NetIQ Sentinel 7.0.1 クイックスタートガイド

2012 年 3 月

Novell®

はじめに

次の情報を使用すると、Sentinel をすばやくインストールおよび実行できます。

システム要件を満たす

Sentinel をインストールするための最小システム要件を満たしていることを確認します。

500 EPS のハードウェア要件 :

- **メモリ :** 6.7GB
- **ハードディスク :** 500GB x 4、7.2K RPM のドライバを RAID 1 で稼動 (256MB のキャッシュを装備)、または同等のストレージエリアネットワーク (SAN)
- **プロセッサ :** Intel Xeon X5470 3.33GHz (4 コア) CPU x 1

オペレーティングシステム :

- SUSE Linux Enterprise Server (SLES) 11 SP1
- Red Hat Enterprise Linux (RHEL) 6

仮想マシン :

- VMWare ESX 4.0
- Xen 4.0
- Hyper-V Server 2008 R2DVD ISO ファイルのみ

DVD ISO:

- Hyper-V Server 2008 R2
- オペレーティングシステムがインストールされていないハードウェア

EPS が 500 EPS より上位または下位の場合のハードウェア要件については、『*NetIQ Sentinel 7.0.1 インストールおよび設定ガイド*』の「「システム要件を満たす」」を参照してください。

Sentinel のインストール

Sentinel はスタンドアロンインストール、またはアプライアンスインストールとしてインストールできます。

ハードウェアへのインストール

Sentinel の標準インストールでは、Sentinel のすべてのコンポーネントが 1 台のマシンにインストールされます。カスタムインストールを実行するか、root 以外のユーザとして Sentinel をインストールする場合は、『*NetIQ Sentinel 7.0.1 インストールおよび設定ガイド*』の「「Sentinel のインストール」」を参照してください。

Sentinel をインストールするには、次の手順に従います。

1. ノベル製品ダウンロード Web ページ (http://download.novell.com/index.jsp) から Sentinel インストールファイルをダウンロードします。
   - **1a** ［*製品または技術*］フィールドで［*SIEM-Sentinel*］をブラウズして選択します。
   - **1b** ［*検索*］をクリックします。
   - **1c** ［*Sentinel 7.0 Evaluation*］の［*ダウンロード*］列のボタンをクリックします。

1d ［*ダウンロードに進む*］をクリックし、お客様名とパスワードを入力します。

1e お使いのプラットフォーム用のインストールバージョンに該当する［*ダウンロード*］をクリックします。

2 次のコマンドを使用してインストールファイルを抽出します。

```
tar xfz <install_filename>
```

<install_filename> は、実際のインストールファイル名に置き換えます。

3 次のコマンドを使用して install-sentinel スクリプトを実行します。

```
./install-sentinel
```

4 インストールを実行する言語の番号を指定し、<Enter> キーを押します。

デフォルト値は英語の「3」です。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

5 スペースキーを押して使用許諾契約を確認します。

6 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

このインストールが完了するまで数分かかることがあります。

7 要求されたら、「1」と入力して Sentinel 7.0 の標準インストールを続行します。

8 設定中に作成されるデフォルトの管理者アカウント用のパスワードを 2 回指定します。

詳細については、『*NetIQ Sentinel 7.0.1 インストールおよび設定ガイド*』の「「Sentinel のインストール」」を参照してください。

アプライアンスのインストール

アプライアンスは、VMware ESX、Xen、および Hyper-V 仮想プラットフォーム用に用意されています。ハードウェアにアプライアンスをインストールすることもできます。次の手順は、VMware ESX サーバを対象にしています。その他のプラットフォーム用の手順については、『*NetIQ Sentinel 7.0.1 インストールおよび設定ガイド*』の「「アプライアンスのインストール」」を参照してください。

1 VMware アプライアンスインストールファイルをダウンロードします。

VMware アプライアンスの正しいファイル名には vmx が含まれます。

2 アプライアンスイメージのインストール先となる ESX データストアを確立します。

3 アプライアンスをインストールするサーバに Administrator としてログインします。

4 次のコマンドを使用して、VM Converter がインストールされているマシンから圧縮されたアプライアンスイメージを抽出します。

```
tar zxvf <install_file>
```

