

インストールガイド

Novell[®] Sentinel Log Manager

1.1

July 08, 2010

www.novell.com



保証と著作権

米国 Novell, Inc. およびノベル株式会社は、本書の内容または本書を使用した結果について、いかなる保証、表明または約束も行っておりません。また、本書の商品性、および特定の目的への適合性について、いかなる明示的または黙示的な保証も否認し、排除します。また、本書の内容は予告なく変更されることがあります。

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、いかなる明示的または黙示的な保証も否認し、排除します。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、米国の輸出規制および他国の商法の制限を受けます。お客様は、すべての輸出規制を遵守し、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。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関する詳細については、[Novell International Trade Services の Web ページ \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) を参照してください。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 © 2009-2010 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, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

オンラインマニュアル: 本製品とその他の Novell 製品の最新のオンラインマニュアルにアクセスするには、[Novell マニュアルの Web ページ \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) を参照してください。

Novell の商標

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。

サードパーティ資料

サードパーティの商標は、それぞれの所有者に帰属します。

目次

このガイドについて	7
1 はじめに	9
1.1 製品の概要	9
1.1.1 イベントソース	11
1.1.2 イベントソースの管理	12
1.1.3 データコレクション	12
1.1.4 コレクタマネージャ	13
1.1.5 データストレージ	13
1.1.6 検索とレポート	14
1.1.7 Sentinel Link	14
1.1.8 Web ベースのユーザインタフェース	15
1.2 インストールの概要	15
2 システム要件	17
2.1 ハードウェア要件	17
2.1.1 Sentinel Log Manager サーバ	17
2.1.2 コレクタマネージャサーバ	18
2.1.3 データストレージ要件の概算	19
2.1.4 仮想環境	20
2.2 サポートされるオペレーティングシステム	20
2.2.1 Sentinel Log Manager	20
2.2.2 コレクタマネージャ	20
2.3 サポートされるブラウザ	21
2.3.1 Linux	21
2.3.2 Windows	21
2.4 サポートされる仮想環境	21
2.5 サポートされるコネクタ	21
2.6 サポートされるイベントソース	22
3 既存の SLES 11 システムへのインストール	25
3.1 作業を開始する前に	25
3.2 標準インストール	26
3.3 カスタムインストール	27
3.4 サイレントインストール	29
3.5 root 以外でのインストール	30
4 アプライアンスのインストール	33
4.1 作業を開始する前に	33
4.2 使用するポート	33
4.2.1 ファイアウォールで開くポート	34
4.2.2 ローカルで使用されるポート	34
4.3 VMware アプライアンスのインストール	35
4.4 Xen アプライアンスのインストール	36
4.5 ハードウェアへのアプライアンスのインストール	38
4.6 アプライアンスのインストール後の設定	39

4.7	WebYaST の環境設定	39
4.8	アップデートの登録	42
5	Web インタフェースにログインします。	45
6	Sentinel Log Manager のアップグレード	49
6.1	1.0 から 1.1 へのアップグレード.	49
6.2	コレクタマネージャのアップグレード	50
6.3	1.0 から 1.1 アプライアンスへの移行.	51
7	追加のコレクタマネージャのインストール	53
7.1	作業を開始する前に	53
7.2	追加のコレクタマネージャの利点	53
7.3	追加のコレクタマネージャのインストール	53
8	Sentinel Log Manager のアンインストール	55
8.1	アプライアンスのアンインストール	55
8.2	既存の SLES 11 システムからのアンインストール.	55
8.3	コレクタマネージャのアンインストール	56
8.3.1	Linux コレクタマネージャのアンインストール	56
8.3.2	Windows コレクタマネージャのアンインストール.	56
8.3.3	手動のディレクトリのクリーンアップ	57
A	インストールのトラブルシューティング	59
A.1	ネットワーク接続が不正なためにインストールが失敗する	59
A.2	SLES 11 上の VMware Player 3 のネットワークの環境設定で問題が発生する	59
A.3	novell ユーザ以外の非 root ユーザでインストールされた Log Manager のアップグレード.	60
	Sentinel の用語	61

このガイドについて

このガイドでは、Novell Sentinel Log Manager の概要とそのインストール方法について説明します。

- ◆ 9 ページの第 1 章「はじめに」
- ◆ 17 ページの第 2 章「システム要件」
- ◆ 25 ページの第 3 章「既存の SLES 11 システムへのインストール」
- ◆ 33 ページの第 4 章「アプライアンスのインストール」
- ◆ 45 ページの第 5 章「Web インタフェースにログインします。」
- ◆ 49 ページの第 6 章「Sentinel Log Manager のアップグレード」
- ◆ 53 ページの第 7 章「追加のコレクタマネージャのインストール」
- ◆ 55 ページの第 8 章「Sentinel Log Manager のアンインストール」
- ◆ 59 ページの付録 A 「インストールのトラブルシューティング」
- ◆ 61 ページの「Sentinel の用語」

対象読者

このガイドは、Novell Sentinel Log Manager の管理者とエンドユーザを対象としています。

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインマニュアルの各ページの下部にあるユーザコメント機能を使用するか、または [Novell Documentation Feedback Web サイト \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html) にアクセスして、コメントを入力してください。

その他のマニュアル

独自プラグイン (JasperReports など) の開発の詳細については、[Sentinel SDK の Web ページ \(http://developer.novell.com/wiki/index.php/Develop_to_Sentinel\)](http://developer.novell.com/wiki/index.php/Develop_to_Sentinel) を参照してください。Sentinel Log Manager レポートプラグインの開発環境は、Novell Sentinel のマニュアルに記載されている環境と同じです。

Sentinel のマニュアルについては、[Sentinel マニュアルの Web サイト \(http://www.novell.com/documentation/sentinel61/index.html\)](http://www.novell.com/documentation/sentinel61/index.html) を参照してください。

Sentinel Log Manager の環境設定の詳細については、『[Sentinel Log Manager 1.1 Administration Guide](#) (Sentinel Log Manager 1.1 管理ガイド)』を参照してください。

Novell の連絡先

- ◆ [Novell Web サイト \(http://www.novell.com\)](http://www.novell.com)
- ◆ [Novell テクニカルサポート \(http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup\)](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)

- ◆ Novell セルフサポート (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- ◆ パッチダウンロードサイト (<http://download.novell.com/index.jsp>)
- ◆ Novell の年中無休サポート (<http://www.novell.com/company/contact.html>)
- ◆ Sentinel TIDS (<http://support.novell.com/products/sentinel>)
- ◆ Sentinel コミュニティサポートフォーラム (<http://forums.novell.com/novell-product-support-forums/sentinel/>)

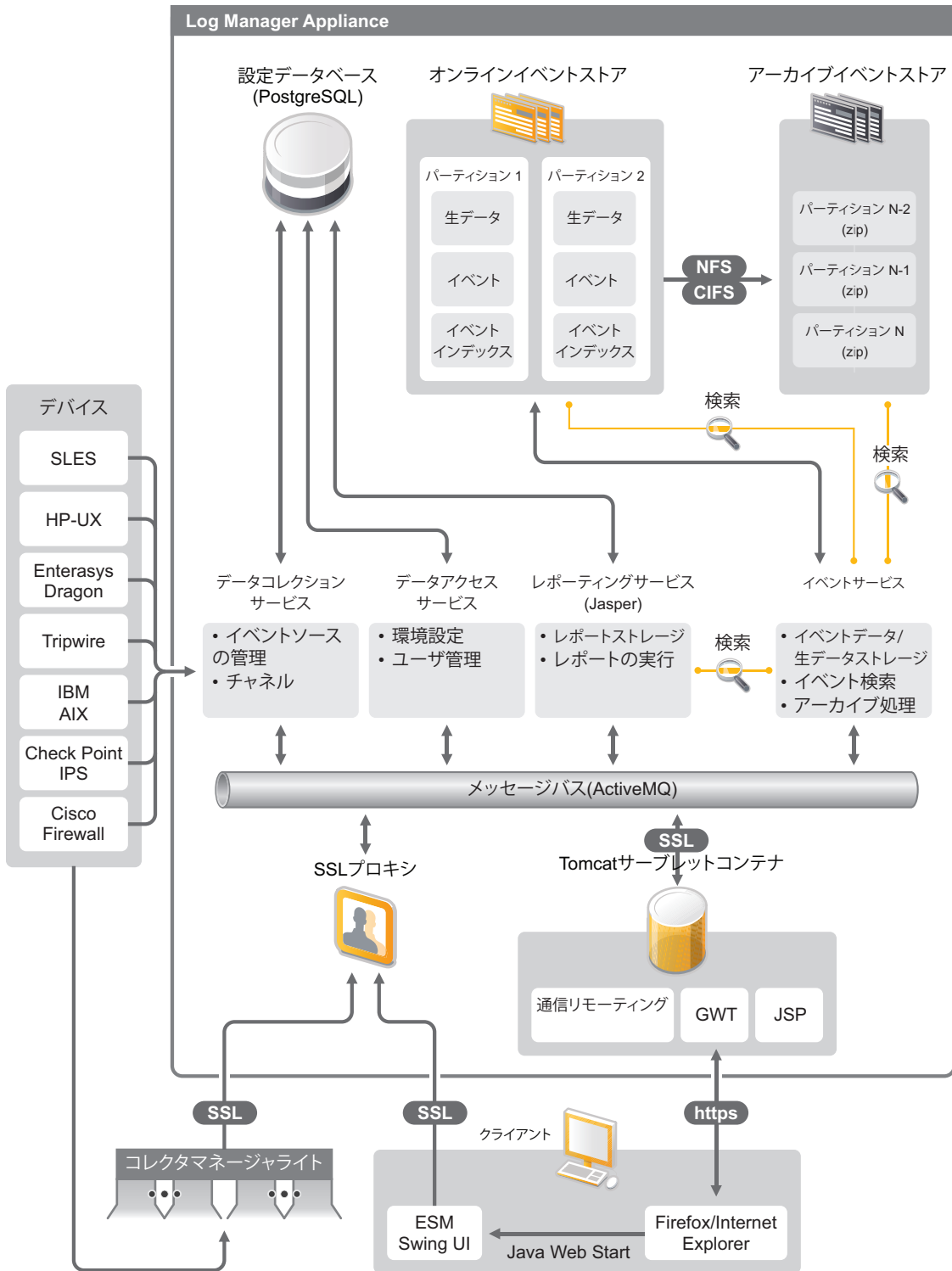
Novell Sentinel Log Manager では、侵入検出システム、ファイアウォール、オペレーティングシステム、ルータ、Web サーバ、データベース、スイッチ、メインフレーム、およびアンチウイルスイベントソースなどの広範なデバイスおよびアプリケーションからデータを収集して管理することができます。Novell Sentinel Log Manager は、発生率の高いイベントの処理、長期的なデータ保持、ポリシーベースのデータ保持、地域別のデータ集約、広範なアプリケーションとデバイスを対象としたシンプルな検索およびレポート機能を提供しています。

- ◆ [9 ページのセクション 1.1 「製品の概要」](#)
- ◆ [15 ページのセクション 1.2 「インストールの概要」](#)

1.1 製品の概要

Novell Sentinel Log Manager 1.1 は、柔軟かつスケーラブルなログ管理ソリューションを組織に提供します。Novell Sentinel Log Manager は、ログの収集および管理に関する基本的な問題に対処するためのログ管理ソリューションです。また、リスク管理におけるコストと複雑さの削減およびコンプライアンス要件の単純化に重点を置いた完全なソリューションを実現します。

図 1-1 Novell Sentinel Log Manager のアーキテクチャ



Novell Sentinel Log Manager には次の特長があります。

- ◆ 分散検索機能により、ローカルの Sentinel Log Manager サーバだけでなく、複数の Sentinel Log Manager サーバで、収集されたイベントを中央のコンソールから検索できます。
- ◆ コンプライアンスレポートがあらかじめ用意されているので、監査および法令分析用のコンプライアンスレポートを簡単に作成できます。
- ◆ 非専有ストレージテクノロジーを使用し、既存のインフラストラクチャを活用してコストを詳細に管理できます。
- ◆ ログデータの収集、保存、レポート、および検索をサポートするブラウザベースのユーザインタフェースが強化され、タスクの監視および管理が大幅に単純化されました。
- ◆ IT 管理者は、新しいグループおよびユーザ権限機能を使用したきめの細かい効率的な管理とカスタマイズが可能になり、IT インフラの動作に関するさらなる透明性を確保できます。

