Oracle® Enterprise Manager

System Monitoring Plug-in インストレーション・ガイド for Check Point Firewall

10*g* リリース 2（10.2）

部品番号 : E05526-01

原典情報 : B28038-02 Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Check Point Firewall, 10*g* Release 2 (10.2)

2007 年 7 月

このドキュメントには、Oracle System Monitoring Plug-in for Check Point Firewall に関する簡単な説明、プラグインでサポートされるバージョンの詳細、およびプラグインのインストールの前提条件が記載されています。また、プラグインのダウンロード、インストール、検査および検証方法の手順も記載されています。

1 説明

System Monitoring Plug-in for Check Point Firewall は、Oracle Enterprise Manager Grid Control を拡張して、Check Point Firewall の管理に対するサポートを追加します。Grid Control 環境にプラグインをデプロイすると、次の Check Point Firewall 管理機能を取得できます。

- Check Point Firewall デバイスの監視。
- Check Point Firewall インスタンスの構成の収集および構成の変更の追跡。
- 監視データおよび構成データに設定されたしきい値に基づくアラートおよび違反の表示。
- 収集データに基づいた、ユーザー・インタフェースに関する豊富なレポートの提供。
- リモート・エージェントによる監視のサポート。リモート監視の場合、Check Point Firewall と同じコンピュータ上にエージェントを配置する必要はありません。

2 サポートされるプラットフォーム

プラグインは、Linux および UNIX 上で Check Point Firewall インスタンスの監視をサポートします。

3 サポートされるバージョン

このプラグインでは、次のバージョンの製品がサポートされます。

- Enterprise Manager Grid Control 10*g* リリース 2 の管理サービスおよびエージェント
- Check Point Firewall のバージョン :
  - NG-AI（R54）
  - NG-AI（R55）
  - NG-AI（R60）
  - NGX

4 前提条件

プラグインをデプロイする前に、次の前提条件を設定する必要があります。

- Oracle Enterprise Manager Grid Control 10*g* リリース 2 以上のシステムおよびエージェント。
- Check Point Firewall インスタンス。
- SNMP コミュニティ（デフォルト・コミュニティの「パブリック」以外）が構成されており、Check Point Firewall ターゲットの監視に必要な場合、この特定の Simple Network Management Protocol（SNMP）コミュニティに対して Enterprise Manager エージェントの IP アドレスを追加する必要があります。
- 事前定義済サービス `snmp`（UDP ポート 161）および `FW1_snmp`（UDP ポート 260）を必要に応じて使用した Enterprise Manager Grid Control システムから Check Point Firewall への接続を許可する構成済セキュリティ・ポリシー・ルール。

  Linux/UNIX オペレーティング・システムの場合、前提条件は次のようになります。

  - ホスト SNMP デーモン（`snmpd`）およびファイアウォール SNMP デーモン（`cpsnmpd`）の両方が Check Point Firewall デバイス上で実行されている必要があります。
  - UCD-SNMP-MIB の登録。

  関連項目： 「UNIX/Linux の前提条件の手順」

ここで示す情報は、Check Point Firewall デバイスで SNMP `gets` を有効にするための前提条件の手順です。追加情報は、Check Point のドキュメントを参照してください。

5 プラグインのデプロイ

前提条件を満たしていることを確認した後、次の手順に従ってプラグインをデプロイします。

1. Check Point Firewall プラグインのアーカイブを、ブラウザを起動しているデスクトップまたはコンピュータにダウンロードします。アーカイブは、Oracle Technology Network（OTN）からダウンロードできます。
2. スーパー管理者として Enterprise Manager Grid Control にログインします。
3. Grid Control ホームページの右上隅にある**「設定」**リンクをクリックし、次に「設定」ページの左側にある**「管理プラグイン」**リンクをクリックします。
4. **「インポート」**をクリックします。
5. **「参照」**をクリックしてプラグインのアーカイブを選択します。
6. **「リスト・アーカイブ」**をクリックします。
7. プラグインを選択して**「OK」**をクリックします。
8. プラグインのデプロイ先のエージェントすべてに優先資格証明を設定したことを確認します。
9. 「管理プラグイン」ページで、Check Point Firewall プラグインの**「デプロイ」**列のアイコンをクリックします。管理プラグインのデプロイ・ウィザードが表示されます。
10. **「エージェントの追加」**をクリックして、プラグインのデプロイ先のエージェントを 1 つ以上選択します。ウィザードが再び表示され、選択したエージェントが表示されます。

11. **「次へ」**をクリックし、**「終了」**をクリックします。

    優先資格証明が設定されていないというエラー・メッセージが表示された場合、「プリファレンス」ページに移動してエージェント・ターゲット・タイプの優先資格証明を追加します。

