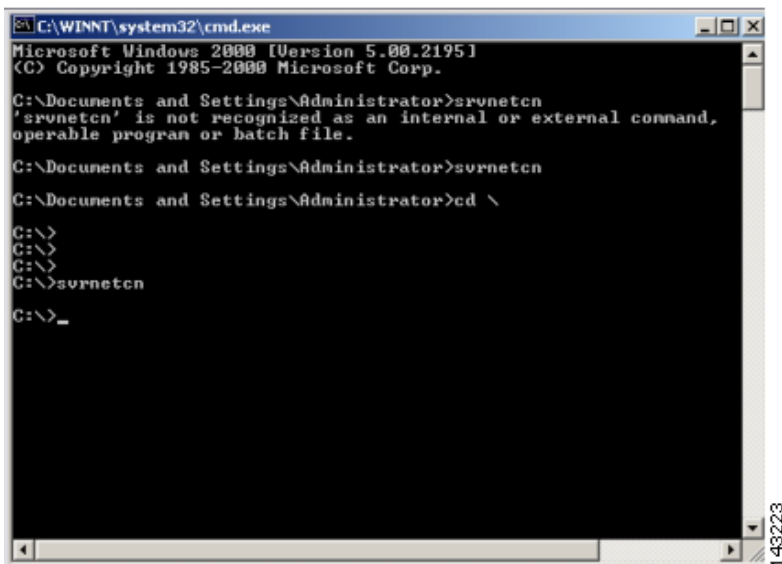
- ・ 必要なデータを生成するための FoundScan の設定
- ・ MARS での FoundScan デバイスの追加および設定

### 必要なデータを生成するための FoundScan の設定

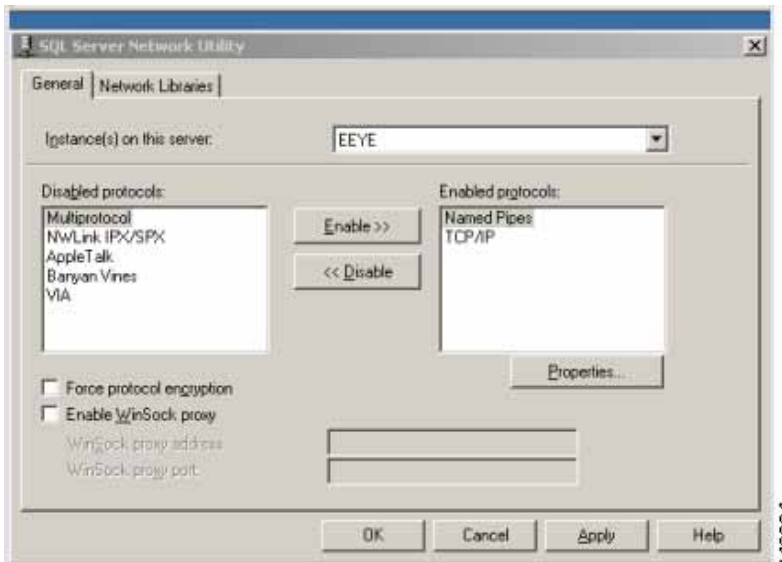
MARS にデータを提供するように FoundScan を設定する手順は、次のとおりです。

---

**ステップ 1** FoundScan がインストールされたホストの DOS プロンプトで、コマンド `svrnetcn` を実行します。



**ステップ 2** SQL Server Network Utility ダイアログボックスで、**TCP/IP** を Disabled Protocols リストから Enabled Protocols リストに移動して、TCP/IP をイネーブルにします。



**ステップ 3** **Apply** をクリックします。

## MARS での FoundScan デバイスの追加および設定

MARS に FoundScan デバイスを追加する手順は、次のとおりです。

**ステップ 1** **Admin > Security and Monitor Devices > Add** の順に選択します。

**ステップ 2** Device Type リストで **Add SW Security apps on a new host** または **Add SW security apps on existing host** を選択します。

**ステップ 3** 新しいホストを追加する場合は、デバイス名および IP アドレスを入力します。

**ステップ 4** **Apply** をクリックします。

**ステップ 5** **Reporting Application** タブをクリックします。

**ステップ 6** Select Application リストで、**Foundstone FoundScan 3.0** を選択します。

**ステップ7** Add をクリックします。

The screenshot shows a configuration window with the following fields and controls:

- \*Database Name: [Text Input]
- \*Access Port: [Text Input with value 1433]
- \*Access Type: [Dropdown Menu with MS SQL selected]
- Login: [Text Input]
- Password: [Text Input]
- Buttons: Cancel, Submit

**ステップ8** 次の情報を入力します。

- ・ **Database Name** — このデータベースの名前
- ・ **Access Port** — デフォルトのアクセス ポートは 1433 です。
- ・ **Access Type** — 値が MS SQL であることを確認します。
- ・ **Login** — データベースのログイン情報
- ・ **Password** — データベースのパスワード

**ステップ9** Submit をクリックします。

**ステップ10** Apply をクリックします。

このデバイスをアクティブにしたら (HTML インターフェイスで Activate をクリックしたら)、MARS がデバイスからデータをプルするスケジュールを定義する必要があります。詳細については、「トポロジー更新のスケジュール」を参照してください。

## eEye REM 1.0

この REM データをプルするように MARS を設定するには、次の 3 つのタスクを実行する必要があります。

- ・ 必要なデータを相関付けるように eEye REM を設定して、データを最新状態に保ちます。
- ・ HTML インターフェイスを使用して、MARS に eEye REM サーバを追加します。
- ・ MARS が eEye REM サーバ データをプルするインターバルをスケジュールします。

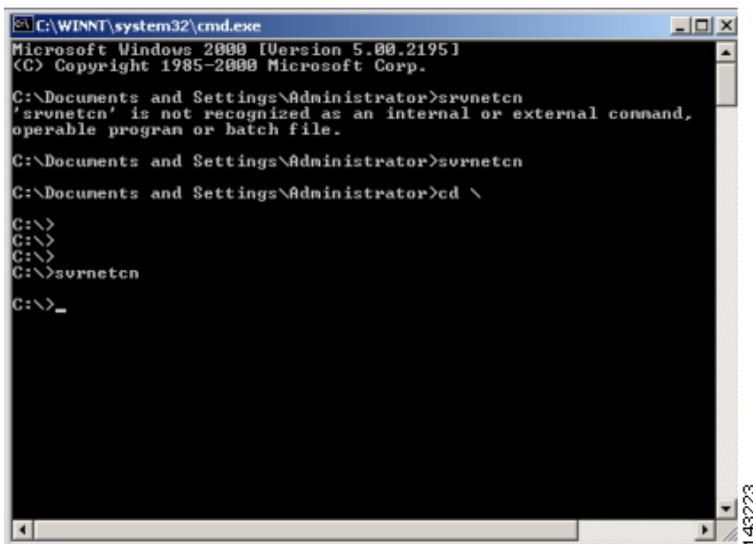
ここで説明する内容は、次のとおりです。

- ・ 必要なデータを生成するための eEye REM の設定
- ・ MARS での eEye REM デバイスの追加および設定

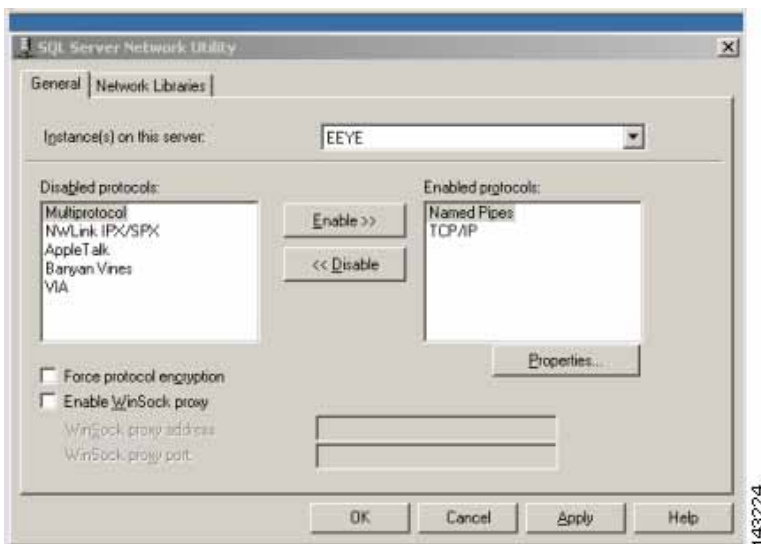
### 必要なデータを生成するための eEye REM の設定

MARS に正しいデータを提供するように eEye REM を設定する手順は、次のとおりです。

**ステップ1** eEye REM がインストールされたホストの DOS プロンプトで、コマンド `svrnetcn` を実行します。



**ステップ 2** SQL Server Network Utility ダイアログボックスで、TCP/IP を Disabled Protocols リストから Enabled Protocols リストに移動して、TCP/IP をイネーブルにします。