このセクションでは、次の項目について説明します。

- ◆ [11 ページのセクション 1.1.1 「イベントソース」](#)
- ◆ [12 ページのセクション 1.1.2 「イベントソースの管理」](#)
- ◆ [12 ページのセクション 1.1.3 「データコレクション」](#)
- ◆ [13 ページのセクション 1.1.4 「コレクタマネージャ」](#)
- ◆ [13 ページのセクション 1.1.5 「データストレージ」](#)
- ◆ [14 ページのセクション 1.1.6 「検索とレポート」](#)
- ◆ [14 ページのセクション 1.1.7 「Sentinel Link」](#)
- ◆ [15 ページのセクション 1.1.8 「Web ベースのユーザインタフェース」](#)

1.1.1 イベントソース

Novell Sentinel Log Manager は、Syslog、Windows イベントログ、ファイル、データベース、SNMP、Novell Audit、Security Device Event Exchange (SDEE)、Check Point Open Platforms for Security (OPSEC)、およびその他のストレージメカニズムやプロトコルにログを生成するイベントソースからデータを収集します。

Sentinel Log Manager では、イベントソースからのデータを解析するための適切なコネクタがあれば、それらのイベントソースをすべてサポートします。Novell Sentinel Log Manager には、各種イベントソース用のコレクタが用意されています。認識されていないイベントソースであっても、適切なコネクタがあれば、一般的なイベントコレクタでデータを収集して処理することができます。

データ収集対象とするイベントソースは、イベントソースの管理インタフェースで設定できます。

サポートされるすべてのイベントソースのリストについては、[22 ページのセクション 2.6 「サポートされるイベントソース」](#)を参照してください。

1.1.2 イベントソースの管理

イベントソースの管理インタフェースにより、Sentinel 6.0 および 6.1 のコネクタとコレクタをインポートおよび環境設定できます。

イベントソースの管理ウィンドウのライブビューを使用して次のタスクを実行できます。

- ◆ 環境設定ウィザードを使用してイベントソースに対する接続を追加または編集する。
- ◆ イベントソースへの接続のステータスをリアルタイムに表示する。
- ◆ ライブビューで、イベントソースの環境設定をインポートまたはエクスポートする。
- ◆ Sentinel とともにインストールされているコネクタとコレクタを表示および環境設定する。
- ◆ 中央リポジトリとの間で、コネクタとコレクタをインポートまたはエクスポートする。
- ◆ 環境設定されたコレクタおよびコネクタを通過するデータを監視する。
- ◆ 生データ情報を表示する。
- ◆ イベントソース階層のコンポーネントを設計、環境設定、および作成し、これらのコンポーネントを使用して必要なアクションを実行する。

詳細については、『*Sentinel ユーザガイド* (<http://www.novell.com/documentation/sentinel61/#admin>)』の「イベントソースの管理」セクションを参照してください。

1.1.3 データコレクション

Novell Sentinel Log Manager は、コネクタおよびコレクタを使用して、環境設定されたイベントソースからデータを収集します。

コレクタは、さまざまなイベントソースからのデータを解析して正規化された Sentinel イベント構造に変換したり、場合によっては外部のデータソースから別の形式のデータを収集したりします。各コレクタは、互換性のあるコネクタと対で展開する必要があります。コネクタは、Sentinel Log Manager コレクタとイベントソースまたはデータソースとの間の接続を容易にします。

Novell Sentinel Log Manager では、Syslog および Novell Audit に対応した Web ベースのユーザインタフェースを通じて、さまざまなイベントソースからログを容易に収集することができます。

Novell Sentinel Log Manager では、次のようなさまざまな接続方式を使用してデータを収集できます。

- ◆ Syslog コネクタは、User Datagram Protocol (UDP)、Transmission Control Protocol (TCP)、またはセキュアな Transport Layer System (TLS) でデータを送信する Syslog データソースを自動的に認識し、環境設定します。
- ◆ 監査コネクタは、監査に対応した Novell データソースを自動的に認識および環境設定します。
- ◆ ファイルコネクタはログファイルを読み込みます。
- ◆ SNMP コネクタは、SNMP トラップを受信します。
- ◆ JDBC コネクタは、データベーステーブルから読み込みます。

- ◆ WMS コネクタは、デスクトップおよびサーバ上の Windows イベントログにアクセスします。
- ◆ SDEE コネクタは Cisco デバイスなどの SDEE プロトコルをサポートするデバイスに接続します。
- ◆ Check Point Log Export API (LEA) コネクタは、Sentinel コレクタと Check Point ファイアウォールサーバ間の統合を容易にします。
- ◆ Sentinel Link コネクタは、他の Novell Sentinel Log Manager サーバからのデータを認識します。
- ◆ プロセスコネクタは、イベントログの出力用に作成されたカスタムプロセスからのデータを認識します。

追加のライセンスを購入して、SAP およびメインフレームオペレーティングシステム用のコネクタをダウンロードすることもできます。

ライセンスを取得するには、1-800-529-3400 にお電話いただくか、Novell テクニカルサポート (<http://support.novell.com>) にお問い合わせください。

コネクタの環境設定の詳細については、Sentinel コンテンツの Web サイト (<http://support.novell.com/products/sentinel/sentinel61.html>) のコネクタのドキュメントを参照してください。

データコレクションの環境設定の詳細については、『*Sentinel Log Manager 1.1 Administration Guide* (Sentinel Log Manager 1.1 管理ガイド)』の「**Configuring Data Collection**」を参照してください。

注: 常に最新バージョンのコレクタおよびコネクタをダウンロードしてインポートする必要があります。最新のコレクタおよびコネクタは定期的に [Sentinel 6.1 のコンテンツの Web サイト \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html) にアップロードされません。コネクタおよびコレクタのアップデートには、プログラムの修正、追加イベントのサポート、パフォーマンスの向上などが含まれます。

1.1.4 コレクタマネージャ

コレクタマネージャは、Sentinel Log Manager のための、柔軟なデータ収集ポイントです。Novell Sentinel Log Manager のインストール時に、デフォルトでコレクタマネージャがインストールされます。ただし、ネットワーク内のリモートな場所にコレクタマネージャをインストールすることもできます。このリモートのコレクタマネージャがコネクタおよびコレクタを使用して収集したデータは、Novell Sentinel Log Manager に転送され、そこで保存および処理されます。

追加のコレクタマネージャのインストールについては、53 ページの「[追加のコレクタマネージャのインストール](#)」を参照してください。

1.1.5 データストレージ

データは、データコレクションコンポーネントからデータストレージコンポーネントに移動します。これらのコンポーネントは、ファイルベースのデータストレージとインデックスシステムを使用して、収集したデバイスログデータを保持します。また、PostgreSQL データベースを使用して、Novell Sentinel Log Manager の環境設定データを保持します。

データはサーバのファイルシステムに圧縮形式で保存され、設定された場所に長期間保存されます。データは、ローカルに保存することも、リモートでマウントされた SMB (CIFS) または NFS 共有に保存することもできます。データファイルは、データ保持ポリシーで設定されたスケジュールに基づいて、ローカルおよびネットワークストレージの場所から削除されます。

データ保持ポリシーは、特定のデータのデータ保持期間の制限を超えた場合、または使用可能なディスクスペースが指定した値を下回った場合に保存場所からデータを削除するように設定することができます。

データストレージの環境設定の詳細については、『[Sentinel Log Manager 1.1 Administration Guide](#) (Sentinel Log Manager 1.1 管理ガイド)』の「[Configuring Data Storage](#)」を参照してください。

1.1.6 検索とレポーティング

検索コンポーネントおよびレポーティングコンポーネントを使用して、ローカルデータストレージやネットワークデータストレージ、およびインデックスシステムで、イベントログデータを検索してレポートを作成することができます。保存されたイベントデータは、全体を検索することも、送信元ユーザ名などの特定のイベントフィールド内を検索することもできます。これらの検索結果は、さらに絞り込んだりフィルタをかけたりすることができるほか、今後使用するレポートのテンプレートとして保存することもできます。

Sentinel Log Manager には、あらかじめいくつかのレポートが用意されています。また、追加のレポートをアップロードすることもできます。レポートは、スケジュールに基づいて実行することも、必要なときに実行することもできます。

デフォルトのレポートの一覧については、『[Sentinel Log Manager 1.1 Administration Guide](#) (Sentinel Log Manager 1.1 管理ガイド)』の「[Reporting](#)」を参照してください。

イベントの検索およびレポートの生成の詳細については、『[Sentinel Log Manager 1.1 Administration Guide](#) (Sentinel Log Manager 1.1 管理ガイド)』の「[検索](#)」および「[Reporting](#)」を参照してください。

1.1.7 Sentinel Link

Sentinel Link は、ある Sentinel Log Manager から別の Sentinel Log Manager にイベントデータを転送するために使用できます。Sentinel Log Manager の階層セットにより、複数の地理的な場所で完全なログを保持しつつ、より重要なイベントを単一の Sentinel Log Manager に転送して一元化された検索とレポーティングを実行することができます。

また、Sentinel Link では、より高度な関連付け、インシデント対応、および価値の高いコンテキスト情報 (サーバの重要度や識別情報管理システムからの識別情報など) の挿入のために、重要なイベントを完全な SIEM(Security Information Event Management) システムである Novell Sentinel に転送することもできます。

1.1.8 Web ベースのユーザインタフェース

Novell Sentinel Log Manager では、Web ベースのユーザインタフェースで Log Manager を環境設定および使用することができます。ユーザインタフェース機能は、Java Web Start に基づく Web サーバおよびグラフィカルユーザインタフェースによって提供されます。すべてのユーザインタフェースとサーバとのやり取りには、暗号化された接続が使用されます。

Novell Sentinel Log Manager では、Web インタフェースを通じて次のタスクを実行できます。

- ◆ イベントの検索
- ◆ 検索基準をレポートテンプレートとして保存
- ◆ レポートの表示と管理
- ◆ イベントソースの管理インタフェースを起動して、Syslog および Novell アプリケーション以外のデータソースのデータコレクションの環境設定をする (管理者のみ)
- ◆ データ転送の環境設定 (管理者のみ)
- ◆ リモートインストール用の Sentinel コレクタマネージャのインストーラのダウンロード (管理者のみ)
- ◆ イベントソースのヘルスの表示 (管理者のみ)
- ◆ Syslog および Novell データソースのデータコレクションの環境設定 (管理者のみ)
- ◆ データストレージの環境設定、およびデータベースのヘルスの表示 (管理者のみ)
- ◆ データアーカイブの環境設定 (管理者のみ)
- ◆ 条件に一致するイベントデータを出力チャンネルに送信するための関連するアクションの環境設定 (管理者のみ)
- ◆ ユーザアカウントおよび権限の管理 (管理者のみ)

1.2 インストールの概要

Novell Sentinel Log Manager は、アプライアンスとしてインストールすることも、既存の SUSE Linux Enterprise Server (SLES) 11 オペレーティングシステムにインストールすることもできます。Sentinel Log Manager をアプライアンスとしてインストールする場合、Log Manager サーバは SLES 11 オペレーティングシステムにインストールされます。

Novell Sentinel Log Manager のインストール時に、デフォルトで次のコンポーネントがインストールされます。

- ◆ Sentinel Log Manager サーバ
- ◆ 通信サーバ
- ◆ Web サーバおよび Web ベースのユーザインタフェース
- ◆ レポートサーバ
- ◆ コレクタマネージャ

これらのコンポーネントには、追加の環境設定が必要なものがあります。

Novell Sentinel Log Manager のインストール時に、デフォルトでコレクタマネージャがインストールされます。追加のコレクタマネージャが必要な場合は、リモートマシンに個別にインストールできます。詳細については、[53 ページの第 7 章「追加のコレクタマネージャのインストール」](#)を参照してください。

システム要件

次のセクションでは、Novell Sentinel Log Manager のハードウェア、オペレーティングシステム、ブラウザ、サポートされるコネクタ、およびイベントソースの互換性の要件について説明します。

- 17 ページのセクション 2.1 「ハードウェア要件」
- 20 ページのセクション 2.2 「サポートされるオペレーティングシステム」
- 21 ページのセクション 2.3 「サポートされるブラウザ」
- 21 ページのセクション 2.4 「サポートされる仮想環境」
- 21 ページのセクション 2.5 「サポートされるコネクタ」
- 22 ページのセクション 2.6 「サポートされるイベントソース」

2.1 ハードウェア要件

- 17 ページのセクション 2.1.1 「Sentinel Log Manager サーバ」
- 18 ページのセクション 2.1.2 「コレクタマネージャサーバ」
- 19 ページのセクション 2.1.3 「データストレージ要件の概算」
- 20 ページのセクション 2.1.4 「仮想環境」

2.1.1 Sentinel Log Manager サーバ

Novell Sentinel Log Manager は、64 ビットの Intel Xeon および AMD Opteron プロセッサではサポートされていますが、Itanium プロセッサではサポートされていません。

