Oracle® Enterprise Manager

System Monitoring Plug-in インストレーション・ガイド for Juniper Networks NetScreen Firewall

リリース 6（2.1.1.0.0）

部品番号 : E06098-01

原典情報 : E11850-01 Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Juniper Networks NetScreen Firewall, Release 6 (2.1.1.0.0)

2008 年 3 月

このドキュメントでは、まず Oracle System Monitoring Plug-in for Juniper Networks NetScreen Firewall の概要を説明し、次に、このプラグインでサポートされるバージョンの詳細、およびインストールの前提条件を示します。さらに、プラグインをダウンロード、インストール、検査および検証するための手順を説明します。

1 説明

System Monitoring Plug-in for Juniper Networks NetScreen Firewall は、Oracle Enterprise Manager Grid Control を拡張して、NetScreen Firewall を管理できるようにするためのプラグインです。このプラグインを Grid Control 環境にデプロイすることで、次の管理機能を使用できるようになります。

- Juniper Networks NetScreen Firewall デバイスの監視。
- Juniper Networks NetScreen Firewall インスタンスの構成データ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、NetScreen 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。
- Juniper NetScreen プラグインは、NSRP クラスタ内に構成されたデバイスのステータス監視をサポートしています。ファイアウォールのステータスが Master から他のステータス（Primary Backup、Ineligible、Inoperable など）に変わると、アラートが生成されます。また、ファイアウォールのステータスが Master に戻ったときにはクリア・メッセージが送信されます。

> **注意 :** NSRP（NetScreen Redundancy Protocol）は、高可用性（HA）サービスを提供するために一部の NetScreen デバイスでサポートされている、プロプライエタリなプロトコルです。NSRP クラスタを構成する NetScreen デバイスのグループでは、全体にわたって同じセキュリティ・ポリシーが施行されるとともに、同じ構成内容が共有されます。詳細は NetScreen のドキュメントを参照してください。

2 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 以上の管理サービスおよびエージェント。
- ScreenOS バージョン 5.0.0 以上の Juniper Networks NetScreen Firewalls、および ScreenOS バージョン 5.0.0 と下位互換性のある Juniper Networks NetScreen Firewalls。次のバージョンの NetScreen Firewall がサポートされます。
  - NetScreen-5 Series
  - NetScreen-25/50
  - NetScreen-204/208
  - NetScreen-500
  - NetScreen-5200/5400
  - ISG Series

3 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。
- NetScreen Firewall インスタンス。
- NetScreen Firewall 上に構成された SNMP コミュニティにエージェントの IP アドレスを追加する必要があります。手順は、「エージェントの IP アドレスの追加」を参照してください。
- Linux の場合、ファイアウォール SNMP デーモンが NetScreen Firewall デバイス上で実行されている必要があります。
- Windows の場合、標準 Windows SNMP エージェントがインストールされ、SNMP サービスが実行されている必要があります。

4 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. Juniper Networks NetScreen 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、NetScreen 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。