<install_filename> は、実際のファイル名に置き換えます。

5 VMware イメージを ESX サーバにインポートするには、VMware Converter を使用して、インストールウィザードの画面の指示に従います。

6 ESX サーバマシンにログインします。

7 インポートしたアプライアンスの VMware イメージを選択して、［*電源オン*］アイコンをクリックします。

8 使用する言語を選択して、［*次へ*］をクリックします。

9 キーボードのレイアウトを選択して、［*次へ*］をクリックします。

10 Novell SUSE Linux Enterprise Server ソフトウェア使用許諾契約書の条項を確認して同意します。

11 NetIQ Sentinel エンドユーザ使用許諾契約の条項を確認して同意します。

12 ［ホスト名］および［ドメイン名］画面で、ホスト名とドメイン名を指定します。

13 ［*ホスト名をループバック IP に割り当てる*］オプションが選択されていることを確認します。

14 ［*次へ*］を選択します。ホスト名の環境設定が保存されます。

15 次のいずれかの操作を行います。

- 現在のネットワーク接続設定を使用するには、［*ネットワーク環境設定 II*］画面の［*次の環境設定を使用する*］を選択します。
- ネットワーク接続設定を変更するには、［*変更*］を選択し、目的の変更を行います。

16 ［*次へ*］をクリックしてネットワーク接続設定を保存します。

17 日付と時刻を設定して、［*次へ*］をクリックし、［*終了*］をクリックします。

インストール後に NTP 環境設定を変更するには、アプライアンスのコマンドラインから YaST を使用します。WebYast を使用して日付と時刻を変更することはできますが、NTP の環境設定を変更することはできません。

インストール直後に時刻が同期されていない場合は、次のコマンドを実行して NTP を再起動します。

```
rcntp restart
```

18 Novell SUSE Linux Enterprise Server の root のパスワードを設定して、［*次へ*］をクリックします。

19 root のパスワードを設定して、［*次へ*］をクリックします。

20 Sentinel の admin と dbauser のパスワードを設定して、［*次へ*］をクリックします。

21 ［*次へ*］をクリックします。ネットワーク接続設定が保存されます。

インストールが完了したら、コンソールに表示されたアプライアンスの IP アドレスをメモします。

インストール後の設定情報については、『*NetIQ Sentinel 7.0.1 インストールおよび設定ガイド*』の「「アプライアンスのインストール後の設定」」を参照してください。

Sentinel Web インタフェースへのアクセス

Sentinel のインストール後の手順として、Sentinel Web インタフェースにアクセスして管理作業を実行し、データを収集するように Sentinel を設定します。

Web インタフェースにアクセスするには、Web ブラウザに次の URL を入力します。

https://<*IP_Address_Sentinel_server*>:8443

8443 番ポートはデフォルト値です。

データの収集

データ収集は、Connector と Collector を通じて行われます。Sentinel には、デフォルトでいくつかの Connector と Collector がインストールおよび設定されています。

デフォルトでは、Sentinel サーバに TCP、UDP、および SSL の各 syslog サーバがインストールされています。アプライアンスを使用している場合、syslog サーバは、ローカル syslog ファイルからイベントの受信を開始するときに自動的に設定されます。

Linux サーバなどの syslog デバイスを設定し、これらの syslog サーバに情報を送信することができます。さらに、その他の Connector を設定し、Sentinel でデータを収集することもできます。

- 3 ページの「syslog 情報を Sentinel に送信するように Linux サーバを設定する」
- 3 ページの 「Windows を対象としたデータ収集の設定」
- 5 ページの 「追加の Connector と Collector の設定」

SYSLOG 情報を SENTINEL に送信するように LINUX サーバを設定する

Sentinel サーバには、次のポートへの着信接続をリスンする、事前に設定された syslog イベントソースサーバが含まれています。

- **TCP:** 1468
- **UDP:** 1514
- **SSL:** 1443

次の情報を使用すると、TCP syslog イベントソースサーバにイベントを送信するように Linux サーバを設定できます。

Linux 上の syslog ファイルを設定するには :

1 /etc/syslog-ng/syslog-ng.conf ファイルを開きます。

2 syslog-ng.conf ファイルの末尾に次のコード行を追加します。

```
# Forward all messages to Sentinel:
#
destination d_slm { tcp("127.0.0.1"
port(1468)); };
log { source(src); destination(d_slm); };
```

3 TCP 値を Linux サーバの IP アドレスに変更します。

4 ファイルを保存して、ファイルを閉じます。

5 syslog サービスを再起動します。

```
/etc/init.d/syslog restart
```

syslog Connector に情報を送信するようにデバイスを設定する方法の詳細については、Sentinel プラグイン Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) にある syslog Connector のマニュアルを参照してください。

WINDOWS を対象としたデータ収集の設定

Windows システムからデータを収集する場合は、Windows イベント (WMI)Connector を設定する必要があります。Windows Event Connector は Collector Manager にインストールされ、Windows サーバにインストールされた Windows イベントコレクションサービスからイベントを受信します。

- 3 ページの 「Windows Event Connector の設定」
- 4 ページの 「Windows サーバでの Windows イベントコレクションサービスのインストール」
- 5 ページの 「Windows イベントコレクションサービスの設定」

