NetIQ Sentinel 7.1

インストールと設定ガイド

June 2013

保証と著作権

NetIQ Sentinel は米国特許番号 05829001 によって保護されています。

本書および本書に記載されているソフトウェアには、ライセンス契約または守秘契約が適用され、これらの条項の下に提供されます。上記ライセンス契約または守秘契約に明示されている場合を除き、NetIQ Corporation は、本書および本書に記載されているソフトウェアを「現状のまま」提供するものとし、明示的、黙示的を問わず、商品性または特定目的への適合性に対する黙示的な保証を含め、いかなる保証も行いません。州によっては、明示的、黙示的を問わず、特定の取引に関する保証の否認が認められていないため、この記述が適用されない場合もあります。

明確にするために、すべてのモジュール、アダプタ、またはそれに類する要素 (「モジュール」) は、そのモジュールが関連または相互作用する NetIQ 製品またはソフトウェアの当該バージョンのエンドユーザライセンス契約の条項と条件に基づいてライセンスが供与されます。また、モジュールを接続、複製、または使用することで、これらの条項に従うことになります。エンドユーザライセンス契約の条項に同意しない場合、モジュールを接続、使用、または複製する権利はありません。また、モジュールのすべての複製を破棄し、詳細については NetIQ にお問い合わせいただく必要があります。

本書および本書に記載されているソフトウェアは、法律によって認められた場合を除き、NetIQ Corporation が書面をもって事前に許可しない限り、貸出、販売、譲渡することはできません。上記ライセンス契約または守秘契約に明示されていない限り、NetIQ Corporation の事前の書面による同意がない場合は、本書および本書に記載されているソフトウェアのいかなる部分も、電子上、あるいは機器上を問わず、いかなる方法、形式においても再現したり、情報取得システムに保存または転送することは禁じられています。本書に記載されている会社名、個人名、データは引用を目的として使用されており、実際の会社、個人、およびデータを示していないことがあります。

本書は技術的な誤りおよび誤植を含むことがあります。本書の情報には定期的に変更が加えられます。上記の変更は、本書の新版に組み込まれることがあります。NetIQ Corporation は、本書に記載されているソフトウェアに対して、随時改良、変更を行うことができます。

米国政府の制限付き権利 : ソフトウェアおよび文書が、米国政府または米国政府の元請人または下請人 (階層を問わず) によって直接または間接的に取得される場合は、48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) および 48 C.F.R. 2.101 および 12.212 (for non-DOD acquisitions) に基づき、ソフトウェアまたは文書の使用、修正、再生、リリース、実行、表示、開示などに関する政府の権利は、このライセンス契約に記載されている商用ライセンスの権利および制限に全面的に従うものとします。

目次

本書およびライブラリについて

本『*インストールと設定ガイド*』では、NetIQ Sentinel の概要を示し、Sentinel をインストールおよび設定する方法について説明します。

本書の読者

このガイドは、Sentinel 管理者およびコンサルタントを対象としています。

ライブラリに含まれるその他の情報

ライブラリには次のマニュアルが含まれています。

Administration Guide

Sentinel の展開を管理するために必要な管理情報および管理作業を説明します。

User Guide

Sentinel に関する概念情報を提供します。また、このマニュアルでは、ユーザインタフェースの概要を説明し、さまざまなタスクを手順を追って説明しています。

NetIQ 社について

当社はグローバルなエンタープライズソフトウェア企業であり、お客様の環境において絶えず挑戦となる変化、複雑さ、リスクという 3 つの要素に焦点を当て、それらをお客様が制御するためにどのようにサポートできるかを常に検討しています。

当社の観点

変化に適応すること、複雑さとリスクを管理することは普通のことである

実際、直面するあらゆる課題の中でも、これらが、物理的、仮想上、およびクラウドのコンピューティング環境を安全に評価し、監視し、管理するために必要な制御能力を脅かす最大の要因かもしれません。

より良くより速い基幹事業サービスを可能にする

当社は、IT 組織に可能な限りの制御能力を付与することが、よりタイムリーでコスト効率の高いサービス提供を実現する唯一の方法だと信じています。組織が継続的な変化を遂げ、組織を管理するために必要なテクノロジが実質的に複雑さを増していくにつれ、変化と複雑さという圧力はこれからも増え続けていくことでしょう。

当社の理念

単なるソフトウェアではなく、インテリジェントなソリューションを販売する

確かな制御手段を提供するために、まずお客様の IT 組織が日々従事している現実のシナリオを把握することに努めます。そのようにしてのみ、実証済みで測定可能な結果を成功裏に生み出す、現実的でインテリジェントな IT ソリューションを開発することができます。これは単にソフトウェアを販売するよりもはるかにやりがいのあることです。

当社の情熱はお客様の成功を推し進めること

お客様が成功するためにわたしたちには何ができるかということが、わたしたちのビジネスの核心にあります。製品の着想から展開まで、当社は次のことを念頭に置いています。お客様は既存資産とシームレスに連動して動作する IT ソリューションを必要としており、展開後も継続的なサポートとトレーニングを必要とし、変化を遂げるときにも共に働きやすいパートナーを必要としている。究極的に、お客様の成功こそがわたしたちの成功なのです。

