

Novell Sentinel 6.1 Rapid Deployment SP2 Readme

2011 年 4 月

Novell®

Sentinel Rapid Deployment は、市場をリードする Novell Sentinel セキュリティ情報 / イベント管理ソリューションの新しいパッケージオプションです。Sentinel Rapid Deployment は Sentinel のすべての機能を含み、小規模な組織または地域でインストールするのに理想的です。

Sentinel 6.1 Rapid Deployment SP2 は、新規インストーラまたはアップグレードインストーラのいずれかを使用してインストールします。アップグレードインストーラでは、ソフトウェアの最新の修正点および強化点が、インストールされている Sentinel Rapid Deployment 6.1 SP1 に適用されます。

- ◆ [1 ページのセクション 1 「新機能」](#)
- ◆ [2 ページのセクション 2 「システム要件」](#)
- ◆ [2 ページのセクション 3 「Novell Sentinel Rapid Deployment のインストール」](#)
- ◆ [3 ページのセクション 4 「Sentinel Rapid Deployment SP2 へのアップグレード」](#)
- ◆ [3 ページのセクション 5 「Sentinel Rapid Deployment ヘルプファイルへのアクセス」](#)
- ◆ [4 ページのセクション 6 「修正された問題点と機能強化」](#)
- ◆ [6 ページのセクション 7 「既知の問題」](#)
- ◆ [8 ページのセクション 8 「マニュアル」](#)
- ◆ [8 ページのセクション 9 「保証と著作権」](#)

1 新機能

- ◆ [1 ページのセクション 1.1 「Sentinel Rapid Deployment 6.1 SP2 の新機能 2」](#)
- ◆ [2 ページのセクション 1.2 「Sentinel Rapid Deployment SP1 の新機能」](#)

1.1 Sentinel Rapid Deployment 6.1 SP2 の新機能 2

- ◆ [1 ページの 「SLES 11 SP1 のサポート」](#)
- ◆ [2 ページの 「レガシコレクタサポートの制限」](#)
- ◆ [2 ページの 「セキュリティの向上」](#)

1.1.1 SLES 11 SP1 のサポート

Sentinel Rapid Deployment は、SUSE Linux Enterprise Server (SLES) 11 SP1 64 ビットプラットフォームでもサポートされるようになりました。

1.1.2 レガシコレクタサポートの制限

Novell は、Sentinel 製品ラインでのレガシコレクタのサポートを終了する予定です。以前のバージョンの Sentinel Rapid Deployment でレガシコレクタをインポートすると、システムが警告を表示します。SP 2 バージョン以降では、Sentinel Rapid Deployment および Collector Manager の新規インストールでレガシコレクタを実行しません。ただし、アップグレードされた Sentinel Rapid Deployment システムおよび Collector Manager は、以前と同様にレガシコレクタの実行を継続します。

注：レガシコレクタは、Legacy Collector Builder アプリケーションを使用して書き込まれます。Legacy Collector Builder は、現行の Sentinel 製品には同梱されておりません。レガシコレクタは JavaScript Collector に置き換えられており、Sentinel Plug-In SDK を使用して書き込まれます。JavaScript Collector は、[Sentinel 6.1 Plugins Web サイト \(http://support.novell.com/products/sentinel/secure/sentinel61.html\)](http://support.novell.com/products/sentinel/secure/sentinel61.html) から入手できます。

1.1.3 セキュリティの向上

Sentinel Rapid Deployment 6.1 SP2 には、製品のセキュリティを向上させるアップデートがいくつか含まれています。

- ◆ Java Runtime Environment(JRE) のバージョンが 1.6.0_24 にアップグレードされました。
- ◆ Apache Tomcat がバージョン 6.0.29 にアップグレードされました。
- ◆ PostgreSQL データベースがバージョン 8.3.12 にアップグレードされました。

1.2 Sentinel Rapid Deployment SP1 の新機能

Sentinel Rapid Deployment 6.1 SP1 の新機能に関する説明は、「[Sentinel Rapid Deployment SP1 Readme](http://www.novell.com/documentation/sentinel61rd/readme/data/s61rd_readme.html#bqtqd85)」(http://www.novell.com/documentation/sentinel61rd/readme/data/s61rd_readme.html#bqtqd85) を参照してください。

2 システム要件

ハードウェア要件、サポートされるオペレーティングシステム、ブラウザに関する詳細は、『*Sentinel Rapid Deployment インストールガイド*』の「[システム要件](#)」を参照してください。

3 Novell Sentinel Rapid Deployment のインストール

インストールが簡素化され、tar ファイル名の入力が必要なくなりました。インストーラをダウンロードでき、それをディレクトリに抽出してから、ルートまたは非ルートユーザとしてスクリプトを実行するだけでインストールできます。コマンドライン引数を与えることもでき、ユーザのみの作成や Rapid Deployment サーバのインストール、システムスタートアップで Sentinel Rapid Deployment を自動起動するためのサービス作成、またはユーザまたはサービスを作成せずに Rapid Deployment サーバのみのインストールを行います。