注：これらは、平均イベントサイズが 300 バイトの場合の要件です。

オンラインデータを 90 日間保持する本番システムの場合、次のハードウェア要件が推奨されます。

表 2-1 Sentinel Log Manager のハードウェア要件

要件	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
圧縮	最大 10:1	最大 10:1	最大 10:1
最大イベントソース	最大 1000	最大 1000	最大 2000
最大イベント数	500	2500	7500

要件	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
CPU	Intel Xeon E5450 3GHz (4 コア) CPU x 1 または Intel Xeon L5240 3GHz (2 コア) CPU x 2(合計 4 コア)	Intel Xeon E5450 3GHz (4 コア) CPU x 1 または Intel Xeon L5240 3GHz (2 コア) CPU x 2(合計 4 コア)	Intel Xeon X5470 3.33GHz (4 コア) CPU x 2(合計 8 コア)
Random Access Memory(RAM)	4GB	4GB	8GB
ストレージ	500GB x 2、7.2k RPM ドライブ (ハードウェア RAID、256MB キャッシュ、RAID 1)	1TB x 2、7.2k RPM ドライブ (ハードウェア RAID、256MB キャッシュ、RAID 1)	450GB x 6、15k RPM ドライブ (ハードウェア RAID、512MB キャッシュ、RAID 10)

注：

- ◆ 1 台のマシンに複数のイベントソースを含めることができます。たとえば、Windows サーバにおいて、Windows オペレーティングシステムとその上でホストされている SQL Server データベースからそれぞれデータを収集するのであれば、2 つの Sentinel イベントソースを含めます。
- ◆ ネットワークストレージの場所は、外部の複数ドライブのストレージエリアネットワーク (SAN) またはネットワーク接続ストレージ (NAS) に設定する必要があります。
- ◆ 推奨される、安定した状態のボリュームは、ライセンスされた最大 EPS の 80% です。この制限に達した場合には、Sentinel Log Manager インスタンスを追加することをお勧めします。

注：最大イベントソースの制限はハード制限ではありませんが、Novell で実施したテストに基づいた推奨値を示すものであり、イベントソースごとの 1 秒当たりの平均イベント数が低いことが前提となっています (3EPS 未満)。EPS が高いと、持続可能な最大イベントソースが少なくなります。最大イベントソース数が上で示した制限を超えていなければ、(最大イベントソース) x (イベントソースごとの平均 EPS) = 最大イベント数という計算式を使用して、特定の平均 EPS レートまたはイベントソース数に対する適切な制限を求めることができます。

2.1.2 コレクタマネージャサーバ

- Intel Xeon E5240 3GHz (2 コア CPU) x 1
- 256MB RAM
- 10GB の空きディスク容量。

2.1.3 データストレージ要件の概算

Sentinel Log Manager では、法令やその他の要件に従って、生データを長期間保持することができます。その際、生データを圧縮することで、ローカルストレージやネットワークストレージのスペースを有効利用できます。それでも、時間が経過するにつれ、ストレージ必要量が大幅に増加する場合があります。

予算に制約のある大規模なストレージシステムでは、データの長期保存には、コスト効果の高いデータストレージシステムを使用する必要があります。コスト効率の高さで言えば、第一に挙げられるのがテープベースのストレージシステムです。ただし、テープの場合、データへのランダムアクセスが不可能なため、高速検索は望めません。そのため、データを長期間にわたって保存する場合には、複数の手法を組み合わせる使用することが望ましいと言えます。つまり、検索する必要があるデータはランダムアクセスストレージシステムに保存し、保持する必要はあっても検索する必要のないデータは、テープなどのコスト効果の高いストレージに格納します。この複数の手法の組み合わせの使用については、『[Sentinel Log Manager 1.1 Administration Guide](#)(Sentinel Log Manager 1.1 管理ガイド)』の「[Using Sequential-Access Storage for Long Term Data Storage](#)」を参照してください。

Sentinel Log Manager に必要なランダムアクセスストレージの容量を確認するには、何日間のデータに対して定期的な検索またはレポートを実行する必要があるかを最初に見積もります。Sentinel Log Manager でデータのアーカイブに使用するための、十分な容量のあるハードドライブを用意する必要があります。そのためには、ローカルの Sentinel Log Manager マシンを使用することも、Server Message Block (SMB) プロトコル、CIFS プロトコル、Network File System (NFS)、または SAN を使用してリモートのドライブに接続することもできます。

また、最低要件の容量に加えて、次に示すハードドライブの容量も必要になります。

- ◆ データの量が想定外に増えた場合を考慮して追加しておく容量。
- ◆ 古いデータの検索およびレポートを実行するために、Sentinel Log Manager とテープとの間でデータをコピーするための容量。

次の計算式を使用してデータの保存に必要な容量を見積もります。

- ◆ **イベントデータストレージサイズ** : { 日数 } x { 1 秒当たりのイベント数 } x { イベントの平均バイトサイズ } x 0.000012 = 必要なストレージ容量 (GB)

イベントサイズは、通常、300 ~ 1000 バイトです。

- ◆ **生データストレージサイズ** : { 日数 } x { 1 秒当たりのイベント数 } x { 生データの平均バイトサイズ } x 0.000012 = 必要なストレージ容量 (GB)

Syslog メッセージの平均的な生データのサイズは 200 バイトです。

- ◆ **合計ストレージサイズ** : ({ イベントの平均バイトサイズ } + { 生データの平均バイトサイズ }) x { 日数 } x { 1 秒当たりのイベント数 } x 0.000012 = 必要な合計ストレージ容量 (GB)

注 : これらの値はあくまでも概算であり、イベントデータのサイズや圧縮データのサイズによって異なります。

上の計算式では、完全に圧縮されたデータを外部ストレージシステムに保存するために必要な最低限のストレージ容量を求めています。ローカルストレージがいっぱいになると、Sentinel Log Manager は (部分的に圧縮された) ローカルのデータを圧縮してそれを (完全に圧縮された) 外部ストレージシステムに移動します。そのため、データを保持するため

には、必要な外部ストレージの容量を見積もることが最も重要になります。最近のデータの検索およびレポーティングのパフォーマンスを向上させるには、ローカルストレージの容量を、Sentinel Log Manager のハードウェア要件とされている容量よりも増やします。ただし、これは必須ではありません。

また、上の計算式を使用して、テープなどの長期間にわたって使用されるデータストレージシステムに必要なストレージ容量を算出することもできます。

2.1.4 仮想環境

Sentinel Log Manager は、広範にわたるテストが実施されており、VMware ESX サーバで完全にサポートされています。仮想環境では、物理マシン上のテストで得られたのと同程度のパフォーマンスが得られますが、そのためには物理マシンで推奨されているのと同様のメモリ、CPU、ディスク容量、および I/O が必要になります。

2.2 サポートされるオペレーティングシステム

このセクションでは、Sentinel Log Manager サーバおよびリモートのコレクタマネージャでサポートされるオペレーティングシステムについて説明します。

- ◆ [20 ページのセクション 2.2.1 「Sentinel Log Manager」](#)
- ◆ [20 ページのセクション 2.2.2 「コレクタマネージャ」](#)

2.2.1 Sentinel Log Manager

このセクションの内容は、既存のオペレーティングシステムに Sentinel Log Manager をインストールする場合にのみ適用されます。

- 64 ビット SUSE Linux Enterprise Server 11
- 高パフォーマンスのファイルシステム。

注：Novell のテストはすべて、ext3 ファイルシステムで実行されます。

2.2.2 コレクタマネージャ

次のオペレーティングシステムに追加のコレクタマネージャをインストールできます。

- ◆ [20 ページの「Linux」](#)
- ◆ [20 ページの「Windows」](#)

Linux

- SUSE Linux Enterprise Server 10 SP2 (32 ビットおよび 64 ビット)
- SUSE Linux Enterprise Server 11 (32 ビットおよび 64 ビット)

Windows

- Windows Server 2003 (32 ビットおよび 64 ビット)

- Windows Server 2003 SP2 (32 ビット版および 64 ビット版)
- Windows Server 2008 (64 ビット)

2.3 サポートされるブラウザ

Sentinel Log Manager のインタフェースは、次のサポートされるブラウザでの 1280 x 1024 以上の解像度での表示用に最適化されています。

- ◆ 21 ページのセクション 2.3.1 「Linux」
- ◆ 21 ページのセクション 2.3.2 「Windows」

2.3.1 Linux

- Mozilla Firefox 3.6

2.3.2 Windows

- Mozilla Firefox 3 (3.6 を推奨)
- Microsoft Internet Explorer 8 (8.0 を推奨)

Internet Explorer 8 の前提条件

- ◆ インターネットのセキュリティ レベルが [高] に設定されている場合、Novell Sentinel Log Manager にログインしても、空白のページしか表示されません。この問題を解決するには、[ツール] > [インターネット オプション] > [セキュリティ] タブ > [信頼済みサイト] に移動します。[サイト] ボタンをクリックして、Sentinel Log Manager の Web サイトを信頼済みサイトのリストに追加します。
- ◆ [ツール] > [互換性表示] オプションが選択されていないことを確認します。
- ◆ [ファイルのダウンロード時に自動的にダイアログを表示] オプションが有効でない場合、ファイルのダウンロードのポップアップがブラウザでブロックされる場合があります。この問題を解決するには、[ツール] > [インターネット オプション] > [セキュリティ] タブ > [レベルのカスタマイズ] に移動して、[ダウンロード] セクションまで下にスクロールし、[ファイルのダウンロード時に自動的にダイアログを表示] オプションの [有効にする] をクリックします。

2.4 サポートされる仮想環境

- VMware ESX/ESXi 3.5/4.0 以上
- VMPlayer 3 (デモ専用)
- Xen 3.1.1

2.5 サポートされるコネクタ

Sentinel Log Manager は、Sentinel および Sentinel RD でサポートされるすべてのコネクタをサポートしています。

- 監査コネクタ

- チェックポイント LEA プロセスコネクタ
- データベースコネクタ
- データジェネレータコネクタ
- ファイルコネクタ
- プロセスコネクタ
- Syslog コネクタ
- SNMP コネクタ
- SDEE コネクタ
- Sentinel Link コネクタ
- WMS コネクタ
- メインフレームコネクタ
- SAP コネクタ

注：メインフレームおよび SAP コネクタには、個別のライセンスが必要です。

2.6 サポートされるイベントソース

Sentinel Log Manager は、侵入検出システム、ファイアウォール、オペレーティングシステム、ルータ、Web サーバ、データベース、スイッチ、メインフレーム、およびアンチウイルスイベントソースなどの広範なデバイスおよびアプリケーションをサポートしています。これらのイベントソースから送信されたデータは解析および正規化されますが、その度合いは、データの処理に、イベントのペイロード全体を 1 つの共通のフィールドに配置する一般的なイベントコレクタを使用するか、データを個別のフィールドに解析するデバイス固有のコレクタを使用するかによって異なります。

Sentinel Log Manager は、次のイベントソースでサポートされます。

- Cisco Firewall (6 および 7)
- Cisco Switch Catalyst 6500 シリーズ (CatOS 8.7)
- Cisco Switch Catalyst 6500 シリーズ (IOS 12.2SX)
- Cisco Switch Catalyst 5000 シリーズ (CatOS 4.x)
- Cisco Switch Catalyst 4900 シリーズ (IOS 12.2SG)
- Cisco Switch Catalyst 4500 シリーズ (IOS 12.2SG)
- Cisco Switch Catalyst 4000 シリーズ (CatOS 4.x)
- Cisco Switch Catalyst 3750 シリーズ (IOS 12.2SE)
- Cisco Switch Catalyst 3650 シリーズ (IOS 12.2SE)
- Cisco Switch Catalyst 3550 シリーズ (IOS 12.2SE)
- Cisco Switch Catalyst 2970 シリーズ (IOS 12.2SE)
- Cisco Switch Catalyst 2960 シリーズ (IOS 12.2SE)
- Cisco VPN 3000 (4.1.5、4.1.7、および 4.7.2)
- Extreme Networks Summit X650 (ExtremeXOS 12.2.2 以前を搭載)
- Extreme Networks Summit X450a (ExtremeXOS 12.2.2 以前を搭載)

