

インストールガイド

Novell[®] Sentinel 6.1 Rapid Deployment

SP2

2011 年 4 月

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、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 © 1999-2011 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, 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 製品の概要	9
1.1 Sentinel 6.1 Rapid Deployment の概要	9
1.2 Sentinel 6.1 Rapid Deployment の環境設定	11
1.3 Sentinel Rapid Deployment のユーザインタフェース	12
1.3.1 Sentinel 6.1 Rapid Deployment Web インタフェース	13
1.3.2 Sentinel コントロールセンター	13
1.3.3 Sentinel Data Manager (Sentinel データマネージャ)	13
1.3.4 Sentinel ソリューションデザイナー	14
1.3.5 Sentinel プラグイン SDK	14
1.4 Sentinel サーバコンポーネント	14
1.4.1 データアクセスサービス	14
1.4.2 メッセージバス	15
1.4.3 Sentinel データベース	15
1.4.4 Sentinel コレクタマネージャ	15
1.4.5 Correlation Engine (相関エンジン)	15
1.4.6 iTRAC	15
1.4.7 Sentinel Advisor とエクスプロイト検出	16
1.4.8 Web サーバ	16
1.5 Sentinel プラグイン	16
1.5.1 コレクタ	16
1.5.2 コネクタとインテグレータ	17
1.5.3 相関ルールとアクション	17
1.5.4 レポート	17
1.5.5 iTRAC ワークフロー	17
1.5.6 ソリューションパック	18
1.6 言語サポート	18
2 システム要件	19
2.1 サポートされているプラットフォーム	19
2.1.1 サポートされるオペレーティングシステム	19
2.2 ハードウェア要件	21
2.3 サポートされる Web ブラウザ	23
2.4 仮想環境	23
2.5 推奨される制限	23
2.5.1 コレクタマネージャの制限	23
2.5.2 レポートの制限	24
2.6 テスト結果	24
3 インストール	27
3.1 概要	27
3.1.1 サーバコンポーネント	27
3.1.2 クライアントアプリケーション	28
3.2 SUSE Linux Enterprise Server へのインストール	29
3.2.1 前提条件	29
3.2.2 Sentinel Rapid Deployment インストール	30

3.3	コレクタマネージャとクライアントアプリケーションのインストール	35
3.3.1	インストーラのダウンロード	35
3.3.2	Sentinel Rapid Deployment のクライアントコンポーネントのポート番号	36
3.3.3	Sentinel クライアントアプリケーションのインストール	37
3.3.4	Sentinel コレクタマネージャのインストール (SLES のまたは Windows の場合)	39
3.4	Sentinel サービスを手作業で開始または停止する	41
3.5	Java の手動アップグレード	42
3.6	インストール後の設定	42
3.6.1	日付と時刻の設定の変更	43
3.6.2	Sentinel 通知を送信するための SMTP インテグレータの設定	43
3.6.3	コレクタマネージャのサービス	43
3.6.4	時刻の管理	44
3.7	LDAP 認証	45
3.7.1	概要	45
3.7.2	前提条件	45
3.7.3	LDAP 認証を可能にする Sentinel サーバの設定	46
3.7.4	複数の LDAP サーバを使用したフェールオーバー構成	49
3.7.5	複数の Active Directory ドメイン向けの LDAP 認証の設定	51
3.7.6	LDAP ユーザの資格情報を使用したログイン	52
3.8	ライセンスキーを評価版キーから製品版キーに更新する	53
4	Sentinel Rapid Deployment のアップグレード	55
4.1	前提条件	55
4.2	サーバへのパッチのインストール	55
4.3	コレクタマネージャおよびクライアントアプリケーションのアップグレード	56
4.3.1	コレクタマネージャのアップグレード	56
4.3.2	クライアントアプリケーションのアップグレード	57
5	Sentinel Rapid Deployment のセキュリティに関する考慮事項	59
5.1	強化	59
5.1.1	導入後直ちに実施できる強化	59
5.1.2	Sentinel Rapid Deployment のデータの保護	60
5.2	ネットワーク経由の通信のセキュリティ保護	60
5.2.1	Sentinel サーバプロセス間の通信	60
5.2.2	Sentinel サーバと Sentinel クライアントアプリケーションとの間の通信	60
5.2.3	サーバとデータベースとの間の通信	61
5.2.4	コレクタマネージャとイベントソースとの間の通信	61
5.2.5	Web ブラウザとの通信	62
5.2.6	データベースと他のクライアントとの間の通信	62
5.3	ユーザとパスワードのセキュリティ保護	62
5.3.1	オペレーティングシステムのユーザ	62
5.3.2	Sentinel アプリケーションおよびデータベースのユーザ	63
5.3.3	ユーザのパスワードポリシーの強制	64
5.4	Sentinel データのセキュリティ保護	64
5.5	情報のバックアップ	67
5.6	オペレーティングシステムのセキュリティ保護	68
5.7	Sentinel 監査イベントの表示	69
5.8	認証局の証明書の使用	69
6	Sentinel Rapid Deployment の機能のテスト	71
6.1	Rapid Deployment のインストールのテスト	71
6.2	テスト後のクリーンアップ	83

6.3	実際のデータの使用	85
7	Sentinel Rapid Deployment のアンインストール	87
7.1	Sentinel Rapid Deployment サーバのアンインストール	87
7.2	リモートコレクタマネージャと Sentinel クライアントアプリケーションのアンインストール	87
7.2.1	Linux	87
7.2.2	Windows	88
7.2.3	アンインストール後の手順	89
A	Sentinel Rapid Deployment のホスト名の更新	91
A.1	サーバ	91
A.2	クライアントアプリケーション	91
B	トラブルシューティングのヒント	93
B.1	無効な資格情報を入力するとデータベースの認証が失敗する	93
B.2	Sentinel Web インタフェースが起動しない	93
B.3	UAC が有効な場合にリモートコレクタマネージャが Windows 2008 で例外をスローする	94
B.4	イメージ作成されたコレクタマネージャに UUID が作成されない	95
C	PostgreSQL データベースのメンテナンスに関するベストプラクティス	97
C.1	メモリの環境設定パラメータの変更	97
C.2	回収 / 分析の I/O に対する影響の低減	98

このガイドについて

このガイドの目的は、Novell Sentinel 6.1 Rapid Deployment サービスパック 2 の概要、およびインストール手順を説明することです。

- ◆ 9 ページの第 1 章「製品の概要」
- ◆ 19 ページの第 2 章「システム要件」
- ◆ 27 ページの第 3 章「インストール」
- ◆ 55 ページの第 4 章「Sentinel Rapid Deployment のアップグレード」
- ◆ 59 ページの第 5 章「Sentinel Rapid Deployment のセキュリティに関する考慮事項」
- ◆ 71 ページの第 6 章「Sentinel Rapid Deployment の機能のテスト」
- ◆ 87 ページの第 7 章「Sentinel Rapid Deployment のアンインストール」
- ◆ 91 ページの付録 A「Sentinel Rapid Deployment のホスト名の更新」
- ◆ 93 ページの付録 B「トラブルシューティングのヒント」
- ◆ 97 ページの付録 C「PostgreSQL データベースのメンテナンスに関するベストプラクティス」

対象読者

このマニュアルは、情報セキュリティの専門家向けです。

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。オンラインドキュメントの各ページの下部にあるユーザコメント機能を使用して、コメントを入力してください。

追加のマニュアル

Sentinel テクニカルマニュアルは、次の分冊から構成されています。

- ◆ *Novell Sentinel Rapid Deployment Installation Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/index.html)
- ◆ *Novell Sentinel Rapid Deployment User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/bookinfo.html)
- ◆ *Novell Sentinel Rapid Deployment Reference Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/bookinfo.html)
- ◆ *Novell Sentinel インストールガイド* (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/)
- ◆ *Novell Sentinel ユーザガイド* (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/)
- ◆ *Novell Sentinel リファレンスガイド* (http://www.novell.com/documentation/sentinel61/s61_reference/?page=/documentation/sentinel61/s61_reference/data/)

- ◆ *Sentinel SDK* (http://www.novell.com/developer/develop_to_sentinel.html)

Sentinel SDK サイトでは、コレクタ (専有または JavaScript) および JavaScript 関連アクションの開発について詳しく説明しています。

Novell の連絡先

- ◆ *Novell Web サイト* (<http://www.novell.com>)
- ◆ *Novell テクニカルサポート* (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/>)
- ◆ *Sentinel プラグイン Web サイト* (<http://support.novell.com/products/sentinel/secure/sentinelplugins.html>)
- ◆ 通知電子メールのリスト : *Sentinel* のプラグイン Web サイト経由のサインアップ

製品の概要

1

Sentinel 6.1 Rapid Deployment は Novell Sentinel の簡易バージョンで、オープンソースの PostgreSQL、activeMQ、JasperReports コンポーネントの機能を活用しています。

以降のセクションでは、Sentinel 6.1 Rapid Deployment システムの主要コンポーネントの概要について説明します。この『*Sentinel Rapid Deployment* インストールガイド』は、インストールおよび設定に関する手順を詳細に説明しています。『*Sentinel Rapid Deployment User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=documentation/sentinel61rd/s61rd_user/data/bookinfo.html)』は、アーキテクチャ、運用、および管理に関する手順を詳細に説明しています。

- ◆ 9 ページのセクション 1.1 「Sentinel 6.1 Rapid Deployment の概要」
- ◆ 11 ページのセクション 1.2 「Sentinel 6.1 Rapid Deployment の環境設定」
- ◆ 12 ページのセクション 1.3 「Sentinel Rapid Deployment のユーザインタフェース」
- ◆ 14 ページのセクション 1.4 「Sentinel サーバコンポーネント」
- ◆ 16 ページのセクション 1.5 「Sentinel プラグイン」
- ◆ 18 ページのセクション 1.6 「言語サポート」

1.1 Sentinel 6.1 Rapid Deployment の概要

Sentinel は、企業全体にわたる多数のソースから情報を受け取り、標準化し、優先順位を付けて提示する、セキュリティ情報およびイベントの管理ソリューションです。Sentinel を使用することにより、脅威、リスク、ポリシーに関連する意思決定を行うことができます。

Sentinel では、ログコレクション、分析、およびレポーティングプロセスを自動化することで、脅威の検出と監査要件を効果的に支援する IT 制御を実行できます。Sentinel では、セキュリティイベントとコンプライアンスイベント、および IT 制御を自動的にかつ継続的に監視できるため、労働集約的な手動プロセスから解放されます。

また、Sentinel では、組織のネットワークインフラストラクチャ全体と、サードパーティのシステム、デバイス、アプリケーションから、セキュリティやセキュリティ以外の情報が収集され、関連付けられます。Sentinel は、収集したデータを GUI 形式で表示し、セキュリティまたはコンプライアンスに関する問題を特定し、改善活動を追跡します。これにより、エラーが発生しやすいプロセスを効率化し、厳格かつ安全な管理プログラムを構築することができます。

インシデント応答管理の自動化により、インシデントやポリシー違反の追跡、エスカレート、および応答のプロセスを文書化して正式なものにすることができます。また、障害報告記録システムとの双方向の統合も可能になります。Sentinel により、インシデントに迅速に対応し、効率的に解決できるようになります。

ソリューションパックを使用すると、Sentinel の関連ルール、ダイナミックリスト、マップ、レポート、および iTRAC ワークフローを簡単に配布してコントロール内にインポートできます。これらのコントロールは、Payment Card Industry Data Security Standard (クレ

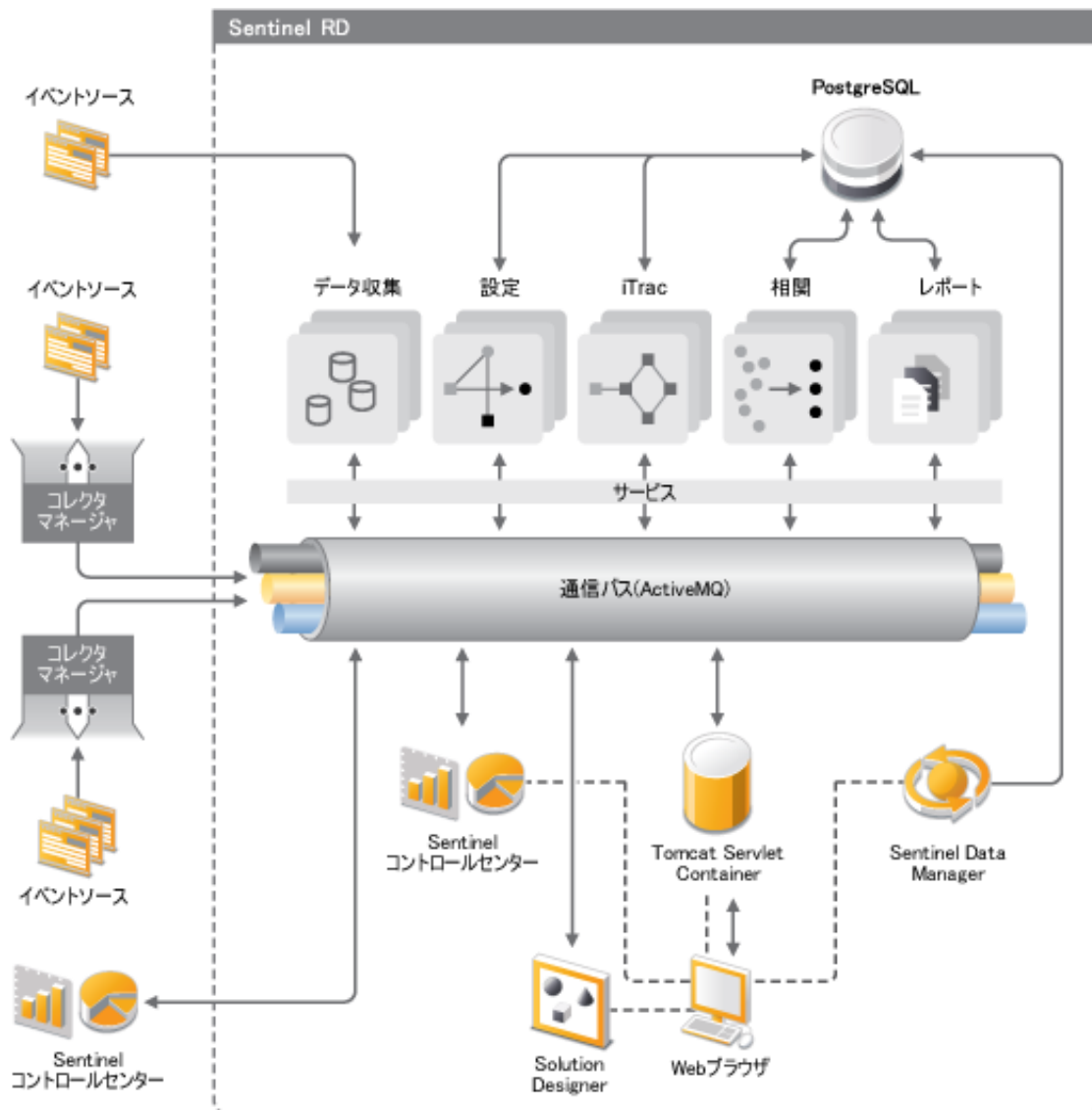
ジット業界のデータセキュリティ基準)などの特定の法規制要件を満たすようにデザインできるだけでなく、データベースのユーザ認証イベントなど、特定のデータソースに関連付けることができます。

Sentinel Rapid Deployment は次のような要素を備えています。

- ◆ 統合および自動化された、すべてのシステムおよびネットワークでのリアルタイムのセキュリティ管理およびコンプライアンス監視
- ◆ ITポリシーおよびアクションを促進するビジネスポリシーを可能にするフレームワーク
- ◆ 企業全体のセキュリティ、システム、アクセスイベントの自動的な文書化とレポート
- ◆ ビルトインのインシデント管理および修正
- ◆ 内部ポリシーや、Sarbanes-Oxley、HIPAA、GLBA、および FISMA などの政府規制とのコンプライアンスを明示および監視する機能これらのコントロールの実装に必要なコンテンツは、ソリューションパックを使用して配布され実装されます。

次に示すのは、Sentinel Rapid Deployment のアーキテクチャの概念図です。これは、セキュリティおよびコンプライアンスの実行にかかわるコンポーネントを示します。

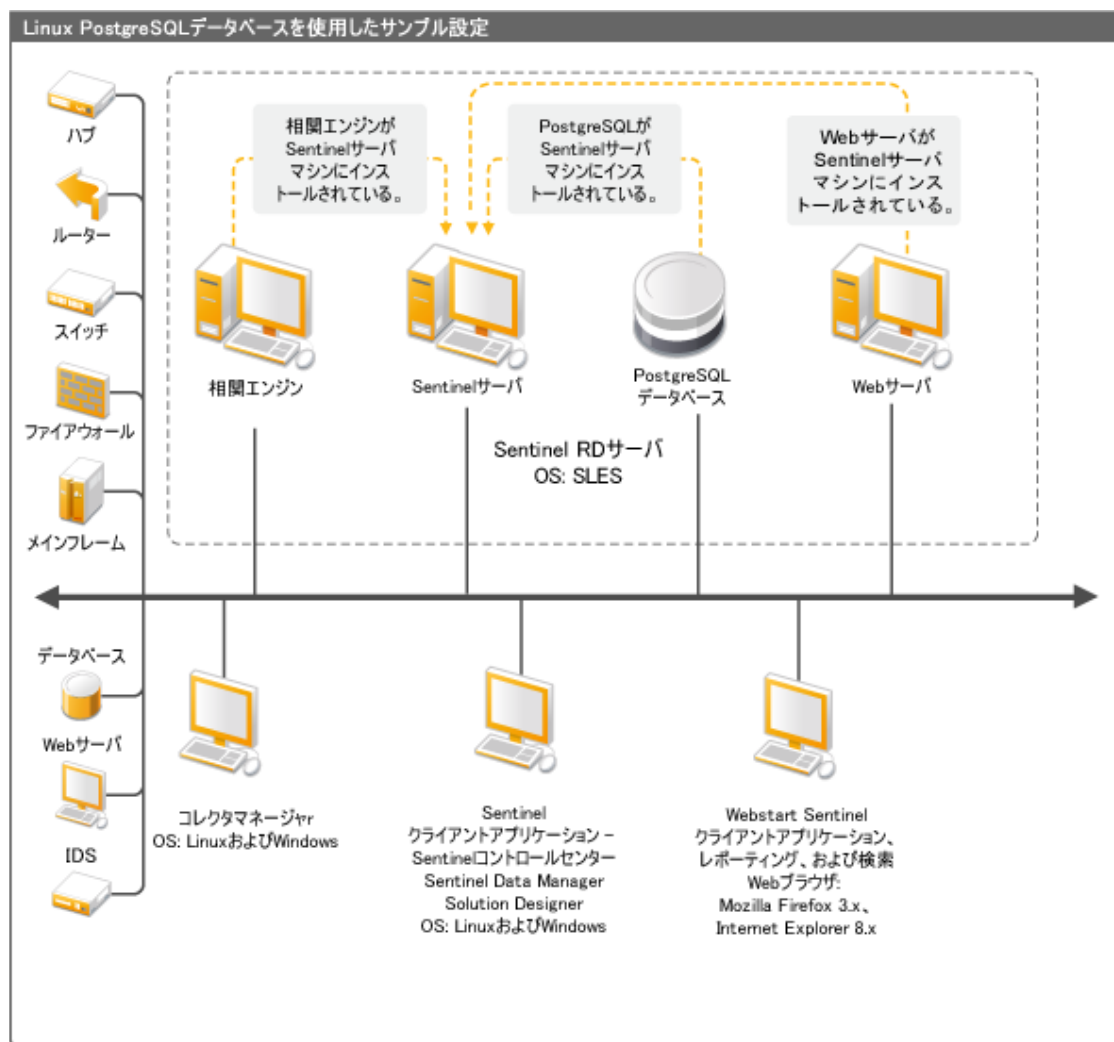
図 1-1 Sentinel のアーキテクチャの概念図



1.2 Sentinel 6.1 Rapid Deployment の環境設定

次の図は、Sentinel 6.1 Rapid Deployment の構成の設定を示しています。

図 1-2 Sentinel 6.1 Rapid Deployment の環境設定



1.3 Sentinel Rapid Deployment のユーザインタフェース

Sentinel には、次のような使いやすいユーザインタフェースが含まれています。

- ◆ [Sentinel 6.1 Rapid Deployment Web インタフェース](#)
- ◆ [Sentinel コントロールセンター](#)
- ◆ [Sentinel Data Manager \(Sentinel データマネージャ\)](#)
- ◆ [Sentinel ソリューションデザイナー](#)
- ◆ [Sentinel プラグイン SDK](#)

1.3.1 Sentinel 6.1 Rapid Deployment Web インタフェース

Novell Sentinel 6.1 Rapid Deployment Web インタフェースからは、レポートの管理のほか、Sentinel コントロールセンター (SCC)、Sentinel Data Manager、および Solution Designer を起動できます。また、Sentinel 6.1 Rapid Deployment Web インタフェースの [アプリケーション] ページでは、コレクタマネージャのインストーラとクライアントのインストーラをダウンロードできます。

詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Managing Sentinel Rapid Deployment Through the Web Interface](#)」を参照してください。

1.3.2 Sentinel コントロールセンター

SCC には、アナリストが新しい傾向や攻撃をすばやく識別し、リアルタイムのグラフィカル情報を操作してインシデントに対応できるようにする、統合型のセキュリティ管理ダッシュボードが用意されています。

SCC は、クライアントアプリケーションとして起動することも、Java Webstart を使用して起動することもできます。

SCC の主な機能は、次のとおりです。

- ◆ **Active Views:** リアルタイムの分析と視覚化
- ◆ **分析:** オフラインクエリの実行と保存
- ◆ **インシデント:** インシデントの作成と管理
- ◆ **相関:** 相関ルールの定義と管理
- ◆ **iTRAC:** インシデント解決プロセスを文書化、実行、および追跡するプロセス管理
- ◆ **レポート:** 履歴レポートとメトリクス
- ◆ **イベントソースの管理:** コレクタの展開と監視
- ◆ **ソリューションマネージャ:** ソリューションパックの内容のインストール、実装、およびテスト

詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Sentinel Control Center](#)」を参照してください。

1.3.3 Sentinel Data Manager (Sentinel データマネージャ)

Sentinel データマネージャを使用して、Sentinel データベースを管理することができます。Sentinel データマネージャでは次の操作を実行できます。

- ◆ データベースの領域使用の監視
- ◆ データベースパーティションの表示および管理
- ◆ データベースアーカイブの管理
- ◆ アーカイブされたデータをデータベースに再度インポートする

詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Sentinel Data Manager](#)」を参照してください。

1.3.4 Sentinel ソリューションデザイナー

Sentinel ソリューションデザイナーは、ソリューションパックの作成と変更に使用します。ソリューションパックには、関連ルール、アクション、iTRAC ワークフロー、およびレポートなどの一連の Sentinel コンテンツがパッケージされています。

Sentinel コンテンツとは、Sentinel システムの拡張機能です。このコンテンツには、Sentinel のアクションやインテグレータ、さらにはコレクタ、コネクタ、ソリューションパックなどの Sentinel プラグインが含まれ、これらのプラグインには、別の種類のプラグインが含まれている可能性があります。これらのモジューラーコンポーネントは、サードパーティのシステムとの統合、コントロールベースのセキュリティソリューション一式のインストール、および検出されたインシデントの自動修復を実現するのに使用されます。

詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Solution Packs](#)」を参照してください。

1.3.5 Sentinel プラグイン SDK

Sentinel プラグイン SDK には、Novell Engineering によって開発されたライブラリやコードに加え、独自のプロジェクトの開発するために使用できるテンプレートとサンプルコードが含まれています。詳細については、「[Sentinel SDK \(http://www.novell.com/developer/develop_to_sentinel.html\)](http://www.novell.com/developer/develop_to_sentinel.html)」を参照してください。

1.4 Sentinel サーバコンポーネント

Sentinel は次のコンポーネントから構成されています。

- ◆ [14 ページのセクション 1.4.1 「データアクセスサービス」](#)
- ◆ [15 ページのセクション 1.4.2 「メッセージバス」](#)
- ◆ [15 ページのセクション 1.4.3 「Sentinel データベース」](#)
- ◆ [15 ページのセクション 1.4.4 「Sentinel コレクタマネージャ」](#)
- ◆ [15 ページのセクション 1.4.5 「Correlation Engine \(関連エンジン \)」](#)
- ◆ [15 ページのセクション 1.4.6 「iTRAC」](#)
- ◆ [16 ページのセクション 1.4.7 「Sentinel Advisor とエクスプロイト検出」](#)
- ◆ [16 ページのセクション 1.4.8 「Web サーバ」](#)