当社のソリューション

- ID およびアクセスのガバナンス
- アクセス管理
- セキュリティ管理
- システムおよびアプリケーション管理

- ワークロード管理
- サービス管理

セールスサポートへのお問い合わせ

製品、価格、および機能についてのご質問は、地域のパートナーへお問い合わせください。パートナーに連絡できない場合は、弊社のセールスサポートチームへお問い合わせください。

各国共通：	www.netiq.com/about_netiq/officelocations.asp
米国およびカナダ：	1-888-323-6768
電子メール：	info@netiq.com
Web サイト：	www.netiq.com

テクニカルサポートへのお問い合わせ

特定の製品に関する問題については、弊社のテクニカルサポートチームへお問い合わせください。

各国共通：	www.netiq.com/support/contactinfo.asp
北米および南米：	1-713-418-5555
ヨーロッパ、中東、アフリカ：	+353 (0) 91-782 677
電子メール：	support@netiq.com
Web サイト：	www.netiq.com/support

マニュアルサポートへのお問い合わせ

弊社の目標は、お客様のニーズを満たすマニュアルの提供です。改善のためのご提案は、www.netiq.com/documentation に掲載されている本マニュアルの HTML 版で、各ページの下にある［**コメントを追加**］をクリックしてください。Documentation-Feedback@netiq.com 宛てに電子メールを送信することもできます。貴重なご意見をぜひお寄せください。

オンラインユーザコミュニティへのお問い合わせ

NetIQ のオンラインコミュニティである Qmunity は、他のユーザや NetIQ のエキスパートとやり取りできるコラボレーションネットワークです。より迅速な情報、有益なリソースへの役立つリンク、NetIQ エキスパートとのやり取りを提供する Qmunity は、信頼のおける IT 投資が持つ可能性を完全に実現するために必要な知識を習得するために役立ちます。詳細については、http://community.netiq.com を参照してください。

Sentinel について

このセクションでは、Sentinel の概要および Sentinel が提供するイベント管理ソリューションについて詳しく説明します。

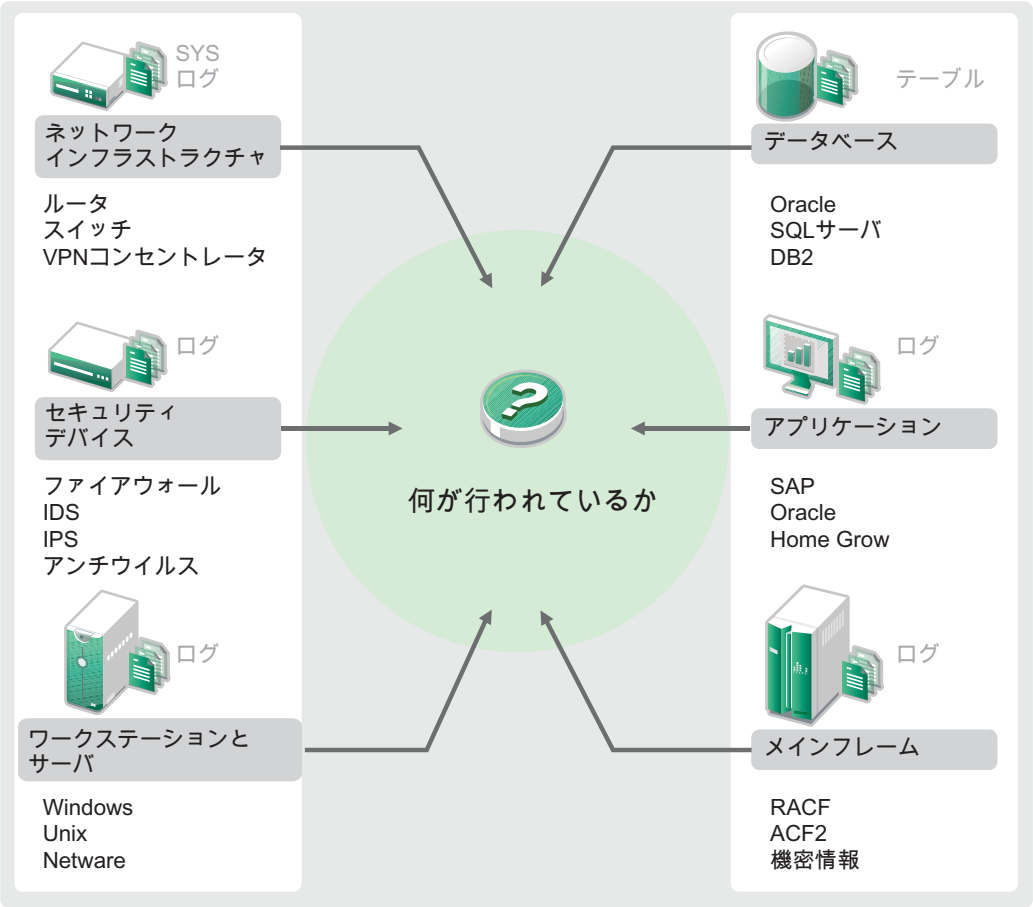
1 Sentinel の概要

Sentinel は、セキュリティ情報とイベント管理のソリューションおよびコンプライアンスモニタリングソリューションです。Sentinel は、最も複雑な IT 環境を自動的にモニタリングし、IT 環境を保護するのに必要なセキュリティを提供します。