- ❑ Extreme Networks Summit X450e (ExtremeXOS 12.2.2 以前を搭載)
- ❑ Extreme Networks Summit X350 (ExtremeXOS 12.2.2 以前を搭載)
- ❑ Extreme Networks Summit X250e (ExtremeXOS 12.2.2 以前を搭載)
- ❑ Extreme Networks Summit X150 (ExtremeXOS 12.2.2 以前を搭載)
- ❑ Enterasys Dragon (7.1 および 7.2)
- ❑ 一般的なイベントコレクタ
- ❑ HP HP-UX (11iv1 および 11iv2)
- ❑ IBM AIX (5.2、5.3、および 6.1)
- ❑ Juniper Netscreen 5 シリーズ
- ❑ McAfee Firewall Enterprise
- ❑ McAfee Network Security Platform (2.1、3.x、および 4.1)
- ❑ McAfee VirusScan Enterprise (8.0i、8.5i、および 8.7i)
- ❑ McAfee ePolicy Orchestrator (3.6 および 4.0)
- ❑ McAfee AV Via ePolicy Orchestrator 8.5
- ❑ Microsoft Active Directory (2000、2003、および 2008)
- ❑ Microsoft SQL Server (2005 および 2008)
- ❑ Nortel VPN (1750、2700、2750、および 5000)
- ❑ Novell Access Manager 3.1
- ❑ Novell Identity Manager 3.6.1
- ❑ Novell Netware 6.5
- ❑ Novell Modular Authentication Services 3.3
- ❑ Novell Open Enterprise Server 2.0.2
- ❑ Novell Privileged User Manager 2.2.1
- ❑ Novell Sentinel Link 1
- ❑ Novell SUSE Linux Enterprise Server
- ❑ Novell サポート Web サイト (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~) にある eDirectory インストラメンテーションパッチを適用した Novell eDirectory 8.8.3
- ❑ Novell iManager 2.7
- ❑ Red Hat Enterprise Linux
- ❑ Sourcefire Snort (2.4.5、2.6.1、2.8.3.2、および 2.8.4)
- ❑ Snare for Windows Intersect Alliance (3.1.4 および 1.1.1)
- ❑ Sun Microsystems Solaris 10
- ❑ Symantec AntiVirus Corporate Edition (9 および 10)
- ❑ TippingPoint Security Management System (2.1 および 3.0)
- ❑ Websense Web Security 7.0
- ❑ Websense Web Filter 7.0

注 : Novell iManager および Novell Netware 6.5 イベントソースからのデータコレクションを有効にするには、各イベントソースの、イベントソースの管理インタフェースで、コレクタおよび子コレクタ (監査コレクタ) のインスタンスを追加します。すると、これらのイベントソースが Sentinel Log Manager Web コンソールの [監視サーバ] タブに表示されます。

追加のイベントソースをサポートするコレクタは、[Sentinel 6.1 のコンテンツの Web サイト \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html) で取得するか、[Sentinel プラグイン SDK の Web サイト \(http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel\)](http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) で入手できる SDK プラグインを使用して構築します。

既存の SLES 11 システムへのインストール

このセクションでは、アプリケーションのインストーラを使用して Sentinel Log Manager を既存の SUSE Linux Enterprise Server (SLES) 11 システムにインストールする手順について説明します。Sentinel Log Manager サーバは、標準インストール、カスタムインストール、またはサイレントインストール (ユーザの入力が不要で、デフォルト値が使用されるインストール) のいずれかの方法でインストールできます。Sentinel Log Manager は、root 以外のユーザとしてインストールすることもできます。

カスタムインストールを選択する場合は、ライセンスキーを使用して製品をインストールすることも、認証オプションを選択することでもできます。データベース認証に加えて、Sentinel Log Manager の LDAP 認証を設定することができます。Sentinel Log Manager の LDAP 認証の環境設定を行うと、ユーザは Novell eDirectory または Microsoft Active Directory の資格情報を使用してサーバにログインすることができます。

複数の Sentinel Log Manager サーバをインストールして展開する場合は、環境設定ファイルにインストールオプションを記録し、そのファイルを使用して無人インストールを実行することができます。詳細については、[29 ページのセクション 3.4 「サイレントインストール」](#) を参照してください。

インストールを実行する前に、[17 ページの第 2 章 「システム要件」](#) で指定された最小要件を満たしていることを確認してください。

- ◆ [25 ページのセクション 3.1 「作業を開始する前に」](#)
- ◆ [26 ページのセクション 3.2 「標準インストール」](#)
- ◆ [27 ページのセクション 3.3 「カスタムインストール」](#)
- ◆ [29 ページのセクション 3.4 「サイレントインストール」](#)
- ◆ [30 ページのセクション 3.5 「root 以外でのインストール」](#)

3.1 作業を開始する前に

- ハードウェアとソフトウェアが、[17 ページの第 2 章 「システム要件」](#) で説明している最低要件を満たしていることを確認してください。
- オペレーティングシステムの環境設定では、`hostname -f` コマンドが有効なホスト名を返すように設定してください。
- ノベルカスタマケアセンター (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) からライセンスキーを取得して、ライセンスされたバージョンをインストールします。
- Network Time Protocol (NTP) を使用して時刻を同期します。
- 次のオペレーティングシステムのコマンドをインストールします。
 - ◆ `mount`
 - ◆ `umount`
 - ◆ `id`

- ◆ df
 - ◆ du
 - ◆ sudo
- ファイアウォールで次のポートが開いていることを確認します。
- TCP 8080、TCP 8443、TCP 61616、TCP 10013、TCP 1289、TCP 1468、TCP 1443、および UDP 1514

3.2 標準インストール

標準インストールの手順では、すべてのオプションがデフォルト値に設定され、90 日間の評価版ライセンスが付与された状態で Sentinel Log Manager がインストールされます。

- 1 Novell ダウンロードサイトからインストールファイルをダウンロードしてコピーします。

- 2 Sentinel Log Manager をインストールするサーバに root としてログインします。

- 3 次のコマンドを指定して、tar ファイルから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。

- 4 次のコマンドを指定して、install-slm スクリプトを実行し、Sentinel Log Manager をインストールします。

```
./install-slm
```

複数のシステムに Sentinel Log Manager をインストールする場合は、インストールオプションをファイルに記録しておくことができます。このファイルを使用して、他のシステムに無人で Sentinel Log Manager をインストールすることができます。インストールオプションを記録するには、次のコマンドを指定します。

```
./install-slm -r responseFile
```

- 5 指定の言語でインストールを進めるには、言語の横に示された番号を選択します。

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。

- 6 エンドユーザの使用許諾契約を読み、「yes」または「y」と入力して契約に同意し、インストールを続行します。

すべての RPM パッケージのインストールが開始されます。このインストールが完了するまで数秒かかることがあります。

インストール時に、novell グループおよび novell ユーザが存在しなければ、それらが作成されます。

- 7 オプションの指定を求められた場合は、指定して標準インストールを続行します。

インストーラに付属の 90 日間の評価版ライセンスキーを使用してインストールを続行します。このライセンスキーは、90 日の評価期間中すべての製品機能を有効にします。評価期間中または評価期間終了後の任意の時点で、評価版のライセンスを購入したライセンスキーで置き換えることができます。

- 8 管理者ユーザのパスワードを指定します。

- 9 確認のため、管理者ユーザのパスワードをもう一度入力します。

インストーラは [データベースのみに認証する] 方法を選択して、インストールを続行します。

Sentinel Log Manager のインストールが完了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスが起動するまでに 5 ~ 10 分かかる場合があります。サーバにログインできるようになるまで、しばらく待ってください。

- 10 Sentinel Log Manager サーバにログインするには、インストールの出力で指定された URL を使用します。この URL は、<https://10.0.0.1:8443/novelllogmanager> のような形式です。サーバへのログインの詳細については、[45 ページの第 5 章「Web インタフェースにログインします。」](#)を参照してください。
- 11 Sentinel Log Manager にデータを送信するイベントソースの環境設定を行うには、『[Sentinel Log Manager 1.1 Administration Guide](#) (Sentinel Log Manager 1.1 管理ガイド)』の「[Configuring Data Collection](#)」を参照してください。

3.3 カスタムインストール

カスタムインストールという方法を選択する場合は、ライセンスキーを使用して製品をインストールできるほか、認証オプションを選択することもできます。Sentinel Log Manager では、データベース認証に加えて、LDAP 認証を使用するように設定することもできます。Sentinel Log Manager で LDAP 認証を使用するように環境設定をすると、ユーザは LDAP ディレクトリ資格情報を使用してサーバにログインできるようになります。

インストール時に、Sentinel Log Manager で LDAP 認証を使用するように環境設定をしなかった場合でも、必要に応じて後で認証の環境設定を行うことができます。インストール後の LDAP 認証の設定については、『[Sentinel Log Manager 1.1 Administration Guide](#) (Sentinel Log Manager 1.1 管理ガイド)』の「[LDAP Authenticationg](#)」を参照してください。

- 1 Novell ダウンロードサイトからインストールファイルをダウンロードしてコピーします。

- 2 Sentinel Log Manager をインストールするサーバに root としてログインします。

- 3 次のコマンドを指定して、tar ファイルから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。

- 4 次のコマンドを指定して、install-slm スクリプトを実行し、Sentinel Log Manager をインストールします。

```
./install-slm
```

- 5 指定の言語でインストールを進めるには、言語の横に示された番号を選択します。

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。

- 6 エンドユーザの使用許諾契約を読み、「yes」または「y」と入力して契約に同意し、インストールを続行します。

すべての RPM パッケージのインストールが開始されます。このインストールが完了するまで数秒かかることがあります。

インストール時に、novell グループおよび novell ユーザが存在しなければ、それらが作成されます。

- 7 オプションの指定を求められた場合は、指定してカスタムインストールを続行します。

- 8 ライセンスキーオプションを指定するよう求められたら、「2」を入力して購入した製品のライセンスキーを指定します。
- 9 ライセンスキーを指定して、<Enter> を押します。
ライセンスキーの詳細については、『[Sentinel Log Manager 1.1 Administration Guide](#) (Sentinel Log Manager 1.1 管理ガイド)』の「[Managing License Keys](#)」を参照してください。
- 10 管理者ユーザのパスワードを指定します。
- 11 確認のため、管理者ユーザのパスワードをもう一度入力します。
- 12 データベース管理者 (dbausser) のパスワードを指定します。
- 13 確認のため、データベース管理者 (dbausser) のパスワードをもう一度入力します。
- 14 次のサービスに対して、指定された範囲内の任意の有効なポート番号を設定できます。
 - ◆ Web サーバ
 - ◆ Java メッセージサービス
 - ◆ クライアントプロキシサービス
 - ◆ データベースサービス
 - ◆ エージェント内部ゲートウェイデフォルトポートを使用する場合は、オプション「6」を入力してカスタムインストールを続行します。
- 15 外部 LDAP ディレクトリを通じてユーザを認証するオプションを指定します。
- 16 LDAP サーバの IP アドレスまたはホスト名を指定します。
デフォルト値は localhost です。ただし、LDAP サーバは Sentinel Log Manager サーバと同じマシンにはインストールしないでください。
- 17 次のいずれかの LDAP 接続のタイプを選択します。
 - ◆ **SSL/TSL LDAP 接続** : ブラウザとサーバと間で認証のためのセキュアな接続を確立します。「1」と入力してこのオプションを指定します。
 - ◆ **暗号化されていない LDAP 接続** : 暗号化されていない接続を確立します。「2」と入力してこのオプションを指定します。
- 18 LDAP サーバのポート番号を指定します。デフォルトの SSL ポートは 636、デフォルトの非 SSL ポートは 389 です。
- 19 (条件付き) SSL/TSL LDAP 接続を選択した場合は、LDAP サーバ証明書が既知の CA で署名されるかどうかを指定します。
- 20 (条件付き) 「n」を指定した場合は、LDAP サーバ証明書のファイル名を指定します。
- 21 LDAP ディレクトリで匿名検索を実行するかどうかを指定します。
 - ◆ **LDAP ディレクトリで匿名検索を実行します**。Sentinel Log Manager サーバは、指定されたユーザ名に基づいて LDAP ディレクトリで匿名検索を実行して、対応する LDAP ユーザの識別名 (DN) を取得します。「1」と入力してこの方法を指定します。
 - ◆ **LDAP ディレクトリで匿名検索を実行しないでください**。「2」と入力してこのオプションを指定します。

- 22 (条件付き) 匿名検索を選択した場合は、検索属性を指定して [ステップ 25](#) に進みます。
- 23 (条件付き) [ステップ 21](#) で匿名検索を選択しなかった場合は、Microsoft Active Directory を使用するかどうかを指定します。
Active Directory では、userPrincipalName 属性 (userName@domainName という形式) をオプションで使用して、ユーザ DN を入力することなく、LDAP ユーザオブジェクトを検索する前にユーザを認証することができます。
- 24 (条件付き) 上で説明した Active Directory を使用する方法を選んだ場合は、ドメイン名を指定します。
- 25 ベース DN を指定します。
- 26 オプションの指定に間違いがなければ、「y」を押します。それ以外の場合は、「n」を押して環境設定を変更します。
- 27 Sentinel Log Manager サーバにログインするには、インストールの出力で指定された URL を使用します。この URL は、https://10.0.0.1:8443/novelllogmanager のような形式です。
サーバへのログインの詳細については、[45 ページの第 5 章「Web インタフェースにログインします。」](#)を参照してください。