1.4.1 データアクセスサービス

Sentinel データアクセスサービスは、Sentinel データベースとの通信に使用される主要なコンポーネントです。データアクセスサーバと他のサーバコンポーネントとの連携により、コレクタマネージャから受け取ったイベントのデータベースへの格納、データのフィルタ処理、アクティブビュー表示の処理、データベースクエリの実行と結果の処理、およびユーザの認証や承認など管理タスクの管理を行うことができます。詳細については、『*Sentinel Rapid Deployment Reference Guide*』の「[Data Access Service](#)」を参照してください。

1.4.2 メッセージバス

Sentinel 6.1 Rapid Deployment は、Apache Active MQ という名前のオープンソースメッセージブローカを使用します。メッセージバスを使用すると、Sentinel のコンポーネント間で何千ものメッセージパッケージを直ちに移動できます。Apache Active Mq のアーキテクチャは、Java メッセージ指向ミドルウェア (JMOM) を基礎として構築され、クライアントアプリケーションとサーバアプリケーションの間の非同期呼び出しをサポートしています。宛先のプログラムがビジーまたは接続されていない場合、メッセージキューによって一時的な保存場所が提供されます。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Communication Server](#)」を参照してください。

1.4.3 Sentinel データベース

Sentinel 製品は、セキュリティイベントおよびすべての Sentinel メタデータを格納するバックエンドデータベースを基に構築されます。Sentinel 6.1 Rapid Deployment は、PostgreSQL をサポートしています。イベントは、アセットおよび脆弱性データ、ID 情報、インシデントおよびワークフローステータス、および多くのその他の種類のデータとともに、正規化された形式で格納されます。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Sentinel Data Manager](#)」を参照してください。

1.4.4 Sentinel コレクタマネージャ

Sentinel コレクタマネージャは、データコレクションを管理し、システムステータスメッセージを監視し、必要に応じてイベントフィルタリングを実行します。コレクタマネージャの主な機能には、イベントの変換、タクソノミを通じてのイベントのビジネスへの関連付け、イベントに対するグローバルフィルタリングの実行、イベントのルーティング、Sentinel サーバへのヘルスメッセージの送信があります。Sentinel コレクタマネージャは、メッセージバスに直接接続します。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Collector Manager](#)」を参照してください。

1.4.5 Correlation Engine (相関エンジン)

相関エンジンにより、受信するイベントストリームの分析を自動化し、特定のパターンを発見できるため、セキュリティイベント管理のインテリジェンスが高まります。相関関係により、重大な脅威や複雑な攻撃パターンを識別するルールを定義できることで、イベントに優先順位をつけるとともに、効果的なインシデント管理と対応が可能になります。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Correlation Tab](#)」を参照してください。

1.4.6 iTRAC

Sentinel には、インシデント応答プロセスを定義して自動化するための、iTRAC ワークフロー管理システムが用意されています。Sentinel で特定されるインシデントは、相関ルールによるものであろうと手動によるものであろうと、iTRAC ワークフローと関連付けることができます。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[iTRAC Workflows](#)」を参照してください。

1.4.7 Sentinel Advisor とエクスプロイト検出

Sentinel Advisor は、既知の攻撃、脆弱性、修正に関する情報を含む、オプションのデータサブスクリプションサービスです。このデータを、既知の脆弱性、そして環境からのリアルタイムの侵入検知 / 防御情報と組み合わせて使用することによって、予防的なエクスプロイト検出を行い、脆弱なシステムに対する攻撃に直ちに対処することができます。

アドバイザデータのスナップショットは Sentinel 6.1 Rapid Deployment のインストール時にデフォルトでインストールされます。アドバイザデータの継続的な更新を購読するには、アドバイザライセンスが必要です。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Advisor Usage and Maintenance](#)」を参照してください。

1.4.8 Web サーバ

Sentinel Rapid Deployment は、Sentinel Rapid Deployment の Web インタフェースに安全な接続ができるように、Web サーバに Apache Tomcat を採用しています。

1.5 Sentinel プラグイン

Sentinel は、システムの機能を拡張および強化するさまざまなプラグインをサポートしています。これらのプラグインの一部はプリインストールされています。その他のプラグイン (および更新) は、[Sentinel 6.1 プラグインの Web サイト \(http://support.novell.com/products/sentinel/secure/sentinelplugins.html\)](http://support.novell.com/products/sentinel/secure/sentinelplugins.html) で入手できます。

Remedy Integrator、IBM Mainframe Connector、Connector for SAP XAL など、いくつかのプラグインをダウンロードするには、追加ライセンスが必要です。

- ◆ [16 ページのセクション 1.5.1 「コレクタ」](#)
- ◆ [17 ページのセクション 1.5.2 「コネクタとインテグレータ」](#)
- ◆ [17 ページのセクション 1.5.3 「関連ルールとアクション」](#)
- ◆ [17 ページのセクション 1.5.4 「レポート」](#)
- ◆ [17 ページのセクション 1.5.5 「iTRAC ワークフロー」](#)
- ◆ [18 ページのセクション 1.5.6 「ソリューションパック」](#)

1.5.1 コレクタ

Sentinel は、ソースデバイスからデータを収集し、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によって、よりリッチなイベントストリームを配信します。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。よりリッチなイベントストリームとは、データを必要なビジネスコンテキストと相互に関連付け、内部または外部の脅威とポリシー違反を特定して回復することを意味しています。

Sentinel コレクタは、次の種類を含む各種のデバイスのデータを解析できます。

-
- | | |
|---------------------|-----------------|
| ◆ 侵入検知システム (ホスト) | ◆ アンチウイルス検出システム |
| ◆ 侵入検知システム (ネットワーク) | ◆ Web サーバ |
| ◆ ファイアウォール | ◆ データベース |
| ◆ オペレーティングシステム | ◆ メインフレーム |
| ◆ ポリシーの監視 | ◆ 脆弱性評価システム |
| ◆ 認証 | ◆ ディレクトリサービス |
| ◆ ルータとスイッチ | ◆ ネットワーク管理システム |
| ◆ VPN | ◆ 専有システム |
-

JavaScript コレクタは、標準的な JavaScript 開発ツールやコレクタ SDK を使用して記述できます。

1.5.2 コネクタとインテグレータ

コネクタにより、JDBC や Syslog などの標準プロトコルを使用して、コレクタマネージャからイベントソースに接続できます。イベントは、解析のためにコネクタからコレクタに渡されます。

インテグレータを使用すると、Sentinel 以外のシステムでの修正アクションが可能になります。たとえば、関連アクションでは、SOAP インテグレータを使用して、Novell Identity Manager ワークフローを開始することができます。

オプションの Remedy AR インテグレータでは、Sentinel のイベントまたはインシデントから Remedy チケットを作成できます。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Action Manager and Integrator](#)」を参照してください。

1.5.3 関連ルールとアクション

関連ルールによって、イベントストリームの重要なパターンが識別されます。関連ルールがトリガされると、電子メール通知の送信、iTRAC ワークフローの開始、またはインテグレータを使用したアクションの実行などの関連アクションが開始されます。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Correlation Tab](#)」を参照してください。

1.5.4 レポート

Sentinel Rapid Deployment Web インタフェースでは、Jasper Reports を使用して、さまざまな種類のダッシュボードおよび運用レポートを実行できます。各レポートは通常、ソリューションパックを介して配布されます。

1.5.5 iTRAC ワークフロー

iTRAC ワークフローは、インシデントを管理するための一貫した反復可能なプロセスを提供します。ワークフローテンプレートは通常、ソリューションパックを介して配布されます。iTRAC には、独自の要件に合うように変更できる一連のデフォルトテンプレートが同梱されています。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[iTRAC Workflows](#)」を参照してください。

1.5.6 ソリューションパック

ソリューションパックには、関連ルール、アクション、iTRAC ワークフロー、レポートなど、関連する Sentinel コンテンツがパッケージされています。Novell は、PCI-DSS ソリューションパックなど、特定のビジネスニーズに特化したソリューションパックを提供しています。この PCI-DSS ソリューションパックは、Payment Card Industry Data Security Standard (クレジット業界のデータセキュリティ基準) へのコンプライアンスに対処したソリューションパックです。Novell は、Windows Active Directory などの特定のイベントソースに特化したコンテンツを含むコレクタパックも作成しています。詳細については、『Sentinel Rapid Deployment User Guide』の「[Solution Packs](#)」を参照してください。

1.6 言語サポート

Sentinel コンポーネントは次の言語に対応しています。

- ◆ チェコ語
- ◆ 英語
- ◆ フランス語
- ◆ ドイツ語
- ◆ イタリア語
- ◆ 日本語
- ◆ オランダ語
- ◆ ポーランド語
- ◆ ポルトガル語
- ◆ 簡体字中国語
- ◆ スペイン語
- ◆ 繁体字中国語

システム要件

最高のパフォーマンスと信頼性を実現するには、このセクションに記載されている認定されたソフトウェアとハードウェア上に Sentinel Rapid Deployment コンポーネントをインストールする必要があります。このセクションに記載されている要件については、品質保証と認証が十分に実施されています。

- ◆ 19 ページのセクション 2.1 「サポートされているプラットフォーム」
- ◆ 21 ページのセクション 2.2 「ハードウェア要件」
- ◆ 23 ページのセクション 2.3 「サポートされる Web ブラウザ」
- ◆ 23 ページのセクション 2.4 「仮想環境」
- ◆ 23 ページのセクション 2.5 「推奨される制限」
- ◆ 24 ページのセクション 2.6 「テスト結果」

2.1 サポートされているプラットフォーム

表 2-1 は、Novell が認定する、またはサポートするソフトウェアとオペレーティングシステムの組み合わせのリストです。認定されている組み合わせは、Novell Engineering の完全なテストスイートを使用してテストされています。サポートされている組み合わせは、すべての機能が動作すると考えられます。

2.1.1 サポートされるオペレーティングシステム

Novell は、このセクションで説明するオペレーティングシステムのバージョンでの Sentinel Rapid Deployment の実行をサポートしています。さらに、セキュリティパッチや修正プログラムなど、これらのオペレーティングシステムに対してマイナーアップデートが加えられたシステムにおける実行もサポートします。ただし、主要な更新または比較的重要でない更新がシステムで行われた場合、そのようなプラットフォームでの Sentinel Rapid Deployment の実行は、Novell がこれらの更新をテストおよび認定するまではサポートされません。

Sentinel Rapid Deployment サーバのコンポーネントには、Communication Server、関連エンジン、データアクセスサービス (DAS)、Web サーバ、およびアドバイザのデータサブスクリプションサービスが含まれます。

Sentinel のクライアントアプリケーションには、Sentinel コントロールセンター (SCC)、Sentinel データマネージャ (SDM)、および Sentinel ソリューションデザイナー (SSD) が含まれます。

コレクタマネージャには、特定のプラットフォーム要件があります。

表 2-1 サポートおよび認定されているオペレーティングシステム

プラットフォーム	サーバコンポーネント	Sentinel クライアントアプリケーション	コレクタマネージャ
SUSE Linux Enterprise Server (SLES) 11 SP1 (64 ビット)	認定済み	認定済み	認定済み
SUSE Linux Enterprise Server (SLES) 11 SP1 (32 ビット)	サポート対象外	サポートあり	サポートあり
SUSE Linux Enterprise Server (SLES) 10 SP3 (64 ビット)	認定済み	サポートあり	サポートあり
SUSE Linux Enterprise Server (SLES) 10 SP3 (32 ビット)	サポートあり	サポートあり	サポートあり
Windows Server 2008 R2 (64 ビット)	サポート対象外	認定済み	認定済み
Windows Server 2003 R2 (64 ビット)	サポート対象外	サポートあり	サポートあり
Windows Server 2003 R2 (32 ビット)	サポート対象外	サポートあり	サポートあり
Windows XP SP3 (32 ビット)	サポート対象外	サポートあり	サポート対象外
Windows Vista SP2 (32 ビット)	サポート対象外	サポートあり	サポート対象外
Windows 7	サポート対象外	認定済み	サポート対象外

最適なパフォーマンス、安定性、および信頼性を得るには、次のガイドラインに従ってください。

- ◆ SLES の場合、Sentinel Rapid Deployment サーバマシンのオペレーティングシステムに少なくともベースサーバと SLES の X Window コンポーネントが含まれている必要があります。
- ◆ Sentinel Rapid Deployment サーバでは、ext3 ファイルシステムを使用します。ファイルシステムの詳細については、『*Storage Administration Guide*』の [Overview of File Systems in Linux](http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) を参照してください。

注：

- ◆ Sentinel Rapid Deployment では、Open Enterprise Server への SLES のインストールはサポートされません。
- ◆ Sentinel 6.1 Rapid Deployment サーバの 32 ビットのデモバージョンは、32 ビットのハードウェアおよびオペレーティングシステムを使用することにより、規模の限られたデモ環境やテスト環境用に設計されています。Sentinel 6.1 Rapid Deployment のサポート契約を結んでいるお客様またはパートナーは、64 ビットの実運用プラットフォーム上で再現する可能性がある問題であれば、このプラットフォームに関して Novell テクニカルサポートから限定的なサポートを受けることができます。32 ビットのハードウェア固有の制限のため、Novell テクニカルサポートは、32 ビットのデモバージョンに関するパフォーマンスや拡張性の問題のトラブルシューティングを行っていません。32 ビットのデモバージョンは、実運用環境ではサポートされていません。

2.2 ハードウェア要件

Sentinel Rapid Deployment サーバコンポーネントは、19 ページのセクション 2.1.1 「サポートされるオペレーティングシステム」で説明されているように、オペレーティングシステムに基づきいくつかの例外を除き、x86-64 (64 ビット) のハードウェア上で実行されます。Sentinel は、AMD Opteron および Intel Xeon ハードウェアで動作することが保証されています。Itanium サーバはサポートされていません。

このセクションでは、Sentinel のシステム設計について、ハードウェアに関する一般的な推奨事項をいくつか示しています。設計上の推奨事項は、イベントレートの範囲に基づいています。ただし、これらの推奨事項は、次のことを前提としています。

- ◆ イベントレートとは、1 秒当たりのイベント数 (EPS) の範囲の最高値。
- ◆ イベントの平均サイズは 1 KB。
- ◆ すべてのイベントがデータベースに格納されている (つまり、イベントをドロップするフィルタがない)。
- ◆ 90 日分のデータがオンラインでデータベースに格納される。
- ◆ アドバイザデータ用のストレージスペースは 22 ページの表 2-2 および 22 ページの表 2-3 の仕様には含まれていません。
- ◆ データベースにすぐに挿入できなかったイベントデータを一時的にキャッシュするために、Sentinel サーバにはデフォルトで 5GB のディスク容量が用意されています。
- ◆ 集約イベントファイルにすぐに挿入できなかったイベント用に、Sentinel サーバにはさらにデフォルトで 5GB のディスク容量が用意されています。
- ◆ オプションのアドバイザサブスクリプションでは、サーバ上にさらに 1GB のディスク容量が必要になります。

Sentinel を実装するためのハードウェアの推奨事項は、個々の実装によって異なるため、Sentinel のアーキテクチャを最終決定する前に、Novell コンサルティングサービスまたは Novell Sentinel パートナーに問い合わせることをお勧めします。以下の推奨事項をガイドラインとして使用できます。

SLES のバージョンでは、データベースは Sentinel Rapid Deployment サーバに組み込まれており、サーバとともに同じマシン上にインストールされています。

注: イベントによって負荷が高くなることと、ローカルキャッシングが必要であることから、Sentinel サーバマシンに、少なくとも 4 個のディスクスピンドルを備えたローカルまたは共有のストライプ化ディスクアレイ (RAID) が必要になります。

表 2-2 単一マシンでの構成 (最大 2000 eps まで)

コンポーネント	RAM	空き容量	CPU
マシン 1: Sentinel Rapid Deployment サーバ <ul style="list-style-type: none"> ◆ 組み込み PostgreSQL データベース (3GB) ◆ コレクタマネージャ (1228MB) ◆ DAS_Core (1579MB) ◆ DAS_Binary (1404MB) ◆ 相関エンジン (1073MB) ◆ 4 コレクタ (汎用、Cisco、Snort、および IBM、それぞれが 500EPS を生成) ◆ 10 個の相関ルールを展開 ◆ 10 個の固有のアクティブビュー ◆ 3 人の同時ユーザ ◆ 2 つのマップを展開 	16GB	1TB、SAS (15Krpm) ハードディスク ハードウェア RAID 10	Dell PowerEdge 2900、クワッドコア Intel Xeon E5310 (1.6GHz)×2、ギガビット Ethernet NIC

表 2-3 3 台マシンでの構成 (最大 5000 eps まで)

コンポーネント	RAM	空き容量	CPU
マシン 1: Sentinel Rapid Deployment サーバ <ul style="list-style-type: none"> ◆ 組み込み PostgreSQL データベース (3GB) ◆ コレクタマネージャ (1228MB) ◆ DAS_Core (1579MB) ◆ DAS_Binary (1404MB) ◆ 相関エンジン (1073MB) ◆ 4 コレクタ (それぞれが 500EPS を生成、リモートの Collector Manager 1 から 1500 EPS、リモートの Collector Manager 2 から 1500 EPS) 	16GB	1TB、SAS (15Krpm) ハードディスク ハードウェア RAID 10	Dell PowerEdge 2900、クワッドコア Intel Xeon E5310 (1.6GHz)×2、ギガビット Ethernet NIC
マシン 2: コレクタマネージャ <ul style="list-style-type: none"> ◆ コレクタマネージャ / コレクタ ◆ 3 コレクタ (それぞれが 500EPS を生成) 	4GB	300GB、SATA(3Gビット/s) ハードディスク	Intel Core 2 Duo E6750 (2.66 GHz)、ギガビット Ethernet NIC
マシン 3: コレクタマネージャ <ul style="list-style-type: none"> ◆ コレクタマネージャ / コレクタ ◆ 3 コレクタ (それぞれが 500EPS を生成) 	4GB	300GB、SATA(3Gビット/s) ハードディスク	Intel Core 2 Duo E6750 (2.66 GHz)、ギガビット Ethernet NIC

2.3 サポートされる Web ブラウザ

- ◆ Mozilla Firefox 3x。
- ◆ Internet Explorer 8x。

2.4 仮想環境

Sentinel Rapid Deployment は、VMware ESX Server 上で広範にテストされており、Novell はこの環境において Sentinel Rapid Deployment を完全にサポートしています。ESX 上の物理マシンまたはその他の仮想環境におけるテストの結果と同等のパフォーマンス結果を達成するには、仮想環境が物理マシンで推奨される内容と同じメモリ、CPU、ディスク容量、および I/O を備える必要があります。

SLES システムに関する物理マシンの推奨事項については、[21 ページのセクション 2.2 「ハードウェア要件」](#) を参照してください。

2.5 推奨される制限

このセクションに記載されている制限は、Novell またはお客様側で実施されたパフォーマンステストに基づいた推奨値を表すものです。これらはハード制限ではありません。推奨値は概算です。極めて動的なシステムでは、バッファを組み込んで、システムに成長の余地を与えることをお勧めします。

- ◆ [23 ページのセクション 2.5.1 「コレクタマネージャの制限」](#)
- ◆ [24 ページのセクション 2.5.2 「レポートの制限」](#)

2.5.1 コレクタマネージャの制限

特に指定がない限り、コレクタマネージャの制限では、SLES11 上で動作し、それぞれが 2.2 GHz4 つの CPU コアと 4 GB の RAM を想定しています。

表 2-4 コレクタマネージャのパフォーマンスに関する数値

属性	制限容量	コメント
コレクタマネージャの最大数	20	この制限は、各コレクタマネージャが低い EPS(100 未満の EPS) で実行していることが前提です。1 秒当たりのイベント数が増加すると、この制限は下がります。
単一のコレクタマネージャ上の (十分に活用されている) 最大コネクタ数	CPU コアごとに 1 つ、オペレーティングシステムおよび他の処理用に少なくとも 1 つの CPU コアが予約されている	十分に活用されているコネクタとは、そのタイプのコネクタで可能な限り最高の EPS で実行しているコネクタのことです。
単一のコレクタマネージャ上の (完全活用されている) 最大コレクタ数	CPU コアごとに 1 つ、オペレーティングシステムおよび他の処理用に少なくとも 1 つの CPU コアが予約されている	十分に活用されているコレクタとは、そのタイプのコレクタで可能な限り最高の EPS で実行しているコレクタのことです。

属性	制限容量	コメント
単一のコレクタマネージャ上のデバイスの最大数	2000	Sentinel Rapid Deployment サーバにおける制限も 2000 なので、単一のコレクタマネージャ上に 2000 個のデバイスが存在する場合、そのコレクタマネージャ単独で Sentinel システム全体のデバイスの制限に達することになります。
Sentinel Rapid Deployment サーバ上のデバイスの最大数	2000	Sentinel Rapid Deployment サーバ上のデバイスの最大数 g は 2000 です。

2.5.2 レポートの制限

表 2-5 レポートのパフォーマンスに関する数値

属性	制限容量	コメント
保存されているレポートの最大数	200	この制限は、レポートのサイズや、サーバ上で利用可能な、システムの他の部分によって使用されていないディスク領域のサイズに応じて増減します。
同時に実行するレポートの最大数	3	この制限は、サーバがデータ収集や他のタスクを実行中で、すでに活用の程度が高くないことが前提です。

2.6 テスト結果

Sentinel Rapid Deployment は、環境のニーズに応じて異なる構成を選択することができます。次のパフォーマンステストの情報は、表に記載されている特定の構成に関して Novell が行ったテストの結果を示します。

Sentinel の導入に関するハードウェアの推奨事項は、導入事例ごとに異なります。そのため、Sentinel のアーキテクチャを最終的に決定する前に、Novell コンサルティングサービスまたは任意の Novell Sentinel パートナーにご相談いただくことをお勧めします。以下のテスト情報は、ガイドラインとして活用できます。

Linux 異なるデバイス数での最大 EPS の測定、および特定の EPS に対するデバイスの最大数の測定のためのテストを実施しました。次のハードウェア構成を使用しました。

- ◆ CPU コアの数: 4
- ◆ CPU Model: Intel Xeon CPU X5770 @ 2.93 GHz
- ◆ RAM: 16GB
- ◆ ハードディスクのサイズ (加えて RAID のタイプと RAID に含まれるディスク数): 1.7 TB (RAID 5、6 ディスク)

注: テストはすべて、Syslog ベースのイベントソースを使用して実施されました。他のコネクタではパフォーマンスが異なる可能性があります。

次の表は、SLES システム上で異なる数のデバイスを使用した場合に、増加させることができる EPS の最大数を示しています。

表 2-6 SLES システムにおける EPS の最大数

システムセットアップ	デバイス	最大 EPS
4 コレクタマネージャ (ローカル x1、リモート x3)、10 コレクタ (それぞれが 500EPS を生成)	25	5,000
4 コレクタマネージャ (ローカル x1、リモート x3)、10 コレクタ (それぞれが 500EPS を生成)	100	5,000
4 コレクタマネージャ (ローカル x1、リモート x3)、10 コレクタ (それぞれが 500EPS を生成)	1,000	5,000

次の表は、SLES システム上で異なる EPS レートで増加させることができるデバイスの最大数を示しています。

表 2-7 SLES システムにおけるデバイスの最大数

システムセットアップ	EPS	最大デバイス数
1 コレクタマネージャ、1 コレクタが 500EPS を生成	500	2,000
1 コレクタマネージャ、2 コレクタがそれぞれ 500EPS を生成	1,000	2,000
1 コレクタマネージャ、3 コレクタがそれぞれ 500EPS を生成	1,500	2,000

注：

- ◆ EPS またはデバイスをさらに増加するには、追加のコレクタマネージャをインストールします。
- ◆ デバイスの最大数はハード制限ではなく、Novell が実施したパフォーマンステストに基づいた推奨の値です。これらのテストでは、デバイスごとの平均イベントレート/秒が低めに想定されています (3EPS 未満)。EPS レートが高いと、持続可能な最大デバイスが少なくなります。最大デバイス数が前記の制限を超えていなければ、(最大デバイス) x (デバイスごとの平均 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 レートまたはデバイス数に対する適切な制限を求めることができます。

インストール

このセクションでは、Sentinel Rapid Deployment のコンポーネントとクライアントコンポーネントのインストールについて説明します。

- ◆ 27 ページのセクション 3.1 「概要」
- ◆ 29 ページのセクション 3.2 「SUSE Linux Enterprise Server へのインストール」
- ◆ 35 ページのセクション 3.3 「コレクタマネージャとクライアントアプリケーションのインストール」
- ◆ 41 ページのセクション 3.4 「Sentinel サービスを手作業で開始または停止する」
- ◆ 42 ページのセクション 3.5 「Java の手動アップグレード」
- ◆ 42 ページのセクション 3.6 「インストール後の設定」
- ◆ 45 ページのセクション 3.7 「LDAP 認証」
- ◆ 53 ページのセクション 3.8 「ライセンスキーを評価版キーから製品版キーに更新する」