Novell Sentinel Rapid Deployment 6.1 SP2 をインストールするには、『*Sentinel Rapid Deployment インストールガイド*』の「[インストール](#)」を参照してください。

4 Sentinel Rapid Deployment SP2 へのアップグレード

アップグレードを進める前に、サービスパックをインストールするシステムに Sentinel 6.1 Rapid Deployment SP1 がインストール済みであることを確認します。

Sentinel Rapid Deployment 6.1 SP2 にアップグレードするには、『*Sentinel Rapid Deployment インストールガイド*』の「[Sentinel Rapid Deployment のアップグレード](#)」を参照してください。

5 Sentinel Rapid Deployment ヘルプファイルへのアクセス

Sentinel コントロールセンターの [\[Help\]](#) > [\[Help\]](#) メニューを順にクリックすると、Sentinel Rapid Deployment のオンラインユーザガイドにアクセスできます。ただし、インターネットの直接アクセスが拒否される安全な環境で作業している場合は、オンラインヘルプファイルをダウンロードし、一度だけの手順として Sentinel Rapid Deployment サーバに抽出できます。ヘルプファイルが指定の場所に抽出された後は、サーバまたはリモートシステムからマニュアルにアクセスできます。ヘルプファイルは Web ブラウザを使用して表示できます。

注：ヘルプファイルは英語のみです。

オンラインヘルプをダウンロードするには、次の操作を行います。

- 1 Sentinel Rapid Deployment マニュアルサイト (<http://www.novell.com/documentation/sentinel61rd/>) に進みます。
- 2 ダウンロード可能なユーザガイドヘルプセクションの `zip` をクリックし、`s61rd_user_help.zip` ファイルをローカルマシンに保存します。
- 3 次のコマンドを使用してダウンロードされたファイルをコピーおよび抽出します。

```
cp s61rd_user_help.zip <Install_Directory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help
cd <Install_Directory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help
unzip s61rd_user_help.zip
```

重要：指定の場所に `s61rd_user_help.zip` ファイルを抽出しない限り、ヘルプファイルにはアクセスできません。

- 4 ヘルプファイルを表示するには、次のどれかを行います。
 - ◆ Sentinel コントロールセンターで、[\[Help\]](#) > [\[Help\]](#) を順にクリックします。
 - ◆ `<Install_Directory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help/s61rd_user_help/index.html` ファイルを開きます。ナビゲーションペインで `Index.html` ファイルがトピックを一覧にします。希望のトピックをクリックし、そのトピックに関するヘルプページを開きます。

注：ヘルプファイルをダウンロードし、Sentinel Rapid Deployment サーバの指定の場所に保存する場合、Sentinel コントロールセンターの [\[Help\]](#) メニューをクリックするといつでも、サーバで使用できるダウンロード済みのヘルプコンテンツが一覧表示されます。

[Help] メニューから、オンラインで利用可能な『Sentinel Rapid Deployment ユーザガイド』にリダイレクトする場合は、Sentinel Rapid Deployment サーバから、<Install_Directory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help フォルダにある s61rd_user_help を削除します。

6 修正された問題点と機能強化

- ◆ 4 ページのセクション 6.1 「修正された問題点」
- ◆ 5 ページのセクション 6.2 「拡張機能」

6.1 修正された問題点

以下の表に、Sentinel Rapid Deployment 6.1 SP2 の問題点の番号と、これらの問題点に対する解決方法を示します。

バグ番号	ソリューション
451892	Sentinel WebStart アプリケーションは、必要なフォントを必要に応じて自動でダウンロードするようになりました。
497131	最新の eDirectory Collector では、レポート機能の中で 2 バイトの日本語の文字を処理できるようになりました。
531114	Report Web ユーザインタフェースを使用してレポートではないファイル (.zip) がアップロードされた場合、ブラウザには Error getting a PluginPackage from package.xml というエラーが表示されるようになりました。
556730	関連エンジンには、30 秒より先のイベントは保存されなくなりましたので、メモリ不足エラーが表示されません。
566973	関連エンジンのリストが、以前に保存された Sentinel コントロールセンターのセッションで開かれた場合であっても、Correlation Engine Manager のウィンドウに表示されるようになりました。
569849	セキュリティの脆弱性を修正するために、Sentinel Rapid Deployment に最新の Apache Tomcat バージョン 6.0.29 がバンドルされるようになりました。
573181	Sentinel のプロセスの場合、メモリがパーセントで割り当てられるようになりました。memory.conf ファイルからのメモリ割り当ての上書きも追加でサポートされるようになりました。
600604	サイズの大きいレポートの実行時にシステムのメモリ不足が発生しないなど、パフォーマンスの改善が図られました。
607145	データマッピング、フィルタ、関連ルール、アクション、および Event Source Management (ESM) に関する Sentinel の管理アクティビティと環境設定の変更を監視するために、追加の監査イベントが作成されるようになりました。
621509	ユーザがイベントを選択してインシデントを作成し、そのイベントがインシデントの一部として保存されると [New Incident] ウィンドウにイベントが表示されるようになりました。
623834	実際のファイルシステムのディスク領域に基づいて計算される上限値に、ディスク領域の使用率が達した場合のみ、Diskspace usage reached upper threshold というメッセージが表示されます。
625930	RulePerformanceSummary イベントのルール名が Null として表示されなくなりました。