3.4 サイレントインストール

複数の Sentinel Log Manager サーバをインストールして展開する必要がある場合は、Sentinel Log Manager のサイレントインストール (無人インストール) が便利です。そのような場合には、最初のインストール時にインストールパラメータを記録し、記録したファイルをその他すべてのサーバで実行します。

- 1 Novell ダウンロードサイトからインストールファイルをダウンロードしてコピーします。
- 2 Sentinel Log Manager をインストールするサーバに root としてログインします。
- 3 次のコマンドを指定して、tar ファイルから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。
- 4 次のコマンドを指定して、install-slm スクリプトを実行し、Sentinel Log Manager をサイレントモードでインストールします。

```
./install-slm -u responseFile
```


応答ファイルの作成の詳細については、[26 ページのセクション 3.2「標準インストール」](#)を参照してください。インストールは、応答ファイルに保存された値を使用して進められます。
- 5 Sentinel Log Manager サーバにログインするには、インストールの出力で指定された URL を使用します。この URL は、https://10.0.0.1:8443/novelllogmanager のような形式です。
サーバへのログインの詳細については、[45 ページの第 5 章「Web インタフェースにログインします。」](#)を参照してください。
- 6 Sentinel Log Manager にデータを送信するイベントソースの環境設定を行うには、『[“Sentinel Log Manager 1.1 Administration Guide”](#) (Sentinel Log Manager 1.1 管理ガイド)』の『[“Configuring Data Collection”](#)』を参照してください。

3.5 root 以外でのインストール

組織のポリシーにより、root として Sentinel Log Manager の完全なインストールを実行することは許可されていなくても、ほとんどのインストール手順は他のユーザとして実行できます。

1 Novell ダウンロードサイトからインストールファイルをダウンロードしてコピーします。

2 次のコマンドを指定して、tar ファイルから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 root として Sentinel Log Manager をインストールするサーバに root としてログインします。

4 次のコマンドを指定します。

```
./bin/root_install_prepare
```

root 権限で実行するコマンドの一覧が表示されます。

これによって、novell グループおよび novell ユーザが存在しなければ、それらが作成されます。

5 コマンドリストを受け入れます。

表示されたコマンドが実行されます。

6 次のコマンドを指定して、新しく作成された、root でない novell ユーザに変更します：
: novell:

```
su novell
```

7 次のコマンドを指定します。

```
./install-slm
```

8 指定の言語でインストールを進めるには、言語の横に示された番号を選択します。

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。

9 エンドユーザの使用許諾契約を読み、「yes」または「y」と入力して契約に同意し、インストールを続行します。

すべての RPM パッケージのインストールが開始されます。このインストールが完了するまで数秒かかることがあります。

10 インストールのモードを指定するように求められます。

- ◆ 標準インストールを選択した場合は、[26 ページのセクション 3.2 「標準インストール」](#) の手順 8 ～手順 11 を実行します。
- ◆ カスタムインストールを選択した場合、[27 ページのセクション 3.3 「カスタムインストール」](#) の手順 8 ～手順 23 を実行します。

Sentinel Log Manager のインストールが終了し、サーバが起動します。

11 次のコマンドを指定して、root ユーザに変更します。

```
su root
```

12 次のコマンドを指定して、インストールを終了します。

```
./bin/root_install_finish
```

- 13 Sentinel Log Manager** サーバにログインするには、インストールの出力で指定された URL を使用します。この URL は、`https://10.0.0.1:8443/novelllogmanager` のような形式です。サーバへのログインの詳細については、[45 ページの第 5 章「Web インタフェースにログインします。」](#)を参照してください。

アプライアンスのインストール

Novell Sentinel Log Manager アプライアンスは、SUSE Studio を基に構築された即座に実行できるソフトウェアアプライアンスです。強化された SUSE Linux Enterprise Server (SLES) 11 オペレーティングシステムと Novell Sentinel Log Manager ソフトウェアの統合アップデートサービスを組み合わせて、ユーザによる既存の投資の活用を可能にし、使いやすいシームレスなユーザエクスペリエンスを実現します。ソフトウェアアプライアンスは、ハードウェアまたは仮想環境にインストールできます。

- ◆ 33 ページのセクション 4.1 「作業を開始する前に」
- ◆ 33 ページのセクション 4.2 「使用するポート」
- ◆ 35 ページのセクション 4.3 「VMware アプライアンスのインストール」
- ◆ 36 ページのセクション 4.4 「Xen アプライアンスのインストール」
- ◆ 38 ページのセクション 4.5 「ハードウェアへのアプライアンスのインストール」
- ◆ 39 ページのセクション 4.6 「アプライアンスのインストール後の設定」
- ◆ 39 ページのセクション 4.7 「WebYaST の環境設定」
- ◆ 42 ページのセクション 4.8 「アップデートの登録」

4.1 作業を開始する前に

- ◆ ハードウェア要件が満たされていることを確認してください。詳細については、17 ページのセクション 2.1 「ハードウェア要件」を参照してください。
- ◆ ノベルカスタマケアセンター (<http://www.novell.com/center>) からライセンスキーを取得して、ライセンスされたバージョンをインストールします。
- ◆ ノベルカスタマケアセンター (<http://www.novell.com/center>) から登録コードを取得して、ソフトウェアのアップデートを登録します。
- ◆ Network Time Protocol (NTP) を使用して時刻を同期します。
- ◆ (条件付き)VMwareを使用する場合は、イメージをVMware ESX サーバにアップロードすると同時に ESX サーバ上で実行可能な形式に変換する VMware Converter が用意されていることを確認してください。

4.2 使用するポート

Novell Sentinel Log Manager アプライアンスでは、通信に次のポートを使用し、それらの一部はファイアウォールで開きます。

- ◆ 34 ページのセクション 4.2.1 「ファイアウォールで開くポート」
- ◆ 34 ページのセクション 4.2.2 「ローカルで使用されるポート」

4.2.1 ファイアウォールで開くポート

表 4-1 Sentinel Log Manager で使用するネットワークポート

ポート	説明
TCP 1289	Novell Audit の接続用に使用されます。
TCP 289	Novell Audit の接続用に 1289 に転送されます。
TCP 22	シェルが Sentinel Log Manager アプライアンスに安全にアクセスできるようにするために使用されます。
UDP 1514	Syslog メッセージ用に使用されます。
UDP 514	Syslog メッセージ用に 1514 に転送されます。
TCP 8080	HTTP 通信用に使用されます。Sentinel Log Manager アプライアンスのアップデートサービスにも使用されます。
TCP 80	Sentinel Log Manager Web サーバの HTTP 通信用に 8080 に転送されます。Sentinel Log Manager アプライアンスのアップデートサービスにも使用されます。
TCP 8443	HTTPS 通信に使用されます。Sentinel Log Manager アプライアンスのアップデートサービスにも使用されます。
TCP 1443	SSL で暗号化された Syslog メッセージに使用されます。
TCP 443	Sentinel Log Manager Web サーバの HTTPS 通信用に 8443 に転送されます。Sentinel Log Manager アプライアンスのアップデートサービスにも使用されます。
TCP 61616	コレクタマネージャとサーバ間の通信に使用されます。
TCP 10013	イベントソースの管理ユーザインタフェースの SSL プロキシで使用されます。
TCP 54984	Sentinel Log Manager アプライアンスの管理コンソール (WebYaST) で使用されます。
TCP 1468	Syslog メッセージ用に使用されます。

4.2.2 ローカルで使用されるポート

表 4-2 ローカルで通信に使用されるポート

ポート	説明
TCP 61617	Web サーバとサーバ間の内部通信用に使用されます。
TCP 5556	internal_gateway_server および internal_gateway により、内部通信のループバックインタフェースで使用されます。これは、エージェントのエンジンとコレクタマネージャ間の通信に使用されます。

ポート	説明
TCP 5432	PostgreSQL データベースで使用されます。デフォルトでこのポートを開く必要はありません。ただし、Sentinel SDK を使用してレポートを作成する場合には、このポートを開く必要があります。詳細については、Sentinel プラグイン SDK の Web サイト (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) を参照してください。
ランダムに選択された 2 つの追加の TCP ポート	エージェントのエンジンとコレクタマネージャ間の内部通信に使用されます。
TCP 8005	Tomcat プロセスとの内部通信に使用されます。
TCP 32000	エージェントのエンジンとコレクタマネージャ間の内部通信に使用されます。

4.3 VMware アプライアンスのインストール

Vmware ESX サーバからアプライアンスイメージを実行するには、アプライアンスイメージをサーバにインポートしてインストールします。

- 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 (例: `Sentinel_Log_Manager_1.1.0.0_64_VMX.x86_64-0.777.0.vmx.tar.gz`)。
- 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。
- 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。
- 次のコマンドを指定して、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。
- 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。
- ESX サーバマシンにログインします。
- 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。
- 使用する言語を選択して、[次へ] をクリックします。
- 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。
- Novell SUSE 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。
- Novell Sentinel Log Manager エンドユーザ使用許諾契約書の条項を確認して同意します。
- [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。[ホスト名を /etc/hosts に書き込む] オプションが選択されていることを確認します。
- [次へ] を選択します。ホスト名の環境設定が保存されます。

- 14 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] を選択します。
- 15 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。

注: 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せんが、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
```

- 16 Novell SUSE 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。
- 17 root のパスワードを設定して、[次へ] をクリックします。
- 18 Sentinel Log Manager 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。
- 19 [次へ] を選択します。ネットワーク接続設定が保存されます。
- インストールが継続されて完了します。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。
- 20 [39 ページのセクション 4.6 「アプライアンスのインストール後の設定」](#) に従って手順を進めます。

4.4 Xen アプライアンスのインストール

- 1 Xen 仮想アプライアンスのインストールファイルをダウンロードして /var/lib/xen/images にコピーします。
- Xen 仮想アプライアンスの正しいファイル名には、xen が含まれます (例: Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.xen.tar.gz)。
- 2 次のコマンドを指定して、ファイルをアンパックします。
- ```
tar -xvzf <install_file>
```
- <install\_file> は、実際のインストールファイル名に置き換えます。
- 3 新しいインストールディレクトリに移動します。このディレクトリには、次のファイルがあります。
- ◆ <file\_name>.raw イメージファイル
  - ◆ <file\_name>.xenconfig ファイル
- 4 テキストエディタを使用して <file\_name>.xenconfig ファイルを開きます。
- 5 このファイルを次のように変更します。
- disk 設定の .raw ファイルのフルパスを指定します。
- ネットワーク環境設定のブリッジ設定を指定します (例: "bridge=br0" または "bridge=xenbr0")。
- name および memory の設定値を指定します。

例：

```
-*- mode: python; -*-
name="Sentinel_Log_Manager_1.1.0.0_64"
memory=4096
disk=["tap:aio:/var/lib/xen/images/Sentinel_Log_Manager_1.1.0.0_64_Xen-
0.777.0/Sentinel_Log_Manager_1.1.0.0_64_Xen.x86_64-0.777.0.raw,xvda,w"]
vif=["bridge=br0"]
```

- 6 <filename>.xenconfig ファイルを修正したら、次のコマンドを指定して VM を作成します。

```
xm create <file_name>.xenconfig
```

- 7 (オプション)VM が作成されたかどうかを確認するには、次のコマンドを指定します。

```
xm list
```

リストに VM が表示されます。

たとえば、.xenconfig ファイルに name=" Sentinel\_Log\_Manager\_1.1.0.0\_64" と環境設定されている場合、VM はその名前で表示されます。

- 8 インストールを実行するには、次のコマンドを指定します。

```
xm console <vm name>
```

<vm name> は、.xenconfig ファイルでの名前設定で指定された名前に置き換えます。これは、[手順 7](#) で返された名前でもあります。例：

```
xm console Sentinel_Log_Manager_1.1.0.0_64
```

- 9 使用する言語を選択して、[次へ] をクリックします。
- 10 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。
- 11 Novell SUSE 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。
- 12 Novell Sentinel Log Manager エンドユーザ使用許諾契約書の条項を確認して同意します。
- 13 [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。[ホスト名を/etc/hosts に書き込む] 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] 画面で [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] を選択します。
- 16 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。

---

**注：**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
```

- 
- 17 Novell SUSE 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。

- 18 Sentinel Log Manager 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。  
インストールが継続されて完了します。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。
- 19 39 ページのセクション 4.6 「アプライアンスのインストール後の設定」に従って手順を進めます。

## 4.5 ハードウェアへのアプライアンスのインストール

ハードウェアにアプライアンスをインストールする前に、アプライアンス ISO ディスクイメージがサポートサイトからダウンロードされ、アンパックされて、DVD で使用可能になっていることを確認します。