3.1 概要

Sentinel のインストールパッケージには、Sentinel Rapid Deployment を実行するのに必要な要素すべてをインストールするための、簡素化されたシングルマシンサーバのインストーラが付属しています。Sentinel Rapid Deployment サーバのインストーラにより、次のコンポーネントがインストールされます。

- ◆ 27 ページのセクション 3.1.1 「サーバコンポーネント」
- ◆ 28 ページのセクション 3.1.2 「クライアントアプリケーション」

3.1.1 サーバコンポーネント

表 3-1 Sentinel サーバのコンポーネントおよびアプリケーション

コンポーネント	説明
	Sentinel データベースは、環境設定とイベントのデータを格納します。
メッセージバス	JMS ベースのメッセージバスにより、Sentinel システムのコンポーネント間の通信が処理されます。
相関エンジン	相関エンジンは、リアルタイムのイベント解析を実行します。
アドバイザ	アドバイザは、検出された IDS 攻撃と脆弱性スキャンの出力とをリアルタイムに関連付けることで、組織に対するリスクが増大すると直ちに通知を行います。
データアクセスサービス	データストレージ、クエリ、ディスプレイ、処理コンポーネントが含まれます。
Web サーバ	Sentinel Rapid Deployment 用の Web インタフェースをサポートします。

コンポーネント	説明
コレクタマネージャ	<p>イベントソースへの接続、データの解析、マッピングなどを処理します。</p> <p>Sentinel Rapid Deployment の Web インタフェースから入手可能なコレクタマネージャインストーラを使用すると、コレクタマネージャを別の場所、別のマシン、および別のオペレーティングシステムに分散できます。たとえば、追加のコレクタマネージャを Windows マシンにインストールして、Windows イベントを収集できます。</p>
iTRAC	<p>Sentinel には、インシデント応答プロセスを定義して自動化するための、iTRAC ワークフロー管理システムが用意されています。Sentinel で特定されるインシデントは、関連ルールによるものであろうと手動によるものであろうと、iTRAC ワークフローと関連付けることができます。</p>

3.1.2 クライアントアプリケーション

クライアントアプリケーションである、Sentinel コントロールセンター、Sentinel データマネージャ、およびソリューションデザイナーは、Sentinel Rapid Deployment サーバにデフォルトでインストールされます。クライアントアプリケーションは、次のいずれかの方法を使用して起動できます。

- ◆ Sentinel Rapid Deployment の Web インタフェースを使用する。クライアントシステムに Java 1.6.0_20 以降をインストールし、Webstart 経由で Sentinel アプリケーションを起動するように JRE パスを設定する必要があります。

JAVA_HOME 環境変数が JRE6 フォルダの場所を指すように設定します。エクスポートパスが JRE6 の場所の bin フォルダを指すようにします。

- ◆ `<install_directory>/bin` を Sentinel Rapid Deployment のインストールファイルの所有者として使用する。例：

```
./bin/<client_application>.sh
```

表 3-2 Sentinel クライアントアプリケーション

コンポーネント	説明
Sentinel Control Center	セキュリティまたはコンプライアンス解析用のメインコンソールです。
Sentinel Data Manager (Sentinel データマネージャ)	データベース管理ユーティリティ。
ソリューションデザイナー	ソリューションパックを作成するためのアプリケーション。
Sentinel コレクタマネージャ	イベントソースへの接続、データの解析、マッピングなどを処理するサービスです。コレクタマネージャは Sentinel サーバにインストールされますが、ダウンロード可能なインストーラを使用すると、リモートの Windows または Linux マシンに追加のコレクタマネージャをインストールできます。

3.2 SUSE Linux Enterprise Server へのインストール

- ◆ 29 ページのセクション 3.2.1 「前提条件」
- ◆ 30 ページのセクション 3.2.2 「Sentinel Rapid Deployment インストール」

3.2.1 前提条件

Sentinel Rapid Deployment をインストールする前に、次の前提条件を満たしていることを確認してください。これらの前提条件 (認定プラットフォームのリストを含む) の詳細については、19 ページの第 2 章「システム要件」を参照してください。

- ◆ 29 ページの「サーバ」
- ◆ 29 ページの「クライアント」
- ◆ 30 ページの「アドバイザー」

重要: フルインストーラを使用する Sentinel Rapid Deployment のインストールは、常にクリーンなシステムで実行する必要があります。いずれかのマシンに以前インストールした Sentinel Classic や Sentinel ログマネージャなど、Sentinel の他のバージョンをご使用の場合は、最初にそれらをアンインストールする必要があります。Sentinel の以前のバージョンをアンインストールする方法については、該当するインストールガイドを参照してください。

- ◆ Sentinel Classic をアンインストールするには、『[Sentinel Installation Guide \(http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html\)](http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html)』の「Uninstalling Sentinel」を参照してください。
 - ◆ Sentinel Log Manager のアンインストールについては、『[Sentinel Log Manager 1.1 Installation Guide \(http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bor9aaf.html\)](http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bor9aaf.html)』の「Uninstalling Sentinel Log Manager」の章を参照してください。
-

サーバ

- ◆ それぞれのサーバマシンが、最小システム要件を満たしていることを確認します。システム要件の詳細については、19 ページの第 2 章「システム要件」を参照してください。
- ◆ 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。
- ◆ Sentinel システムから電子メール通知を送信できるようにする場合は、SMTP サーバをインストールして設定します。

クライアント

- ◆ それぞれのクライアントマシンが、最小システム要件を満たしていることを確認します。これらの前提条件の詳細については、19 ページの第 2 章「システム要件」を参照してください。
- ◆ インストーラを実行するディレクトリは、ASCII 文字のみを含む名前で作成してください (特殊文字は使用できません)。

- ◆ **Linux** を実行しているマシンにリモートコレクタマネージャまたはクライアントアプリケーションをインストールする場合は、管理者ユーザについて、フォルダレベルの制限が /tmp フォルダに対して設定されていないことを確認します。
- ◆ コレクタマネージャをインストールするには通常のユーザ権限では十分ではないため、**Windows** 上ではコレクタマネージャ用のドメインユーザにパワーユーザの権限を与えるようにしてください。
- ◆ コレクタマネージャを 64 ビットマシンにインストールする場合は、32 ビットライブラリが使用可能であることを確認します。32 ビットライブラリは、専有のコレクタ言語で記述されているコレクタ (2008 年 6 月以前に作成されたほとんどのコレクタを含む) を実行する場合や、LEA コネクタなどの特定のコネクタを実行する場合に必要です。JavaScript ベースのコレクタと Sentinel の残りの部分は 64 ビットに対応しています。これらのライブラリがデフォルトで用意されていない可能性がある **Linux** プラットフォームでは、これらが使用できることを確認することは特に重要です。

アドバイザー

アドバイザーをインストールする場合、Sentinel のエクスプロイト検出およびアドバイザーデータ購読を購入する必要があります。データ購読を購入した後、Novell eLogin を使用してアドバイザーのデータをダウンロードし、更新します。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Advisor Usage and Maintenance](#)」を参照してください。

3.2.2 Sentinel Rapid Deployment インストール

Sentinel Rapid Deployment サーバは、次の方法でインストールできます。

- ◆ [30 ページの「ルート特権を持つ単一スクリプトのインストール」](#)
- ◆ [33 ページの「ルート以外のインストール」](#)

Sentinel Rapid Deployment のインストーラスクリプトは、インストール中に次のオプションを提示します。

- ◆ **-all:** このオプションを使用するには、root ユーザでなければなりません。このオプションは、ユーザ (デフォルト: novell)、ユーザグループ (デフォルト: novell) を作成した後に、Sentinel Rapid Deployment サーバをインストールします。また、システム起動時に Sentinel Rapid Deployment のサービスを自動的に実行します。
- ◆ **-install:** このオプションは、Sentinel Rapid Deployment サーバのみインストールします。
- ◆ **-createuser:** このオプションを使用するには、root ユーザでなければなりません。このオプションは、ユーザ (デフォルト: novell)、およびユーザグループ (デフォルト: novell) のみ作成します。
- ◆ **-createservice:** このオプションを使用するには、root ユーザでなければなりません。このオプションは、Sentinel Rapid Deployment のサービスがシステムの起動時に自動的に実行されるようにするだけです。
- ◆ **-help:** このオプションは、インストールスクリプトのオプションの使用方法に関するヘルプを表示します。

ルート特権を持つ単一スクリプトのインストール

- 1 root ユーザとしてログインします。

インストールを実行しているユーザは、インストーラファイルがダウンロードされる一時ディレクトリへの書き込みアクセス権を持っている必要があります。

- 2 **Novell download site** (<http://download.novell.com/>) から `sentinel6_rd_linux_x86-64.tar.gz` インストーラを一時ディレクトリにダウンロードします。

- 3 インストーラの抽出:

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

- 4 インストーラを抽出したディレクトリに移動します。

```
cd sentinel6_rd_linux_x86-64
```

- 5 `install.sh` スクリプトを `-all` オプションを指定して実行します。

```
./install.sh -all
```

インストールスクリプトは、使用可能なメモリとディスク領域を最初にチェックします。使用可能なメモリが 1 ギガバイトよりも少ない場合、スクリプトは自動的にインストールを終了します。利用可能なメモリが 1 ギガバイト以上 4GB 未満の場合、推奨よりもメモリの容量が少ないというメッセージがスクリプトによって表示されます。さらに、スクリプトによってインストールを続行するかどうかも尋ねられます。インストールを続行する場合は「y」と入力し、続行しない場合は「n」と入力します。

- 6 ユーザ名を指定するか、<Enter> キーを押してデフォルトのユーザ名を選択します。デフォルトのユーザ名は、Novell です。

指定したユーザ名がすでに存在する場合、ユーザが存在することを伝えるメッセージが表示され、ユーザのグループが一覧表示されます。ステップ 8 に従って手順を進めます。

指定したユーザ名が存在しない場合、インストーラはそのユーザ名を作成します。ステップ 7 に従って手順を進めます。

- 7 グループ名を指定するか、<Enter> キーを押してデフォルトのグループ名を選択します。デフォルトのグループ名は、Novell です。

指定したグループ名がすでに存在する場合、インストーラはインストールを続行します。指定したグループ名が存在しない場合、インストーラはグループを作成し、指定したユーザ名が指定したグループの下に作成されたことを伝えるメッセージが表示されます。

指定したユーザおよびグループが Sentinel Rapid のインストールおよび実行中のプロセスの所有者になります。

- 8 インストールパスを指定するか、<Enter> キーを押してデフォルトのパスを選択します。デフォルトのパスは `/opt/novell` です。

指定するインストールパスにはスペースを含めないでください。スペースが含まれていると、インストールスクリプトによってスペースを含まないインストールパスを入力するように求められます。

- 9 次の言語のうちいずれかを、対応する番号を入力して選択します。

シリアル番号	言語
1	チェコ語
2	英語
3	フランス語

シリアル番号	言語
4	ドイツ語
5	イタリア語
6	日本語
7	オランダ語
8	ポーランド語
9	ポルトガル語
10	簡体字中国語
11	スペイン語
12	繁体字中国語

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。

- 10** エンドユーザの使用許諾契約を読み、各条項に同意してインストールを続行する場合は「1」と入力します。インストールを終了する場合は、「2」を入力します。

インストーラがファイルの解凍を開始し、ライセンスを入力するように求められます。

- 11** 90 日間の評価ライセンスキーを使用するには「1」を、有効なライセンスキーを使用するには「2」を入力します。

「2」と入力した場合、Sentinel RD の有効なライセンスキーを入力するように求められます。指定したライセンスキーが無効な場合、有効なライセンスキーを指定するように再度求められます。2 回目の試行で指定したライセンスキーが無効の場合は、90 日間の評価ライセンスキーが自動的にインストールされます。後から有効なライセンスを入力できます。

その後、スクリプトが評価ライセンスまたは有効なライセンスをロードします。

- 12** dbauser ユーザのパスワードを入力し、確認のために再度入力します。

dbauser の資格情報を使用して、PostgreSQL データベースにテーブルとパーティションが作成されます。

- 13** admin ユーザのパスワードを入力し、確認のために再度入力します。

PostgreSQL データベースでは、円記号 (¥) やアポストロフィ (') 文字を許可しないので、admin ユーザおよび dbauser ユーザ用のパスワードを入力するように求められても、それらの文字をパスワードには使用しないでください。

インストールスクリプトは、PostgreSQL データベースをインストールし、テーブルおよびパーティションを作成し、Sentinel Rapid Deployment サーバをインストールします。

インストールが完了すると、以下を実行できます。

- ◆ https://<SERVER_IP>:8443/sentinel に移動して、Sentinel Rapid Deployment の Web インタフェースを起動します。<SERVER_IP> とは、Sentinel Rapid Deployment がインストールされているマシンの IP アドレスです。
- ◆ **ステップ 6** で作成したユーザで <install_directory>/bin/control_center.sh を実行し、Sentinel コントロールセンターを起動します。

ルート以外のインストール

組織のポリシーによって、root としてフルインストールプロセスを実行することが禁止されている場合は、インストールを 2 段階で実行することができます。インストール手順の最初の段階は、root 特権で実行する必要があり、次の段階は Sentinel 管理者ユーザ (最初の段階で作成されるユーザ) として実行されます。

- 1 Sentinel Rapid Deployment をインストールするサーバにログインします。

インストールを実行しているユーザは、インストーラファイルがダウンロードされる一時ディレクトリへの書き込みアクセス権を持っている必要があります。

- 2 [Novell download site \(http://download.novell.com/\)](http://download.novell.com/) から sentinel6_rd_linux_x86-64.tar.gz インストーラを一時ディレクトリにダウンロードします。

- 3 インストーラの抽出:

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

- 4 root ユーザとしてログインします。

- 5 インストーラを抽出したディレクトリに移動します。

```
cd sentinel6_rd_linux_x86-64
```

- 6 install.sh スクリプトを -createuser オプションを指定して実行します。

```
./install.sh -createuser
```

- 7 ユーザ名を指定するか、<Enter> キーを押してデフォルトのユーザ名を選択します。デフォルトのユーザ名は、Novell です。

指定したユーザ名がすでに存在する場合、ユーザが存在することを伝えるメッセージが表示され、ユーザのグループが一覧表示されます。ステップ 9 に従って手順を進めます。

指定したユーザ名が存在しない場合、インストーラはそのユーザ名を作成します。ステップ 8 に従って手順を進めます。

- 8 グループ名を指定するか、<Enter> キーを押してデフォルトのグループ名を選択します。デフォルトのグループ名は、Novell です。

指定したグループ名がすでに存在する場合、インストーラはインストールを続行します。指定したグループ名が存在しない場合、インストーラはグループを作成し、指定したユーザ名が指定したグループの下に作成されたことを伝えるメッセージが表示されます。

指定したユーザおよびグループが Sentinel Rapid のインストールおよび実行中のプロセスの所有者になります。

- 9 インストールパスを指定するか、<Enter> キーを押してデフォルトのパスを選択します。デフォルトのパスは /opt/novell です。

指定するインストールパスにはスペースを含めないでください。スペースが含まれていると、インストールスクリプトによってスペースを含まないインストールパスを入力するように求められます。

- 10 ルート以外のユーザでログインします。例:

```
su - novell
```

- 11 インストールスクリプトを -install オプションを指定して実行します。

```
./install.sh -install
```

インストールスクリプトは、使用可能なメモリとディスク領域を最初にチェックします。使用可能なメモリが1ギガバイトよりも少ない場合、スクリプトは自動的にインストールを終了します。利用可能なメモリが1ギガバイト以上4GB未満の場合、推奨よりもメモリの容量が少ないというメッセージがスクリプトによって表示されます。さらに、スクリプトによってインストールを続行するかどうかも尋ねられます。インストールを続行する場合は「y」と入力し、続行しない場合は「n」と入力します。

- 12** インストールパスを指定するか、<Enter> キーを押してデフォルトのパスを選択します。デフォルトのパスは /opt/novell です。

指定するインストールパスにはスペースを含めないでください。スペースが含まれていると、インストールスクリプトによってスペースを含まないインストールパスを入力するように求められます。

- 13** 次の言語のうちいずれかを、対応する番号を入力して選択します。

シリアル番号	言語
1	チェコ語
2	英語
3	フランス語
4	ドイツ語
5	イタリア語
6	日本語
7	オランダ語
8	ポーランド語
9	ポルトガル語
10	簡体字中国語
11	スペイン語
12	繁体字中国語

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。

- 14** エンドユーザの使用許諾契約を読み、各条項に同意してインストールを続行する場合は「1」と入力します。インストールを終了する場合は、「2」を入力します。

インストーラがファイルの解凍を開始し、ライセンスを入力するように求められます。

- 15** 90日間の評価ライセンスキーを使用するには「1」を、有効なライセンスキーを使用するには「2」を入力します。

「2」と入力した場合、Sentinel RDの有効なライセンスキーを入力するように求められます。指定したライセンスキーが無効な場合、有効なライセンスキーを指定するように再度求められます。2回目の試行で指定したライセンスキーが無効の場合は、90日間の評価ライセンスキーが自動的にインストールされます。後から有効なライセンスを入力できます。

その後、スクリプトが評価ライセンスまたは有効なライセンスをロードします。

- 16 dbauser ユーザのパスワードを入力し、確認のために再度入力します。
dbauser の資格情報を使用して、PostgreSQL データベースにテーブルとパーティションが作成されます。
- 17 admin ユーザのパスワードを入力し、確認のために再度入力します。
PostgreSQL データベースでは、円記号 (¥) やアポストロフィ (') 文字を許可しないので、admin ユーザおよび dbauser ユーザ用のパスワードを入力するように求められても、それらの文字をパスワードには使用しないでください。
- 18 (オプション) インストールが完了したら、システムの起動時に Sentinel Rapid Deployment サービスを自動的に実行したい場合は、root ユーザで install.sh スクリプトを -createservice オプションを指定して実行します。

```
./install.sh -createservice
```

インストールが完了すると、以下を実行できます。

- ◆ https://<SERVER_IP>:8443/sentinel に移動して、Sentinel Rapid Deployment の Web インタフェースを起動します。<SERVER_IP> とは、Sentinel Rapid Deployment がインストールされているマシンの IP アドレスです。
- ◆ 前述の [ステップ 7](#) で作成したユーザで <install_directory>/bin/control_center.sh を実行し、Sentinel コントロールセンターを起動します。

3.3 コレクタマネージャとクライアントアプリケーションのインストール

Novell Sentinel Rapid Deployment の Web インタフェースを使用して、コレクタマネージャのインストーラおよびクライアントのインストーラをダウンロードします。

- ◆ [35 ページのセクション 3.3.1 「インストーラのダウンロード」](#)
- ◆ [36 ページのセクション 3.3.2 「Sentinel Rapid Deployment のクライアントコンポーネントのポート番号」](#)
- ◆ [37 ページのセクション 3.3.3 「Sentinel クライアントアプリケーションのインストール」](#)
- ◆ [39 ページのセクション 3.3.4 「Sentinel コレクタマネージャのインストール \(SLES のまたは Windows の場合\)」](#)

3.3.1 インストーラのダウンロード

- 1 Web ブラウザを開いて、次の URL を入力します。

```
https://<svrname.example.com>:8443/sentinel
```


<svrname.example.com> を、Sentinel を実行しているサーバの実際の DNS 名または IP アドレスに置換します。URL では、大文字と小文字が区別されます。
- 2 証明書の確認を要求された場合は、証明書情報を確認して、有効である場合は [はい] をクリックします。
- 3 Sentinel アカウントにアクセスするためのユーザ名とパスワードを指定します。
- 4 [言語] ドロップダウンリストを使用して、言語を選択します。
ここで選択するのは、Sentinel Rapid Deployment サーバおよびローカルコンピュータの言語コードと同じ言語です。ブラウザの言語設定で、この言語がサポートされていることを確認します。

- 5 [サインイン] をクリックします。
- 6 [アプリケーション] を選択します。
次のインストーラをダウンロードできます。

オプション	説明	アクション
コレクタマネージャのインストーラ	コレクタマネージャのインストーラを使用すると、Sentinel コレクタマネージャをサポートされている Windows および Linux プラットフォームにインストールすることができます。	[download Collector Manager installer(コレクタマネージャのインストーラのダウンロード)] をクリックし、画面の指示に従います。
クライアントインストーラ	クライアントインストーラを使用すると、サポートされているプラットフォームに Sentinel コントロールセンター、Sentinel ソリューションデザイナー、および Sentinel データマネージャをインストールできます。	[クライアントインストーラのダウンロード] をクリックし、画面の指示に従います。

コレクタマネージャのインストールに関する詳細については、[39 ページのセクション 3.3.4 「Sentinel コレクタマネージャのインストール \(SLES のまたは Windows の場合\)」](#)を参照してください。クライアントインストーラのインストールについては、[37 ページのセクション 3.3.3 「Sentinel クライアントアプリケーションのインストール」](#)を参照してください。

3.3.2 Sentinel Rapid Deployment のクライアントコンポーネントのポート番号

次のポートを使用して、Sentinel Rapid Deployment サーバとクライアントコンポーネント間のアクセスが可能になるようにファイアウォールの設定を構成します。

表 3-3 Sentinel Rapid Deployment のコンポーネント用の互換ポート番号

ポート番号	説明
61616	リモートのコントローラマネージャがこのポート番号を使用して、ActiveMQ 経由で Sentinel Rapid Deployment サーバに接続します。
10013	Sentinel コントロールセンターがこのポート番号を使用して、プロキシ経由で Sentinel Rapid Deployment サーバに接続します。
5432	Sentinel データマネージャがこのポート番号を使用して、PostgreSQL データベースに接続します。
8443	Web クライアントがこのポート番号を使用して、Sentinel Rapid Deployment サーバに接続します。

3.3.3 Sentinel クライアントアプリケーションのインストール

Sentinel クライアントアプリケーションは、Linux または Windows システムのいずれかにインストールできます。クライアントアプリケーションをインストールするには：

- 1 クライアントインストーラをダウンロードしたフォルダを参照します。
- 2 ファイルからインストールスクリプトを展開します。

プラットフォーム	アクション
Windows	client_installer.zip ファイルを解凍します。 ファイルは、disk1 というディレクトリに解凍されます。
Linux	ルート特権によって、次のコマンドを実行します。 unzip client_installer.zip ファイルは、disk1 というディレクトリに解凍されます。

- 3 インストールディレクトリに移動して、インストールを開始します。

プラットフォーム	アクション
Windows	disk1\setup.bat を実行します。 注： Windows Vista マシンで、右クリックメニューオプションの [管理者として実行] オプションを使用してコマンドプロンプトを起動します。
Linux	<ul style="list-style-type: none">◆ GUI モードの場合： <install_directory>/disk1/setup.sh◆ コンソールモードの場合： <install_directory>/disk1/setup.sh - console

以下の手順は、GUI モード専用です。

- 4 下向き矢印をクリックし、いずれかの言語を選択します。
- 5 [よろこそ] 画面で [次へ] をクリックします。
- 6 エンドユーザ使用許諾契約を読み、同意します。 [次へ] をクリックします。
- 7 デフォルトのインストールディレクトリをそのまま使用するか、 [参照] をクリックして、インストールディレクトリを指定します。 [次へ] をクリックします。

重要： 名前に特殊文字または ASCII 以外の文字を含むディレクトリにインストールすることはできません。たとえば、Sentinel Rapid Deployment を Windows x86-64 にインストールする場合、デフォルトパスは C:\Program Files(x86) になります。インストールを続行するには、(x86) に含まれる括弧などの特殊文字を避けるようにこのデフォルトパスを変更する必要があります。

- 8 インストールする Sentinel アプリケーションを選択します。
次のオプションを指定できます。

コンポーネント	説明
Sentinel Control Center	セキュリティまたはコンプライアンス解析用のメインコンソールです。
Sentinel データマネージャ (SDM)	手作業でのデータベース管理操作に使用されます。
ソリューションデザイナー	ソリューションパックの作成に役立ちます。

- 9** Sentinel コントロールセンターをインストールすることを選択した場合、Sentinel コントロールセンターに割り当てられる最大メモリ領域を入力するよう求められます。Sentinel コントロールセンターが専用で使用される最大 JVM ヒープサイズ (MB) を指定します。

有効範囲は 64 ~ 1024 MB です。

いずれかの Sentinel アプリケーションがすでにインストールされている場合、このオプションは使用できません。

- 10** ユーザ名を指定するか、<Enter> キーを押してデフォルトのユーザ名を選択します。デフォルトのユーザ名は `esecadm` です。
- これは、インストールされた Sentinel 製品を所有するユーザのユーザ名です。このユーザがまだ存在していない場合は、指定したディレクトリ内のホームディレクトリと共に作成されます。
- 11** ユーザのホームディレクトリを指定するか、<Enter> キーを押してデフォルトディレクトリを選択します。デフォルトディレクトリは `/export/home` です。
- ユーザ名が `esecadm` の場合、対応するホームディレクトリは `/export/home/esecadm` です。
- 12** ステップ 10 でデフォルトのユーザ名を選択した場合は、`esecadm` ユーザでログインするためのユーザのパスワードを入力します。それ以外の場合は、ステップ 10 で作成したユーザのパスワードを設定します。
- 13** 次の情報を指定します。