バグ番号	ソリューション
626402	ESM に複数のイベントソースを持つコネクタを再起動しても、タイムアウトの例外が発生しなくなりました。
629716	Sentinel コントロールセンター (SCC) のインスタンスが、デッドロックの問題でフリーズしなくなりました。
641087	セキュリティの脆弱性を修正するために、Sentinel Rapid Deployment に最新の PostgreSQL パッチバージョン 8.3.12 がバンドルされました。
644821	ESM の表示権限を持つユーザは、キーボードの <Delete> キーを押しても、ノード (イベントソース、コレクタ、コレクタマネージャ) を削除できません。
648554	Sentinel Data Manager (SDM) の環境設定ファイルは、SDM が起動される場所ではなく、ユーザのホームディレクトリに作成されるようになりました。
651181	クエリ時間を短縮するために、大きなレポートを実行する場合は Jasper virtualizer が使用されます。
651524	Advisor フィードのファイルは、プロキシサーバを使用してダウンロードできるようになり、プロキシのパスワードは、ダウンロードマネージャを使用して更新されるようになりました。
656595	長時間アイドル状態になっているオープンランザクションのロックが解放されるので、データベースへの接続によって接続がリークすることはありません。
656715	ActiveMQ 経由で送信されるデータは、現在のネットワーク帯域幅を改善するために圧縮されるようになりました。
662213	電子メールイベントアクションおよび電子メールインシデントアクションで複数の受信者のアドレスに電子メールを送信できるようになりました。
668443	pgadmin を使用した接続に加えて、コマンドラインを使用して PostgreSQL データベースに接続できるようになりました。
672058	指定した時間内にデータを受信しなかった場合に警告するように設定されているイベントソースを再起動しても、イベントソースが重複するイベント (NoDataAlert) およびログメッセージを生成しなくなりました。
682235	セキュリティの脆弱性を修正するために、Sentinel Rapid Deployment に最新の Java バージョン 1.6.0_24 がバンドルされました。

6.2 拡張機能

以下の表に、使いやすさを向上させるために Sentinel Rapid Deployment 6.1 SP2 で拡張された機能を一覧表示します。

バグ番号	説明
547390	das_core.xml ファイルの中で最大イベントプロパティを設定することで、オフラインクエリの制限を設定できるようになりました。
642690	オフラインクエリが拡張され、das_core.xml ファイルの中で所与の時間間隔以下のクエリ時間を設定できるようになりました。
642691	オフラインクエリ情報の更新ステータスが das_core ログファイルに保存されるようになりました。

バグ番号	説明
648108	[Advisor Status] ウィンドウにすべてのフィードファイルの情報が表示されるようになりました。
673362	JasperPrint オブジェクトファイル (つまり、結果を呼び出した生結果ファイル) がレポート結果にはバンドルされなくなりました。このファイルは Sentinel では使用されないの、削除するとレポートのパフォーマンスが向上し、ディスク容量を節約できます。
680054	Sentinel Rapid Deployment サーバで、フェールオーバーの仕組みとして結合された IP アドレスのサポートが追加されました。

7 既知の問題

バグ番号	説明
486932	問題: ユーザがアクティブな iTRAC プロセスに関連付けられているアクティビティを削除できる。 解決策: なし。
517568	問題: Solution Designer を単独でインストールしようとすると、インストールできない。 解決策: Sentinel コントロールセンターまたは Sentinel Data Manager のいずれかを使用して Solution Designe をインストールします。
525334	問題: Identity Browser に Active Directory ドメインのデータが重複して表示される。 解決策: なし。
598473	問題: ESM ユーザインタフェースを英語以外のシステムから起動すると、6r9 ファイルコネクタが期待どおりに SCP プロトコルを使用してリモートファイルを取得しない。 解決策: なし。これは、File Connector のバージョン 6r10 で修正される予定です。
674008	問題: Linux マシンで Installshield Wizard に Novell アイコンおよび著作権情報が表示されない。 解決策: なし。
674720	問題: コレクタビルダオプションのサポートが Sentinel 6.1 Rapid Deployment SP2 に含まれていないにもかかわらず、コレクタビルダの情報が使用許諾契約に表示される。 解決策: なし。