- 1 DVD ドライブからその DVD を使用して物理マシンをブートします。
- 2 インストールウィザードの画面の指示に従います。
- 3 ブートメニューの一番上のエントリを選択して、ライブ DVD のアプライアンスイメージを実行します。
- 4 Novell SUSE 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。
- 5 Novell Sentinel Log Manager エンドユーザ使用許諾契約書の条項を確認して同意します。
- 6 [次へ] を選択します。
- 7 [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。  
[ホスト名を/etc/hosts に書き込む] オプションが選択されていることを確認します。
- 8 [次へ] を選択します。ホスト名の環境設定が保存されます。
- 9 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] 画面で [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] を選択します。
- 10 [次へ] を選択します。ネットワーク接続設定が保存されます。
- 11 日付と時刻を設定して、[次へ] をクリックします。

---

**注:** 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せんが、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
```

- 
- 12 root のパスワードを設定して、[次へ] をクリックします。
  - 13 Sentinel Log Manager 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。
  - 14 コンソールでユーザ名とパスワードを入力して、アプライアンスにログインします。

ユーザ名のデフォルト値は root で、パスワードは password です。

- 15 物理サーバにアプライアンスをインストールするには、次のコマンドを実行します。

```
/sbin/yast2 live-installer
```

インストールが続きされて完了します。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。

- 16 [39 ページのセクション 4.6 「アプライアンスのインストール後の設定」](#)に従って手順を進めます。

## 4.6 アプライアンスのインストール後の設定

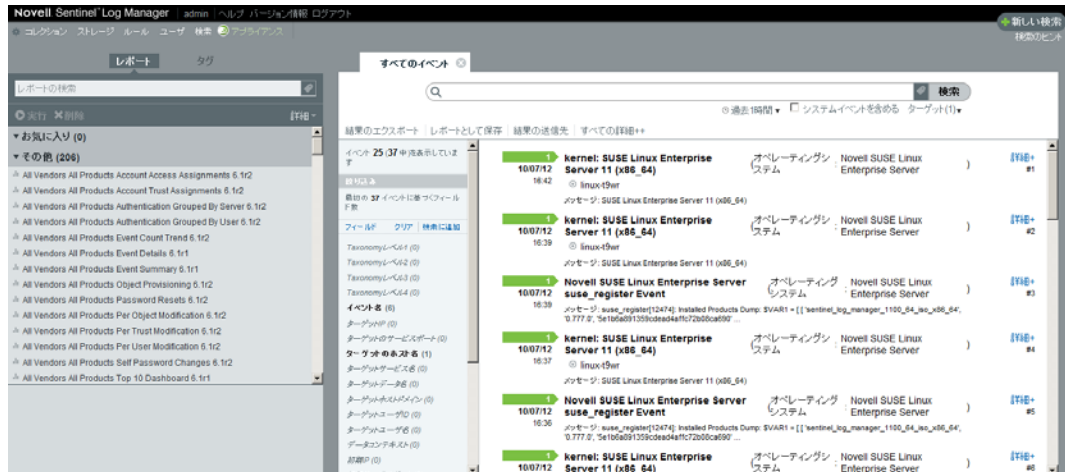
アプライアンスの Web コンソールにログインしてソフトウェアを初期化するには、次の手順を実行します。

- 1 Web ブラウザを開いて、<https://<IP address>:8443> にログインします。Sentinel Log Manager の Web ページが表示されます。  
インストールが完了してサーバが再起動すると、アプライアンスの IP アドレスがアプライアンスコンソールに表示されます。
- 2 Sentinel Log Manager アプライアンスでデータストレージおよびデータコレクションの環境設定を行えます。アプライアンスの環境設定の詳細については、『[Sentinel Log Manager 1.1 Administration Guide](#) (Sentinel Log Manager 1.1 管理ガイド)』を参照してください。
- 3 アップデートを登録するには、[42 ページのセクション 4.8 「アップデートの登録」](#)を参照してください。

## 4.7 WebYaST の環境設定

Novell Sentinel Log Manager アプライアンスのユーザインタフェースには、WebYaST が備わっています。WebYaST は、SUSE Linux Enterprise に基づいた、アプライアンスを制御するための Web ベースのリモートコンソールです。WebYaST を使用して、Sentinel Log Manager アプライアンスに対するアクセス、環境設定、監視を行います。次に、WebYaST の環境設定の手順について簡単に説明します。環境設定の詳細については、『[WebYaST User Guide \(http://www.novell.com/documentation/webyast/\)](http://www.novell.com/documentation/webyast/)(WebYaST ユーザガイド)』を参照してください。

- 1 Sentinel Log Manager アプライアンスにログインします。

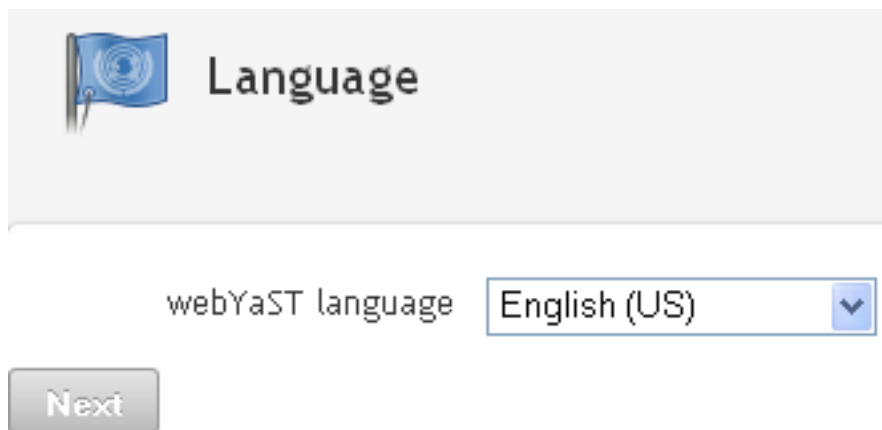


2 [アプライアンス] をクリックします。



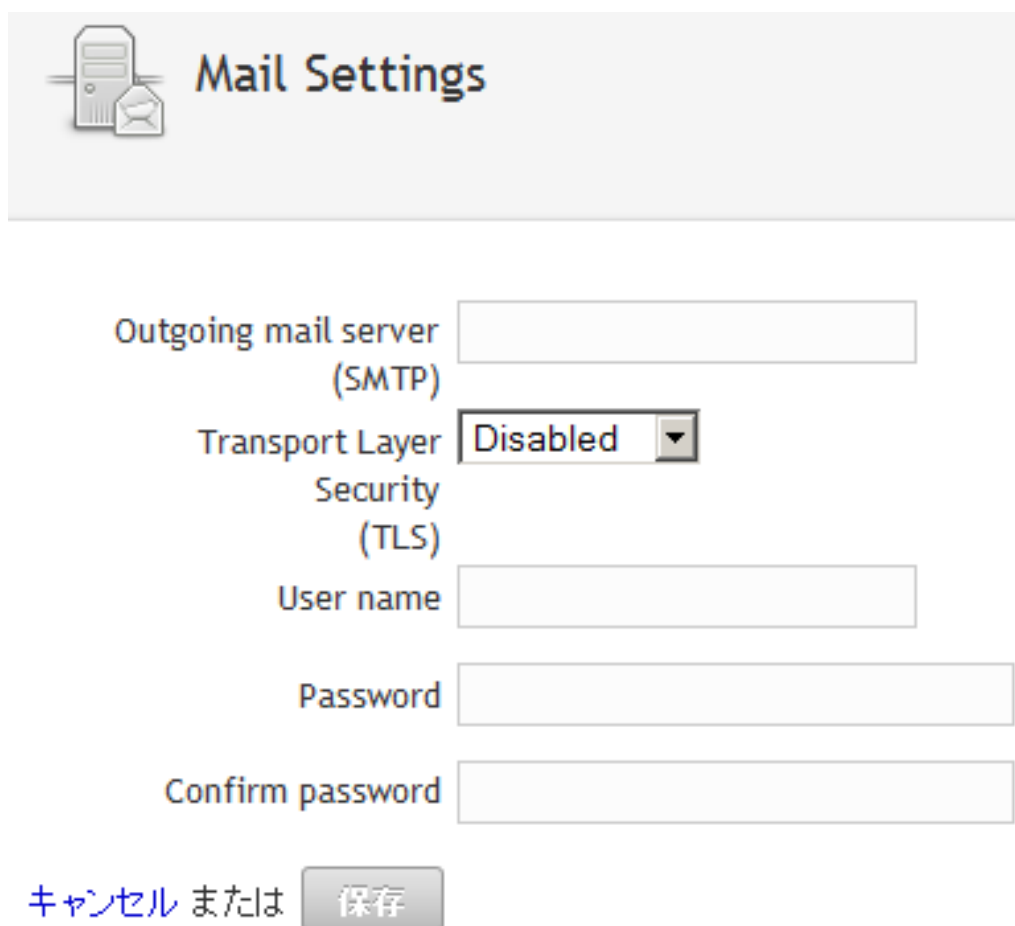
3 システムのログイン資格情報を指定して、[ログイン] をクリックします。





The screenshot shows a 'Language' configuration screen. At the top left is a blue flag icon with a globe. To its right is the title 'Language'. Below this, the text 'webYaST language' is followed by a dropdown menu currently set to 'English (US)'. At the bottom left is a grey button labeled 'Next'.

- 4 使用する言語を選択して、[次へ] をクリックします。

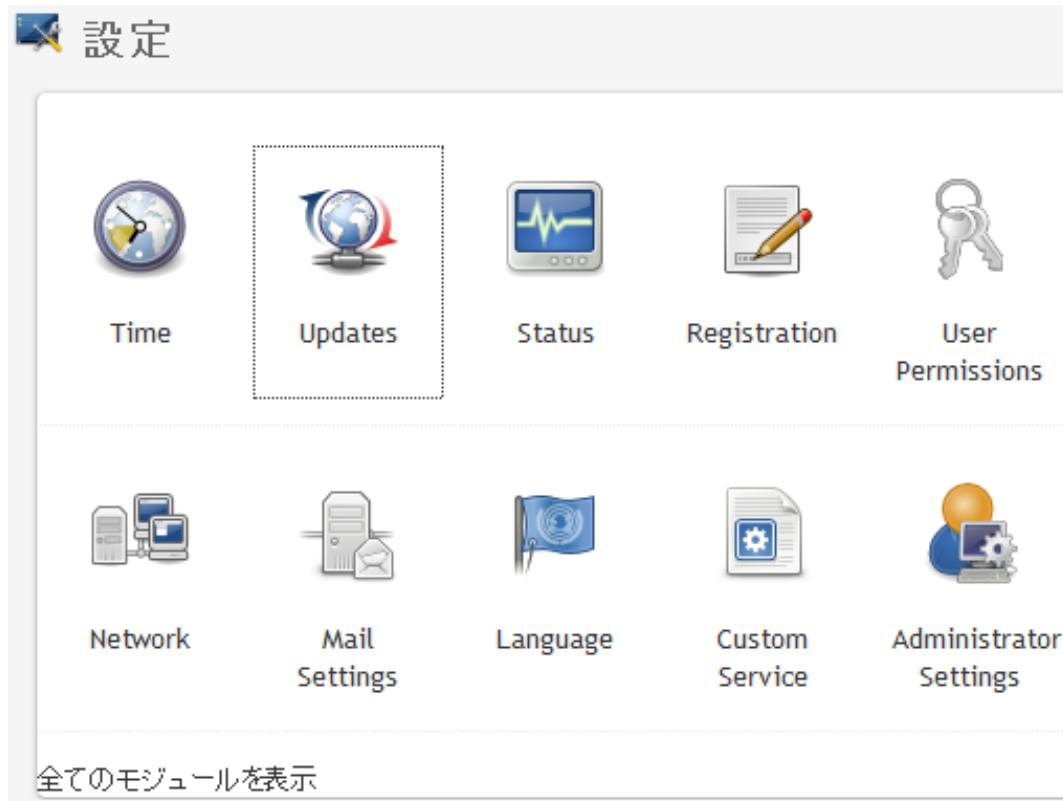


The screenshot shows a 'Mail Settings' configuration screen. At the top left is an icon of a server tower and an envelope. To its right is the title 'Mail Settings'. Below this are several input fields: 'Outgoing mail server (SMTP)' with an empty text box; 'Transport Layer Security (TLS)' with a dropdown menu set to 'Disabled'; 'User name' with an empty text box; 'Password' with an empty text box; and 'Confirm password' with an empty text box. At the bottom left is a blue link 'キャンセル' followed by a grey button '保存'.

- 5 メールサーバの環境設定の詳細を指定して、[保存] をクリックします。  
登録ページが表示されます。
- 6 [42 ページのセクション 4.8 「アップデートの登録」](#) の説明にあるように、アップデートを受信する Sentinel Log Manager サーバの環境設定を行います。
- 7 [次へ] をクリックして、初期設定を完了します。

## 4.8 アップデートの登録

- 1 Sentinel Log Manager アプライアンスにログインします。  
Sentinel Log Manager の Web ユーザインタフェースが表示されます。
- 2 [アプライアンス] をクリックして、WebYaST を起動します。



- 3 [登録] をクリックします。



## Registration

### Mandatory Information

Email

System name

regcode-slm

[Show Details](#)

[キャンセル](#) または

- 4 アプライアンス登録コードを指定します。
- 5 [保存] をクリックします。
- 6 アップデートがあるかどうかを確認するには、[更新] をクリックします。  
そこで表示されるページに、アップデートがあるかどうかが表示されます。



## Updates

Your system is up to date.



# Web インタフェースにログインします。

インストール時に作成された管理者ユーザは、Web インタフェースにログインして、Sentinel Log Manager の環境設定を行ったり、使用したりすることができます。

- 1 対応 Web ブラウザを開きます。詳細については、[21 ページのセクション 2.3 「サポートされるブラウザ」](#)を参照してください。
- 2 Novell Sentinel Log Manager の URL ページ ( 例 : <https://10.0.0.1:8443/novelllogmanager>) を指定して、<Enter> を押します。
- 3 ( 条件付き )Sentinel Log Manager にはじめてログインすると、証明書に同意するように求められます。証明書に同意すると、Sentinel Log Manager のログインページが表示されます。



4 Sentinel Log Manager 管理者のユーザ名とパスワードを指定します。

5 Sentinel Log Manager のインターフェースの言語を選択します。

Sentinel Log Manager のユーザインターフェースは、英語、ポルトガル語、フランス語、イタリア語、ドイツ語、スペイン語、日本語、繁体字中国語、または簡体字中国語を使用できます。

6 [サインイン] をクリックします。

Novell Sentinel Log Manager の Web ユーザーインターフェースが表示されます。

The screenshot displays the Novell Sentinel Log Manager web interface. The top navigation bar includes the title "Novell Sentinel Log Manager" and user information "admin". The main content area is titled "すべてのイベント" (All Events) and shows a list of system events. The left sidebar contains a "レポート" (Reports) section with a search bar and a list of report categories. The main event list includes columns for time, event name, category, and source. The events shown are related to kernel and suse\_register events on a SUSE Linux Enterprise Server 11 (x86\_64).

| Time          | Event Name                                              | Category     | Source                              | Details                                                                                                                                  |
|---------------|---------------------------------------------------------|--------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| 1007/12 16:42 | kernel: SUSE Linux Enterprise Server 11 (x86_64)        | オペレーティングシステム | Novell SUSE Linux Enterprise Server | linux-49hr                                                                                                                               |
| 1007/12 16:39 | kernel: SUSE Linux Enterprise Server 11 (x86_64)        | オペレーティングシステム | Novell SUSE Linux Enterprise Server | linux-49hr                                                                                                                               |
| 1007/12 16:39 | Novell SUSE Linux Enterprise Server suse_register Event | オペレーティングシステム | Novell SUSE Linux Enterprise Server | suse_register(1247): Installed Products Dump: SVAR1 = [{"sentinel_log_manager_1100_64_x86_64_0.777.0", "5e106a091208c0ea4efc7200ca690"}] |
| 1007/12 16:37 | kernel: SUSE Linux Enterprise Server 11 (x86_64)        | オペレーティングシステム | Novell SUSE Linux Enterprise Server | linux-49hr                                                                                                                               |
| 1007/12 16:36 | Novell SUSE Linux Enterprise Server suse_register Event | オペレーティングシステム | Novell SUSE Linux Enterprise Server | suse_register(1247): Installed Products Dump: SVAR1 = [{"sentinel_log_manager_1100_64_x86_64_0.777.0", "5e106a091208c0ea4efc7200ca690"}] |
| 1007/12 16:37 | kernel: SUSE Linux Enterprise Server 11 (x86_64)        | オペレーティングシステム | Novell SUSE Linux Enterprise Server | linux-49hr                                                                                                                               |





# Sentinel Log Manager のアップグレード

# 6

アップグレードスクリプトを使用して、Novell Sentinel Log Manager 1.0.0.4 以上から Sentinel Log Manager 1.1 にアップグレードできます。

- [49 ページのセクション 6.1 「1.0 から 1.1 へのアップグレード」](#)
- [50 ページのセクション 6.2 「コレクタマネージャのアップグレード」](#)
- [51 ページのセクション 6.3 「1.0 から 1.1 アプライアンスへの移行」](#)

## 6.1 1.0 から 1.1 へのアップグレード

- 1 Sentinel Log Manager サーバのバージョンが 1.0.0.4 より古い場合、まず 1.0.0.4 以上にアップグレードする必要があります。
- 2 Novell ダウンロードサイトからインストールファイルをダウンロードしてコピーします。
- 3 Sentinel Log Manager をインストールするサーバに root としてログインします。
- 4 次のコマンドを指定して Sentinel Log Manager サーバを停止します。