- ◆ **メッセージバスのポート** : Communication Server がリスンしているポート。Communication Server に直接接続するコンポーネントは、このポートを使用します。デフォルトのポート番号は 61616 です。
- ◆ **Sentinel Control Center プロキシポート** : SSL プロキシサーバ (データアクセスサーバプロキシ) がユーザ名とパスワードを受け付けるためにリスンするポート。SSL プロキシサーバは、認証された接続に基づいて資格情報を受け付けます。Sentinel Control Center は、このポートを使用して Sentinel サーバに接続します。デフォルトのポート番号は 10013 です。
- ◆ **Communication Server ホスト名** : Sentinel Rapid Deployment サーバがインストールされるマシンの IP アドレスまたはホスト名。

通信が可能になるように、ポート番号は Sentinel Rapid Deployment サーバ上の `<install_directory>/config/configuration.xml` のものと同じになるようにしてください。将来、他のマシンにインストールする場合に備えて、ポート番号をメモしておいてください。ポート番号の詳細については、[36 ページのセクション 3.3.2 「Sentinel Rapid Deployment のクライアントコンポーネントのポート番号」](#) を参照してください。

- 14** [Next] をクリックします。
- インストールの概要が表示されます。

15 [Install] をクリックします。

16 [完了] をクリックし、インストールを完了します。

注: 再度ログインするときは、[ステップ 10](#) で指定したユーザ名を使用します。

設定したユーザ名を忘れた場合は、端末コンソールを開き、root ユーザで次のコマンドを入力します。

```
env | grep ESEC_USER
```

ユーザがすでに作成され、環境変数が設定されている場合、このコマンドによってユーザ名が返されます。

3.3.4 Sentinel コレクタマネージャのインストール (SLES のまたは Windows の場合)

Sentinel コレクタマネージャのインストーラは、Sentinel Rapid Deployment の Web インタフェースの [アプリケーション] ページからダウンロードできます。コレクタマネージャをインストールするには：

- 1 コレクタマネージャのインストーラをダウンロードしたフォルダを参照します。
- 2 ファイルからインストールスクリプトを展開します。

プラットフォーム	アクション
Windows	scm_installer.zip ファイルを解凍します。 ファイルは、disk1 というディレクトリに解凍されます。
Linux	ルート特権によって、次のコマンドを実行します。 unzip scm_installer.zip ファイルは、disk1 というディレクトリに解凍されます。

- 3 disk1 ディレクトリに移動して、インストールを開始します。

プラットフォーム	アクション
Windows	次のコマンドを実行します。 disk1\setup.bat
Linux	<ul style="list-style-type: none">◆ GUI モードの場合 : <install_directory>/disk1/setup.sh◆ コンソールモードの場合 : <install_directory>/disk1/setup.sh - console

- 4 インストールを続行する言語を選択します。
- 5 [ようこそ] 画面の情報を読み、[次へ] をクリックします。
- 6 エンドユーザ使用許諾契約を読み、同意します。[次へ] をクリックします。
- 7 デフォルトのインストールディレクトリをそのまま使用するか、[参照] をクリックしてインストールディレクトリを指定し、[次へ] をクリックします。

重要：名前に特殊文字または ASCII 以外の文字を含むディレクトリにインストールすることはできません。たとえば、Sentinel を Windows x86-64 にインストールする場合、デフォルトパスは C:\Program Files (x86) になります。インストールを続行するには、(x86) に含まれる括弧などの特殊文字を避けるようにこのデフォルトパスを変更する必要があります。

8 Sentinel 管理者のユーザ名と、対応するホームディレクトリのパスを指定します。

Sentinel アプリケーションがすでにインストールされている場合、このオプションは使用できません。

- ◆ **OS Sentinel 管理者のユーザ名：**デフォルトは esecadm です。

これは、インストールされた Sentinel 製品を所有するユーザのユーザ名です。このユーザがまだ存在していない場合は、指定したディレクトリ内の対応するホームディレクトリと共に作成されます。

- ◆ **OS Sentinel 管理者ユーザのホームディレクトリ：**デフォルトでは /export/home です。ユーザ名が esecadm の場合、対応するホームディレクトリは /export/home/esecadm です。

esecadm ユーザとしてログインするには、最初にパスワードを設定する必要があります。

9 次の情報を指定します。

- ◆ **メッセージバスのポート：**Communication Server がリスンしているポート。Communication Server に直接接続するコンポーネントは、このポートを使用します。デフォルトのポート番号は 61616 です。
- ◆ **Communication Server のホスト名：**Sentinel Rapid Deployment サーバがインストールされるマシンの IP またはホスト名。

通信を可能にするため、Sentinel システムのすべてのマシンでポート番号が同じであることを確認してください。将来、他のマシンにインストールする場合に備えて、ポート番号をメモしておいてください。

10 [Next] をクリックします。

11 次の情報を指定します。

- ◆ **自動メモリ設定：**コネクタマネージャに割り当てるメモリの合計容量を選択します。インストーラは、推定されるオペレーティングシステムとデータベースのオーバーヘッドを考慮に入れて、コンポーネント間でのメモリの最適な分配を自動的に決定します。

重要：configuration.xml ファイルの -Xmx の値を変更すると、コネクタマネージャプロセスに割り当てられる RAM の容量を変更できます。configuration.xml ファイルは、Linux の場合は <install_directory>/config に、Windows の場合は <install_directory>/config にあります。

- ◆ **カスタムメモリ設定：**[設定] をクリックして、メモリの割り当てを調整します。このオプションは、マシンに十分なメモリがある場合のみ使用可能です。

12 [Next] をクリックします。

概要画面に、インストールを選択した機能が表示されます。

13 [Install] をクリックします。

14 インストールが完了すると、ActiveMQ JMS 方式でブローカへの接続に使用されるユーザ名およびパスワードの入力が要求されます。

Sentinel サーバの `<install_directory>/config/activemqusers.properties` ファイルに含まれるユーザ名 `collectormanager` とそれに対応するパスワードを入力します。

`activemqusers.properties` ファイルの中にある資格情報の例としては、次のとおりです。

```
collectormanager=cefc76062c58e2835aa3d777778f9295
```

`collectormanager` がユーザ名で、`cefc76062c58e2835aa3d777778f9295` がそれに対応するパスワードです。

コレクタマネージャサービスのインストール中は、`collectormanager` ユーザとそのパスワードを使用する必要があります。この場合、`collectormanager` ユーザは、コレクタマネージャの操作に必要な通信チャネルだけにアクセス権を持ちます。

インストールが終了すると、再起動するか、再ログインしてから Sentinel サービスを手作業で開始するよう求められます。

15 [終了] をクリックし、システムを再起動します。

16 **ステップ 8** で指定したユーザ名を使用して再度ログインします。

ユーザ名を忘れた場合は、端末コンソールを開き、`root` の資格情報を使用して次のコマンドを入力します。

```
env | grep ESEC_USER
```

ユーザがすでに作成され、環境変数が設定されている場合、このコマンドによってユーザ名が返されます。

注: Windows 2008 プラットフォームおよびイメージされたコレクタマネージャにコレクタマネージャをインストールする場合、いくつかの問題があります。これらの問題のトラブルシューティングに関する詳細については、[93 ページの付録 B「トラブルシューティングのヒント」](#)を参照してください。

3.4 Sentinel サービスを手作業で開始または停止する

Sentinel サービスを手作業で開始するには、次のいずれかのコマンドを使用します。

プラットフォーム	コマンド
Linux	<code><install_directory>/bin/sentinel.sh start</code>
Windows	<code><install_directory>/bin/sentinel.bat start</code>

Sentinel サービスを手作業で停止するには、次のいずれかのコマンドを使用します。

プラットフォーム	コマンド
Linux	<code><install_directory>/bin/sentinel.sh stop</code>
Windows	<code><install_directory>/bin/sentinel.bat stop</code>

次のコマンドを使用して Sentinel サービスを起動または停止することもできます。

```
/etc/init.d/sentinel.sh stop|start
```

3.5 Java の手動アップグレード

Sentinel Rapid Deployment サーバのインストーラには、Java バージョン 1.6.0_24 がバンドルされており、Sentinel Rapid Deployment サーバのインストール時にインストールされます。ただし、Java をサーバ上で最新バージョンにアップグレードする場合、Sentinel Rapid Deployment が最新バージョンを使用するようにするために、次の手順を実行する必要があります。

- 1 Sentinel Rapid Deployment サーバがインストールされているオペレーティングシステムに基づいて jre バンドルをダウンロードします。

アップグレードを実施するユーザは、Sentinel Rapid Deployment のインストールディレクトリとアップグレードファイルがダウンロードされるディレクトリに対して書き込み権限を持っている必要があります。

- ◆ Sentinel Rapid Deployment を SUSE Linux Enterprise Server にインストールしたのであれば、32 ビットと 64 ビット両方の jre バンドルを [Java のダウンロードサイト \(http://www.java.com/en/download/manual.jsp\)](http://www.java.com/en/download/manual.jsp) からダウンロードします。

- 2 Sentinel Rapid Deployment のインストールディレクトリの jre および jre64 フォルダの名前を、それぞれ jre_old および jre64_old に変更します。

```
cd <install_path>/sentinel_rd
mv jre jre_old
mv jre64 jre64_old
```

注: この名前変更は、Java のアップグレードが正常に機能しない場合に、古いバージョンに戻すために必要です。アップグレードに Java が問題なく機能するのであれば、名前を変更したフォルダは削除できます。

- 3 ダウンロードした jre バンドルを解凍します。
- 4 32 ビットのフォルダ名を jre に、64 ビットのディレクトリ名を jre64 に変更します。
- 5 名前を変更した jre および jre64 フォルダを Sentinel Rapid Deployment のインストールディレクトリにコピーします。

```
copy jre <install_path>/sentinel_rd/
copy jre64 <install_path>/sentinel_rd/
```

- 6 (オプション) jre および jre64 フォルダの必要な所有者とアクセス権限を Sentinel Rapid Deployment サーバを実行するユーザに必ず変更してください。
- 7 Sentinel Rapid Deployment サーバを再起動し、ブラウザを再起動して、Java が正しくインストールされているかを確認します。

3.6 インストール後の設定

ここでは、Sentinel Rapid Deployment サービスのインストール後の設定について説明します。

- ◆ 43 ページのセクション 3.6.1 「日付と時刻の設定の変更」
- ◆ 43 ページのセクション 3.6.2 「Sentinel 通知を送信するための SMTP インテグレータの設定」
- ◆ 43 ページのセクション 3.6.3 「コレクタマネージャのサービス」
- ◆ 44 ページのセクション 3.6.4 「時刻の管理」

3.6.1 日付と時刻の設定の変更

Sentinel コントロールセンターのデフォルトの日付と時刻の形式は無効にできます。ご使用のローカルタイムゾーンに時刻の形式をカスタマイズする方法の詳細については、[Java Web サイト \(http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html\)](http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html) を参照してください。

- 1 SentinelPreferences.properties ファイルを編集します。

```
<install_directory>/config/SentinelPreferences.properties
```

- 2 次の行からコメントを削除し、Sentinel コントロールセンター用のイベント日付 / 時刻フィールドの日付と時刻の形式をカスタマイズします。

```
com.eSecurity.Sentinel.event.datetimetypeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
```

3.6.2 Sentinel 通知を送信するための SMTP インテグレータの設定

Sentinel Rapid Deployment では、JavaScript の SendEmail アクションが SMTP インテグレータと共に動作し、Sentinel インタフェース内の各種コンテキストからメール受信者宛てにメールメッセージを送信します。SMTP インテグレータを動作させるには、あらかじめ有効な接続情報を使用して設定する必要があります。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Sending an E-mail](#)」を参照してください。

Sentinel の各インストールについて、SendEmail アクションプラグインのアクションインスタンスが 1 つずつ、自動的に作成されます。メールメッセージの受信者およびメッセージの内容がアクションパラメータで設定される以外、SendEmail アクションへの設定は必要ありません。

SendEmail アクションは Sentinel で内部的にトリガされ、次の場合にメールが送信されます。

- ◆ 相関ルールが生成されると、SendEmail アクションがトリガされます。この Send Email アクションは、歯車のアイコンで示されているアクションで、相互関連についてのみ有効です (JS JavaScript アイコンで示されている JavaScript の SendEmail アクションとは異なります)。
- ◆ ワークフローに、電子メールを送信するように構成されているメールステップやアクティビティが含まれている場合。
- ◆ ユーザがインシデントを開いて、電子メールを送信するように構成されているアクティビティを実行する場合。
- ◆ ユーザがイベントを右クリックして [電子メール] を選択する場合。
- ◆ ユーザがインシデントを開いて [電子メールインシデント] を選択する場合。

3.6.3 コレクタマネージャのサービス

- ◆ [44 ページの「コレクタマネージャの追加」](#)
- ◆ [44 ページの「汎用コレクタの使用」](#)

コレクタマネージャの追加

コレクタマネージャは、データ収集プロセスとデータ解析をすべて管理します。マシン間で負荷を分散させるために、Sentinel 環境に追加の Sentinel コレクタマネージャノードを追加することが必要になる場合があります。リモートのコレクタマネージャには、以下のようないくつかの利点があります。

- ◆ イベントの解析および処理の分散化によりシステムパフォーマンスが向上します。
- ◆ イベントソースとのつながりを介して、ソースシステムでデータのフィルタリング、圧縮、暗号化が可能です。これにより、ネットワーク帯域幅の要件が軽減し、データセキュリティが強化されます。
- ◆ これらは、追加のオペレーティングシステムにインストールできます。たとえば、Microsoft Windows にコレクタマネージャノードをインストールし、WMI プロトコルによるデータ収集を有効にできます。
- ◆ ファイルキャッシングにより、サーバがアーカイブ処理や多数のイベントの処理で一時的にビジーである場合に、リモートのコレクタマネージャで大量のデータをキャッシュできます。これは、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。

コレクタマネージャコンポーネントは、これらのコンポーネントのインスタンスを追加のマシンにインストールすることで負荷分散できます。新しいマシン上でインストーラを実行することで、追加のコレクタマネージャをインストールできます。コレクタマネージャのインストールの詳細については、39 ページのセクション 3.3.4 「Sentinel コレクタマネージャのインストール (SLES のまたは Windows の場合)」を参照してください。

汎用コレクタの使用

Sentinel Rapid Deployment サーバのインストール中に、汎用コレクタと呼ばれるコレクタが設定されます。このコレクタは、デフォルトで毎秒 5 イベント (eps) の割合でイベントを作成します。

システムにコレクタを追加したい場合は、Novell Web サイト (<http://support.novell.com/products/sentinel/collectors.html>) からダウンロードできます。

3.6.4 時刻の管理

Sentinel サーバは、NTP (Network Time Protocol) サーバまたは他の種類のタイムサーバに接続する必要があります。マシン間でシステム時刻が同期していない場合、Sentinel 関連エンジンおよびアクティブビューは正しく動作しません。コレクタマネージャからのイベントは、リアルタイムとは見なされないため、Sentinel Control Center および関連エンジンを通らずに Sentinel データベースに直接送信されることはありません。

デフォルトでは、リアルタイムデータのしきい値は 120 秒です。この値は、event-router.properties ファイル内の esecurity.router.event.realtime.expiration の値を変更することで修正できます。Sentinel イベントの時刻は、信頼デバイス時刻またはコレクタマネージャ時刻に基づいて設定されます。コレクタの設定中に信頼デバイス時刻を選択することができます。信頼デバイス時刻はログがデバイスによって生成された時刻で、コレクタマネージャ時刻はコレクタマネージャシステムのローカルシステム時刻です。

3.7 LDAP 認証

Sentinel Rapid Deployment は、データベース認証に加えて、LDAP 認証もサポートしています。Sentinel Rapid Deployment サーバで LDAP 認証が可能になるように設定することによって、ユーザが自分の Novell eDirectory または Microsoft Active Directory の資格情報を使用して Sentinel Rapid Deployment にログインできるようにできます。

- ◆ [45 ページのセクション 3.7.1 「概要」](#)
- ◆ [45 ページのセクション 3.7.2 「前提条件」](#)
- ◆ [46 ページのセクション 3.7.3 「LDAP 認証を可能にする Sentinel サーバの設定」](#)
- ◆ [49 ページのセクション 3.7.4 「複数の LDAP サーバを使用したフェールオーバー構成」](#)
- ◆ [51 ページのセクション 3.7.5 「複数の Active Directory ドメイン向けの LDAP 認証の設定」](#)
- ◆ [52 ページのセクション 3.7.6 「LDAP ユーザの資格情報を使用したログイン」](#)

3.7.1 概要

セキュリティで保護された SSL 接続を使用して LDAP 認証するように Sentinel Rapid Deployment サーバを設定できます。この時、LDAP ディレクトリの匿名検索の使用または不使用を指定できます。

注：LDAP ディレクトリに対する匿名検索を無効にする場合、Sentinel Rapid Deployment サーバで匿名検索を使用するように設定しないでください。

- ◆ **匿名検索：** Sentinel Rapid Deployment の LDAP ユーザアカウントを作成する際、ディレクトリ名を指定する必要がありますが、ユーザの識別名 (DN) を指定する必要はありません。

LDAP ユーザが Sentinel Rapid Deployment にログインすると、Sentinel Rapid Deployment サーバが指定されたユーザ名に基づいて LDAP ディレクトリに対する匿名検索を実行し、そのユーザに対応する DN を発見すると、その DN を使用して LDAP ディレクトリに対するユーザログインの認証を行います。

- ◆ **非匿名検索：** Sentinel Rapid Deployment の LDAP ユーザアカウントを作成する際、ディレクトリのユーザ名とユーザ DN の両方を指定する必要があります。

LDAP ユーザが Sentinel Rapid Deployment にログインすると、Sentinel Rapid Deployment サーバが指定されたユーザ名を使用して LDAP ディレクトリに対するユーザログインの認証を行います。この時、LDAP ディレクトリに対する匿名検索は実行されません。

Active Directory にのみ適用される別の方法があります。詳細については、[Active Directory における UserPrincipalName 属性を使用した非匿名の LDAP 認証](#)を参照してください。

3.7.2 前提条件

- ◆ [46 ページの「LDAP サーバの CA 証明書のエクスポート」](#)
- ◆ [46 ページの「LDAP ディレクトリにおける匿名検索の有効化」](#)

LDAP サーバの CA 証明書のエクスポート

LDAP サーバに対してセキュリティで保護された SSL 接続を行うには、Base64 エンコードのファイルにエクスポートする必要がある LDAP サーバの CA 証明書が必要です。

- ◆ **eDirectory: Organizational CA** の自己署名証明書のエクスポート (<http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html>) を参照してください。

iManager で eDirectory CA 証明書をエクスポートするには、iManager 用の Novell 証明書サーバプラグインをインストールする必要があります。

- ◆ **Active Directory: サードパーティ認証局を使用して SSL 経由で LDAP を有効化する方法** (<http://support.microsoft.com/kb/321051>) を参照してください。

LDAP ディレクトリにおける匿名検索の有効化

匿名検索を使用して LDAP 認証を実行するには、LDAP ディレクトリで匿名検索を有効にする必要があります。匿名検索は、デフォルトでは eDirectory では有効、Active Directory では無効になっています。

LDAP ディレクトリで匿名検索を有効にするには、次を参照してください。

- ◆ **eDirectory: LDAP サーバオブジェクトに関する属性** (<http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html>) のセクションにある `ldapBindRestrictions` を参照してください。
- ◆ **Active Directory: ANONYMOUS LOGON ユーザオブジェクト** には、`sAMAccountName` および `objectclass` 属性に対する適切なリスト権限と読み取りアクセス権が付与されなければなりません。詳細については、**匿名によるクエリを可能にする Active Directory の設定** (<http://support.microsoft.com/kb/320528>) を参照してください。

Windows Server 2003 の場合、追加の設定を実行する必要があります。詳細については、**Windows Server 2003 上での Active Directory の設定** (<http://support.microsoft.com/kb/326690/en-us>) を参照してください。

3.7.3 LDAP 認証を可能にする Sentinel サーバの設定

- 1 45 ページのセクション 3.7.2 「前提条件」の要件を満たしていることを確認してください。
- 2 Sentinel Rapid Deployment サーバに root ユーザでログインします。
- 3 エクスポートされた LDAP サーバ CA 証明書ファイルを `<install_directory>/config` ディレクトリにコピーします。
- 4 証明書ファイルの所有権とアクセス権を次のように設定します。

```
chown novell:novell <install_directory>/config/<cert-file>
chmod 700 <install_directory>/config/<cert-file>
```
- 5 novell ユーザに切り替えます。

```
su - novell
```
- 6 `<install_directory>/bin` ディレクトリに変更します。
- 7 LDAP 認証の環境設定スクリプトを実行します。

```
./ldap_auth_config.sh
```

このスクリプトにより、LDAP 用に変更される前に auth.login および configuration.xml 環境設定ファイルのバックアップが config ディレクトリの中に auth.login.sav および configuration.xml.sav として作成されます。

8 次の情報を指定します。

<Enter> キーを押してデフォルト値をそのまま使用するか、新しい値を指定してデフォルトを無効にします。

- ◆ **Sentinel install location (Sentinel のインストール場所):** Sentinel サーバ上のインストールディレクトリ。
- ◆ **LDAP サーバのホスト名または IP アドレス :** LDAP データベースがインストールされるマシンのホスト名または IP アドレス。デフォルト値は localhost です。ただし、LDAP サーバは Sentinel 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。
- ◆ **LDAP server port (LDAP サーバのポート):** セキュリティで保護された LDAP 接続用のポート番号。デフォルトのポート番号は 636 です。
- ◆ **Anonymous searches on LDAP directory (LDAP ディレクトリに対する匿名検索):** 匿名検索を実行するには「y」を指定します。それ以外は「n」を指定します。デフォルト値は「y」です。
n を指定する場合は、LDAP の構成を完了し、[48 ページの「匿名検索を実行しない LDAP 認証」](#)のセクションで説明されている手順を実行します。
- ◆ **LDAP Directory used (使用される LDAP ディレクトリ):** このパラメータは、匿名検索で「y」を指定した場合のみ表示されます。Novell eDirectory には「1」を、Active Directory には「2」を指定します。デフォルト値は「1」です。
- ◆ **LDAP subtree to search for users (ユーザを検索する LDAP サブツリー):** このパラメータは、匿名検索で「y」を指定した場合のみ表示され、ディレクトリ内のユーザオブジェクトを含むサブツリーです。次に、eDirectory と Active Directory のサブツリーを指定する例を示します。

- ◆ **eDirectory:**

```
ou=users,o=novell
```

注: eDirectory の場合、サブツリーが指定されていないと、ディレクトリ全体に対して検索が実行されます。

- ◆ **Active Directory:**

```
CN=users,DC=TESTAD,DC=provo, DC=novell,DC=com
```

注: Active Directory の場合、サブツリーを空白にすることはできません。

- ◆ **Filename of the LDAP server certificate (LDAP サーバ証明書のファイル名):** [ステップ 3](#) でコピーした eDirectory/Active Directory の CA 証明書のファイル名。

9 次のいずれかを入力します。

- ◆ 入力した値を受け入れるには、「y」
- ◆ 新しい値を入力するには、「n」
- ◆ 設定を終了するには、「q」

正常に設定された場合：

- LDAP サーバ証明書が <install_directory>/config/ldap_server.keystore という名前のキーストアに追加されます。
- LDAP 認証を有効化するために、<install_directory>/config 内の auth.login および configuration.xml 環境設定ファイルが更新されます。

10 「y」と入力し、Sentinel サービスを再起動します。

重要：エラーがある場合、config ディレクトリ内の auth.login および configuration.xml 環境設定ファイルに加えられた変更を元に戻します。

```
cp -p auth.login.sav auth.login
cp -p configuration.xml.sav configuration.xml
```

11 (オプション) [Anonymous searches on LDAP directory \(LDAP ディレクトリに対する匿名検索\)](#) : で n を指定した場合、48 ページの「匿名検索を実行しない LDAP 認証」に進みます。

匿名検索を実行しない LDAP 認証

LDAP 認証が可能となるように Sentinel Rapid Deployment を設定する際、LDAP ディレクトリに対する匿名検索に「n」を指定すると、LDAP 認証は匿名検索を実行しません。

Sentinel コントロールセンターを使用して LDAP ユーザアカウントを作成する場合、非匿名の LDAP 認証に [LDAP user DN] を必ず指定してください。eDirectory と Active Directory の両方でこのアプローチを使用できます。

詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Creating an LDAP User Account for Sentinel](#)」を参照してください。

さらには、Active Directory の場合、匿名検索なしで LDAP 認証を実行する別の方法もあります。詳細については、[Active Directory における UserPrincipalName 属性を使用した非匿名の LDAP 認証](#)を参照してください。