6 監視対象インスタンスの追加

プラグインを正常にデプロイした後、プラグイン・ターゲットを集中監視および管理するために、次の手順に従って Grid Control に追加します。

1. Check Point Firewall プラグインをデプロイしたエージェントのホームページで、**「追加」**ドロップダウン・リストから **Check Point Firewall** ターゲット・タイプを選択し、**「実行」**をクリックします。Check Point Firewall の追加ページが表示されます。
2. プロパティに次の情報を入力します。
   - **名前 :** プラグインの名前（My_Check_Point_1 など）。
   - **ファイアウォールのホスト名または IP アドレス :** Check Point Firewall デバイスの名前 /IP アドレス。
   - **Check Point SNMP デーモンのポート :** Check Point SNMP デーモンが実行されているポート番号。Linux プラットフォームの場合、デフォルトは 260 です。
   - **ホスト SNMP デーモンのポート :** OS のネイティブ SNMP デーモンが実行されているポート番号。デフォルトは 161 です。
   - **SNMP コミュニティ :** エージェントの IP アドレスを追加するコミュニティの名前。デフォルトは「パブリック」です。
   - **SNMP タイムアウト :** SNMP コールを終了するタイムアウト値。値は 5 に設定することをお薦めします。
   - **Check Point Firewall Web UI の URL:** Check Point Web インタフェースの URL。
   - **Telnet の有効化（y/n）:** Check Point Firewall デバイスで Telnet が有効になっている場合、デフォルト値の**「Y」**を指定します。それ以外の場合、このフィールドは空白にしておきます。
3. **「接続テスト」**をクリックして、入力したパラメータが正しいことを確認します。
4. 接続テストが成功した場合、手順 2 の暗号化されたパラメータを再入力して、**「OK」**をクリックします。

注意 : プラグインをデプロイして、環境内で 1 つ以上のターゲットを監視するように構成した後、プラグインの監視設定をカスタマイズできます。これにより、環境の特別な要件を満たすようにメトリックの収集間隔およびしきい値の設定を変更できます。メトリックの収集を 1 つ以上無効にした場合、メトリックなどに関するレポートに影響を与える可能性があります。

---

7 プラグインの検査および検証

プラグインでデータの収集が開始するまで数分間待機した後、次の手順を使用して、プラグイン・ターゲットが Enterprise Manager で適切に監視されていることを検査および検証します。

1. エージェントのホームページの「監視ターゲット」表で、Check Point Firewall ターゲット・リンクをクリックします。Check Point Firewall のホームページが表示されます。
2. 「メトリック」表に、メトリック収集エラーが報告されていないことを確認します。
3. **「レポート」**プロパティ・ページを選択して、レポートが表示されていること、およびエラーが報告されていないことを確認します。
4. 「構成」セクションの**「構成の表示」**リンクをクリックして、構成データが表示されていることを確認します。構成データがすぐに表示されない場合は、「構成の表示」ページで**「リフレッシュ」**をクリックします。

8 UNIX/Linux の前提条件の手順

「プラグインのデプロイ」に進む前に、次の操作を実行します。

1. `/etc/snmp` または `/etc/SnmpAgent.d` にある `snmpd.conf` ファイルを見つけます。詳細は、次の SNMP.CONF Web サイトで、「Directories Searched」セクションを参照してください。

   `http://net-snmp.sourceforge.net/docs/man/snmp_config.html`

2. `snmpd.conf` ファイルを編集し、次の OID に対して SNMP コールを有効にします。

```
# Make at least snmpwalk -v 1 localhost -c public system fast again.
#       name           incl/excl     subtree         mask(optional)
view    systemview    included   .1.3.6.1.2.1.1
view    systemview    included   .1.3.6.1.2.1.2
view    systemview    included   .1.3.6.1.4.1.2021.11
view    systemview    included   .1.3.6.1.4.1.2021.4
view    systemview    included   .1.3.6.1.2.1.25
view     systemview     included   .1.3.6.1.2.1.4
```

3. Check Point Firewall デバイスに対して、次のコマンドを順次実行します。
   1. `service snmpd stop`

      `snmpd` サービスが実行中の場合、コマンドの出力は次のようになります。

      ```
      stopping snmpd              [OK]
      ```

      `snmpd` サービスが実行中でない場合、コマンドの出力は次のようになります。

      ```
      stopping snmpd              [FAILED]
      ```

   2. service snmpd start

      コマンドの出力は次のようになります。

      ```
      starting snmpd              [OK]
      ```

4. `cpconfig` コマンドを使用して、Check Point の SNMP 拡張を有効にします。

   UNIX プラットフォームには、`cpsnmpd` という特殊な Check Point SNMP デーモンがインストールされています。このデーモンでは、VPN-1 Pro 固有オブジェクトのステータス情報が提供されます。このデーモンは、デフォルトでは実行されません。デーモンを有効または無効にするには、`cpconfig` を使用します。有効になると、デーモンはポート 260 でリスニングします。