```
<install_directory>/bin/server.sh stop
```

```
例 : /opt/novell/sentinel_log_mgr_1.0_x86-64/bin/server.sh stop
```

- 5 次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

```
tar xzf <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。

- 6 次のコマンドを指定して、install-slm スクリプトを実行し、Sentinel Log Manager をアップグレードします。

```
./install-slm
```

- 7 指定の言語でインストールを進めるには、言語の横に示された番号を選択します。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。
- 8 エンドユーザの使用許諾契約を読み、「yes」または「y」と入力して契約に同意し、インストールを続行します。
- 9 インストールスクリプトで、古いバージョンの製品が存在していることが検出され、製品をアップグレードするかどうかを指定するよう求められます。「n」を押すと、インストールは終了します。アップグレードを続行するには、「y」を押します。

すべての RPM パッケージのインストールが開始されます。このインストールが完了するまで数秒かかることがあります。

既にインストールされている Sentinel Log Manager 1.0 は、次の点を除いて、そのまま残されます。

- 通常、イベントデータおよび生データのディレクトリは非常に大きくなるので、1.0 のデータディレクトリ (/opt/novell/sentinel\_log\_manager\_1.0\_x86-64/data など) と 1.1 のデータディレクトリ (/var/opt/novell/sentinel\_log\_mgr/data など) が同じファイルシステムにある場合、<1.0>/data/eventuate および <1.0>/data/rawdata サブディレクトリは、

1.1 の場所に移動します。1.0 と 1.1 のデータディレクトリが異なるファイルシステムにある場合、イベントデータと生データのサブディレクトリは 1.1 の場所にコピーされ、1.0 のファイルはそのまま残されます。

- ◆ 既存の 1.0 のデータディレクトリ (/opt/novell/sentinel\_log\_mgr\_1.0\_x86-64 など) が個別にマウントされたファイルシステムにあり、1.1 のデータディレクトリ (/var/opt/novell/sentinel\_log\_mgr/data) を含むファイルシステムに十分な領域がない場合は、インストーラでファイルシステムが 1.0 の場所から 1.1 の場所に再マウントされるようにすることができます。/etc/fstab にある任意のエントリもアップデートされます。インストーラで既存のファイルシステムが再マウントされないようにする場合、アップグレードは終了します。その場合は、1.1 のデータディレクトリのファイルシステムに十分な領域を作成します。

- 10 Sentinel Log Manager 1.1 のインストールが成功し、サーバが機能していたら、次のコマンドを指定して手動で Sentinel Log Manager 1.0 ディレクトリを削除する必要があります。**

```
rm -rf /opt/novell/slm_1.0_install_directory
```

例:

```
rm -rf /opt/novell/sentinel_log_mgr_1.0_x86-64
```

インストールディレクトリを完全に削除すると、インストールされていた Sentinel Log Manager 1.0 が削除されます。

## 6.2 コレクタマネージャのアップグレード

- 1 管理者として Sentinel Log Manager にログインします。
- 2 [コレクション] > [高度] の順に選択します。
- 3 コレクタマネージャアップグレードインストーラセクションで、[インストーラのダウンロード] リンクをクリックします。  
ウィンドウには、ローカルマシンに scm\_upgrade\_installer.zip ファイルを保存したり、ローカルマシンで開いたりするためのオプションが表示されます。ファイルを保存します。
- 4 ファイルを一時的な場所にコピーします。
- 5 .zip ファイルの内容を抽出します。
- 6 Collector Manager インストールの所有者として、オペレーティングシステムに応じて以下のアップグレードファイルのいずれかを実行します。
  - ◆ Windows Collector Manager をアップグレードするには、service\_pack.bat を実行します。
  - ◆ Linux Collector Manager をアップグレードするには、service\_pack.sh を実行します。
- 7 画面の指示に従ってインストールを実行します。
- 8 マシンを再起動します。

## 6.3 1.0 から 1.1 アプライアンスへの移行

Sentinel Log Manager 1.0 がインストールされている環境を Sentinel Log Manager アプライアンス 1.1 に移行する場合は、次の手順を実行してデータおよび環境設定を移行します。

- 1 (条件付き) インストールされている Sentinel Log Manager のバージョンが 1.0 ホットフィックス 4 より前の場合、Sentinel Log Manager 1.0 ホットフィックス 5 にアップグレードすると、最新のホットフィックスを使用できます。Novell パッチダウンロードサイト (<http://download.novell.com/protected/Summary.jsp?buildid=VgZ3aerzjYc~>) からホットフィックスをダウンロードします。

---

**注:** パッチのダウンロードは登録済みのユーザが行う必要があります。登録が済んでいない場合、[登録する] をクリックしてパッチダウンロードサイトでユーザアカウントを作成します。

---

- 2 Sentinel Log Manager 1.1 にアップグレードします。詳細については、[49 ページのセクション 6.1 「1.0 から 1.1 へのアップグレード」](#) を参照してください。

- 3 次のコマンドを指定して、novell ユーザに変更します。

```
su -novell
```

- 4 次のコマンドを指定して、/bin ディレクトリに移動します。

```
cd /opt/novell/sentinel_log_mgr/bin
```

- 5 次のコマンドを指定して Sentinel Log Manager 1.1 のデータと環境設定を完全にバックアップします。

```
./backup_util.sh -m backup -c -e -l -r -s -w -f $APP_HOME/data/
<backupfilename>
```

<backupfilename> は、バックアップデータを保存するファイルの名前に置き換えます。

バックアップデータの詳細については、「[“Backing Up and Restoring Data”](#)」を参照してください。

- 6 Sentinel Log Manager アプライアンス 1.1 を個別のマシンにインストールします。詳細については、[33 ページの第 4 章 「アプライアンスのインストール」](#) を参照してください。

- 7 バックアップデータを含むファイルを、新しくインストールされた Sentinel Log Manager 1.1 アプライアンスにコピーします。

- 8 次のコマンドを指定します。

```
chown novell:novell <backfupfilename>
```

- 9 次のコマンドを指定して、/bin ディレクトリに移動します。

```
cd /opt/novell/sentinel_log_mgr/bin
```

- 10 次のコマンドを指定して、Sentinel Log Manager 1.1 アプリケーションからバックアップされたデータを完全に復元します。

```
./backup_util.sh -m restore -f $APP_HOME/data/<backupfilename>
```

詳細については、「[“Backing Up and Restoring Data”](#)」を参照してください。



# 追加のコレクタマネージャのインストール

コレクタマネージャでは、Novell Sentinel Log Manager のすべてのデータコレクションおよびデータ解析を管理します。Sentinel Log Manager のインストール時に、デフォルトでコレクタマネージャが Sentinel Log Manager サーバにインストールされます。ただし、分散設定で複数のコレクタマネージャをインストールすることができます。

- ◆ 53 ページのセクション 7.1 「作業を開始する前に」
- ◆ 53 ページのセクション 7.2 「追加のコレクタマネージャの利点」
- ◆ 53 ページのセクション 7.3 「追加のコレクタマネージャのインストール」

## 7.1 作業を開始する前に

- ◆ ハードウェアとソフトウェアが、17 ページの第 2 章「システム要件」で説明している最低要件を満たしていることを確認してください。
- ◆ Network Time Protocol (NTP) を使用して時刻を同期します。
- ◆ コレクタマネージャは、Sentinel Log Manager サーバ上のメッセージバスポート (61616) にネットワーク接続する必要があります。コレクタマネージャのインストールを開始する前に、すべてのファイアウォールおよびその他のネットワーク設定で、このポートでの通信が許可されていることを確認してください。