1.1 IT 環境のセキュリティ保護の課題

IT 環境のセキュリティ保護は、環境が複雑であるため挑戦となります。さまざまなアプリケーション、データベース、メインフレーム、ワークステーション、およびサーバが多くあり、それらすべてにイベントのログがあります。また、セキュリティデバイスとネットワークインフラストラクチャデバイスがあり、それらすべてに IT 環境で発生したことを記録するログが含まれています。

図 1-1 *環境で発生していること*



問題を困難にしているのは、次のような状況です。

- IT 環境にデバイスがたくさんある
- ログの形式が異なる
- ログがサイロ式に格納されている
- ログで生成される情報量
- すべてのログを手動で解析しなければ、誰が何を実行したか特定できない

ログデータを活用するには、次のことを行える必要があります。

- データを収集する
- データを集約する
- 異種のデータを標準化してイベントにし、簡単に比較できるようにする
- イベントを標準規制に対応付けする
- データを分析する
- 複数のシステム間のイベントを比較し、セキュリティの問題があるかどうかを判断する
- データが基準を外れているときに通知を送信する

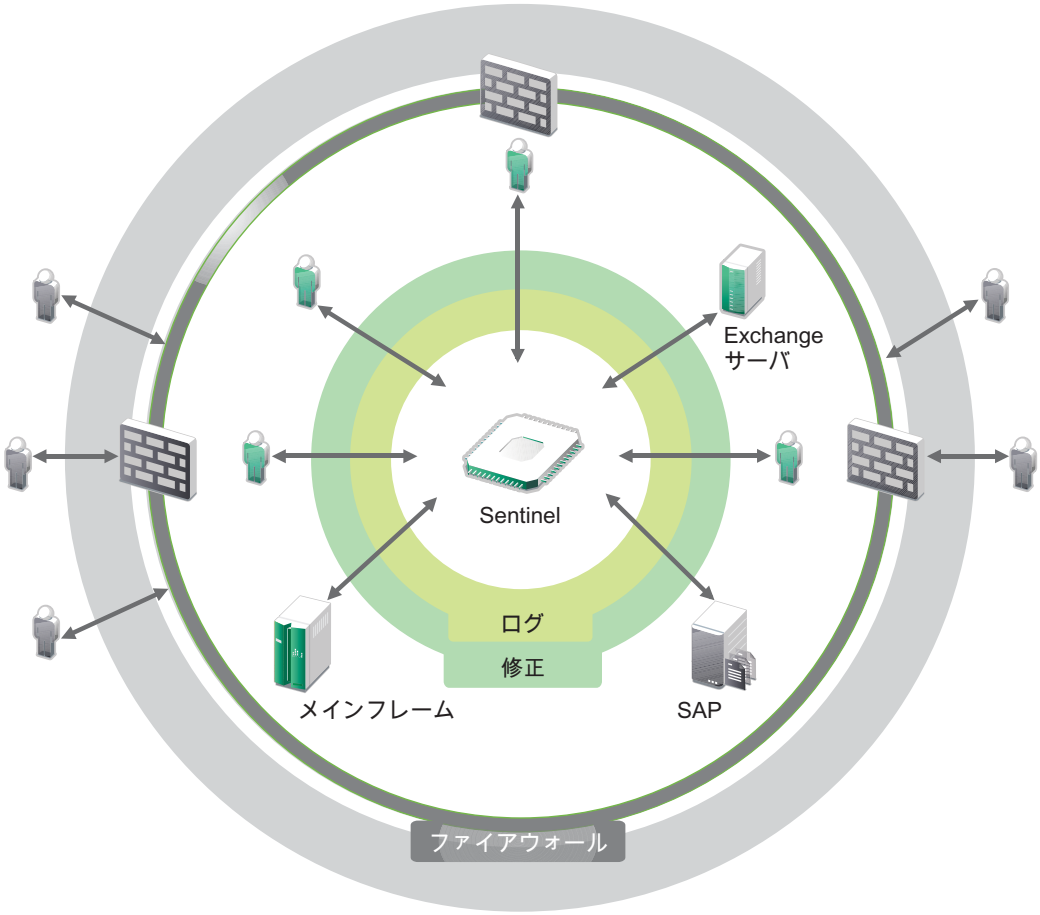
- ビジネスポリシーに従って通知に対する行動をとる
- コンプライアンスの証明のためにレポートを生成する

IT 環境をセキュリティ保護するうえでの課題を把握したら、企業システムを、ユーザのために、そしてユーザから保護する方法を見極める必要があります。その際、ユーザを悪意あるユーザとして扱ったり、ユーザの生産性に影響を与えたりすることなく行う必要があります。Sentinel がソリューションを提供します。

1.2 Sentinel が提供するソリューション

Sentinel は企業のセキュリティの中枢神経系として動作します。アプリケーション、データベース、サーバ、ストレージ、セキュリティデバイスなどのインフラストラクチャ全体からデータを取り込みます。データを分析して相関させ、データに自動または手動で対処できるようにします。

図 1-2 *Sentinel が提供するソリューション*



その結果、任意の時点で、IT 環境で生じている事柄を知ることができ、特定のアクションで使われたリソースと、そのアクションを実行した人物を結び付けることができます。これにより、ユーザの操作を特定し、コントロールを効果的に監視できます。その人物が内部者であるかに関係なく、その人物により実行されたすべてのアクションを結びつけて、損害が発生する前に不正な操作を明らかにすることができます。