Active Directory における UserPrincipalName 属性を使用した非匿名の LDAP 認証

Active Directory の場合、userPrincipalName 属性を使用することで匿名検索せずに LDAP 認証を行うこともできます。

- 1 Active Directory ユーザの userPrincipalName 属性を <sAMAccountName@domain> に設定してください。

詳細については、[User-Principal-Name 属性 \(http://msdn.microsoft.com/en-us/library/ms680857\(VS.85\).aspx\)](http://msdn.microsoft.com/en-us/library/ms680857(VS.85).aspx) を参照してください。

- 2 46 ページのステップ 1 から 48 ページのステップ 10 まで実行し、47 ページの「[Anonymous searches on LDAP directory \(LDAP ディレクトリに対する匿名検索\)](#) :」で「n」と指定したことを確認します。
- 3 Sentinel サーバ上で、<Install Directory>/config/auth.login ファイル内の LdapLogin セクションを編集します。


```
LdapLogin {
  com.sun.security.auth.module.LdapLoginModule required
  userProvider="ldap://LDAP server IP:636/DN of the Container that contains
the user objects"
  authIdentity="{USERNAME}@Domain Name"
  userFilter="(&(sAMAccountName={USERNAME})) (objectclass=user)"
  useSSL=true;
};
```

例:

```
LdapLogin {
  com.sun.security.auth.module.LdapLoginModule required
  userProvider="ldap://137.65.151.12:636/DC=Test-
AD,DC=provo,DC=novell,DC=com"
  authIdentity="{USERNAME}@Test-AD.provo.novell.com"
  userFilter="(&(sAMAccountName={USERNAME})) (objectclass=user)"
  useSSL=true;
};
```

- 4 次のように Sentinel サービスを再起動します。

```
/etc/init.d/sentinel stop
/etc/init.d/sentinel start
```

3.7.4 複数の LDAP サーバを使用したフェールオーバー構成

1 つ以上の LDAP サーバを LDAP 認証用のフェールオーバーとして設定するには:

- 1 46 ページのステップ 2 から 48 ページのステップ 10 までの内容に従って、プライマリ LDAP サーバに対する Sentinel サーバの LDAP 認証を設定してください。
- 2 Sentinel サーバに novell ユーザでログインします。
- 3 Sentinel サービスを停止します。

```
/etc/init.d/sentinel stop
```

- 4 <install_directory>/config ディレクトリに移動します。

```
cd <install_directory>/config
```

- 5 編集用に auth.login ファイルを開きます。

```
vi auth.login
```

- 6 LdapLogin セクションの userProvider を更新し、複数の LDAP URL を指定します。各 URL は空白で区切ります。

例:

```
userProvider="ldap://ldap-url1 ldap://ldap-url2"
```

Active Directory の場合、LDAP URL のサブツリーが空白でないことを確認します。

複数の LDAP URL の指定に関する詳細については、[Class LdapLogin Module \(http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html\)](http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html) の userProvider オプションの説明を参照してください。

- 7 変更内容を保存します。
- 8 フェールオーバー LDAP サーバごとの証明書をエクスポートし、Sentinel サーバの <install_directory>/config ディレクトリに証明書ファイルをコピーします。
詳細については、46 ページの「LDAP サーバの CA 証明書のエクスポート」を参照してください。

- 9 フェールオーバー LDAP サーバごとに、証明書ファイルに必要な所有権およびアクセス権を設定してください。

```
chown novell:novell <install_directory>/config/<cert-file>
chmod 700 <install_directory>/config/<cert-file>
```

- 10 46 ページの「LDAP 認証を可能にする Sentinel サーバの設定」セクションのステップ 8 で作成されたキーストローク `ldap_server.keystore` に、それぞれのフェールオーバー LDAP サーバ証明書を追加します。

```
<install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
-file <certificate-file> -alias <alias_name> -keystore
ldap_server.keystore -storepass sentinel
```

`<certificate-file>` をエンコード形式の LDAP 証明書ファイル名で置き換え、`<alias_name>` をインポートされる証明書の別名で置き換えます。

重要: 別名を必ず指定してください。別名が指定されていない場合、鍵ツールは `mykey` をデフォルトでエイリアスだと認識します。別名を指定せずにキーストアに複数の証明書をインポートすると、別名がすでに存在しているというエラーが鍵ツールによって報告されます。

- 11 Sentinel サービスを開始します。

```
/etc/init.d/sentinel start
```

プライマリ LDAP サーバがダウンしていることを認識する前に Sentinel サーバがタイムアウトすると、サービスがフェールオーバー LDAP サーバに接続できないことがあります。Sentinel サーバがタイムアウトせずにフェールオーバー LDAP サーバに接続できるようにするには:

- 1 Sentinel サーバに root ユーザでログインします。
- 2 `sysctl.conf` ファイルを編集用を開きます。

```
vi /etc/sysctl.conf
```
- 3 `net.ipv4.tcp_syn_retries` の値が 3 に設定されているのを確認します。エントリが存在しない場合、エントリを追加します。ファイルの保存:

```
net.ipv4.tcp_syn_retries = 3
```
- 4 コマンドを実行し、変更を有効にします。

```
/sbin/sysctl -p
/sbin/sysctl -w net.ipv4.route.flush=1
```
- 5 `-Desecurity.remote.timeout=60` パラメータを `<install_directory>/bin` ディレクトリ内の `control_center.sh` と `solution_designer.sh` に追加して Sentinel サーバのタイムアウト値を設定します。

control_center.sh:

```
"<install_directory>/jre/bin/java" $MEMORY -
Dcom.esecurity.configurationfile=$ESEC_CONF_FILE -
Desecurity.cache.directory="<install_directory>/data/
control_center.cache" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<install_directory>/config/
control_center_log.prop" -
Djava.security.auth.login.config="<install_directory>/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
Dice.pilots.html4.baseFontFamily="Arial Unicode MS" -
Desecurity.remote.timeout=60 -jar ../lib/console.jar
```

solution_designer.sh:

```
"<install_directory>/jre/bin/java" -classpath $LOCAL_CLASSPATH $MEMORY -
Dcom.esecurity.configurationfile="$ESEC_CONF_FILE" -
Dsentinel.installer.jar.location="<install_directory>/lib/
contentinstaller.jar" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<install_directory>/config/
solution_designer_log.prop" -
Djava.security.auth.login.config="<install_directory>/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -Desecurity.cache.directory=../
data/solution_designer.cache -Desecurity.remote.timeout=60
com.esecurity.content.exportUI.ContentPackBuilder
```

3.7.5 複数の Active Directory ドメイン向けの LDAP 認証の設定

認証される LDAP ユーザが複数の Active Directory ドメインに属している場合、Sentinel Rapid Deployment サーバを次のように設定し、LDAP 認証を行うことができます。

- 1 [46 ページのステップ 2](#) から [48 ページのステップ 10](#) までの説明に従って、最初のドメインの Active Directory ドメインコントローラに対して LDAP 認証を行うように Sentinel サーバを設定してください。また、[47 ページの「Anonymous searches on LDAP directory \(LDAP ディレクトリに対する匿名検索\):」](#) では必ず n を指定してください。
- 2 Sentinel サーバに novell ユーザでログインします。
- 3 Sentinel サービスを停止します。
/etc/init.d/sentinel stop
- 4 <install_directory>/config ディレクトリに移動します。
cd <install_directory>/config
- 5 編集用に auth.login ファイルを開きます。
vi auth.login
- 6 LdapLogin セクションを編集し、複数の LDAP の URL を空欄で区切って指定します。
例：

```
LdapLogin {
    com.sun.security.auth.module.LdapLoginModule required
    userProvider="ldap://<IP of the domain 1 domain controller>:636
ldap://<IP of the domain 2 domain controller>:636"
    authIdentity="{USERNAME}"
    useSSL=true;
};
```

複数の LDAP URL の指定に関する詳細については、[Class LdapLogin Module \(http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html\)](http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html) の userProvider オプションの説明を参照してください。

7 変更内容を保存します。

8 ドメインごとにドメインコントローラの証明書をエクスポートし、その証明書を Sentinel サーバ上の <install_directory>/config ディレクトリにコピーします。

詳細については、[46 ページの「LDAP サーバの CA 証明書のエクスポート」](#) を参照してください。

9 証明書ファイルに必要な所有権およびアクセス権を設定してください。

```
chown novell:novell <install_directory>/config/<cert-file>
chmod 700 <install_directory>/config/<cert-file>
```

10 [46 ページの「LDAP 認証を可能にする Sentinel サーバの設定」](#) セクションのステップ 8 で作成されたキーストローク ldap_server.keystore に、それぞれの証明書を追加します。

```
<install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
-file <certificate-file> -alias <alias_name> -keystore
ldap_server.keystore -storepass sentinel
```

<certificate-file> をエンコード形式の LDAP 証明書ファイル名で置き換え、<alias_name> をインポートされる証明書の別名で置き換えます。

重要: 別名を必ず指定してください。別名が指定されていない場合、鍵ツールは mykey をデフォルトでエイリアスだと認識します。別名を指定せずにキーストアに複数の証明書をインポートすると、別名がすでに存在しているというエラーが鍵ツールによって報告されます。

11 Sentinel サービスを開始します。

```
/etc/init.d/sentinel start
```

3.7.6 LDAP ユーザの資格情報を使用したログイン

LDAP 認証用に Sentinel サーバを正常に設定したら、Sentinel コントロールセンターの Sentinel LDAP ユーザアカウントを作成できます。LDAP ユーザアカウントの作成に関する詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Creating an LDAP User Account for Sentinel](#)」を参照してください。

LDAP ユーザアカウントを作成したら、LDAP ユーザ名およびパスワードを使用して Sentinel Rapid Deployment の Web ユーザインタフェース、Sentinel コントロールセンター、Sentinel ソリューションデザイナーにログインできます。

注: 既存の LDAP 設定を変更するには、ldap_auth_config スクリプトを再度実行し、パラメータに新しい値を指定します。

3.8 ライセンスキーを評価版キーから製品版キーに更新する

評価後に製品を購入した場合は、次の手順に従ってライセンスキーを更新し、再インストールを回避します。

- 1 Sentinel Rapid Deployment がインストールされているマシンに、Sentinel 管理者のオペレーティングシステム上のユーザ (デフォルトユーザは novell) でログインします。
- 2 コマンドプロンプトで `<install_directory>/bin` ディレクトリに移動します。
- 3 次のコマンドを入力します。
`./softwarekey.sh`
- 4 プライマリキーを設定するには 1 を指定します。 <Enter> キーを押します。
- 5 新しい有効なライセンスキーを入力し、ライセンスキーを更新し、画面上の指示に従って終了します。

Sentinel Rapid Deployment のアップグレード

4

このセクションでは、Sentinel Rapid Deployment の既存のバージョンの最新パッチへのアップグレードについて説明します。

注：このパッチは、Sentinel Rapid Deployment の 64 ビットのインストールにのみ適用されます。32 ビットのデモシステムにこのパッチを適用すると、そのインストールは機能しなくなります。

- 55 ページのセクション 4.1 「前提条件」
- 55 ページのセクション 4.2 「サーバへのパッチのインストール」
- 56 ページのセクション 4.3 「コレクタマネージャおよびクライアントアプリケーションのアップグレード」

4.1 前提条件

- アップグレードするシステムに、Sentinel 6.1 Rapid Deployment SP1 がすでにインストールされていることを確認します。
- Online Current パーティションが P_MAX に達することがないように、Sentinel データマネージャのジョブが有効になっていることを確認します。このパーティションが P_MAX に達し、手動でパーティションを追加すると、Sentinel コントロールセンターが正常に起動しません。

4.2 サーバへのパッチのインストール

- 1 パッチをインストールするサーバに novell ユーザでログインします。

パッチをインストールする前に次のコマンドを使用して、Sentinel データベース、config フォルダ、およびデータフォルダを必ずバックアップしてください。

Sentinel データベース：

```
tar -cf backup.tar <install_directory>/3rdparty/postgresql/database_files
tar -cf backupdata.tar <install_directory>/3rdparty/postgresql/data
```

config フォルダ：

```
tar -cf backupconfig.tar <install_directory>/config
```

データフォルダ：

```
tar -cf backupdata.tar <install_directory>/data
```

これらのコマンドの詳細については、PostgreSQL Wb サイトの [ファイルシステムレベルのバックアップ \(http://www.postgresql.org/docs/8.1/static/backup-file.html\)](http://www.postgresql.org/docs/8.1/static/backup-file.html) を参照してください。

- 2 イベントソースの管理 (ESM) の環境設定をバックアップし、ESM エクスポートを作成します。

詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Exporting a Configuration](#)」を参照してください。

- 3 **Novell Patch Finder** (<http://download.novell.com/patch/finder/>) から Sentinel Rapid Deployment 用のパッチインストーラをダウンロードします。
- 4 ダウンロードしたインストーラパッケージを一時ディレクトリにコピーします。
- 5 Sentinel サービスを停止します。

```
sentinel.sh stop
```
- 6 次のコマンドを入力し、インストーラパッケージに含まれるファイルを抽出します。

```
unzip <install_filename>
```

<install_filename> をインストーラファイルの実際の名前に置き換えます。
- 7 インストーラファイルを抽出したディレクトリに移動します。

```
cd <directory_name>
```

<directory_name> をファイルが抽出されたディレクトリの実際の名前に置き換えます。
- 8 次のコマンドを入力してサーバにパッチを適用し、画面上の指示に従います。

```
./service_pack.sh
```

インストール後は、Sentinel サービスが自動的に開始されます。
- 9 コレクタマネージャまたはクライアントアプリケーション (あるいはその両方) を実行しているすべてのマシンにパッチを適用します。

4.3 コレクタマネージャおよびクライアントアプリケーションのアップグレード

- ◆ [56 ページのセクション 4.3.1 「コレクタマネージャのアップグレード」](#)
- ◆ [57 ページのセクション 4.3.2 「クライアントアプリケーションのアップグレード」](#)

4.3.1 コレクタマネージャのアップグレード

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

Linux

- 1 Sentinel Rapid Deployment のコレクタマネージャに root ユーザでログインします。
- 2 **Novell Patch Finder** (<http://download.novell.com/patch/finder/>) から Sentinel Rapid Deployment 用のパッチインストーラをダウンロードします。
- 3 ダウンロードしたインストーラファイルを一時ディレクトリにコピーします。
- 4 次のコマンドを入力し、インストーラの zip パッケージに含まれるファイルを抽出します。

```
unzip <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。
- 5 インストーラファイルを抽出したディレクトリに移動します。

```
cd <directory_name>
```


<directory_name> をインストーラファイルが抽出されたディレクトリの実際の名前に置き換えます。

- 6 コレクタマネージャのサービスを停止します。

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

- 7 サービスパックインストーラを実行し、画面上の指示に従います。

```
./service_pack.sh
```

インストール後は、コレクタマネージャのサービスが自動的に開始されます。

Windows

- 1 Sentinel Rapid Deployment のコレクタマネージャに管理者ユーザでログインします。

- 2 [Novell Patch Finder \(http://download.novell.com/patch/finder/\)](http://download.novell.com/patch/finder/) から Sentinel Rapid Deployment 用のパッチインストーラをダウンロードします。

- 3 インストーラファイルを一時ディレクトリにコピーします。

- 4 インストーラパッケージに含まれるファイルを抽出します。

- 5 コレクタマネージャのサービスを停止します。

```
<install_directory>\bin\sentinel.bat stop
```

- 6 インストーラファイルを抽出したディレクトリに移動します。

- 7 次のいずれかの操作を行ってインストーラを実行します。

- service_pack.bat ファイルをダブルクリックし、画面上の指示に従います。
- コマンドプロンプトから service_pack.bat ファイルを実行し、画面上の指示に従います。

インストール後は、コレクタマネージャのサービスが自動的に開始されます。

4.3.2 クライアントアプリケーションのアップグレード

- [57 ページの「Linux」](#)
- [58 ページの「Windows」](#)

Linux

- 1 root ユーザで Novell Sentinel Rapid Deployment のクライアントアプリケーションが実行されているマシンにログインします。

- 2 [Novell Patch Finder \(http://download.novell.com/patch/finder/\)](http://download.novell.com/patch/finder/) から Sentinel Rapid Deployment 用のパッチインストーラをダウンロードします。

- 3 ダウンロードしたインストーラパッケージを一時ディレクトリにコピーします。

- 4 次のコマンドを入力し、インストーラパッケージに含まれるファイルを抽出します。

```
unzip <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。

- 5 インストーラファイルを抽出したディレクトリに移動します。

```
cd <directory_name>
```

<directory_name> をファイルが抽出されたディレクトリの実際の名前に置き換えます。

- 6 インストーラを実行し、画面上の指示に従います。

```
./service_pack.sh
```

Windows

- 1 管理者ユーザで Novell Sentinel Rapid Deployment のクライアントアプリケーションが実行されているマシンにログインします。
- 2 [Novell Patch Finder \(http://download.novell.com/patch/finder/\)](http://download.novell.com/patch/finder/) から Sentinel Rapid Deployment 用のパッチインストーラをダウンロードします。
- 3 ダウンロードしたインストーラファイルを一時ディレクトリにコピーします。
- 4 インストーラパッケージに含まれるファイルを抽出します。
- 5 インストーラファイルを抽出したディレクトリに移動します。
- 6 次のいずれかの操作を行ってインストーラを実行します。
 - ◆ service_pack.bat ファイルをダブルクリックし、画面上の指示に従います。
 - ◆ コマンドプロンプトから service_pack.bat ファイルを実行し、画面上の指示に従います。

Sentinel Rapid Deployment のセキュリティに関する考慮事項

5

ここでは、Novell Sentinel Rapid Deployment を安全にインストール、設定、および保守する方法について説明します。

- ◆ 59 ページのセクション 5.1 「強化」
- ◆ 60 ページのセクション 5.2 「ネットワーク経由の通信のセキュリティ保護」
- ◆ 62 ページのセクション 5.3 「ユーザとパスワードのセキュリティ保護」
- ◆ 64 ページのセクション 5.4 「Sentinel データのセキュリティ保護」
- ◆ 67 ページのセクション 5.5 「情報のバックアップ」
- ◆ 68 ページのセクション 5.6 「オペレーティングシステムのセキュリティ保護」
- ◆ 69 ページのセクション 5.7 「Sentinel 監査イベントの表示」
- ◆ 69 ページのセクション 5.8 「認証局の証明書の使用」

5.1 強化

- ◆ 59 ページのセクション 5.1.1 「導入後直ちに実施できる強化」
- ◆ 60 ページのセクション 5.1.2 「Sentinel Rapid Deployment のデータの保護」

5.1.1 導入後直ちに実施できる強化

- ◆ 不必要なポートはすべてオフになります。
- ◆ 可能な限り、サービスポートはローカル接続のみをリスンし、リモート接続を許可しません。
- ◆ ファイルは、少数のユーザのみが読み取ることができるように、最小限の権限でインストールされます。
- ◆ デフォルトのパスワードは許可されません。
- ◆ データベースに対するレポートは、select 権限のみを持つユーザで実行されます。
- ◆ すべての Web インタフェースで HTTPS が必要です。
- ◆ アプリケーションに対して脆弱性スキャンが実行され、潜在的なセキュリティ問題のすべてに対処します。
- ◆ ネットワーク上のすべての通信にはデフォルトで SSL が使用され、認証の設定が行われます。
- ◆ ファイルシステムやデータベースに格納される際、ユーザアカウントのパスワードはデフォルトで暗号化されます。

5.1.2 Sentinel Rapid Deployment のデータの保護

Sentinel Rapid Deployment のデータは機密性が高いため、マシンのセキュリティを物理的に保護し、ネットワーク上の安全な領域に配置する必要があります。セキュリティ保護されたネットワークの外部のイベントソースからデータを収集するには、リモートコレクタマネージャを使用します。コレクタマネージャの詳細については、「[35 ページのセクション 3.3 「コレクタマネージャとクライアントアプリケーションのインストール」](#)」を参照してください。

5.2 ネットワーク経由の通信のセキュリティ保護

Sentinel Rapid Deployment のさまざまなコンポーネント間の通信はネットワーク経由で行われるため、システム全体にわたって各種の通信プロトコルが使用されます。

- ◆ [60 ページのセクション 5.2.1 「Sentinel サーバプロセス間の通信」](#)
- ◆ [60 ページのセクション 5.2.2 「Sentinel サーバと Sentinel クライアントアプリケーションとの間の通信」](#)
- ◆ [61 ページのセクション 5.2.3 「サーバとデータベースとの間の通信」](#)
- ◆ [61 ページのセクション 5.2.4 「コレクタマネージャとイベントソースとの間の通信」](#)
- ◆ [62 ページのセクション 5.2.5 「Web ブラウザとの通信」](#)
- ◆ [62 ページのセクション 5.2.6 「データベースと他のクライアントとの間の通信」](#)

5.2.1 Sentinel サーバプロセス間の通信

Sentinel サーバプロセスには、DAS Core、Das Binary、相関エンジン、コレクタマネージャ、Web サーバが含まれます。これらは、ActiveMQ を使用して互いに通信を行います。

デフォルトでは、これらのサーバプロセス間の通信は SSL を介して、ActiveMQ メッセージバス経由で行われます。SSL を設定するには、`<Install_Directory>/configuration.xml` に次の情報を指定します。

```
<jms brokerURL="failover://(ssl://localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
```

カスタムのサーバおよびクライアントの証明書をセットアップする方法の詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Processes](#)」を参照してください。

5.2.2 Sentinel サーバと Sentinel クライアントアプリケーションとの間の通信

Sentinel コントロールセンター (SCC)、Sentinel Data Manager (SDM)、Solution Designer などの Sentinel クライアントアプリケーションは、デフォルトでは SSL プロキシサーバ経由の SSL 通信を使用します。

サーバ上ですべてがクライアントアプリケーションとして実行される SCC、SDM、および Solution Designer と Sentinel サーバ間の通信を有効にするには、<install_directory>/configuration.xml に次の情報を指定します。

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedClientStrategyFactory">
  <transport type="ssl">
    <ssl host="localhost" keystore="<install_directory>/config/.proxyClientKeystore" port="10013" usecacerts="false"/>
  </transport>
</strategy>
```

Web Start 経由で実行される SCC、SDM、および Solution Designer と Sentinel サーバ間で通信を有効にするために、サーバの <install_directory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/configuration.xml ファイルで次のように定義します。

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedClientStrategyFactory" >
  <transport type="ssl">
    <ssl host="127.0.0.1" port="10013" keystore="./novell/sentinel/.proxyClientKeystore" />
  </transport>
</strategy>
```

カスタムのサーバおよびクライアントの証明書をセットアップする方法の詳細については、『Sentinel Rapid Deployment User Guide』の「Processes」を参照してください。

5.2.3 サーバとデータベースとの間の通信

サーバとデータベース間の通信に使用されるプロトコルは、JDBC ドライバによって定義されます。一部のドライバでは、データベースとの間の通信を暗号化できます。

Sentinel Rapid Deployment は、PostgreSQL データベースに接続するために、PostgreSQL ドライバ (postgresql-<version>.jdbc3.jar) を使用します。これは Java (タイプ 4) 実装で、[PostgreSQL ダウンロードページ \(http://jdbc.postgresql.org/download.html\)](http://jdbc.postgresql.org/download.html) で入手できます。このドライバは、データ通信の暗号化をサポートしています。データ通信の暗号化を設定する方法については、[PostgreSQL の暗号化オプション \(http://www.postgresql.org/docs/8.1/static/encryption-options.html\)](http://www.postgresql.org/docs/8.1/static/encryption-options.html) を参照してください。

注：暗号化をオンにすると、システムのパフォーマンスに影響が及ぶ可能性があります。そのため、データベースの通信はデフォルトでは暗号化されていません。ただし、このことは、データベースとサーバ間の通信はループバックネットワークインタフェース経由で行われるのであって、オープンなネットワークにさらされるわけではないので、セキュリティ上の問題ではありません。

5.2.4 コレクタマネージャとイベントソースとの間の通信

さまざまなイベントソースからデータを収集するように Sentinel Rapid Deployment を設定できます。ただし、セキュリティで保護されたデータ収集は、イベントソースがサポートする特定のプロトコルによって決まります。たとえば、イベントソースとの通信を暗号化するように Check Point LEA、Syslog、および Audit のコネクタを設定できます。

有効化が可能なセキュリティ機能の詳細については、[Novell Sentinel プラグイン Web サイト \(http://support.novell.com/products/sentinel/secure/sentinelplugins.html\)](http://support.novell.com/products/sentinel/secure/sentinelplugins.html) から入手可能な接続タブおよびイベントソースベンダのマニュアルを参照してください。

5.2.5 Web ブラウザとの通信

Web サーバはデフォルトで HTTPS 経由で通信を行うように設定されます。詳細については、[Tomcat のマニュアル \(http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html\)](http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html) を参照してください。