## 7.2 追加のコレクタマネージャの利点

分散ネットワーク環境で複数のコレクタマネージャをインストールすると、次のような利点があります。

- ◆ システムのパフォーマンスの向上：コレクタマネージャを追加すると、分散環境でイベントデータを解析および処理できるため、システムのパフォーマンスが向上します。
- ◆ データのセキュリティの強化およびネットワーク帯域幅要件の低下：コレクタマネージャがイベントソースと同じ場所にあると、フィルタ、暗号化、およびデータの圧縮を同じソースで実行できます。
- ◆ 別のオペレーティングシステムからデータを収集する機能：たとえば、Microsoft Windows にコレクタマネージャをインストールすると、WMI プロトコルを介してデータを収集できます。
- ◆ ファイルキャッシング ファイルキャッシングを有効にすると、サーバでイベントのアーカイブなどの処理が一時的に大量に発生した場合、リモートのコレクタマネージャは大量のデータをキャッシュできます。この機能は、syslog などのイベントキャッシングをネイティブでサポートしないプロトコルの場合に役立ちます。

## 7.3 追加のコレクタマネージャのインストール

- 1 管理者として Sentinel Log Manager にログインします。

- 2 [コレクション] > [高度] の順に選択します。
  - 3 コレクタマネージャのインストーラセクションで、[インストーラのダウンロード] リンクをクリックします。

ウィンドウには、ローカルマシンに scm\_installer.zip ファイルを保存するオプションと開くオプションが表示されます。ファイルを保存します。
  - 4 コレクタマネージャをインストールする場所にファイルをコピーして抽出します。
  - 5 オペレーティングシステムに応じて、次のインストールファイルのいずれかを実行します。
    - ◆ Windows システムにコレクタマネージャをインストールするには、setup.bat を実行します。
    - ◆ Linux システムにコレクタマネージャをインストールするには、setup.sh を実行します。
  - 6 言語を選択して、[OK] をクリックします。

InstallShield が表示されます。
  - 7 [OK] をクリックします。
  - 8 使用許諾契約書の条項を確認して同意し、[次へ] をクリックします。
  - 9 デフォルトのインストールディレクトリを受け入れるか、ディレクトリを参照して選択して、[次へ] をクリックします。
  - 10 デフォルトのメッセージバスポート (61616) はそのままにして、通信サーバのホスト名を指定し、[次へ] をクリックします。
  - 11 [次へ] をクリックして、デフォルトの自動メモリ環境設定 (256MB) を受け入れます。

インストールの概要が表示されます。
  - 12 [インストール] をクリックします。
  - 13 コレクタマネージャのユーザ名とパスワードを指定します。
- 
- 注:** ユーザ名とパスワードは、Sentinel Log Manager サーバにある /etc/opt/novell/sentinel\_log\_mgr/config/activemqusers.properties ファイルに保存されます。
- 
- 14 証明書に同意するよう求められたら常に同意します。
  - 15 [完了] をクリックし、インストールを完了します。
  - 16 マシンを再起動します。

# Sentinel Log Manager のアンインストール

# 8

このセクションでは、Novell Sentinel Log Manager サーバおよびコレクタマネージャをアンインストールする手順について説明します。

- [55 ページのセクション 8.1 「アプライアンスのアンインストール」](#)
- [55 ページのセクション 8.2 「既存の SLES 11 システムからのアンインストール」](#)
- [56 ページのセクション 8.3 「コレクタマネージャのアンインストール」](#)

## 8.1 アプライアンスのアンインストール

Log Manager のデータを保持する場合、後でデータを復元できるように、アプライアンスをアンインストールする前にデータをバックアップする必要があります。詳細については、『[Sentinel Log Manager 1.1 Administration Guide](#) (Sentinel Log Manager 1.1 管理ガイド)』の「[Backing Up and Restoring Data](#)」を参照してください。

データを保持する必要がない場合、次の手順を実行してアプライアンスをアンインストールします。

- **VMware ESX アプライアンス** : 仮想マシンが Novell Sentinel Log Manager 専用になっていて、データを保持する必要がない場合は、仮想マシンを削除して、Log Manager 仮想アプライアンスをアンインストールします。
- **Xen アプライアンス** : Xen 仮想マシンが Novell Sentinel Log Manager 専用になっていて、データを保持する必要がない場合は、Xen 仮想マシンを削除して、Log Manager 仮想アプライアンスをアンインストールします。
- **ハードウェアアプライアンス** : システムが Novell Sentinel Log Manager 専用になっていて、データを保持する必要がない場合は、ハードドライブを再フォーマットして、物理マシン上の Log Manager をアンインストールします。

## 8.2 既存の SLES 11 システムからのアンインストール

- 1 Sentinel Log Manager サーバに root としてログインします。
- 2 アンインストールスクリプトを実行するには、次のコマンドを実行します。  
`/opt/novell/sentinel_log_mgr/setup/uninstall-slm`
- 3 アンインストールを続行するか再確認されたら、「y」を押します。  
Sentinel Log Manager サーバは、まず停止してからアンインストールされます。

## 8.3 コレクタマネージャのアンインストール

このセクションでは、Windows または Linux マシン上にインストールされた Sentinel コレクタマネージャをアンインストールする手順について説明します。

- ◆ [56 ページのセクション 8.3.1 「Linux コレクタマネージャのアンインストール」](#)
- ◆ [56 ページのセクション 8.3.2 「Windows コレクタマネージャのアンインストール」](#)
- ◆ [57 ページのセクション 8.3.3 「手動のディレクトリのクリーンアップ」](#)

### 8.3.1 Linux コレクタマネージャのアンインストール

- 1 root としてログインします。
- 2 コレクタマネージャがインストールされているマシンで、次の場所に移動します。  
`$ESEC_HOME/_unist`
- 3 次のコマンドを実行します。  
`./uninstall.bin`
- 4 言語を選択して、[OK] をクリックします。
- 5 ItainstallShield ウィザードで、[次へ] をクリックします。
- 6 アンインストールする機能を選択し、[次へ] をクリックします。
- 7 実行中の Sentinel Log Manager アプリケーションをすべて停止し、[次へ] をクリックします。
- 8 [アンインストール] をクリックします。
- 9 [終了] をクリックします。
- 10 [システムの再起動] を選択して、[終了] をクリックします。

### 8.3.2 Windows コレクタマネージャのアンインストール

- 1 管理者としてログインします。
- 2 Sentinel Log Manager サーバを停止します。
- 3 [スタート] > [ファイル名を指定して実行] の順にクリックします。
- 4 次の項目を指定します。  
`%Esec_home%\_unist`
- 5 [uninstall.exe] をダブルクリックしてそれを実行します。
- 6 言語を選択して、[OK] をクリックします。  
InstallShield ウィザードが表示されます。
- 7 [次へ] をクリックします。
- 8 アンインストールする機能を選択し、[次へ] をクリックします。
- 9 実行中の Sentinel Log Manager アプリケーションをすべて停止し、[次へ] をクリックします。
- 10 [アンインストール] をクリックします。



- 11 [終了] をクリックします。
- 12 [システムの再起動] を選択して、[終了] をクリックします。

### 8.3.3 手動のディレクトリのクリーンアップ

- ◆ 57 ページの「Linux」
- ◆ 57 ページの「Windows」

#### Linux

- 1 コレクタマネージャをアンインストールしたマシンに root としてログインします。
- 2 すべての Sentinel Log Manager プロセスを停止します。
- 3 /opt/novell/sentinel6 の内容を削除します。

#### Windows

- 1 コレクタマネージャをアンインストールしたマシンに管理者としてログインします。
- 2 %CommonProgramFiles%\InstallShield\Universal フォルダと、その内容をすべて削除します。
- 3 %ESEC\_HOME% フォルダを削除します。これは、デフォルトでは C:\Program Files\Novell\Sentinel6 です。



# インストールのトラブルシューティング

# A

このセクションでは、インストール時に発生しうるいくつかの問題とそれを解決する手順について説明します。

- [59 ページのセクション A.1 「ネットワーク接続が不正なためにインストールが失敗する」](#)
- [59 ページのセクション A.2 「SLES 11 上の VMware Player 3 のネットワークの環境設定で問題が発生する」](#)
- [60 ページのセクション A.3 「novell ユーザ以外の非 root ユーザでインストールされた Log Manager のアップグレード」](#)

## A.1 ネットワーク接続が不正なためにインストールが失敗する

最初のブート時に、インストーラでネットワーク設定が不正であることを検出すると、エラーメッセージが表示されます。ネットワークが使用できない場合、アプライアンスへの Sentinel Log Manager のインストールは失敗します。

この問題を解決するには、ネットワークを正しく設定します。環境設定を検証するには、`ifconfig` コマンドで正しい IP アドレスが返され、`hostname -f` コマンドで有効なホスト名が返されることを確認します。

## A.2 SLES 11 上の VMware Player 3 のネットワークの環境設定で問題が発生する

SLES 11 上の VMware Player 3 でネットワークの環境設定を行おうとすると、次のエラーが発生する場合があります。

```
Jan 12 14:57:34.761: vmx| VNET: MACVNetPortOpenDevice: Ethernet0: can't open
vmnet device (No such device or address)
Jan 12 14:57:34.761: vmx| VNET: MACVNetPort_Connect: Ethernet0: can't open
data fd
Jan 12 14:57:34.761: vmx| Msg_Post: Error
Jan 12 14:57:34.761: vmx| [msg.vnet.connectvnet] Could not connect Ethernet0
to virtual network "/dev/vmnet0". More information can be found in the
vmware.log file.
Jan 12 14:57:34.761: vmx| [msg.device.badconnect] Failed to connect virtual
device Ethernet0.
Jan 12 14:57:34.761: vmx| --
```

このエラーは、VMX ファイルが別の VM で開かれている可能性があることを示します。この問題を解決するには、次のように VMX ファイルの MAC アドレスを更新する必要があります。

- 1 テキストエディタで VMX ファイルを開きます。
- 2 `ethernet0.generatedAddress` フィールドから MAC アドレスをコピーします。

- 3 ゲストオペレーティングシステムから `/etc/udev/rules.d/70-persistent-net.rules` を開きます。
- 4 元の行をコメントアウトして、SUBSYSTEM の行を次のように入力します。  

```
SUBSYSTEM=="net", DRIVERS=="?* ", ATTRS{address}=="<MAC address> ,
NAME="eth0"
```
- 5 `<MAC address>` は、[ステップ 2](#) でコピーした MAC アドレスに置き換えます。
- 6 ファイルを保存して閉じます。
- 7 VMware Player で VM を開きます。

## A.3 novell ユーザ以外の非 root ユーザでインストールされた Log Manager のアップグレード

novell ユーザ以外の非 root ユーザでインストールされた Novell Sentinel Log Manager 1.0 サーバをアップグレードしようとする、失敗します。この問題は、Sentinel Log Manager 1.0 のインストール時に設定されたファイルの権限の種類が原因で発生します。

novell ユーザ以外の非 root ユーザでインストールされた Novell Sentinel Log Manager 1.0 サーバをアップグレードするには、次の手順を実行します。

- 1 novell ユーザを作成します。
- 2 Sentinel Log Manager 1.0 インストールの所有者を `novell:novell` に変更します。  

```
chown -R novell:novell /opt/novell/<install_directory>
```

`<install_directory>` は、インストールディレクトリの名前に置き換えます。たとえば、次のように指定します。

```
chown -R novell:novell /opt/novell/sentinel_log_mgr_1.0_x86-64
```
- 3 `config/escuser.properties` の `ESEC_USER` エントリを `novell` に変更します。
- 4 root としてログインして、Sentinel Log Manager 1.1 にアップグレードします。アップグレードについての詳細は、[49 ページのセクション 6.1 「1.0 から 1.1 へのアップグレード」](#) を参照してください。

# Sentinel の用語

このセクションでは、このマニュアルで使用されている用語について説明します。

## コレクタ

データを解析し、**Taxonomy**、エクスプロイト検出、およびビジネス適合性をデータストリームに組み込むことで、よりリッチなイベントストリームを配信するユーティリティ。イベントはその後で相互に関連付けられ、分析されて、データベースに送信されます。

## コネクタ

業界標準の方法を使用してデータソースに接続し、生データを取得するユーティリティ。

## データ保持

**Sentinel Log Manager** サーバからイベントが削除されるまで保持される期間を定義するポリシー。

## イベントソース

イベントのログを記録する実行者またはシステム。

## イベントソースの管理

**ESM. Sentinel** と、**Sentinel** コネクタおよび **Sentinel** コレクタを使用するイベントソースとの接続を管理および監視するためのインタフェース。

## Events per Second

**EPS**. ネットワークでセキュリティデバイスおよびアプリケーションからデータを生成する速度を示す値。これは、**Sentinel Log Manager** でセキュリティデバイスからデータを収集して保存するレートでもあります。

## インテグレータ

**Sentinel** システムが別の外部システムと接続するためのプラグイン。**JavaScript** のアクションでインテグレータを使用して他のシステムと相互作用できます。

## 生データ

コネクタで受信され、**Sentinel Log Manager** メッセージバスに直接送信されて、**Sentinel Log Manager** サーバ上のディスクに書き込まれる未処理のイベント。生データは、デバイスに保存されるデータの形式によって、コネクタごとに異なります。