Sentinel では、以下のコスト効率の高い方法でこれを実行します。

- 単一のソリューションを使用して、複数の規制にまたがる IT コントロールに対処する .
- ネットワーク環境で行われるはずのことと実際に行われていることの間にある知識のギャップを埋める
- 組織でセキュリティコントロールに関する文書化、監視、報告を行っていることを監査担当者および監督機関に実証する
- すぐに使えるコンプライアンスモニタリングおよびレポーティングプログラムを提供する
- 組織のコンプライアンスプログラムおよびセキュリティプログラムの有効性を継続的に評価するために必要な可視性とコントロールを得る

Sentinel では、ログの収集、分析、およびレポーティングプロセスが自動化されるので、IT コントロールが効果的に脅威の検出と監査要件をサポートします。Sentinel では、セキュリティイベント、コンプライアンスイベント、IT コントロールの自動モニタリングが提供されているため、セキュリティ違反またはコンプライアンス違反イベントが発生した場合に、即座に対処することができます。また、Sentinel では、環境に関するサマリ情報を簡単に収集できるため、セキュリティに対する全般的な方針を重要な利害関係者に伝達できます。

2 Sentinel の動作原理

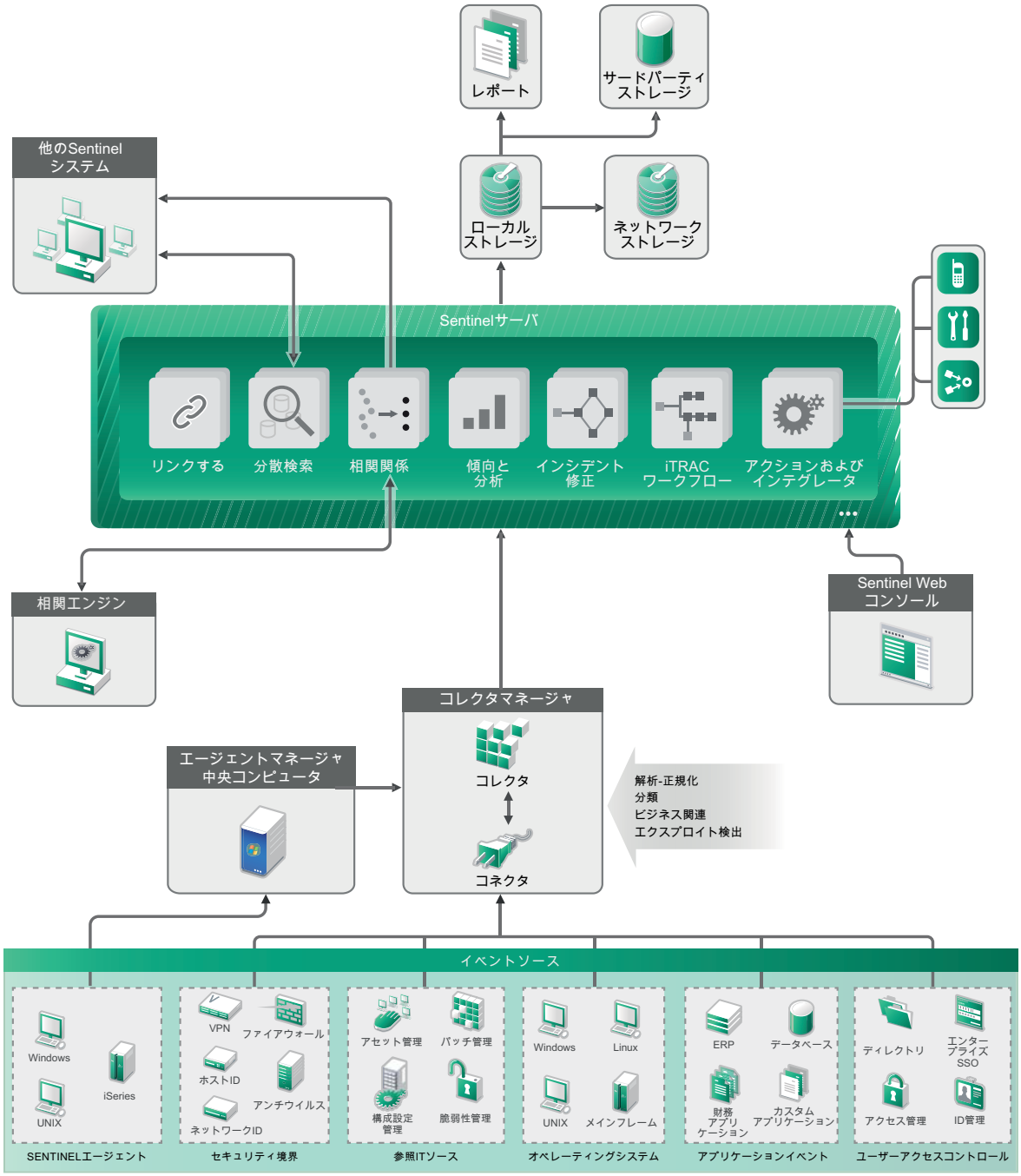
Sentinel では、IT 環境全体のセキュリティ情報とイベントを継続的に管理することで、完全なモニタリングソリューションを提供します。