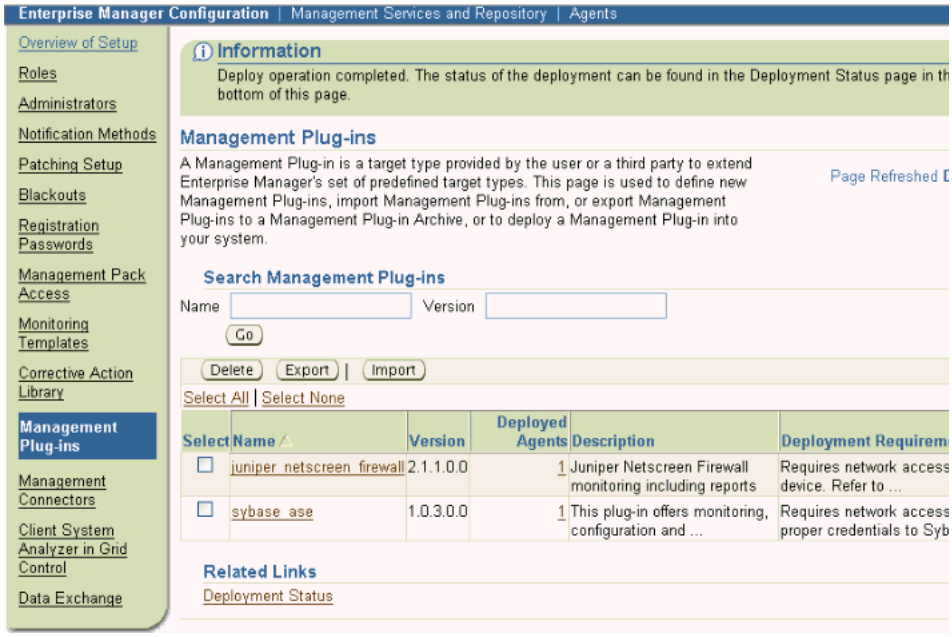
10. **「エージェントの追加」**をクリックして、プラグインのデプロイ先のエージェントを 1 つ以上選択します。ウィザードが再び表示され、選択したエージェントが表示されます。

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・タイプおよびエージェントがあるホスト・ターゲット・タイプの優先資格証明を追加します。

    エラーがなければ、次の画面が表示されます。

図 1　デプロイ成功時の画面



5 監視対象インスタンスの追加

プラグインが正常にデプロイできたら、次の手順に従って、プラグイン・ターゲットを Grid Control に追加します。これにより、ターゲットが集中的な監視および管理の対象になります。

1. Juniper Networks NetScreen 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 **NetScreen Firewall** ターゲット・タイプを選択し、**「実行」**をクリックします。Juniper NetScreen 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 Juniper 1 など）。
   - **ファイアウォールのホスト名または IP アドレス :** 監視対象の NetScreen Firewall の名前または IP アドレス。

- **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 NetScreen Firewall 上のポート番号。デフォルトは 161 です。

  NetScreen Firewall コマンドライン・インタフェースで、コマンド `get snmp settings` を使用するか、ファイアウォールの Web インタフェースから次の操作を実行すると、ポート番号を特定できます。

  – **「Configuration」**リンクをクリックします。

  – **「Report Settings」**リンクをクリックします。

  – **「SNMP」**リンクをクリックします。

  Web UI でリスニング・ポートに指定された値は、SNMP デーモンのポートです。

- **SNMP コミュニティ :** エージェントの IP アドレスを追加する SNMP コミュニティの名前。デフォルトは「パブリック」です。

  NetScreen Firewall コマンドライン・インタフェースで、コマンド `get snmp settings` を使用するか、ファイアウォールの Web インタフェースから次の操作を実行すると、コミュニティの名前を特定できます。