5.2.6 データベースと他のクライアントとの間の通信

PostgreSQL SIEM データベースは、Sentinel Data Manager、または Pgadmin など任意のサードパーティアプリケーションを使用して、任意のクライアントマシンからの接続を許可するように設定できます。

Sentinel Data Manager に任意のクライアントマシンから接続できるようにするには、`<Install_Directory>/3rdparty/postgresql/data/pg_hba.conf` ファイルに次の行を追加します。

```
host all all 0.0.0.0/0 md5
```

実行を許可され、SDM 経由でデータベースに接続できるクライアント接続を制限するには、上記の行をホストの IP アドレスに置き換えます。pg_hba.conf に次の行を指定すると、PostgreSQL はローカルマシンからの接続を受け付けるようになるため、Sentinel データマネージャはサーバ上でのみ実行可能になります。

```
host all all 127.0.0.1/32 md5
```

他のクライアントマシンからの接続を制限するには、host エントリを追加する必要があります。

5.3 ユーザとパスワードのセキュリティ保護

- ◆ [62 ページのセクション 5.3.1 「オペレーティングシステムのユーザ」](#)
- ◆ [63 ページのセクション 5.3.2 「Sentinel アプリケーションおよびデータベースのユーザ」](#)
- ◆ [64 ページのセクション 5.3.3 「ユーザのパスワードポリシーの強制」](#)

5.3.1 オペレーティングシステムのユーザ

- ◆ [62 ページの 「サーバのインストール」](#)
- ◆ [63 ページの 「コレクタマネージャのインストール」](#)

サーバのインストール

Sentinel Rapid Deployment サーバをインストールすると、インストールされたファイルを所有するシステムユーザとグループが `<install_directory>` 内に作成されます。このユーザが存在しない場合は作成され、ホームディレクトリが `<install_directory>` に設定されます。新しいユーザが作成されても、セキュリティを最大限に高めるために、そのユーザのパスワードはデフォルトでは設定されません。インストール時に作成されたそのユーザでシステムにログインするには、インストール後にユーザのパスワードを設定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

システムユーザは、コレクタマネージャがインストールされているオペレーティングシステムに応じてセキュリティレベルが異なる場合があります。

Linux: インストールされるファイルを所有するシステムユーザの名前と、そのホームディレクトリを作成する場所を指定するよう求められます。デフォルトでは、システムユーザは `esecadm` ですが、このシステムユーザ名は変更できます。このユーザが存在しない場合、ホームディレクトリと共に作成されます。新しいユーザが作成されても、セキュリティを最大限に高めるために、インストール時にそのユーザのパスワードは設定されません。そのユーザでシステムにログインするには、インストール後にユーザのパスワードを設定する必要があります。デフォルトのグループは `esec` です。

クライアントのインストール時に、ユーザがすでに存在している場合は、再度ユーザを指定することは求められません。この動作は、ソフトウェアのアンインストールや再インストール時の動作と同様です。ただし、次の方法でインストーラに再びユーザを指定するように求めさせることができます。

- 1 最初のインストール時に作成されたユーザとグループを削除します。
- 2 `/etc/profile` から `ESEC_USER` 環境変数を消去します。

Windows: ユーザは作成されません。

システムユーザのパスワードポリシーは、使用されているオペレーティングシステムによって定義されます。

5.3.2 Sentinel アプリケーションおよびデータベースのユーザ

Sentinel Rapid Deployment アプリケーションのユーザはすべてネイティブのデータベースユーザで、これらのユーザのパスワードはネイティブのデータベースプラットフォームが従う手順を使用して保護されます。これらのユーザは、データベースに対してクエリを実行できるように、データベースの特定のテーブルに対する読み取りアクセスのみが与えられます。

インストーラによって、PostgreSQL データベースが作成および設定されます。その際、以下のユーザも作成されます。

- ◆ **admin:** `admin` ユーザは、ログインするすべての Sentinel アプリケーションの管理者ユーザです。
- ◆ **dbauser:** `dbauser` は、データベースを管理できるスーパーユーザとして作成されます。`dbauser` のパスワードは、Sentinel Rapid Deployment サーバのインストール時に設定されます。このパスワードは、`<user home directory>/pgpass` に保存されます。システムは、PostgreSQL データベースのパスワードポリシーに従います。詳細については、[64 ページのセクション 5.3.3 「ユーザのパスワードポリシーの強制」](#) を参照してください。
- ◆ **appuser:** `appuser` は、Sentinel アプリケーションがデータベースに接続するのに使用する非スーパーユーザです。デフォルトでは、`appuser` はインストール時に無作為に生成されたパスワードを使用します。このパスワードは、暗号化されて `<install_directory>/config` ディレクトリ内の XML ファイル (`das_core.xml`、`das_binary.xml`、および `advisor_client.xml`) に保存されます。`appuser` のパスワードを変更するには、`<install_directory>/bin/dbconfig` ユーティリティを使用します。詳細については、『Sentinel Rapid Deployment Reference Guide』の「[DAS Container Files](#)」を参照してください。

注: システムデータベーステーブルを含むデータベース全体を所有する PostgreSQL というデータベースユーザも存在します。デフォルトでは、PostgreSQL データベースユーザは NOLOGIN として設定されるため、PostgreSQL ユーザとしてログインすることはできません。

5.3.3 ユーザのパスワードポリシーの強制

Sentinel Rapid Deployment は、簡単にパスワードポリシーを強制できるように標準ベースのメカニズムを採用しています。

インストーラによって、PostgreSQL データベースが作成および設定されます。その際、以下のユーザも作成されます。

dbauser: データベースの所有者 (データベース管理者ユーザ)。そのパスワードはインストールプロセスで設定されます。

appuser: これは、Sentinel Rapid Deployment からデータベースにログインするのに使用されるユーザです。そのパスワードはインストールプロセスでランダムに生成され、内部でのみ使用されることを目的としています。

admin: Sentinel Rapid Deployment の Web インタフェースへのログインに管理者の資格情報を使用できます。そのパスワードはインストールプロセスで設定されます。

デフォルトでは、ユーザのパスワードは Sentinel Rapid Deployment に組み込まれている PostgreSQL データベース内に保存されます。PostgreSQL は、PostgreSQL のマニュアルの [クライアント認証 \(http://www.postgresql.org/docs/8.3/static/client-authentication.html\)](http://www.postgresql.org/docs/8.3/static/client-authentication.html) のセクションで説明されている、さまざまな標準ベースの認証メカニズムを利用するオプションを提供します。

これらのメカニズムを活用すると、Web アプリケーションユーザや dbauser および appuser などのバックエンドサービスでのみ使用されるアカウントを含む、Sentinel Rapid Deployment 内のすべてのユーザアカウントに影響を与えます。

より簡単なオプションとしては、Web アプリケーションユーザを認証するのに LDAP ディレクトリを使用することが挙げられます。Sentinel Rapid Deployment サーバでこのオプションを有効にするには、[45 ページのセクション 3.7 「LDAP 認証」](#) を参照してください。このオプションは、バックエンドサービスが使用するアカウントには影響を与えません。これらのアカウントは、PostgreSQL の環境設定を変更しない限り、PostgreSQL 経由で認証し続けます。

これらの標準ベースのメカニズムと、環境内ですでに使用されている LDAP ディレクトリなどのメカニズムとを使用することで、Sentinel Rapid Deployment のパスワードポリシーの強固な強制を実現できます。

5.4 Sentinel データのセキュリティ保護

重要: Sentinel サーバのデータは機密性が高いため、マシンのセキュリティを物理的に保護し、ネットワーク上の安全な領域に配置する必要があります。セキュリティ保護されたネットワークの外部のイベントソースからデータを収集するには、リモートコレクタマネージャを使用します。

特定のコンポーネントでは、システムがデータベースやイベントソースなどのリソースに接続するときには使用できるように、パスワードを格納しておく必要があります。この場合、クリアテキストパスワードに対して認証されていないアクセスが行われないよう、パスワードを格納する際は最初に暗号化が行われます。

パスワードが暗号化されているとしても、パスワードの漏洩を避けるため、格納されているパスワードデータへのアクセスが保護されるように注意する必要があります。たとえば、機密性のあるデータを含むファイルのアクセス許可が、権限のないユーザーによって読み取り可能ではないことを確認します。

ファイル

advisor_client.xml

データベース資格情報

データベースの資格情報は、<installation_directory>/config/server.xml ファイルに保存されています。

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
  <property name="username">appuser</property>
  <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

アドバイザの資格情報

```
<obj-component id="DownloadComponent">
  <class>esecurity.ccs.comp.advisor.feed.NewAdvClientDownload</class>
  <property name="advisor.downloadfrom.url">https://secure-www.novell.com/sentinel/advisor/advisordata</property>
  <property name="username">admin</property>
  <!-- Set the password (encrypted) using the adv_change_password script ->
  <property name="password">jqhlWIX8HD6GDHVX9FApWg==</property>
<property name="compression.enabled">true</property>
  <!--
    Set the following properties to connect through an HTTP proxy.
    Set the proxy password (encrypted) using the adv_change_password script
    (make a
      copy of the script and add "-x" to the java cmd line to set the proxy
      password
      instead of the advisor password.
    -->
  <!--
  <property name="proxy_host"></property>
  <property name="proxy_port"></property>
  <property name="proxy_username"></property>
  <property name="proxy_password"></property>
  -->
</obj-component>
```

Configuration.xml

```
<strategy active="yes" id="jms"
location="com.esecurity.common.communication.strategy.jmsstrategy.activemq.Ac
tiveMQStrategyFactory" name="ActiveMQ">
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
</strategy>
```

das_binary.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
<property name="username">appuser</property>
<property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

das_core.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
<property name="username">appuser</property>
<property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

一部のデータベーステーブルにはパスワードや証明書が保存されます。この機密データは暗号化され、以下に一覧表示するテーブルに格納されます。これらのテーブルへのアクセスは制限する必要があります。

- ◆ **evt_src:** evt_src_config 列のデータ
- ◆ **evt_src_collector:** 列 : evt_src_collector_props
- ◆ **evt_src_grp (doubt):** 列 : evt_src_default_config
- ◆ **md_config:** 列 : data
- ◆ **integrator_config:** 列 : integrator_properties
- ◆ **md_view_config:** 列 : view_data
- ◆ **esec_content:** 列 : content_context、content_hash
- ◆ **esec_content_grp_content:** 列 : content_hash
- ◆ **sentinel_plugin:** 列 : content_pkg、file_hash

Sentinel Rapid Deployment は、設定データとイベントデータの両方を格納します。このデータは次の場所に格納されます。

コンポーネント	設定データの場所	イベントデータの場所
Sentinel Rapid Deployment サーバ	データベースのテーブルとファイルシステム (<install_directory>/config) この設定情報には、暗号化されたデータベース、イベントソース、インテグレーション、パスワードが含まれます。	データベース (EVENTS、CORRELATED_EVENTS、および EVT_SMRY_、AUDIT_RECORD テーブル) と <Install_Directory>/data/eventdata および <Install_Directory>/data/raw data にあるファイルシステム。 データは、パーティション管理ジョブの一部としてファイルシステムにアーカイブできます。
関連エンジン	ファイルシステム (<Install_Directory>/config) 機密性のある設定情報は、メッセージバスへの接続に使用されるクライアントキーのペアのみです。	correlation_engine.cache
DAS Core	<Install_Directory>/config	das_core.cache
DAS_Binary	<Install_Directory>/config	データベースが停止中の場合、データがキャッシュされることがあります。 das_binary.cache
コレクタマネージャ	ファイルシステム (<Install_Directory>/config) 機密性のある環境設定情報は、メッセージバスへの接続に使用されるコレクタマネージャユーザのパスワードのみです。	イベントデータは、メッセージバスの停止時やイベントのオーバーフロー時などのエラーが発生した状況では、ファイルシステムにキャッシュされることがあります。このイベントデータは <Install_Directory>/data/collector_mgr.cache ディレクトリに保存されます。
クライアントアプリケーション	ファイルシステム (install_directory/config) クライアントアプリケーションは機密情報を自身の環境設定ファイルに保存しません。 たとえば、クライアントアプリケーションは ESM データをローカルのファイルシステムにエクスポートできます。エクスポートされたイベントソースの設定に暗号化されたパスワードが含まれている場合、そのパスワードがエクスポートされたファイルに含まれます。パスワードは暗号化されますが、ESM のエクスポート許可は、この特権について信頼できるユーザにのみ付与するようにしてください。	None - なし。

5.5 情報のバックアップ

- イベントは定期的にバックアップする必要があります。バックアップメディアは、安全な外部の施設に保存する必要があります。

- ◆ システムデータをバックアップします。詳細については、『*Sentinel Rapid Deployment User Guide*』の「[Backup and Restore Utility](#)」を参照してください。
- ◆ 機密性のあるデータについては、次のいずれかの方法でデータを暗号化してバックアップします。
 - ◆ データを作成するアプリケーションが暗号化をサポートしている場合、データ自体を暗号化します。たとえば、データベース製品やサードパーティのツールはデータの暗号化をサポートしています。バックアップ時にデータを暗号化できるバックアップソフトウェアを使用します。この方法では、パフォーマンスと管理性の問題が発生することがあります。特に、暗号化キーの管理に問題が発生します。
 - ◆ データをバックアップする際に、機密性のあるバックアップメディアを暗号化する暗号化アプライアンスを使用します。
- ◆ メディアを外部に移して格納する場合、メディアの輸送と保管を専門としている企業に依頼します。テープがバーコードによって追跡され、環境上適切な条件で保管され、メディアを適切に扱う能力に定評のある企業によって管理されるようにします。
- ◆ 回復証明書をロードします。Novell Sentinel サービスは、デフォルトでは回復エージェント用に設定されていません。YaST によるサーバの設定時に、回復エージェントのパスを必ず設定します。このパスには、サービスがロードされ、ユーザが選択するための証明書のリストが含まれている必要があります。

詳細については、『*Sentinel Rapid Deployment Reference Guide*』の「[Certificate Management for Sentinel 6.1 Rapid Deployment Server](#)」を参照してください。

YaST には、X.509 証明書の基本管理用のモジュールが含まれています。これは、CA、サブ CA、およびそれらの証明書を作成するのに主に使用されます。証明書の管理と更新を行う方法の詳細については、『*SUSE Linux Enterprise Server 10 Installation and Administration Guide* (http://www.novell.com/documentation/sles10/sles_admin/data/bookinfo_book_sles_admin.html)』の [Managing X.509 Certification](http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html) (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html) を参照してください。

5.6 オペレーティングシステムのセキュリティ保護

- ◆ Sentinel Rapid Deployment は、SUSE Linux Enterprise Server (SLES) 10 SP3 およびそれ以降でサポートされています。SLES のマシンを確保するの詳細については、[SUSE Linux Enterprise Server 10 のマニュアル](http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html) (http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html) を参照してください。
- ◆ Sentinel Rapid Deployment サーバへのアクセスのセキュリティを、ファイアウォールを使用して保護します。Sentinel サーバが企業ネットワークの外部からアクセス可能な場合は、不正侵入者による直接アクセスを防ぐためにファイアウォールを使用する必要があります。

ファイアウォールで、次のポートを有効にします。

コンポーネント	ポート
ActiveMQ	61616
PostgreSQL	5432
Tomcat	8443
Sentinel Control Center のプロキシクライアントポート	10013

コンポーネント	ポート
プロキシが適用される信頼済みクライアント	10014
エンジンとマネージャとの間で使用される internal_gateway_server と internal_gateway	5556
internal_router_server と internal_router_client	5558
イベントルータ、クライアント、およびサーバ間で使用	
イベント待ち受けポート	35000
(config/collector_mgr.properties の中で "esecurity.agentmanager.event.port" と設定される)	

注: アスタリスクで示されているポートは、インストール時にそのポートがすでに使用されていた場合には異なる可能性があります。インストール時にこれらのポートが使用されていた場合、インストール時に入力を求められたポート番号に置き換えてください。

SLES 10 のファイアウォールを有効にする方法の詳細については、『*SLES 10 Administration Guide*』の「[Configuring Firewalls with YaST \(http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html\)](http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html)」を参照してください。

5.7 Sentinel 監査イベントの表示

Sentinel Rapid Deployment は、ユーザが実行するさまざまなアクション、およびシステムアクティビティ用に内部で実行されるアクション向けに監査イベントを生成します。これらのイベントは、アクティブビューで参照でき、検索またはレポートによってアクセスできます。ただし、システムイベントを表示するには、必要な権限を持っている必要があります。

詳細については、『*Sentinel Rapid Deployment User Guide*』の「[System Events for Sentinel](#)」を参照してください。

5.8 認証局の証明書の使用

自己署名された証明書を、VeriSign、Thawte、Entrust などの主要な認証局 (CA) によって署名された証明書と置き換えることができます。また、自己署名された証明書を、自社や組織内の CA など、一般的ではない CA によって署名された証明書と置き換えることもできます。

詳細については、『*Sentinel Rapid Deployment Reference Guide*』の「[Certificate Management for Sentinel 6.1 Rapid Deployment Server](#)」を参照してください。

Sentinel Rapid Deployment の機能 のテスト

6

Sentinel Rapid Deployment のインストール時には、システムの基本機能の多くをテストするのに使用できる汎用コレクタも付属してインストールされます。このコレクタを使用し、アクティブビュー、インシデントの作成、関連ルール、およびレポートをテストできます。

- 71 ページのセクション 6.1 「Rapid Deployment のインストールのテスト」
- 83 ページのセクション 6.2 「テスト後のクリーンアップ」
- 85 ページのセクション 6.3 「実際のデータの使用」

6.1 Rapid Deployment のインストールのテスト

ここでは、Sentinel Rapid Deployment システムのテスト手順と予想される結果について説明します。同じイベントは表示されない場合がありますが、次のような結果が表示されるはずですが。

基本レベルで、これらのテストでは次のことを確認できます。

- Sentinel サービスが起動し動作している。
- メッセージバス経由の通信が機能している。
- 内部の監査イベントが送信されている。
- イベントをコレクタマネージャから送信できる。
- イベントがデータベースに挿入され、レポートを使用して取得できること。
- インシデントを作成および表示できる。
- ルールが評価され、関連イベントが関連エンジンによってトリガされること。
- Sentinel データマネージャがデータベースに接続し、パーティション情報を読み込むこと。

これらのテストが失敗した場合は、インストールログおよびその他のログファイルを確認し、必要に応じて、Novell テクニカルサポート (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) にご連絡ください。

インストールをテストするには：

- 1 Sentinel Rapid Deployment の Web インタフェースにログインします。
詳細については、『Sentinel Rapid Deployment User Guide』の「[Accessing the Novell Sentinel Web Interface](#)」を参照してください。
- 2 [検索] ページを選択し、任意の内部イベントを検索します。1 つ以上のイベントが返されます。
たとえば、重大度の範囲 3 ~ 5 に含まれる内部イベントを検索するには、[Include System Events] を選択し、[Search] フィールドに「sev:[3 TO 5]」と入力します。

検索に関する詳細については、『Sentinel Rapid Deployment User Guide』の「Running an Event Search」を参照してください。

SP2 では、デフォルトでは検索機能が有効になっていません。ただし、この機能を有効にするには、『Sentinel Rapid Deployment User Guide』の「Enabling the Search Option in Web User Interface」を参照してください。

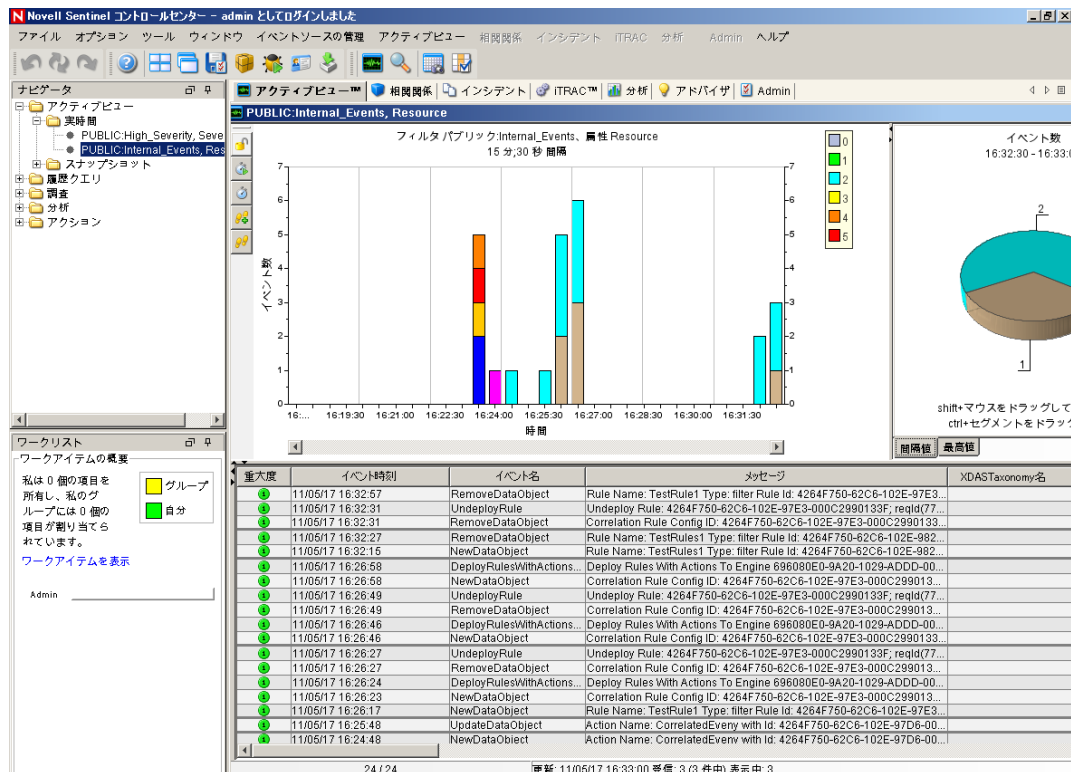
- 3 [レポート] ページを選択し、パラメータを指定してレポートを実行します。

たとえば、[Run] ボタンをクリックし、必要なパラメータを指定して [Run] クリックします。

詳細については、『Sentinel Rapid Deployment User Guide』の「Running Reports」を参照してください。

- 4 [アプリケーション] ページで、[Sentinel Control Center の起動] をクリックします。
- 5 インストール中に指定した Sentinel 管理者ユーザを使用してシステムにログインします (デフォルトでは admin)。

Sentinel コントロールセンターが開き、パブリックフィルタの *Internal_Events* と *High_Severity* によってフィルタされたイベントを含む [アクティブビュー] タブが表示されます。



- 6 [イベントソースの管理] メニューに移動し、[ライブビュー] を選択します。
- 7 グラフィカルビューで、5 eps イベントソースを右クリックし、[開始] を選択します。
- 8 [イベントソースの管理] の [ライブビュー] ウィンドウを閉じます。
- 9 [アクティブビュー] タブをクリックします。

「PUBLIC: High_Severity, Severity」というタイトルのアクティブウィンドウが表示されます。コレクタが開始してこのウィンドウにデータが表示されるまでにしばらく時間がかかる場合があります。

- 10 ツールバーにある [Event Query] ボタンをクリックします。[履歴イベントクエリ] ウィンドウが表示されます。
- 11 [履歴イベントクエリ] ウィンドウで、[フィルタ] の下矢印をクリックしてフィルタを選択します。[Public: All] フィルタを選択します。
- 12 コレクタがアクティブだった時刻を含む期間を選択します。[From] および [To] ドロップダウンリストを使用して日付範囲を選択します。
- 13 バッチサイズを選択します。
- 14 拡大鏡アイコンをクリックしてクエリを実行します。