**ステップ 3** Apply をクリックします。

## MARS での eEye REM デバイスの追加および設定

MARS で eEye REM デバイスを追加する手順は、次のとおりです。

**ステップ 1** Admin > Security and Monitor Devices > Add の順に選択します。

**ステップ 2** Device Type リストで Add SW Security apps on a new host または Add SW security apps on existing host を選択します。

**ステップ 3** 新しいホストを追加する場合は、デバイス名および IP アドレスを入力します。

**ステップ 4** Apply をクリックします。

**ステップ 5** Reporting Applications タブをクリックします。

**ステップ 6** Select Application リストで、eEye REM 1.0 を選択します。

**ステップ7 Add** をクリックします。

**ステップ8** 次の情報を入力します。

- ・ **Database Name** — このデータベースの名前
- ・ **Access Port** — デフォルトのアクセス ポートは 1433 です。
- ・ **Login** — データベースのログイン情報
- ・ **Password** — データベースのパスワード情報

**ステップ9 Submit** をクリックします。

**ステップ10 Apply** をクリックします。

このデバイスをアクティブにしたら (HTML インターフェイスで Activate をクリックしたら)、MARS がデバイスからデータをプルするスケジュールを定義する必要があります。詳細については、「トポロジー更新のスケジュール」を参照してください。

## Qualys QualysGuard デバイス

MARS では、QualysGuard デバイスは、QualysGuard API Server (Qualys によってホストされる中央 API サーバ) に対する特定のレポートクエリーを表します。QualysGuard API Server は、MARS と連携するように設定する唯一のサーバです。各 MARS アプライアンスは、モニタ対象のネットワーク セグメントのフォールス ポジティブを識別する役割を負っているため、MARS アプライアンスでモニタ中のネットワーク セグメントのデバイスに関するレポートを QualysGuard API Server によって確実に提供できるようにします。

ユーザが QualysGuard サービスに加入している場合、MARS は QualysGuard XML API バージョン 3.3 を使用して、QualysGuard データベースから VA データをプルすることができます。このデータをプルするように MARS を設定するには、次の 3 つのタスクを実行する必要があります。

- ・ 必要なデータを収集するように QualysGuard を設定して、データを最新状態に保ちます。
- ・ HTML インターフェイスを使用して、MARS へのレポートクエリーを表す QualysGuard デバイスを追加します。
- ・ MARS が QualysGuard デバイス データをプルするインターバルをスケジュールします。



**注** プロキシ サーバが QualysGuard サーバと MARS アプライアンスの間に配置されている場合は、Admin > System Parameters > Proxy Settings ページで定義された設定が使用されます。詳細については、「[Specify the Proxy Settings for the Global Controller or Local Controller](#)」(p.6-12)を参照してください。

ここで説明する内容は、次のとおりです。

- ・ ネットワークをスキャンするための QualysGuard の設定
- ・ MARS での QualysGuard デバイスの追加および設定
- ・ データをプルするインターバルのスケジュール

QualysGuard 統合に関するトラブルシューティング

## ネットワークをスキャンするための QualysGuard の設定

MARS は SSL (TCP ポート 443) を介して QualysGuard XML API およびパスワードベース認証を使用して、QualysGuard API Server からスキャン レポートを取得します。したがって、MARS との接続を許可するように QualysGuard サーバを設定する必要はありません。必要なのは、アクティブなアカウントを保持し、ネットワークを正しくスキャンするように設定された Qualys に加入することだけです。

MARS はデフォルトで、QualysGuard サーバに保存された最新のスキャン レポートを取得する必要があると想定しています。分析する IP アドレス数に応じて、QualysGuard スキャンの所要時間は数秒から数分になります。この所要時間を予測することにより、保存された最新のスキャン レポートを使用できるようにネットワークを特定の頻度で自動スキャンするようにスケジュールすることができます。QualysGuard の管理インターフェイスを使用すると、スキャンの所要時間を判別し、それに従ってスケジュールを設定することができます。