Sentinel は次の処理を行います。

- IT 環境におけるすべての異なるイベントソースからログ、イベント、およびセキュリティ情報を収集します。
- 収集したログ、イベント、およびセキュリティ情報を共通の形式に正規化します。
- 柔軟でカスタマイズ可能なデータ保持ポリシーを使用して、ファイルベースのデータストアにイベントを格納します。
- Sentinel Log Manager を含む複数の Sentinel システムを階層的にリンクする機能を提供します。
- ローカルの Sentinel サーバはもとより、世界中に分散している Sentinel サーバでもイベントを検索できる機能を提供します。
- 統計分析を実行してベースラインを定義し、次にベースラインと発生中の事象を比較し、未知の問題が発生していないかどうかを判断します。
- 指定された期間の類似または比較可能なイベントのセットを相関させて、パターンを特定します。
- 対応管理および追跡を効率的に行うため、イベントをインシデントにまとめます。
- リアルタイムおよび履歴イベントに基づいたレポートを提供します。

次の図は、Sentinel がどのように動作するのかを示しています。

図 2-1 Sentinel のアーキテクチャ



以下のセクションでは、Sentinel コンポーネントについて詳しく説明します。

- 21 ページのセクション 2.1「イベントソース」
- 21 ページのセクション 2.2「Sentinel イベント」
- 23 ページのセクション 2.3「コレクタマネージャ」
- 24 ページのセクション 2.4「エージェントマネージャ」
- 24 ページのセクション 2.5「相関」

2.1 イベントソース

Sentinel では、IT 環境における多くの異なるソースからセキュリティ情報とイベントを収集します。このようなソースはイベントソースと呼ばれます。イベントソースはネットワーク上に存在する各種アイテムであったりします。

セキュリティの境界 : ユーザ環境にセキュリティ境界を作成するために使用するハードウェアやソフトウェアを含むセキュリティデバイス (ファイアウォール、IDS、および VPN など)。

オペレーティングシステム : ネットワークで稼動中の各オペレーティングシステムからのイベント。

参照用 IT ソース : アセット、パッチ、環境設定、および脆弱性を保守および追跡するのに使用するソフトウェア。

アプリケーションイベント : ネットワーク内にインストールされているアプリケーションから生成されるイベント。

ユーザアクセス制御 : ユーザによる会社のリソースへのアクセスを許可するアプリケーションまたはデバイスから生成されるイベント。

2.2 Sentinel イベント

Sentinel は、デバイスから情報を受信し、この情報をイベントと呼ばれる構造に正規化し、そのイベントを分類してから処理用に送信します。イベントに分類情報 (Taxonomy) を追加することで、異なった形でイベントをレポートするシステム間でのイベントの比較をより簡単に行えます。例として、認証の失敗などが挙げられます。イベントは、リアルタイム表示、相関エンジン、ダッシュボード、およびバックエンドサーバによって処理されます。

イベントは 200 を超えるフィールドで構成されます。イベントフィールドの種類と目的はさまざまです。重大度、重大性、宛先 IP、宛先ポートなど、定義済みのフィールドがいくつかあります。構成可能なフィールドが 2 種類あります。予約済みフィールドは、将来の拡張のために Sentinel が内部で使用します。顧客フィールドは、顧客が拡張に使用します。

名前を変更することで、フィールドの目的を再設定できます。フィールドのソースは、外部 (デバイスまたは対応するコレクタによって明示的に設定されます)、または参照の場合があります。参照フィールドの値は、マッピングサービスを使用して 1 つ以上の他のフィールドに応じて計算され

ます。たとえば、イベントの宛先 IP として指定されているアセットを含む建物の建物コードになるようフィールドを定義できます。たとえば、イベントの宛先 IP を使用する顧客定義マップを使用してマッピングサービスによってフィールドを計算することができます。

- 22 ページのセクション 2.2.1「マッピングサービス」
- 22 ページのセクション 2.2.2「マップのストリーミング」
- 22 ページのセクション 2.2.3「エクスプロイト検出 (マッピングサービス)」

2.2.1 マッピングサービス

マッピングサービスにより、システム全体にビジネス関連データを伝達する高度なメカニズムが使用できるようになります。このデータによってイベントは参照情報で充実したものとなるため、アナリストは、より適切な決定、より有用なレポートの作成、考え抜かれた相関ルールの作成を行うことができます。

ソースデバイスからの着信イベントにホストと識別情報の詳細などの情報を追加するマップを使用することで、イベントデータを充実させることができます。この追加情報は、高度な相関とレポーティングに使用できます。システムは複数の組み込みマップとユーザ定義のカスタムマップをサポートしています。

Sentinel で定義されるマップは 2 つの方法で格納されます。

- 組み込みマップは、データベースに格納され、コレクタコードで API を使用して更新され、マッピングサービスに自動的にエクスポートされます。
- カスタムマップは、CSV ファイルとして格納され、ファイルシステム上またはマップデータの環境設定 UI を使用して更新され、マッピングサービスによってロードされます。

いずれの場合も、CSV ファイルは中核となる Sentinel サーバに保存されますが、マップへの変更は、各コレクタマネージャに分散され、ローカルに適用されます。この分散処理で、マッピング動作によるメインサーバのオーバーロードを防止できます。

2.2.2 マップのストリーミング

マップサービスにはダイナミック更新モデルが採用されており、ある場所から別の場所にマップをストリーミングして、ダイナミックメモリ内に大きなスタティックマップが蓄積されるのを回避します。このストリーミング機能は、システム上の一時的な負荷に関係なく、予測されるデータ移動を着実かつ迅速に行う必要がある Sentinel などのミッションクリティカルなリアルタイムシステムで特に重要です。