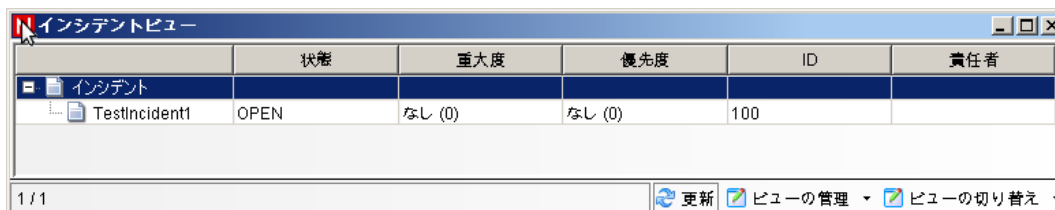
重大度	イベント時刻	イベント名	メッセージ
●	11/05/17 16:48:50	NewDataObject	Rule Name: CorrelatedEvent Type: filter Rule Id: 4264F750-
○	11/05/17 16:47:20	CombinedPersistentMap...	Total 6 persistent maps with 0KB in 2 entries; total of 0 fetche
○	11/05/17 16:47:09	CombinedPersistentMap...	Total 6 persistent maps with 0KB in 2 entries; total of 0 fetche
○	11/05/17 16:47:04	CombinedPersistentMap...	Total 11 persistent maps with 2KB in 17 entries; total of 13 fe
○	11/05/17 16:46:15	EnginePerformanceSum...	Engine tchlinux.dublinlab.vistatec.ie:172.22.19.161 has pro
○	11/05/17 16:46:13	EventThroughputCapacity	Event throughput capacity is at 0% for the past 15.00 min.
○	11/05/17 16:46:05	EventThroughputCapacity	Event throughput capacity is at 0% for the past 15.00 min.
○	11/05/17 16:45:58	CombinedPersistentMap...	Total 6 persistent maps with 0KB in 2 entries; total of 0 fetche
○	11/05/17 16:45:02	CombinedRealTimeSum...	Total 2 Active Views and combined cardinality of 16, total 10
○	11/05/17 16:45:01	EventThroughputCapacity	Event throughput capacity is at 0% for the past 15.00 min.
●	11/05/17 16:32:57	RemoveDataObject	Rule Name: TestRule1 Type: filter Rule Id: 4264F750-62C6-
●	11/05/17 16:32:31	UndeployRule	Undeploy Rule: 4264F750-62C6-102E-97E3-000C2990133
●	11/05/17 16:32:31	RemoveDataObject	Correlation Rule Config ID: 4264F750-62C6-102E-97E3-00i
●	11/05/17 16:32:27	RemoveDataObject	Rule Name: TestRules1 Type: filter Rule Id: 4264F750-62CE
○	11/05/17 16:32:20	CombinedPersistentMap...	Total 6 persistent maps with 0KB in 2 entries; total of 0 fetche

→ バッチを受信しました。詳細な結果については、[詳細]をクリックしてください。達成点 1... 45% 回数: 100

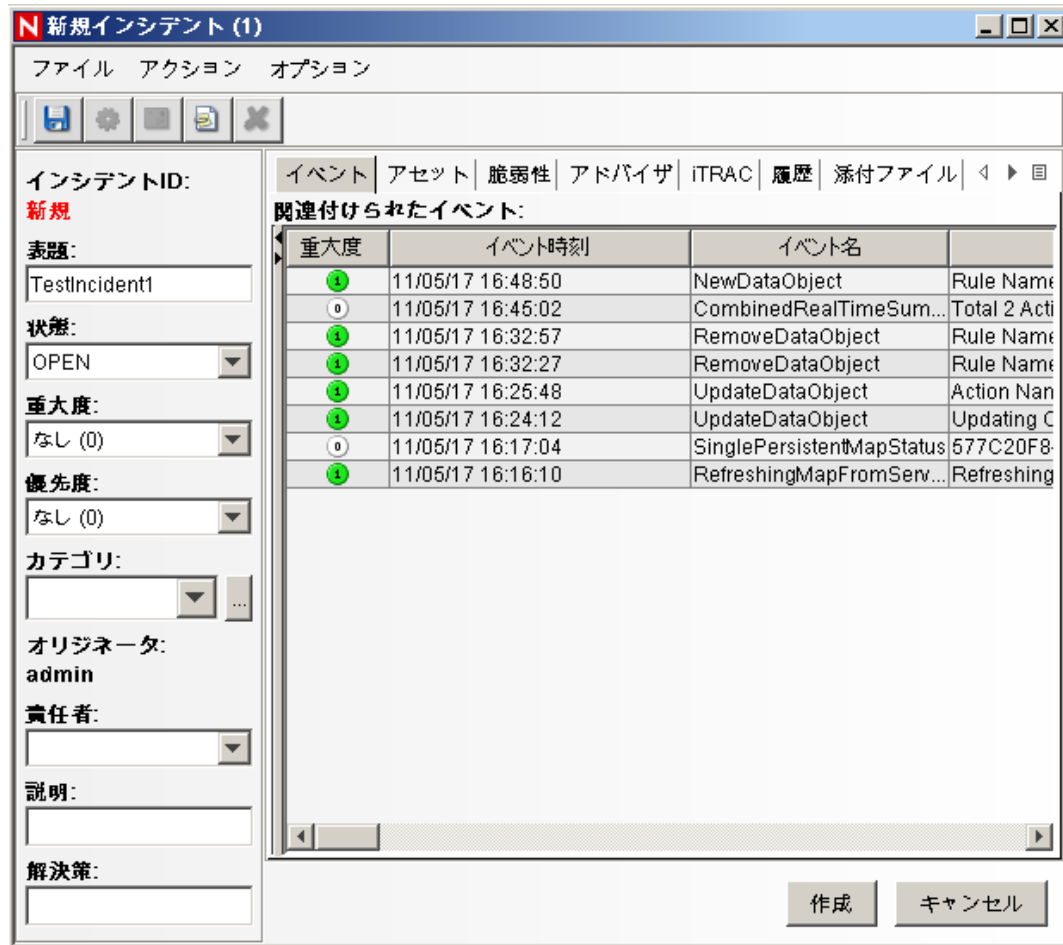
- 15 [履歴イベントクエリ] ウィンドウで、<Ctrl> キーまたは <Shift> キーを押しながら複数のイベントを選択します。
- 16 ウィンドウ内で右クリックし [Create Incident] を選択して [New Incident] ウィンドウを表示します。



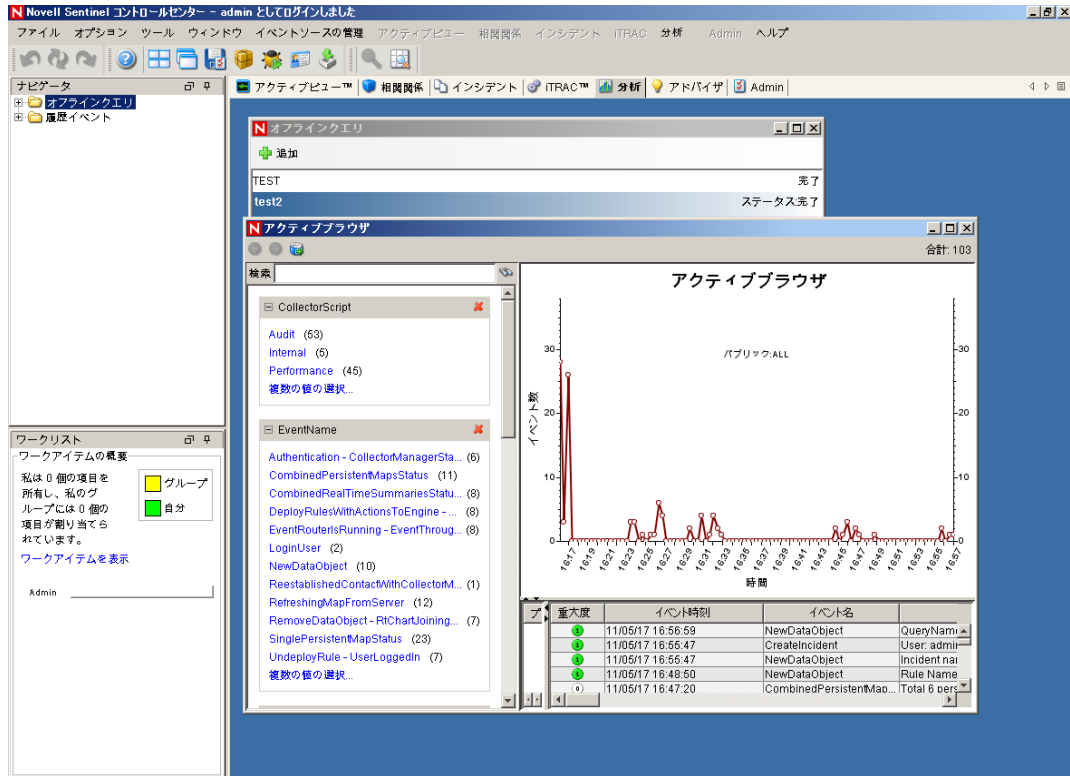
- 17 インシデントに「TestIncident1」と名前を付け、[作成] をクリックします。成功の通知が表示されたら、[保存] をクリックします。
- 18 インシデントビューマネージャで作成したインシデントを表示するには、[インシデント] タブをクリックします。



- 19 インシデントをダブルクリックしてイベントを表示します。

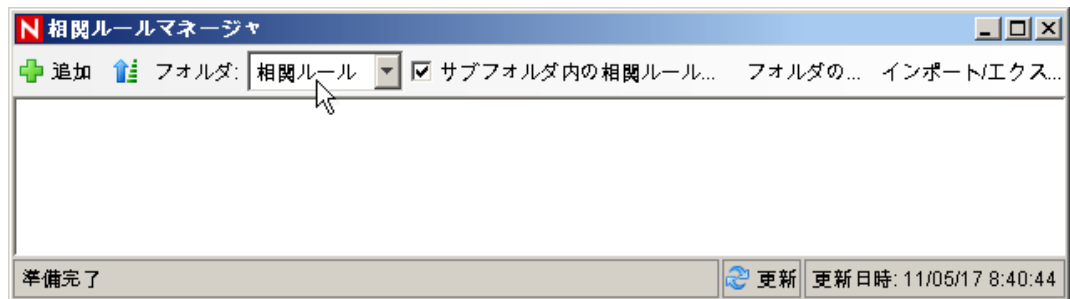


- 20 [インシデント] ウィンドウを閉じます。
- 21 [分析] タブをクリックします。
- 22 [分析] メニューまたはナビゲータから [Offline Queries] をクリックします。
- 23 [Offline Query] ウィンドウで、[Add] をクリックします。
- 24 名前を指定し、フィルタを選択し、期間を選択して [OK] をクリックします。
- 25 [Active Browser] ウィンドウにイベントのリストと関連する詳細を表示するには、[Browse] をクリックします。



コレクタ、ターゲット IP、重大度、ターゲットサービスポート、およびリソースなどの詳細を表示することができます。

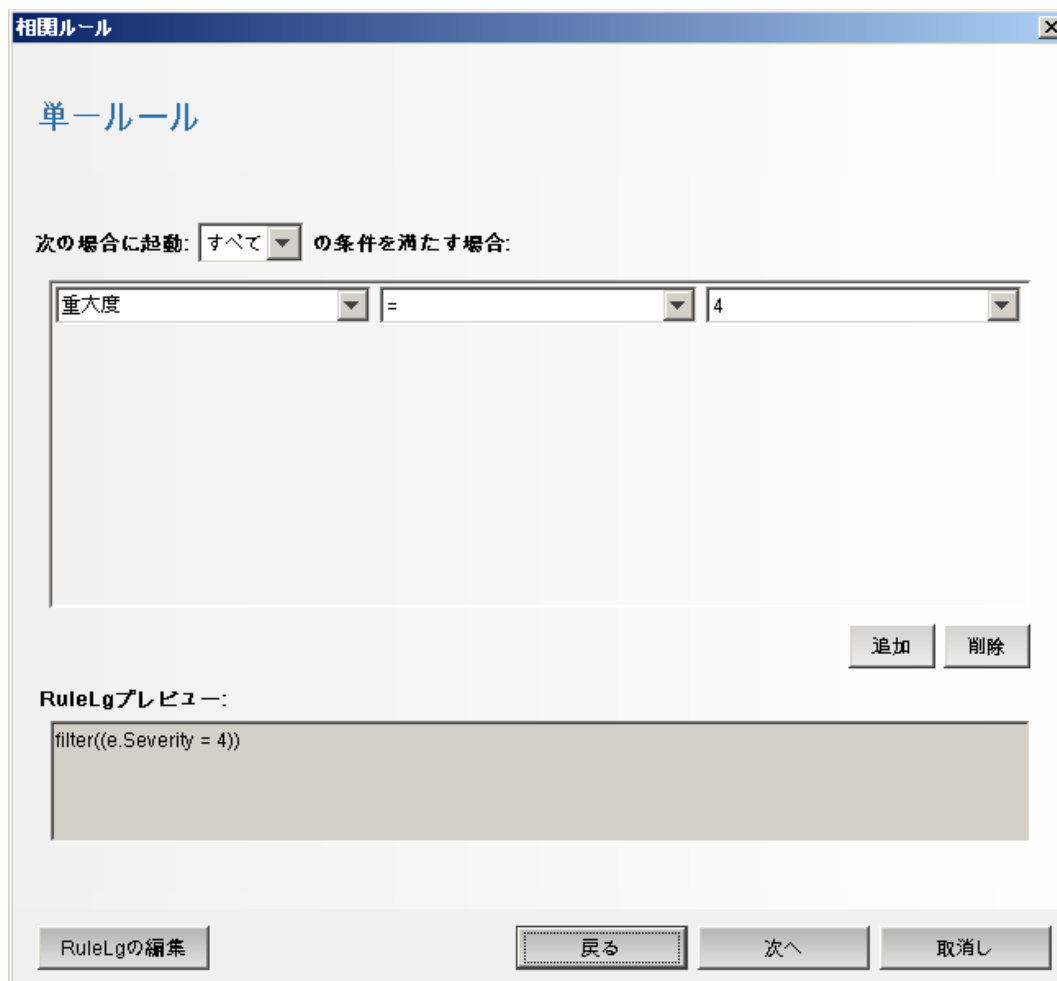
- 26 [Correlation] タブを選択します。相関ルールマネージャが表示されます。



- 27 [追加] をクリックします。相関ルールウィザードが表示されます。



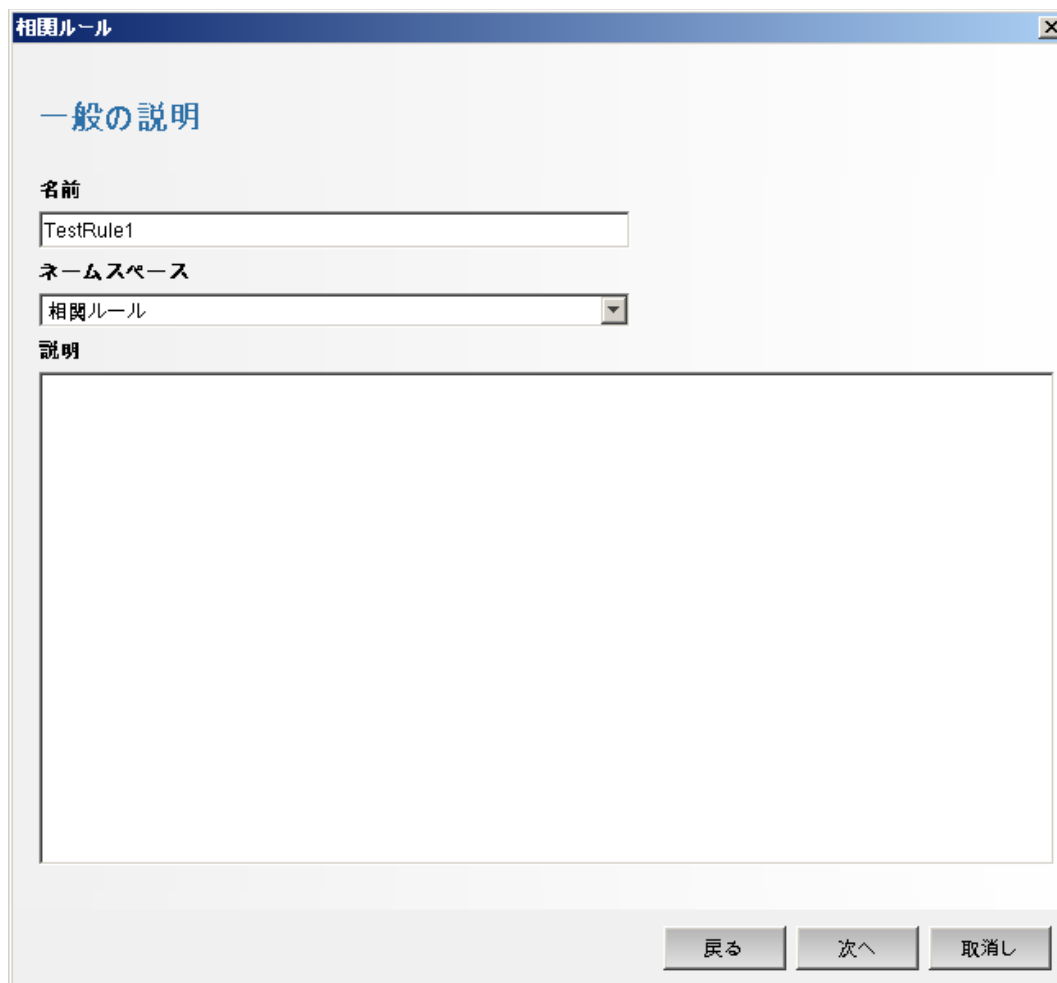
28 [シンプル] をクリックします。[Simple Rule] ウィンドウが表示されます。



- 29 ドロップダウンメニューを使用して、「重大度 =4」という条件を設定し、[次へ] をクリックします。[Update Criteria] ウィンドウが表示されます。



- 30 [Do not perform actions every time this rule fires] を選択し、ドロップダウンメニューを使用して時間範囲を1分に設定し、[次へ] をクリックします。[General Description] ウィンドウが表示されます。



相関ルール

一般の説明

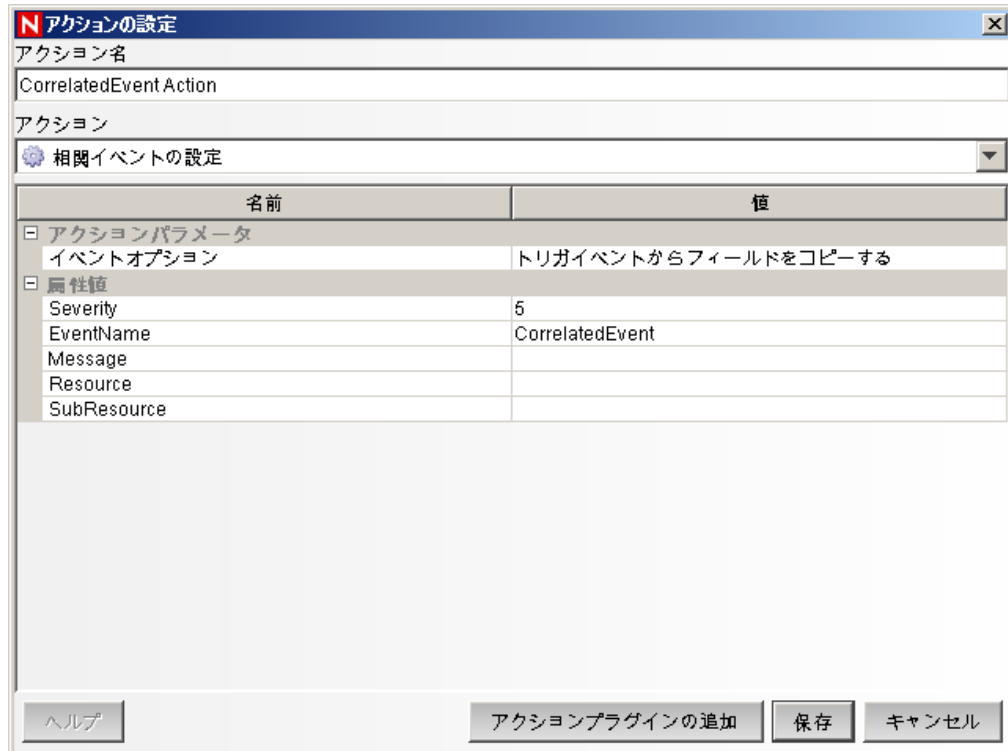
名前
TestRule1

ネームスペース
相関ルール

説明

戻る 次へ 取消し

- 31 ルールに「*TestRule1*」と名前を付け、説明を入力し、[次へ] をクリックします。
 - 32 [いいえ。別のルールは作成しません。] を選択し、[次へ] をクリックします。
 - 33 作成したルールに関連付けるアクションを作成します。
 - 33a 次のいずれかを実行します。
 - ◆ [Tools] > [Action Manager] > [Add] を選択します。
 - ◆ [Deploy Rule] ウィンドウで [Add Action] をクリックします。詳細については、[ステップ 34](#) から [81 ページのステップ 35](#) を参照してください。
- [Configure Action] ウィンドウが表示されます。



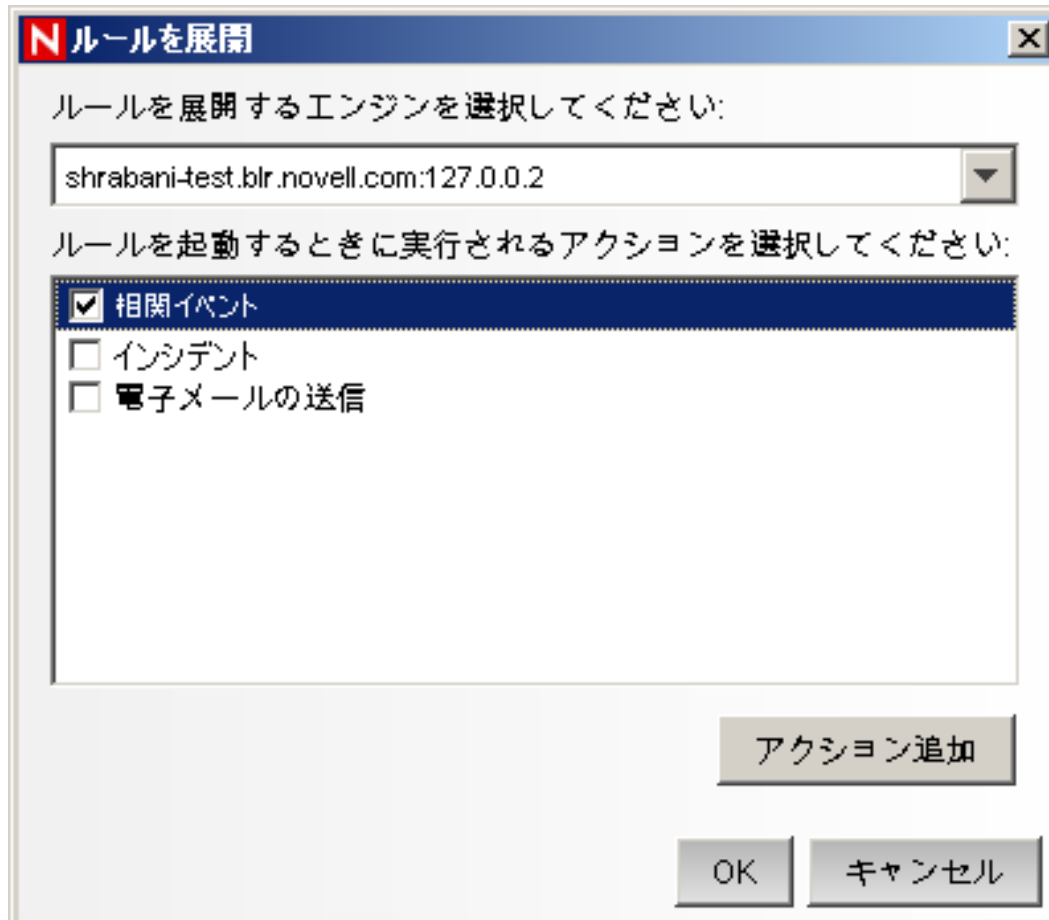
33b [Configure Action] ウィンドウで、次の内容を指定します。

- ◆ CorrelatedEvent アクションなどのアクション名を指定します。
- ◆ [Action] ドロップダウンリストから [Configure Correlated Event] を選択します。
- ◆ [Event Options] を設定します。
- ◆ [Severity] を 5 に設定します。
- ◆ [EventName] に「CorrelatedEvent」などを指定します。
- ◆ 必要に応じてメッセージを指定します。

アクションの作成に関する詳細については、『Sentinel Rapid Deployment User Guide』の「[Creating Actions](#)」を参照してください。

33c [Save] をクリックします。

- 34** [相関ルールマネージャ] ウィンドウを開きます。
- 35** ルールを選択し、[Deploy Rules] リンクをクリックします。[Deploy Rule] ウィンドウが表示されます。
- 36** [Deploy Rule] ウィンドウで、ルールを展開するエンジンを選択します。
- 37** [80 ページのステップ 33](#) で作成したアクションを選んでルールに関連付け、[OK] をクリックします。



38 [相関エンジンマネージャ] を選択します。

相関エンジンの下に、ルールが展開され有効になっていることが表示されます。

相関エンジンマネージャ									
名前	ホスト名	ホストID	ヘルス	有効/無効	ID	平均処理時...	ステータス...	処理回数	起動回数
Sentinel									
shrabani-st.blr.novell	shrabani-st.blr	172.22.19...	ヘルス	使用可能	696080E0-...	0 ミリ秒	10.50 分	58	
TestRule1			ヘルス	使用可能	4264F750-...	0 ミリ秒		0	0
CorrelatedEventy									
準備完了								更新	更新日時: 11/05/17 8:34:47

39 認証の失敗などの重大度 4 のイベントをトリガし、展開された相関ルールを発動します。

たとえば、SentinelControl Center のログインウィンドウを開き、誤ったユーザの資格情報を入力してイベントを生成します。

40 [Active Views] タブをクリックし、相関イベントが生成されるかどうかを確認します。

重大度	イベント時刻	イベント名	メッセージ	XDASTaxonomy名
4	11/05/17 16:16:29	ReestablishedContactWit...	Reestablished contact with collector manager Collector Manager (DAS)...	
4	11/05/17 16:16:23	CollectorManagerInitializ...	Initialized Collector Manager...; reqId(39345DB0-62C6-102E-A549-000...	
4	11/05/17 16:16:23	CollectorManagerStarted	Started Collector Manager...; reqId(39345DB0-62C6-102E-A547-000C...	
4	11/05/17 16:16:23	CollectorManagerStarting	Starting Collector Manager...; reqId(39345DB0-62C6-102E-A545-000C...	
4	11/05/17 16:16:23	CollectorManagerInitializ...	Initializing Collector Manager...; reqId(39345DB0-62C6-102E-A534-00...	