バグ番号	説明
679830	<p>問題: Windows のコレクタマネージャで、マッピング機能が期待どおりに働かない場合がある。</p> <p>解決策: 次の手順を実行します。</p> <ol style="list-style-type: none"> コレクタマネージャを停止します。 <pre><install_directory>/bin/sentinel.bat stop</pre> コレクタマネージャのログファイル collector_mgr0.0.log を <install_directory>/log ディレクトリから開きます。 以下の内容と類似するエラーを検索します。 <pre>System temporary directory (java.io.tmpdir property) of C:\Windows\system32\config\systemprofile\AppData\Local\Temp\ appears to be invalid.</pre> Temp という名前のフォルダを以下の場所に作成します。 <p>Windows 64 ビットシステムの場合: C:\Windows\syswow64\config\systemprofile\AppData\Local\</p> <p>Windows 32 ビットシステムの場合: C:\Windows\system32\config\systemprofile\AppData\Local\</p> コレクタマネージャを再起動します。 <pre><install_directory>/bin/sentinel.bat start</pre>
680054	<p>問題: Sentinel Rapid Deployment サーバが IP アドレスの自動決定に失敗する。</p> <p>解決策: 次の手順を実行します。</p> <ol style="list-style-type: none"> start_tomcat.properties ファイルを <install_directory>/sentinel_rd/config ディレクトリに作成します。 <p>Sentinel Rapid Deployment サーバを実行するユーザがこのファイルを所有し、実行権限を持つようにします。</p> 次の行を追加して、新しく作成されたファイルに IP アドレスを指定します: <pre>SERVER_IP=<ip_address_value></pre> ファイルを保存します。 Sentinel インストール・ファイルを所有するユーザでログインし、次のコマンドを使用してサーバを再起動します。 <pre>sentinel.sh restart</pre> 次の場所に含まれる IP アドレスを確認し、上書きされた IP アドレスが使用されているかどうかを確認します。 <pre>jnlp files under \$ESEC_HOME/3rdparty/tomcat/webapps/ROOT/ novellsiemdownloads</pre>
680154	<p>問題: Sentinel Data Manage 上の [Tablespace] タブに表示される使用済みディスク領域と空き領域が間違っている。使用済みのディスク領域と空き領域は、実際のディスク領域ではなく、sendata1 テーブルスペースに基づいて計算されます。</p> <p>解決策: なし。</p>

バグ番号	説明
685187	<p>問題: コンソールモードを使用してコレクタマネージャをリモートにインストールしようすると、インストール中にサーバからのブローカ証明書のインポートが失敗する。</p> <p>解決策: ssh をグラフィックモードでシステムに接続することで、コンソールモードを使用してリモートシステム上にコレクタマネージャをインストールできます。たとえば、<code>ssh -x <system_IP></code> というように実行します。</p>

8 マニュアル

最新のマニュアルおよびリリースノートは、[Sentinel Rapid Deployment マニュアルサイト \(http://www.novell.com/documentation/sentinel61rd/index.html\)](http://www.novell.com/documentation/sentinel61rd/index.html) で入手できます。

9 保証と著作権

米国 Novell, Inc. およびノベル株式会社は、この文書の内容または使用について、いかなる保証、表明または約束も行っておりません。また文書の商品性、および特定の目的への適合性については、明示と黙示を問わず一切保証しないものとします。米国 Novell, Inc. およびノベル株式会社は、本書の内容を改訂または変更する権利を常に留保します。米国 Novell, Inc. およびノベル株式会社は、このような改訂または変更を個人または事業体に通知する義務を負いません。

米国 Novell, Inc. およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っておりません。またノベル製ソフトウェアの商品性、および特定の目的への適合性については、明示と黙示を問わず一切保証しないものとします。米国 Novell, Inc. およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。

本契約の下で提供される製品または技術情報はすべて、米国の輸出管理規定およびその他の国の輸出関連法規の制限を受けます。お客様は、輸出管理の法令すべてを順守することに同意します。また、発送物の輸出、再輸出、または輸入のために必要なライセンスまたは格付けを取得します。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。ノベル製ソフトウェアの輸出については、[Novell International Trade Services \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) の Web ページをご参照ください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとします。

Copyright © 2011 Novell, Inc. All rights reserved. 本ドキュメントの一部または全体を無断で複製・転載することは、その形態を問わず禁じます。

Novell の商標一覧については、「[商標とサービスの一覧 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html)」を参照してください。

サードパーティの商標は、それぞれの所有者に属します。