2.2.3 エクスプロイト検出 (マッピングサービス)

Sentinel は、イベントデータ署名と脆弱性スキャナデータを相互参照する機能を提供します。攻撃により脆弱なシステムが悪用されそうになると直ちに、自動的にユーザに対し通知が送信されます。これは次のような機能によって実現できます。

- アドバイザのフィード
- 侵入検出
- 脆弱性スキャン
- ファイアウォール

アドバイザは、イベントデータ署名と脆弱性スキャナデータとの相互参照を提供します。アドバイザのフィードには、脆弱性と脅威、さらにイベント署名と脆弱性プラグインの正規化に関する情報が含まれます。アドバイザの詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「「Configuring Advisor」」を参照してください。

2.3 コレクタマネージャ

コレクタマネージャは、データ収集を管理し、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要な機能は次のとおりです。

- イベントを変換する
- マッピングサービスによってイベントにビジネスとの関連性を追加する
- イベントのグローバルフィルタリングを実行する
- イベントをルーティングする
- リアルタイム、脆弱性、アセット、または非リアルタイムデータを特定する
- ヘルスメッセージを Sentinel サーバに送信する

2.3.1 コレクタ

コレクタは、コネクタから情報を収集して正規化します。コレクタは JavaScript で記述されており、次の動作のロジックを定義します。

- 生データをコネクタから受信する。
- データを解析および正規化する。
- 反復可能なロジックをデータに適用する。
- デバイス固有のデータを Sentinel 固有のデータに変換する。
- イベントの形式設定を行う。
- 正規化、解析、および形式設定を行ったデータをコレクタマネージャに渡す。
- イベントをデバイス固有でフィルタリングする。

2.3.2 コネクタ

コネクタにより、イベントソースから Sentinel システムへの接続が提供されます。コネクタは、syslog などのイベントを取得する際は業界標準のプロトコル、データベーステーブルから読み込むには JDBC、Windows イベントログからの読み込みには WMI を、それぞれ使用します。コネクタは以下の機能を提供します。

- イベントソースからコレクタへの生イベントデータの転送。
- 接続固有のフィルタリング。
- 接続エラー処理。

2.4 エージェントマネージャ

エージェントマネージャは、次のことを可能にすることで、ホストベースのデータ収集を提供してエージェントを使用しないデータ収集を補完します。

- ネットワークから取得できないログにアクセスする。
- 厳重に管理されたネットワーク環境で運用する。
- 基幹サーバの攻撃露呈部分を制限することにより、セキュリティ体制を向上する。
- ネットワーク中断時も信頼性の高いデータ収集を行う。

エージェントマネージャによって、エージェントを展開し、エージェント設定を管理することができます。また、エージェントマネージャは Sentinel に流れ込むイベントの収集ポイントとして機能します。エージェントマネージャの詳細については、エージェントマネージャの資料を参照してください。

2.5 相関

1 件のイベントはささいに思えるかもしれませんが、他のイベントと組み合わさると潜在的な問題について警告する場合があります。Sentinel では、ユーザが作成したルールを使用してこのようなイベントを相関させ、相関エンジンに展開し、適切な対策を講じて、問題を緩和することができます。

相関関係により、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、『*NetIQ Sentinel 7.1 User Guide*』の「「Correlating Event Data」」を参照してください。

相関ルールに従ってイベントを監視するには、相関ルールを相関エンジンに展開する必要があります。ルールの条件に合ったイベントが発生すると、相関エンジンはそのパターンを記述する相関イベントを生成します。詳細については、『*NetIQ Sentinel 7.1 User Guide*』の「「Correlation Engine」」を参照してください。

2.6 セキュリティインテリジェンス

Sentinel の相関機能では、セキュリティ、コンプライアンス、またはその他の理由による既知のパターンの動作に対する機能が提供されます。セキュリティインテリジェンス機能では、通常の動作から外れた、悪意のある動作である可能性があるが、既知のパターンとは一致しない動作を検索します。

Sentinel のセキュリティインテリジェンス機能では、時系列データの統計分析を採用しており、自動化された統計エンジンまたは手動解釈用の統計データの視覚表示によって、分析者が逸脱 (アノマリー) を識別および分析することができます。詳細については、『*NetIQ Sentinel 7.1 User Guide*』の「「Analyzing Trends in Data」」を参照してください。

2.7 インシデントの修復

Sentinel には自動インシデント応答管理システムが備わっており、これ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、対応のプロセスを文書化および形式化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連携も可能になります。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。詳細については、『*NetIQ Sentinel 7.1 User Guide*』の「「Configuring Incidents」」を参照してください。

2.8 iTrac ワークフロー

iTRAC ワークフローは、企業のインシデント対応プロセスの自動化および追跡を行うための、シンプルで柔軟性のあるソリューションを提供するように設計されています。iTRAC では Sentinel の内部インシデントシステムを活用し、相関ルールまたは手動識別による識別から解決に至るまで、セキュリティやシステム上の問題を追跡できます。