注意： Check Point デーモンの前に標準 UNIX SNMP デーモンがロードされ、ポート 161 にバインディングされます。標準デーモンが実行されていない場合、cpsnmpd は両方のポート（161 および 260）にバインディングされます。両方のポートが前のプロセスに占有されている場合、Check Point デーモンは実行されません。さらに、認識されない OID に対するリクエストを Check Point デーモンが受信した場合、このリクエストは OS の標準 SNMP デーモンに転送されません。

9 プラグインのアンデプロイ

プラグインをエージェントからアンデプロイするには、次の手順を実行します。

1. スーパー管理者として Enterprise Manager Grid Control にログインします。
2. **「ターゲット」**タブを選択して、次に**「すべてのターゲット」**サブタブを選択します。「すべてのターゲット」ページが表示されます。
3. Check Point Firewall プラグイン・ターゲットを選択して**「削除」**をクリックします。この手順は、プラグインのすべてのターゲットに対して実行する必要があります。
4. プラグインのデプロイ先のエージェントに優先資格証明が設定されていることを確認します。
5. 「すべてのターゲット」ページの右上隅にある**「設定」**リンクをクリックし、次に「設定」ページの左側にある**「管理プラグイン」**リンクをクリックします。「管理プラグイン」ページが表示されます。
6. Check Point Firewall プラグインの**「アンデプロイ」**列のアイコンをクリックします。「管理プラグインのアンデプロイ」ページが表示されます。
7. Check Point Firewall プラグインに現在デプロイされているエージェントをすべて選択して**「OK」**をクリックします。

   プラグインを Enterprise Manager から完全に削除するには、システムのすべてのエージェントからアンデプロイする必要があります。
8. 「管理プラグイン」ページで Check Point Firewall プラグインを選択して、**「削除」**をクリックします。

10 ドキュメントのアクセシビリティについて

オラクル社は、障害のあるお客様にもオラクル社の製品、サービスおよびサポート・ドキュメントを簡単にご利用いただけることを目標としています。オラクル社のドキュメントには、ユーザーが障害支援技術を使用して情報を利用できる機能が組み込まれています。HTML 形式のドキュメントで用意されており、障害のあるお客様が簡単にアクセスできるようにマークアップされています。標準規格は改善されつつあります。オラクル社はドキュメントをすべてのお客様がご利用できるように、市場をリードする他の技術ベンダーと積極的に連携して技術的な問題に対応しています。オラクル社のアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト http://www.oracle.com/accessibility/ を参照してください。

ドキュメント内のサンプル・コードのアクセシビリティについて

スクリーン・リーダーは、ドキュメント内のサンプル・コードを正確に読めない場合があります。コード表記規則では閉じ括弧だけを行に記述する必要があります。しかし JAWS は括弧だけの行を読まない場合があります。

外部 Web サイトのドキュメントのアクセシビリティについて

このドキュメントにはオラクル社およびその関連会社が所有または管理しない Web サイトへのリンクが含まれている場合があります。オラクル社およびその関連会社は、それらの Web サイトのアクセシビリティに関しての評価や言及は行っておりません。

Oracle サポート・サービスへの TTY アクセス

アメリカ国内では、Oracle サポート・サービスへ 24 時間年中無休でテキスト電話（TTY）アクセスが提供されています。TTY サポートについては、(800)446-2398 にお電話ください。

11 サポートおよびサービス

次の各項に、各サービスに接続するための URL を記載します。

Oracle サポート・サービス

オラクル製品サポートの購入方法、および Oracle サポート・サービスへの連絡方法の詳細は、次の URL を参照してください。

```
http://www.oracle.co.jp/support/
```

製品マニュアル

製品のマニュアルは、次の URL にあります。

```
http://otn.oracle.co.jp/document/
```

研修およびトレーニング

研修に関する情報とスケジュールは、次の URL で入手できます。

```
http://www.oracle.co.jp/education/
```

その他の情報

オラクル製品やサービスに関するその他の情報については、次の URL から参照してください。

```
http://www.oracle.co.jp
http://otn.oracle.co.jp
```

注意： ドキュメント内に記載されている URL や参照ドキュメントには、Oracle Corporation が提供する英語の情報も含まれています。日本語版の情報については、前述の URL を参照してください。