Windows Event Connector の設定

1 Sentinel Web インタフェースにログインします。

https://<*IP_Address_Sentinel_server*>:8443

8443 番ポートはデフォルトのポートです。

2 ツールバーの［*アプリケーション*］をクリックし、［*コントロールセンターの起動*］をクリックします。

3 管理ユーザ名とパスワードを使用し、［*ログイン*］をクリックして、Sentinel コントロールセンターにログインします。

4 ツールバーの［*イベントソースの管理*］、［*ライブビュー*］の順にクリックします。

5 Windows 専用の Collector を Collector Manager に追加します。

Windows Event Connector を追加するには、Windows 専用の Collector を設定しておく必要があります。

5a Collector Manager を右クリックし、［*Collector の追加*］をクリックします。

5b ［*ベンダ*］列の［*Microsoft*］を選択し、［バージョン］列で Windows または Active Directory のバージョンを選択します。

5c *［次へ］* をクリックします。

5d 表示するスクリプトを選択し、［*次へ*］をクリックします。

5e 任意の設定パラメータを変更し、［*次へ*］をクリックします。

5f Collector のその他の設定パラメータを設定し、［*終了*］をクリックします。

6 ステップ 5 で作成した Collector に Windows Event Connector を追加します。

6a Collector を右クリックし、［*Connector の追加*］をクリックします。

6b Windows Event Connector を選択し、［*次へ*］をクリックします。

6c Windows Event Connector サーバのネットワーク設定を設定し、［*次へ*］をクリックします。

6d SSL 設定を設定し、［*次へ*］をクリックします。

6e Windows Event Connector の管理方法を選択します。

- **手動 :** イベントソースを手動で管理するには、このオプションを選択します。
- **自動 :** Active Directory と自動的に同期するには、このオプションを選択します。

6f *［次へ］* をクリックします。

6g Windows イベントコレクションサービスおよびイベントソースへの接続に使用するユーザの資格情報を指定します。

6h 設定パラメータを指定し、［*終了*］をクリックします。

7 データを収集する Windows システムのイベントソースを追加します。

7a Windows Event Connector を右クリックし、［*イベントソースの追加*］をクリックします。

7b Windows システムの IP アドレスまたはホスト名を指定します。

または

Active Directory から Windows システムを選択し、［*次へ*］をクリックします。

7c イベントソースの接続モードを選択し、［*次へ*］をクリックします。

7d イベントソースの設定パラメータを指定し、［*終了*］をクリックします。

Windows サーバでの Windows イベントコレクションサービスのインストール

1 Windows イベントコレクションサービスを実行し、リモートの Windows システムの Windows イベントログからイベントを収集するために、適切な権限のあるユーザアカウントを Windows サーバで作成したことを確認します。次の権限が必要です。

- Windows イベントログにアクセスする許可
- WMI の許可
- DOCM の許可
- すべてのイベントログの種類について、Distributed COM Users グループに、ACL の読み込み、書き込み、および削除権限が割り当てられている必要があります。
- セキュリティイベントログの読み込み許可
- ユーザには、Windows エージェントをインストールするための管理権限が必要です。
- ユーザには、*サービスとしてログオンする*権限が必要です。

詳細については、Sentinel プラグイン Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) にある Windows Event Connector のマニュアルを参照してください。許可情報は第 4 章および第 5 章に記載されています。

2 WindowsEvent-CollectionService.msi ファイルを、Windows Event Connector .zip ファイルから、Windows イベントコレクションサービスをインストールする Windows サーバにコピーします。

3 WindowsEvent-CollectionService.msi ファイルをダブルクリックして Windows イベントコレクションサービスのセットアップウィザードを起動します。

4 初期画面で、［*次へ*］をクリックします。

5 (条件付き) サポートの制限に関する警告を確認し、［*次へ*］をクリックします。

6 エンドユーザ使用許諾契約に同意し、［*次へ*］をクリックします。

7 次の情報を使用して、Windows イベントコレクションサービスの設定をカスタマイズします。

その他の機能 : インストールする機能を選択します。デフォルトでは、一部の機能はインストールされません。機能は次のとおりです。

- **コレクションサービス :** Sentinel と通信する Windows イベントコレクションサービスをインストールします。

- **マニュアル：**Connector に付属しているマニュアルをインストールします。

ロケーション：（オプション）［*ブラウズ*］をクリックし、新しいロケーションを選択して、デフォルトのインストールロケーションを変更します。デフォルトのインストールロケーションは Program Files\Novell\SentinelWECS です。

ディスクの使用状況：（オプション）［*ディスク使用状況*］をクリックして、Windows イベントコレクションサービスのインストールに利用できる十分な空きディスク領域があることを確認します。