ワークフローは、手動ステップと自動ステップを使用して構築できます。分岐、時間ベースのエスカレーション、およびローカル変数などの高度な機能がサポートされています。外部のスクリプトおよびプラグインとの統合により、サードパーティシステムとの柔軟なやり取りが可能になります。包括的なレポーティングにより、管理者はインシデント応答プロセスを理解し、微調整することができます。詳細については、『*NetIQ Sentinel 7.1 User Guide*』の「「Configuring iTRAC Workflows」」を参照してください。

2.9 アクションとインテグレータ

アクションは、メールの送信など、Sentinel の何らかの処理を手動または自動で実行します。アクションのトリガとなるものには、ルーティングルール、イベントやインシデント操作の手動実行、そして相関ルールがあります。Sentinel には、一連の事前定義アクションが提供されています。デフォルトのアクションを使用し必要に応じてそれらを再設定するか、新規のアクションを追加することができます。詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「「Configuring Action」」を参照してください。

アクションを単独で実行することも、インテグレータプラグインで設定したインテグレータインスタンスを利用することもできます。インテグレータプラグインは、Sentinel 修正アクションの特長と機能性を拡充します。インテグレータによって、LDAP サーバ、SMTP サーバ、SOAP サーバなどの外部システムに接続してアクションを実行することができます。詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「「Configuring Integrators」」を参照してください。

2.10 レポート

Sentinel は、収集したデータでレポートを実行する機能を提供します。Sentinel には、さまざまな種類のカスタマイズ可能なレポートが事前にパッケージされています。結果に表示するカラムを指定できるような、柔軟に作成できるレポートもあります。

PDF レポートを実行したり、スケジュールしたり、電子メールで送信したりすることができます。また、任意のレポートを検索として実行し、検索条件を絞ったり結果に対してアクションを実行したりするなど、検索の場合と同じように結果を処理することができます。地理的に異なる場所に分散している Sentinel サーバ上でレポートを実行することもできます。詳細については、『*NetIQ Sentinel 7.1 User Guide*』の「「Reporting」」を参照してください。

2.11 イベント分析

Sentinel では、重大なイベントデータを簡単に検索して分析できる強力なツールのセットが提供されています。システムは特定の種類の分析に合わせて、効率が最大限になるように調整、最適化され、1 つの種類の分析から別の分析にシームレスで簡単に移行できる方法が提供されています。

Sentinel でのイベントの調査は、ほぼリアルタイムのアクティブビューで開始する場合がよくあります。さらに高度なツールも使用できますが、アクティブビューではフィルタされたイベントストリームがサマリチャートと一緒に表示されるため、イベントの傾向とイベントデータのシンプルでおおまかな分析や、特定のイベントの識別に使用できます。時間の経過と共に、相関からの出力など、特定のクラスのデータに対して調整されたフィルタを構築します。アクティブビューは、運用とセキュリティに関する全般的な方針を示すダッシュボードとして使用できます。

さらにインタラクティブ検索を使用して、より詳細なイベントの分析を実行できます。これにより、特定のユーザや特定のシステムによる動作など、特定のクエリに関連するデータをすばやく簡単に検索して見つけることができます。イベントデータをクリックしたり、左側の絞り込みウィンドウを使用すると、簡単に目的のイベントに焦点を絞ることができます。

多数のイベントを分析する場合、Sentinel のレポーティング機能ではイベントのレイアウトに対するカスタムコントロールが提供されているため、より多くのデータを表示できます。Sentinel では検索インタフェースで構築されたインタラクティブ検索をレポーティングテンプレートに移動できるため、この移行が簡単です。そのため、多数のイベントにより適した形式で同じデータを表示するレポートを即座に作成できます。

Sentinel にはこの目的のためのテンプレートが多数含まれています。一部のテンプレートは、認証データやユーザ作成など、特定の種類の情報を表示するように調整されています。また、一部のテンプレートは汎用的なテンプレートで、レポートのグループと列をインタラクティブにカスタマイズできます。

時間の経過と共に、共通して使用するフィルタとレポートを開発して、ワークフローをより簡単にできます。Sentinel では、この情報の保存と、組織内のユーザへの配布が完全にサポートされています。詳細については、『*NetIQ Sentinel 7.1 User Guide*』を参照してください。

2.12 Sentinel データのルーティングとストレージ

Sentinel では、収集したデータのルーティング、保管、および抽出に、複数のオプションを提供しています。デフォルトでは、Sentinel は 2 つの独立した、関連するデータストリーム (解析済みデータと生データ) をコレクタマネージャから受信します。生データは、セキュアなエビデンスチェーンを提供するために、保護されたパーティションの中に即時に格納されます。解析済みデータは、定義したルールに従ってルーティングされます。フィルタリングされたり、ストレージに送信されたり、リアルタイム分析に送信されたり、外部システムにルーティングされたりします。ストレージに送信されるすべてのイベントデータは、さらにユーザ定義の保持ポリシーと突き合わされます。イベントデータはこのポリシーによって決定されるパーティションに配置され、このポリシーが定義するグルーミングポリシーに従ってイベントデータの保持と最終的な削除が行われます。

Sentinel のデータストレージは 3 層構造になっています。

- **オンラインストレージ**
  - **プライマリまたはローカルストレージ :** 迅速な書き込みと高速な取得のために最適化されています。ごく最近に収集されたイベントデータ (および頻繁に検索されるイベントデータ) はここに保管されます。