- 41 Sentinel コントロールセンターを閉じます。
- 42 [アプリケーション] ページで、[Sentinel データマネージャの起動] をクリックします。
- 43 インストール中に指定したデータベース管理者ユーザを使用して Sentinel データマネージャにログインします (デフォルトでは dbauser)。

データベースに接続

サーバ
PostgreSQL

データベース: SIEM ホスト: test ポート: 5432

ユーザ名: パスワード:

接続設定を保存する

接続

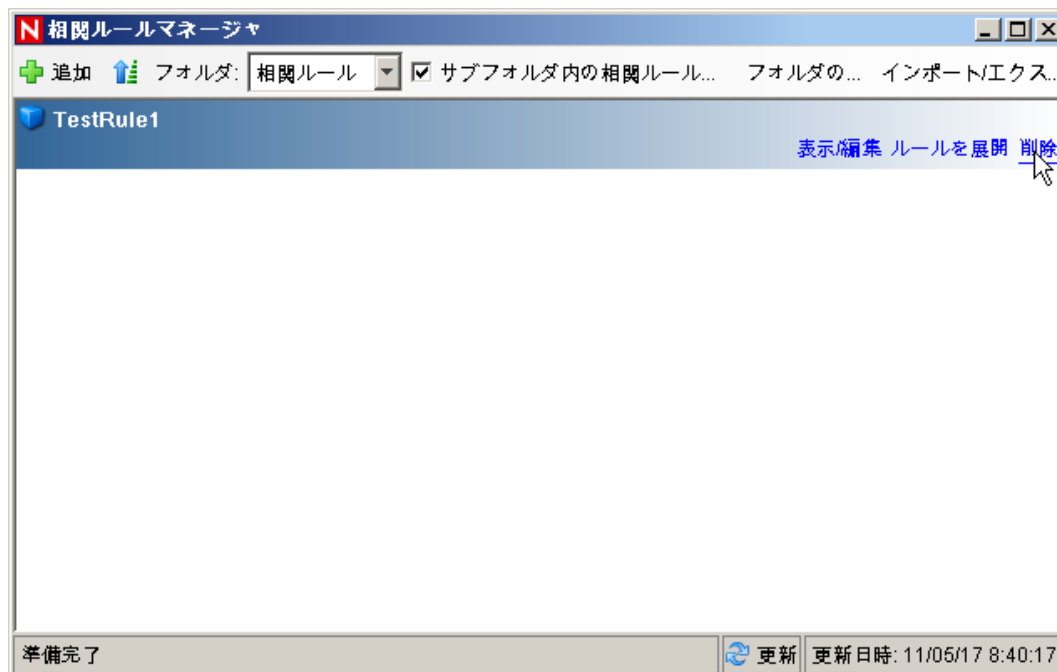
- 44 各タブをクリックして、アクセスできることを確認します。
- 45 Sentinel データマネージャを閉じます。

以上の手順をすべてエラーなしで実行したら、Sentinel システムのインストールの基本的な確認が完了しました。

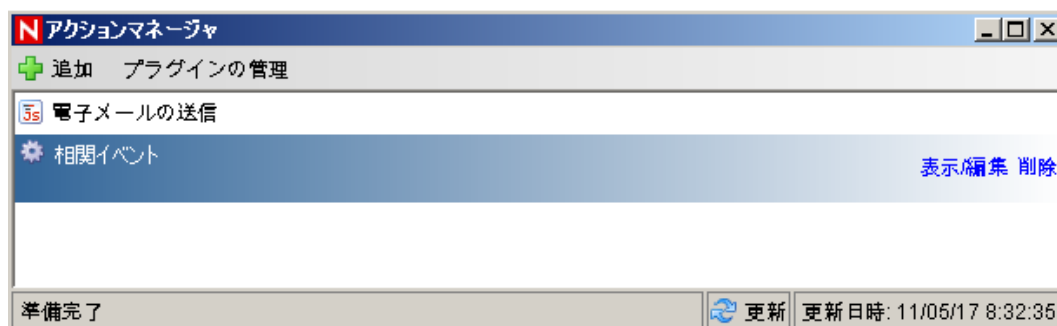
6.2 テスト後のクリーンアップ

システム確認を完了した後、テスト用に作成したオブジェクトを削除する必要があります。

- 1 インストール中に指定した Sentinel 管理者ユーザを使用してシステムにログインします (デフォルトでは admin)。
- 2 [Correlation] タブを選択します。
- 3 相関エンジンマネージャを開きます。
- 4 相関エンジンマネージャで [TestRule1] を右クリックし、[Undeploy] を選択します。
- 5 相関ルールマネージャを開きます。
- 6 [TestRule1] を選択し、[削除] をクリックします。



- 7 [Tools] > [Action Manager] を選択して [Action Manager] ウィンドウを表示します。
- 8 [CorrelatedEvent] アクションを選択し、[削除]、[はい] の順にクリックして削除を確認します。



- 9 [イベントソースの管理] メニューを選択し、[ライブビュー] を選択します。
- 10 グラフィカルイベントソース階層で、[General Collector] を右クリックし、[停止] を選択します。
- 11 [イベントソースの管理] ウィンドウを閉じます。
- 12 [インシデント] タブをクリックします。
- 13 インシデントビューマネージャを開きます。
- 14 [TestIncident1] を選択し、右クリックして [削除] を選択します。

6.3 実際のデータの使用

実際のデータで始める前に、環境に適したコレクタのインポートと設定、独自のルールの設定、iTRAC ワークフローの構築などを行う必要があります。詳細については、『*Sentinel Rapid Deployment User Guide*』を参照してください。Sentinel ソリューションパックを使用すると、すばやく始めることができます。詳細については、[Sentinel コンテンツページ \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html) を参照してください。

Sentinel Rapid Deployment のアンインストール

7

- ◆ [87 ページのセクション 7.1 「Sentinel Rapid Deployment サーバのアンインストール」](#)
- ◆ [87 ページのセクション 7.2 「リモートコレクタマネージャと Sentinel クライアントアプリケーションのアンインストール」](#)

7.1 Sentinel Rapid Deployment サーバのアンインストール

- 1 root ユーザとしてログインします。
- 2 setup ディレクトリに移動します。
`cd <install_directory>/setup`
- 3 `uninstall.sh` スクリプトを実行し、Sentinel Rapid Deployment サーバをアンインストールします。
`./uninstall.sh`
Sentinel Rapid Deployment が完全に削除されることを伝えるメッセージがスクリプトによって表示されます。
- 4 Sentinel Rapid Deployment サーバのアンインストールと同時にユーザを保持するか削除するか指定します。ユーザを削除するには「y」を押し、ユーザを保持するには「n」を押しします。
- 5 Sentinel Rapid Deployment サーバのアンインストールと同時にグループを保持するか削除するか指定します。グループを削除するには「y」を押し、グループを保持するには「n」を押しします。
- 6 アンインストールするには「y」と入力し、アンインストールを終了するには「n」と入力します。

7.2 リモートコレクタマネージャと Sentinel クライアントアプリケーションのアンインストール

- ◆ [87 ページのセクション 7.2.1 「Linux」](#)
- ◆ [88 ページのセクション 7.2.2 「Windows」](#)
- ◆ [89 ページのセクション 7.2.3 「アンインストール後の手順」](#)

7.2.1 Linux

- 1 root としてログインします。
- 2 (オプション) コレクタマネージャをアンインストールする場合、次の手順で Sentinel Rapid Deployment のサービスを停止します。
`<install_directory>/bin/sentinel.sh stop`

- 3 次の場所へ移動します。
`<install_directory>_uninst`

- 4 次のいずれかを実行します。

モード	コマンド
GUI	<code>./uninstall.bin</code> 88 ページのステップ 5 に進んでください。
コンソール	<code>./uninstall.bin -console</code> 画面の指示に従って操作を続行します。

- 5 言語を選択して [OK] をクリックします。
- 6 Sentinel UninstallShield ウィザードで、[次へ] をクリックします。
- 7 アンインストールするコンポーネントを選択して、[次へ] をクリックします。
- 8 実行中の Sentinel アプリケーションがすべて停止したことを確認し、[次へ] をクリックします。
アンインストールを選択した機能の概要が表示されます。
- 9 [アンインストール] をクリックします。
- 10 [終了] をクリックします。

7.2.2 Windows

- 1 管理者ユーザとしてログインします。
- 2 (オプション) コレクタマネージャをアンインストールする場合、次の手順で Sentinel Rapid Deployment のサービスを停止します。
`<install_directory>\bin\sentinel.bat stop`
- 3 次のいずれかを実行します。
- [スタート] > [すべてのプログラム] > [Sentinel] > [Sentinel のアンインストール] を選択します。
 - [スタート] > [ファイル名を指定して実行] を選択し、「`<Install_Directory>_uninst`」と入力してから [uninstall.exe] をダブルクリックします。
- 4 言語を選択して [OK] をクリックします。
Sentinel Rapid Deployment UninstallShield ウィザードが表示されます。
- 5 [次へ] をクリックします。
- 6 アンインストールするコンポーネントを選択して、[次へ] をクリックします。
- 7 実行中の Sentinel アプリケーションがすべて停止したことを確認し、[次へ] をクリックします。
アンインストールを選択した機能の概要が表示されます。
- 8 [アンインストール] をクリックします。
- 9 システムを再起動することを選択し、[終了] をクリックします。

7.2.3 アンインストール後の手順

アプリケーションのアンインストール後に特定のシステム設定が残りますが、これらは手作業で削除できます。これらの設定は、特に Sentinel のアンインストールでエラーが発生した場合に、Sentinel のクリーンインストールを実行する前に削除する必要があります。

注: Linux では、コレクタマネージャまたはクライアントアプリケーションをアンインストールしても、Sentinel 管理者ユーザがオペレーティングシステムから削除されません。必要に応じて、このユーザを手作業で削除する必要があります。

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

Linux

- 1 root としてログインします。
- 2 Sentinel ソフトウェアがインストールされている `<Install_Directory>` の内容を削除します。
- 3 `/etc/init.d` ディレクトリに次のファイルがある場合は削除します。
sentinel

これは、コレクタマネージャがインストールされている場合にのみ適用されます。
- 4 Sentinel 管理者ユーザ (デフォルトでは `esecadm`) としてログインしているユーザがないことを確認してから、ユーザ、ホームディレクトリ、および `esec` グループを削除します。
 - ◆ `userdel -r esecadm` を実行します。
 - ◆ `groupdel esec` を実行します。
- 5 `/root/InstallShield` ディレクトリを削除します。
- 6 `/etc/profile` の `InstallShield` セクションを削除します。
- 7 マシンを再起動します。

Windows

- 1 `%CommonProgramFiles%\InstallShield\Universal` フォルダと、その内容をすべて削除します。
- 2 `<Install_Directory>` フォルダ (デフォルトでは `C:\Program Files\Novell\Sentinel6`) を削除します。
- 3 [マイコンピュータ] を右クリックし、[プロパティ] > [詳細設定] タブの順にクリックします。
- 4 [環境変数] ボタンをクリックします。
- 5 存在する場合は、以下の変数を削除します。
 - ◆ `ESEC_HOME`
 - ◆ `ESEC_VERSION`
 - ◆ `ESEC_JAVA_HOME`
 - ◆ `ESEC_CONF_FILE`
 - ◆ `WORKBENCH_HOME`

- 6 Path 環境変数で、Sentinel のインストールフォルダを指すエントリを削除します。
- 7 デスクトップからすべての Sentinel のショートカットを削除します。
- 8 [スタート] メニューから、[スタート] > [プログラム] > [Sentinel] のショートカットフォルダを削除します。
- 9 マシンを再起動します。

Sentinel Rapid Deployment のホスト名の更新

A

- ◆ 91 ページのセクション A.1 「サーバ」
- ◆ 91 ページのセクション A.2 「クライアントアプリケーション」

A.1 サーバ

Sentinel サーバでは、ホスト名の変更は実行時またはインストール時に自動的に更新されます。ホスト名の更新後にサーバが正常に動作しない場合、次の点を手作業で確認する必要があります。

- ◆ すべての `jnlp` ファイルと `configuration.xml` ファイルが Sentinel の再起動時に更新されている。
- ◆ `sentinel_host` データベーステーブルの `hostname` エントリが更新されている。
- ◆ `<install_directory>/config/configuration.xml` ファイルにあるローカルループ (`localhost` または `127.0.0.1`) に対するすべての参照が影響を受けていない。

A.2 クライアントアプリケーション

クライアントアプリケーションでは、次の場所にあるサーバのホスト名または IP アドレスを、正しいサーバを指すように手作業で変更する必要があります。

- ◆ `<install_directory>/config/configuration.xml`。

Sentinel Control Center とソリューションデザイナーではこの情報を使用します。

- ◆ `<install_directory>/config/SentinelPreferences.properties` ファイルに指定されているヘルプの URL。
- ◆ 次のコマンドを実行して、`sdm.connect` ファイルのホスト名を更新します。

```
sdm -action saveConnection -server <postgresql> -host <hostIpaddress/  
hostName> -port <portnum> -database <databaseName/SID> [-driverProps  
<propertiesFile> {-user <dbUser> -password <dbPass> | -winAuth} -  
connectFile <filenameToSaveConnection>
```


トラブルシューティングのヒント

B

ここでは、Sentinel Rapid Deployment のインストールに関する一部の問題解決に役立つ、トラブルシューティングのヒントについて説明します。

- ◆ 93 ページのセクション B.1 「無効な資格情報を入力するとデータベースの認証が失敗する」
- ◆ 93 ページのセクション B.2 「Sentinel Web インタフェースが起動しない」
- ◆ 94 ページのセクション B.3 「UAC が有効な場合にリモートコレクタマネージャが Windows 2008 で例外をスローする」
- ◆ 95 ページのセクション B.4 「イメージ作成されたコレクタマネージャに UUID が作成されない」

B.1 無効な資格情報を入力するとデータベースの認証が失敗する

一般的な原因：LDAP 認証向けに Sentinel Rapid Deployment サーバを設定している際、無効な LDAP サーバのホスト名または IP アドレスを入力するとデータベース認証が失敗します。

アクション：有効な LDAP サーバのホスト名または IP アドレスが入力されているか確認します。

B.2 Sentinel Web インタフェースが起動しない

一般的な原因：Sentinel Rapid Deployment をインストールしたマシン上で、Identity Audit プロセスが実行中であるか、または Sentinel 6.1 Rapid Deployment のアンインストールが完了していません。

アクション：Sentinel Rapid Deployment と Novell Identity Audit は同じマシンにインストールできません。Identity Audit がインストールされているマシンに Sentinel Rapid Deployment をインストールする前に、Identity Audit を完全にアンインストールしてください。

Identity Audit プロセスが完全に停止されていないと、Identity Audit のアンインストールが適切に完了されません。この場合、Sentinel Rapid Deployment のインストール中、またはそのアプリケーションの起動時に競合が発生する可能性があります。

- 1 次のコマンドを実行して、Identity Audit サービスを停止します。

```
/etc/init.d/identity_audit stop
```

- 2 次のコマンドを実行して、すべての Identity Audit プロセスが動作を停止していることを確認します。

```
ps -ef | grep novell
```

- 3 必要に応じて、残りのプロセスを手動で停止します。

```
kill -9 pid
```

4 必要な root 権限を使用して、Identity Audit をアンインストールします。

詳細については、『Identity Audit ガイド (<http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/>)』を参照してください。

B.3 UAC が有効な場合にリモートコレクタマネージャが Windows 2008 で例外をスローする

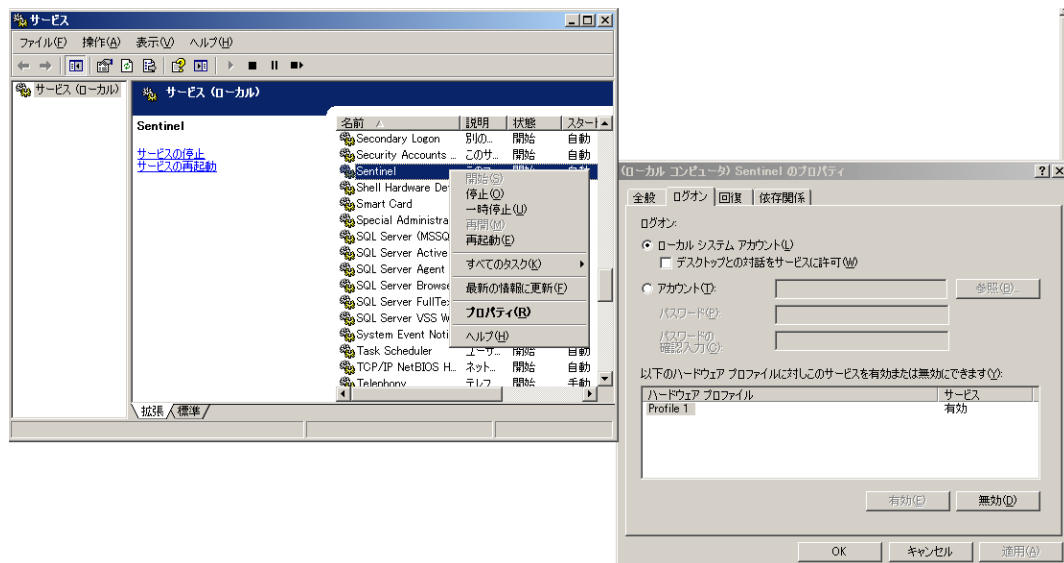
問題 : Administrator グループに属するユーザでログインします。端末プロンプトで setup.bat コマンドを実行してコレクタマネージャをインストールします。システムを再起動するか、コレクタマネージャサービスを手作業で開始してから、同じユーザの資格情報でログインします。次に挙げるコレクタマネージャの機能に影響を与える例外は、collector_manager0.0.log にログが記録されます。

- ◆ マップが初期化されない。
- ◆ コレクタマネージャ (Win2008) マシンのファイルシステムにあるイベントソースファイルを、ファイルコネクタを使用して選択することができない。

一般的な原因 : コレクタマネージャが、Windows 2008 SP1 Standard Edition 64 ビットにインストールされている。デフォルトでは、マシンのユーザアクセス制御 (UAC) が [Enabled] に設定されています。

アクション : Sentinel Rapid Deployment サービスのログオン所有者を現在のユーザに変更します。デフォルトでは、ログオン所有者はローカルシステムアカウントに設定されています。デフォルトオプションを変更するには：

- 1 services.msc を実行して、[サービス] ウィンドウを開きます。
- 2 [Sentinel] を右クリックして [プロパティ] を選択します。



- 3 [Sentinel Properties (Sentinel のプロパティ)] ウィンドウで、[ログオン] タブを選択します。
- 4 [アカウント] を選択し、コレクタマネージャをインストールするために使用した現在のユーザの資格情報を指定します。

B.4 イメージ作成されたコレクタマネージャに UUID が作成されない

コレクタマネージャサーバのイメージを作成し(たとえば、ZenWorks イメージングを使用)、別のマシンにそのイメージを復元する場合、Sentinel Rapid Deployment はコレクタマネージャの新しいインスタンスを一意的に識別しません。これは UUID が重複するために発生します。

新しくインストールしたコレクタマネージャのシステム上で次の手順を実行し、UUID を生成する必要があります。

- 1 <install_directory>/data フォルダにある host.id または sentinel.id ファイルを削除します。
- 2 コレクタマネージャを再起動します。
コレクタマネージャが自動的に UUID を生成します。

PostgreSQL データベースのメンテナンスに関するベストプラクティス

C

データベースを微調整してデータベースサーバのパフォーマンスを向上させることができます。このセクションに記載されている制限は、おおよその推奨事項です。これらはハード制限ではありません。ただし、極めて動的なシステムでは、バッファを組み込んで、システムに成長の余地を与えることをお勧めします。

- ◆ 97 ページのセクション C.1 「メモリの環境設定パラメータの変更」
- ◆ 98 ページのセクション C.2 「回収 / 分析の I/O に対する影響の低減」

C.1 メモリの環境設定パラメータの変更

PostgreSQL データベースサーバを微調整するには、`<install_dir>/3rd party/postgresql/data/postgresql.conf` ファイルに含まれる次のメモリ環境設定パラメータを変更します。

- ◆ **shared_buffers:** データをキャッシュするため、どのくらいのメモリが PostgreSQL 専用を与えられているかを決定します。パフォーマンスを向上させるには、このパラメータの値を利用可能な RAM の 4 分の 1 に設定します。
- ◆ **effective_cache_size:** オペレーティングシステムによるディスクのキャッシングやデータベース内のディスクのキャッシングに使用できるメモリの量を決定します。オペレーティングシステムや他のアプリケーションによって使用される量を考慮してこのパラメータのサイズを見積もることができます。このパラメータには、利用可能なシステムメモリの合計の半分を割り当てることができます。
- ◆ **work_mem:** 一時ディスクファイルに切り替わるまで内部のソート操作とハッシュテーブルが使用するメモリの量を決定します。値はキロバイト単位で指定されています。デフォルト値は 1024KB(1MB) です。

複雑なクエリの場合、複数のソートまたはハッシュ操作が並行して実行される可能性があります。各操作では、データを一時ディスクファイルに格納する前に、`work_mem` に指定された値までメモリが使用されます。Sentinel Rapid Deployment システム上でより多くのレポートの実行をスケジュールする場合、この値は 500MB ~ 1GB の間で設定します。

- ◆ **maintenance_work_mem:** VACUUM、CREATE INDEX、および ALTER TABLE ADD FOREIGN KEY などのデータベース保守の操作で使用されるメモリの量を決定します。値はキロバイト単位で指定されています。デフォルト値は 16384KB (16MB) です。

設定値を大きくすると、不要領域を回収するパフォーマンスやデータベースのダンプを復元するパフォーマンスを改善できる可能性があります。Sentinel Rapid Deployment を操作するにはデフォルト値で十分なので、このパラメータは変更しないでください。

C.2 回収 / 分析の I/O に対する影響の低減

PostgreSQL データベースのパフォーマンスは、次のいずれかの方法で改善できます。

- ◆ 次の 2 つのパラメータは、自動回収操作を制御し、Sentinel Rapid Deployment サーバのインストール時にはデフォルトでコメントアウトされているので、コメントアウトを解除して値を設定する必要があります。
 - ◆ **vacuum_cost_delay:** コスト制限を超過した場合にプロセスがスリープする期間を決定します。この値は、たとえば 100 に設定できます。
 - ◆ **vacuum_cost_limit:** 回収プロセスがスリープするまでの累積コストを決定します。この値は、たとえば 10000 に設定できます。これらのパラメータ値をゼロ以外の値に設定すると、回収と分析命令が一般的なデータベースの動作に対して与える I/O の影響を低減できます。回収は以前よりも時間がかかるので、レポートの実行時には、パフォーマンスへの影響としては取るに足らない程度である可能性があります。
- ◆ デフォルトでは、autovacuum プロセスが true に設定されており、ディスク領域を回復しプランナーの統計情報を更新するために定期的に行われます。データベースのサイズが増加すると、autovacuum はすべてのデータベースオブジェクトを維持できなくなります。そのような場合、パフォーマンスが遅いのであれば、cron ジョブとして AnalyzePartitions.sh スクリプトを実行します。この cron ジョブは、Sentinel Rapid Deployment のプロセスを所有するユーザが設定する必要があります。

例：

```
30 11 * * * $ESEC_HOME/bin/AnalyzePartitions.sh
```

各要素の内容は次のとおりです。

- ◆ 30 は時間 (分単位) です。
- ◆ 11 は時間 (時単位) です。
- ◆ ESEC_HOME はデータベースの絶対パスです。

この例では、スクリプトは毎日 11:30 に実行されます。

- ◆ レポート作成中にアーカイブが実行されないようにスケジュールしてください。両方のプロセスを一緒にスケジュールすると、PostgreSQL のバグのためにレポート作成が待ち状態になり、アーカイブジョブの完了後にデータの処理を開始します。この変更は、データベースのパフォーマンスに影響を与えます。