  – **「Configuration」**リンクをクリックします。

  – **「Report Settings」**リンクをクリックします。

  – **「SNMP」**リンクをクリックします。

  – Enterprise Manager エージェントの IP アドレスを追加したコミュニティを選択します。

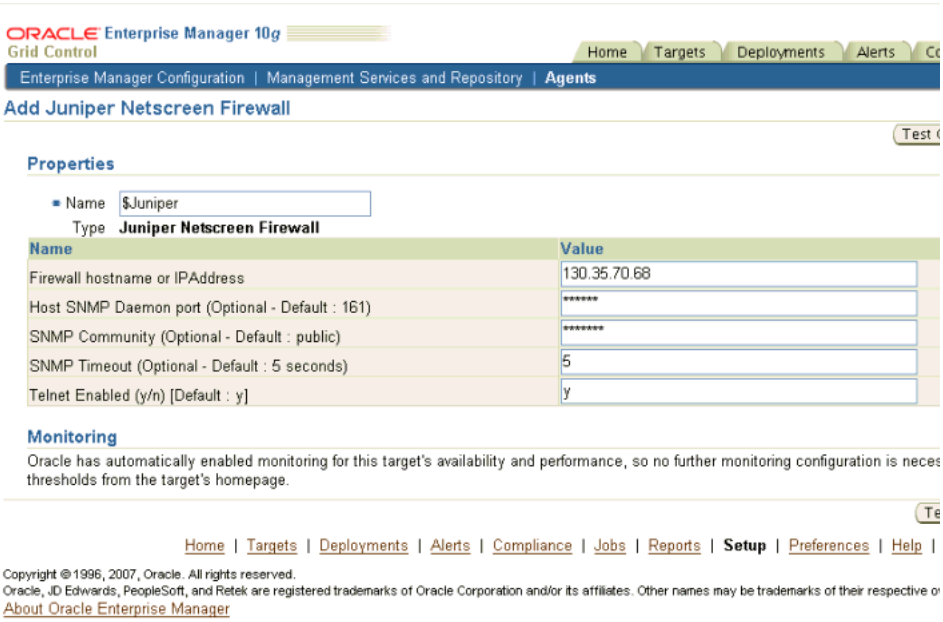
- **SNMP タイムアウト :** SNMP コールを終了するタイムアウト値。デフォルト値は 5 秒です。

- **Telnet 有効（y/n）:** Netscreen 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設定した後、プラグインの監視設定をカスタマイズして、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することができます。なお、1 つ以上のメトリックについて収集を無効にした場合、それらのメトリックを使用したレポートに影響が及ぶ可能性があります。

図 2　Juniper NetScreen Firewall の追加ページ

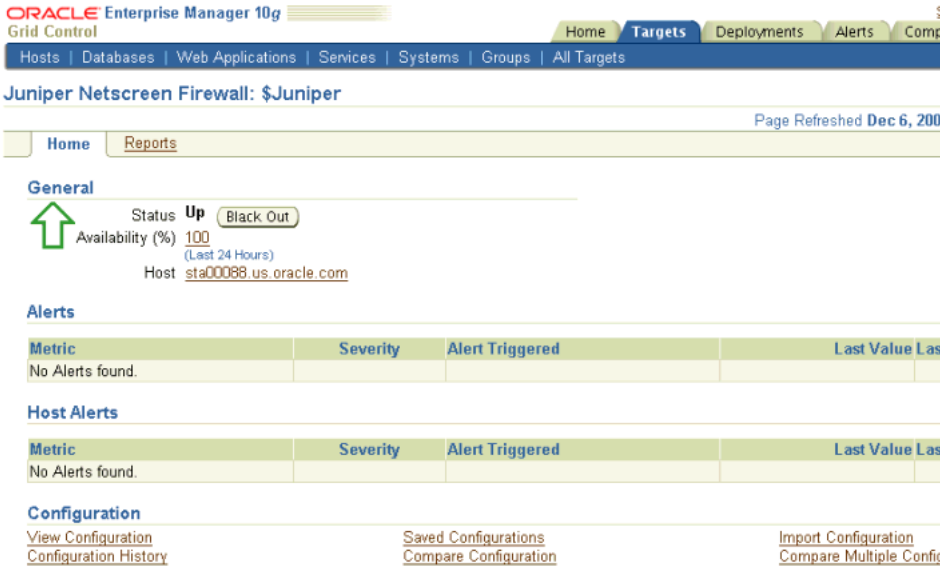


6 プラグインの検査および検証

プラグインがデータの収集を開始するまで数分間待機したら、次の手順を実行して、プラグイン・ターゲットが Enterprise Manager で適切に監視されているかどうかを確認および検証します。

1. エージェントのホームページの「監視ターゲット」表で、Juniper NetScreen Firewall ターゲット・リンクをクリックします。Juniper NetScreen Firewall のホームページが表示されます。

図 3　Juniper Netscreen Firewall のホームページ



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」**サブタブを選択して、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。