## MARS での QualysGuard デバイスの追加および設定

内部 QualysGuard API Server をレポート デバイスとして追加すると、レポートをプルする元になるサーバまたはアプライアンスが識別され、MARS がデバイスにログインしてレポートをプルする場合に使用できる証明書が作成されます。スケジュールで実行される保存済みスキャン レポートをプルするかどうか、またはオンデマンド スキャン レポートを開始して取得するかどうかを指定できます。

QualysGuard デバイスを追加する手順は、次のとおりです。

**ステップ 1** Admin > Security and Monitor Devices > Add の順に選択します。

**ステップ 2** Device Type リストで、QualysGuard 3.x を選択します。

Note:

1. \* denotes a required field.

Device Type:

→ *Device Name:	<input type="text"/>
→ Access IP:	165.193.18.12
→ *URL:	<input type="text" value="https://qualysapi.qualys.com/mssp/scan_report_list.php?last=yes"/>
Login:	<input type="text"/>
Password:	<input type="text"/>

143206

**ステップ 3** Device Name フィールドに Qualys デバイスの名前を入力します。

この名前は、MARS 内で Qualys デバイスを一意に識別する場合に使用されます。レポートおよびクエリー結果でこのデバイスを識別する場合にも、この名前が使用されます。

IP アドレス フィールドは読み取り専用です。この値は 165.193.18.12 に固定されていますが、これは重要なことです。Local Controller では、Qualys デバイスとして定義されたレポート クエリーをすべてプルする場合、定義できるスケジュールが 1 つに限定されるためです。ただし、複数の Local Controller 全体で一意的なスケジュールを定義することもできます。詳細については、「トポロジー更新のスケジュール」を参照してください。

**ステップ 4** URL フィールドに、デバイスおよびレポートのタイプを識別する URL を入力します。

URL は次の情報を提供します。

- **Server** - レポートをプルする元となるサーバを識別します。この値は、プライマリ Qualys サーバを識別するホスト名または IP アドレスとして指定することができます。

**Report type** - Real-time または Last Saved. デフォルト値は次のとおりです。

- *Real-time Report.* `qualysguard.qualys.com/msp/scan.php?ip=[addresses]`

`addresses` 属性はスキャン要求のターゲット IP アドレスを指定します。

IP アドレスは複数の IP アドレス、IP 範囲、または両方の組み合わせで入力できます。複数の IP アドレスを指定する場合は、次のようにカンマで区切る必要があります。

123.123.123.1,123.123.123.4,123.123.123.5

IP アドレス範囲は、次のように IP アドレスの先頭と末尾をダッシュ(-)で区切って指定します。

123.123.123.1-123.123.123.8

IP アドレスと IP 範囲を組み合わせで指定できます。複数のエントリを指定する場合は、次のようにカンマで区切る必要があります。

123.123.123.1-123.123.123.5,194.90.90.3,194.90.90.9



**注** Scanner Appliance を使用して、内部ネットワークのプライベート IP アドレスをスキャンする必要があります。

- *Last Saved Report.* `qualysapi.qualys.com/msp/scan_report_list.php?last=yes`

**ステップ 5** Login フィールドに、MARS が Qualys デバイスにアクセスするために使用するアカウントのユーザ名を入力します。

**ステップ 6** Password フィールドに、ステップ 5 で特定したアカウントに対応するパスワードを入力します。

**ステップ 7** (任意)設定が正しいこと、および MARS アプライアンスがこの Qualys デバイスと通信できることを確認するには、**Test Connectivity** をクリックします。

テスト中にエラーメッセージが表示された場合は、「QualysGuard 統合に関するトラブルシューティング」を参照してください。

**ステップ 8** MARS データベースにデバイスを追加するには、**Submit** をクリックします。

このデバイスをアクティブにしたら (HTML インターフェイスで **Activate** をクリックしたら)、MARS がデバイスからデータをプルするスケジュールを定義する必要があります。詳細については、「データをプルするインターバルのスケジュール」を参照してください。