8 *［次へ］*をクリックします。

9 Windows イベントコレクションサービスが外部の Windows イベントソースへの接続に使用するサービスアカウントを定義します。

ローカルシステムアカウント：ローカルシステムアカウントユーザとして Windows イベントコレクションサービスを実行する場合は、このオプションを選択します。このオプションを選択する場合は、Collector Manager に Windows Event Connector を展開中に、ユーザ資格情報を入力する必要があります。

このアカウント名：Windows イベントコレクションサービスを特定のユーザとして実行するか、ドメインユーザとして実行する場合は、このオプションを選択します。Windows イベントコレクションサービスを実行する権限を持っているユーザの資格情報を使用します。

Windows イベントコレクションサービスシステムでは、監視する各イベントソースシステム上の Windows イベントログに対する読み込みアクセス権が必要です。そのため、作成されるユーザには、各イベントソースシステムで適切な許可が与えられている必要があります。

インストール後すぐにサービスを開始：インストールの完了後、すぐに Windows イベントコレクションサービスを開始する場合は、このオプションを選択します。

10 *［次へ］*をクリックします。

11 ［*インストール*］をクリックして Windows イベントコレクションサービスをインストールします。

12 ［*終了*］をクリックして設定ウィザードを終了します。

Windows イベントコレクションサービスが動作するためには、インストール後に設定が必要です。

Windows イベントコレクションサービスの設定

1 ファイルエディタを使用して eventManagement.config ファイルを開きます。

ファイルのデフォルトのロケーションは Program Files\Novell\SentinelWECS です。

2 <client> セクションで、endPoint address 行をコピーし、既存の行の下に貼り付けます。既存の IP アドレスを、Windows イベントコレクションサービスが接続するサーバ (Collector Manager) の IP アドレスおよび Connector と通信するために経由するポート番号と置き換えます。

例：

```
<client>
    <!-- Additional collectors/plugins can be
added with different host/
port configurations -->
     <!-- <endPoint address="tcp://
127.0.0.1:1024"
behaviorConfiguration="localhost" />-->
     <endPoint address="tcp://
<IP_address_Sentinel_server:<port_number>"
behaviorConfiguration="localhost" />-->
  </client>
```

3 ステップ 2 を繰り返して、必要な数の Connector を設定できます。1 つのエージェントを複数のコネクタに対して設定するか、1 つのエージェントを 1 つの Connector に対して設定することができます。

4 eventManagement.config ファイルを保存して閉じます。

5 ［サービス］ウィンドウを開いて Windows イベントコレクションサービスを開始します。

   5a ［*スタート*］、［*ファイル名を指定して実行*］の順にクリックして［ファイル名を指定して実行］ダイアログボックスを開きます。

   5b「services.msc」と入力して［*OK*］をクリックします。

6 ［*Sentinel Windows イベント接続サービス*］を選択して右クリックし、［*開始*］をクリックして Windows イベントコレクションサービスを開始します。

7 ［サービス］ウィンドウを閉じます。

Microsoft Active Directory、Windows Collector、および Window Event(WMI)Connector の詳細については、Sentinel プラグイン Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) を参照してください。

追加の CONNECTOR と COLLECTOR の設定

使用可能な Connector と Collector は、Sentinel のインストール時に Sentinel サーバにインストールされます。ただし、多くの場合、更新された新しい Connector と Collector を入手可能です。

更新されたバージョンの Connector と Collector については、Sentinel プラグイン Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) で確認してください。

デフォルトで設定されない Connector または Collector を設定する必要がある場合は、『*NetIQ Sentinel 7.0.1 インストールおよび設定ガイド*』の「「Sentinel コンポーネントの追加」」を参照してください。

次に行う作業

この時点で、Sentinel はインストールされています。Sentinel の設定には、『*NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1 管理ガイド)*』および『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』の 2 つのガイドが参考になります。

『管理ガイド』には、管理権限を持っているユーザのみが実行できる作業の設定情報が記載されています。例 :

- 「ユーザと役割の設定」
- 「データストレージの設定」
- 「データ収集の設定」
- 「分散環境でのイベントの検索とレポート」

これらの作業およびその他の管理作業の詳細については、『*NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1 管理ガイド)*』を参照してください。

『ユーザガイド』には、Sentinel でユーザが実行する作業に関する指示が記載されています。例 :

- 「イベントの検索」
- 「データのトレンドの分析」
- 「レポーティング」
- 「インシデントの設定」

これらの作業およびその他のユーザ作業の詳細については、『*NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1 ユーザガイド)*』を参照してください。

Sentinel を設定して、イベントの分析、相関ルールを使用したデータの追加、ベースラインの設定、情報に対するワークフローの設定などを行うことができます。Sentinel のこれらの機能を設定する際は、『*NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1 管理ガイド)*』の情報を参考にしてください。