7 エージェントの IP アドレスの追加

Juniper Networks NetScreen Firewall 上の既存の SNMP コミュニティにエージェントの IP アドレスを追加するには、次の操作を実行します。

1. ターゲット NetScreen Firewall の Web インタフェースに移動します。
2. **「Configuration」**リンクをクリックします。
3. **「Report Settings」**リンクをクリックします。
4. **「SNMP」**リンクをクリックします。
5. エージェントを追加するコミュニティの**「Edit」**をクリックします。
6. プロパティに次の情報を入力し、**「Go」**をクリックします。
   - **Permissions:** 「Write」、「Trap」、「Including Traffic Alarms」から選択します。
     - **Write:** SNMP コミュニティに対する MIB II データの読取り / 書込み権限を割り当てる場合に選択します。それ以外の場合は、選択解除して読取り専用権限を割り当てます。
     - **Trap:** コミュニティに通知（トラップ）を送信する場合に選択します。コールド・スタート / リンク・アップ / リンク・ダウンの各トラップが、NetScreen デバイスから、トラップを受信するように設定したコミュニティ内のすべてのホストに送信されます。
     - **Including Traffic Alarms:** SNMP コミュニティに通信の警告を送信する場合に選択します。
   - **Version:** 「V1」を選択します。
   - **Host IP Address/Netmask:** エージェントの IP アドレスおよびネットマスクを入力します。
   - **Source Interface:** SNMP メッセージの送信元インタフェースを指定します。

かわりに、新規 SNMP コミュニティを追加するには、次の操作を実行します。

1. ターゲット NetScreen Firewall の Web インタフェースに移動します。
2. **「Configuration」**リンクをクリックします。
3. **「Report Settings」**リンクをクリックします。
4. **「SNMP」**リンクをクリックします。
5. **「New Community」**リンクをクリックします。

   ファイアウォールに SNMP コミュニティがすでに 3 つ構成されている場合、「New Community」リンクは表示されません。NetScreen デバイス管理者は SNMP コミュニティを最大 3 個作成できます。各コミュニティにはホストを最大 8 個含めることができます。この場合、既存の SNMP コミュニティをこの項の冒頭で説明したように編集します。

6. プロパティに次の情報を入力し、**「Go」**をクリックします。

   - **Community Name:** SNMP エージェントで収集されたデータの表示権限、およびシステム・イベントの SNMP 通知の受信権限がある管理者のグループまたはコミュニティの名前を入力します。
   - **Permissions:**
     - **Write:** SNMP コミュニティに対する MIB II データの読取り / 書込み権限を割り当てる場合に選択します。それ以外の場合は、選択解除して読取り専用権限を割り当てます。
     - **Trap:** コミュニティに通知（トラップ）を送信する場合に選択します。コールド・スタート / リンク・アップ / リンク・ダウンの各トラップが、NetScreen デバイスから、トラップを受信するように設定したコミュニティ内のすべてのホストに送信されます。
     - **Including Traffic Alarms:** SNMP コミュニティに通信の警告を送信する場合に選択します。
   - **Version:**「V1」を選択します。
   - **Hosts IP Address/Netmask:** コミュニティのメンバーとして定義するホスト（ワークステーションまたはサブネット）の IP アドレスおよびネットマスクを入力します。
   - **Trap Version:**「V1」を選択します。
   - **Source Interface:** SNMP メッセージの送信元インタフェースを指定します。

8 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. Juniper NetScreen 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. NetScreen 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. NetScreen 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 Juniper NetScreen Firewall プラグインを選択して、**「削除」**をクリックします。

9 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。

10 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。

Oracle Enterprise Manager System Monitoring Plug-in インストレーション・ガイド for Juniper Networks NetScreen Firewall, リリース 6（2.1.1.0.0）

部品番号 : E06098-01

原本名 : Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Juniper Networks NetScreen Firewall, Release 6 (2.1.1.0.0)

原本部品番号 : E11850-01