## データをプルするインターバルのスケジュール

Qualys デバイスをアクティブにしたら (各デバイスが QualysGuard API Server で実行される特定のレポートクエリーを表している場合)、MARS がデバイスからデータをプルするスケジュールを定義する必要があります。定義するスケジュール (更新規則) は、すべての Qualys デバイスで同一です。この更新規則は、Qualys Access IP である固定 IP アドレス (165.193.18.12) に基づいて設定されます。このアドレスを使用して更新規則を定義する場合は、すべての Qualys デバイスがこのスケジュールに基づいて更新されます。MARS が Qualys デバイスに問い合わせ中のときは、ネットワーク上に Qualys デバイスが複数配置されている場合でも、スタガすることはできません。ただし、複数の Local Controller 全体で一意的スケジュールを定義することはできません。

更新規則のさまざまな使用方法については、「トポロジー更新のスケジュール」を参照してください。

Qualys デバイスをすべて検出するための規則を定義する手順は、次のとおりです。

**ステップ 1** **Admin > Topology/Monitored Device Update Scheduler** の順にクリックします。

Topology/Monitored Device Update Scheduler ページが表示されます。

**ステップ 2** **Add** をクリックします。

**ステップ 3** Name フィールドに *Qualys Devices* などの有意な値を入力します。

この名前は、Topology/Monitored Device Update Scheduler ページに表示される規則リスト内の規則を識別します。

**ステップ 4** **Network IP** オプション ボタンを選択し、Network IP フィールドと Mask フィールドに 165.193.18.12 および 255.255.255.255 をそれぞれ入力します。

**ステップ 5 Add** をクリックして、選択したフィールドにデバイスを移動します。

**ステップ 6** Schedule テーブルで **Daily** を選択し、**Time of Day** リストで時間値を選択します。

このデータはオフピークの時間帯に毎日プルすることを推奨します。ただし、組織に適した任意のインターバルを定義することができます。

**ステップ 7 Submit** をクリックします。

Topology/Monitored Device Update Scheduler ページのリストに更新規則が表示されます。

**ステップ 8 Activate** をクリックします。



**ヒント** この検出をオンデマンドで実行するには、定義した規則の横にあるチェックボックスをオンにして、**Run Now** をクリックします。

## QualysGuard 統合に関するトラブルシューティング

表 9-1 に、発生する可能性のあるエラー、および考えられる原因やソリューションを示します。

**表 9-1 QualysGuard および MARS の統合に関するエラー表**

エラー/現象	対処法/ソリューション
テスト接続に失敗した(詳細については、View Errors ボタンをクリックしてください)。 サーバを使用できない。	このエラーは、MARS と Qualys デバイスを接続できなかったことを意味します。このメッセージの原因として、2 つの問題が考えられます。 <ul style="list-style-type: none"> <li>URL フィールドに無効なホスト名または IP アドレスを入力した可能性があります。入力した値が正しいかどうかを確認します。</li> <li>ネットワーク上のプロキシ サーバやファイアウォール、およびゲートウェイによってトラフィックがブロックされている可能性があります。MARS アプライアンスと Qualys デバイス間で SSH トラフィック(TCP ポート 443)を送受信できるようにします。Admin&gt; System Parameters&gt; Proxy Setting ページで、プロキシ サーバの設定を正しく入力します。</li> </ul>
スキャン レポートを解析できない。	このエラーは、MARS が Qualys デバイスからプルされたスキャン レポートを解析できなかったことを意味します。このメッセージの原因として、2 つの問題が考えられます。 <ul style="list-style-type: none"> <li>QualysGuard デバイスのデータが破壊されています。</li> <li>QualysGuard デバイスの問題または QualysGuard デバイスのソフトウェア アップグレードにより、レポートのフォーマットが変更されています。</li> </ul> QualysGuard デバイスで稼働しているバージョンがサポートされていること、およびデバイスデータが破損していないことを確認します。
ユーザ証明書が無効である。	このエラーは、MARS が Qualys デバイスを認証できなかったことを意味します。このメッセージの原因として、2 つの問題が考えられます。 <ul style="list-style-type: none"> <li>指定したログイン証明書が正しくない可能性があります。値が正しく入力されたこと、および指定したアカウントに十分な権限が設定されていることを確認します。</li> <li>アカウントの期限が切れている可能性があります。Qualys による加入サービスを更新します。</li> </ul>