WBM の起動とカスタマイズ

Detector の WBM にアクセスするには、まず CLI を使用して Detector の WBM サービスをイネーブルにし、クライアントの IP アドレスから WBM へのネットワーク アクセスを許可します。この作業を終えると、クライアントの Web ブラウザを使用して、ネットワーク接続経由で Detector の WBM にアクセスすることができます。

この章は、次の項で構成されています。

WBM のネットワーク アクセスの設定

WBM サービスをイネーブルにし、WBM から Detector へのネットワーク アクセスを許可するには、Detector の CLI を使用します。必要な設定変更を行うには、Administration ユーザ特権レベルまたは Configuration ユーザ特権レベルの権限を持つユーザとしてログインする必要があります。Detector の CLI へのアクセスと使用方法の詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

WBM のネットワーク アクセスを設定するには、次の手順を実行します。

ステップ 1　コンソールまたは Secure Shell（SSH）接続を使用して、Detector の CLI にログインします。

ステップ 2　次のコマンドをグローバル モードで入力して、設定モードに入ります。

```
admin@GUARD# configure
```

ステップ 3　次のコマンドを入力して、WBM サービスをイネーブルにします。

```
admin@DETECTOR-conf# service wbm
```

ステップ 4　次のコマンドを入力して、WBM から Detector へのアクセスを許可します。

```
admin@DETECTOR-conf# permit wbm ip-addr [ip-mask]
```

引数 *ip-addr* および *ip-mask* は、WBM から接続するときの接続元 IP アドレスを定義します。

次の例は、IP アドレス 192.168.30.32 を使用して接続する WBM のネットワーク アクセスを設定する方法を示しています。

```
admin@DETECTOR# configure
admin@DETECTOR-conf# service wbm
admin@DETECTOR-conf# permit wbm 192.168.30.32
```

Detector 上で WBM のネットワーク アクセスを設定した後は、CLI を終了し、Web ブラウザを使用して WBM を起動することができます。

WBM の起動

WBM を起動するには、次の手順を実行します。

ステップ 1　Web ブラウザを開いて、Secure HTTP（HTTPS）を使用して Detector の IP アドレスを入力します。

```
https://Detector-ip-address/
```

Detector-ip-address 引数には、Detector の管理 IP アドレスを指定します。

Detector WBM のログイン ウィンドウが表示されます。

ステップ 2　ユーザ名とパスワードを入力し、**OK** をクリックします。WBM のホーム ページが表示されます。

（注）　TACACS+ 認証が設定されている場合、ユーザ認証にはローカル データベースではなく、TACACS+ ユーザ データベースが使用されます。TACACS+ サーバ上に詳細な認証アトリビュート（パスワードの有効期限など）が設定されている場合、Detector は、TACACS+ サーバ上のユーザの設定に基づいて、ユーザに新しいパスワードを要求したり、パスワードの有効期限が近づいたときに通知したりできます。

ユーザ認証方式を設定するには、Detector CLI を使用します。Detector の CLI へのアクセスと使用の詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

Detector への接続に失敗した場合は、次のトラブルシューティングに関するヒントを確認します。

- 有効なユーザ名とパスワードを入力したことを確認します。
- Detector の管理 IP アドレスを正しく入力し、HTTPS を使用していることを確認します。

- WBM と Detector の両方のネットワーク接続を確認します。
- SSH を使用して WBM から Detector に接続できることを確認します。SSH を使用して接続することにより、WBM と Detector の間のネットワーク接続が確認されます。
- WBM サービスがイネーブルになっていて、WBM の IP アドレスから Detector へのアクセスが許可されていることを確認します（詳細については、P.2-2 の「WBM のネットワーク アクセスの設定」を参照）。

ログイン バナーの設定

ログイン バナーは、SSH セッション、コンソール ポート接続、または Detector に対する WBM セッションを開いたときにユーザ認証の前に画面に表示されるテキストです。

ログイン バナーは、次の位置に表示されます。

- CLI：パスワード ログイン プロンプトの前
- WBM：Detector ログイン ウィンドウの右側

ログイン バナーを設定するには、Detector **login-banner** CLI コマンドを使用します。必要な設定変更を行うには、Administration ユーザ特権レベルまたは Configuration ユーザ特権レベルの権限を持つユーザとしてログインする必要があります。

ログイン バナーの設定とインポートの詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

WBM ロゴの設定

WBM Web ページに会社のロゴ（あるいは、カスタマイズした任意のロゴ）を追加することで、WBM インターフェイスをカスタマイズできます。

新しいロゴは、次の位置に表示されます。

- Detector Login ページでは、Cisco Systems ロゴの下
- Detector Login ページ以外のすべての WBM ページでは、Cisco Systems ロゴの右側

WBM ロゴを設定するには、Detector **copy wbm-logo** CLI コマンドを使用します。必要な設定変更を行うには、Administration ユーザ特権レベルまたは Configuration ユーザ特権レベルの権限を持つユーザとしてログインする必要があります。

WBM ロゴのインポートの詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。