- **セカンダリまたはネットワークストレージ :** 高速な取得をサポートしながらも、スペース使用量を減らすために最適化されています。Sentinel は自動的にデータパーティションをセカンダリストレージに移行します。

注 : セカンダリストレージの使用はオプションです。データ保持ポリシー、検索、およびレポートは、それ自体がプライマリストレージとセカンダリストレージのどちらにあるか、または両方にあるかにかかわらず、イベントデータパーティションで実行されます。

- **オフラインストレージまたはアーカイブストレージ**

  パーティションを閉じた後に、閉じたパーティションのデータを廉価なマスストレージなどのオフラインストレージや、Amazon Glacier などにバックアップすることができます。必要であれば、オフラインパーティションを一時的に再インポートして、長期間の捜査分析に利用できます。

データ同期ポリシーを使用して、イベントデータとイベントデータ要約を外部データベースに抽出するように Sentinel を設定することもできます。詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「「Configuring Data Storage」」を参照してください。

Sentinel のインストール計画

このセクションでは、Sentinel をインストールする前の計画に関する考慮事項について説明します。後述のセクションで指定されていない環境設定でインストールする場合、または質問がある場合は、NetIQ テクニカルサポートまでお問い合わせください。

3 実装チェックリスト

下記のチェックリストを使って、Sentinel に関する計画、Sentinel のインストールおよび環境設定まで行うことができます。

❒	タスク	参照先
❒	Sentinel コンポーネントについて知るために、製品のアーキテクチャ情報を確認します。	13 ページのパート I「Sentinel について」
❒	Sentinel の評価版とエンタープライズ版のどちらをインストールする必要があるかを判断するために、Sentinel のライセンスを確認します。	33 ページの第 4 章「ライセンス情報について」
❒	ハードウェア構成を確認するために、使用している環境を評価します。Sentinel およびそのコンポーネントのインストール先となるコンピュータが指定された要件を満たしていることを確認します。	35 ページの第 5 章「システム要件を満たす」
❒	デフォルトでは、Sentinel にはコレクタマネージャと相関エンジンが 1 つずつ付属しています。コレクタマネージャと相関エンジンの毎秒イベント数 (EPS) を確認し、パフォーマンスと負荷分散を改善するために、コレクタマネージャと相関エンジンをさらにインストールする必要があるかどうかを判断します。	68 ページのセクション 9.1「追加のコレクタマネージャの利点」および 68 ページのセクション 9.2「相関エンジンを追加することの利点」.
❒	Sentinel をインストールします。	65 ページのパート III「Sentinel のインストール」
❒	Sentinel サーバの時刻を必ず設定してください。	103 ページの第 16 章「時刻の設定」
❒	Sentinel をインストールすると、その Sentinel リリースの時点で利用可能な Sentinel プラグインがデフォルトでインストールされます。インストール直後のプラグインを、データ収集とレポート作成の用途に合わせて設定します。	107 ページの第 17 章「付属プラグインの環境設定」.
❒	ご使用の環境で必要であれば、コレクタとコネクタを追加インストールします。	95 ページの第 13 章「コレクタとコネクタの追加インストール」.
❒	ご使用の環境で必要であれば、コレクタマネージャと相関エンジンを追加インストールします。	78 ページのセクション 11.6「追加のコレクタマネージャのインストールおよび相関エンジンのインストール」

4 ライセンス情報について

Sentinel で使用できるライセンスは数種類あります。デフォルトでは、Sentinel には評価版ライセンスが付帯しています。

4.1 評価版ライセンス

Sentinel のデフォルトライセンスにより、90 日間の評価期間中、すべての Sentinel エンタープライズ版機能を使用できます。評価版ライセンスで稼働しているシステムでは、Web インタフェース上に、一時ライセンスキーが使用されていることが示されます。また、機能の残り日数および、フルライセンスへのアップグレード方法も表示されます。

注 : システムの有効期限は、システム内で最も古いデータに基づきます。古いイベントをシステムで復元すると、それに従って有効期限が調整されます。

90 日の評価期間後、ほとんどの機能は無効になりますが、ログインしてエンタープライズライセンスキーを使用するようにシステムを更新することはできます。

エンタープライズライセンスにアップグレードすると、すべての機能が復元されます。機能の中断を防ぐには、期限までにシステムをエンタープライズライセンスでアップグレードする必要があります。

4.2 エンタープライズライセンス

Sentinel を購入すると、お客様向けポータルから、ライセンスキーを受け取ります。購入したライセンスに応じて、ライセンスキーによって特定の機能、データ収集レート、およびイベントソースが有効になります。ライセンスキーでは強制されない追加のライセンス条件が存在する可能性があるため、使用許諾契約は十分に確認してください。

ライセンスを変更する場合は、アカウントマネージャにお問い合わせください。システムにライセンスキーを追加するには、『*NetIQ Sentinel 7.1 Administration Guide*』を参照してください。

5 システム要件を満たす

本章では、Sentinel のハードウェア、オペレーティングシステム、およびブラウザの要件について説明します。

5.1 サポートされるオペレーティングシステムとプラットフォーム

NetIQ は、以下に示すオペレーティングシステムでの Sentinel の運用をサポートします。また、これらのオペレーティングシステムにマイナーなアップデート (セキュリティパッチやホットフィックスなど) が適用されたシステムでも、Sentinel をサポートします。ただし、これらのオペレーティングシステムにメジャーアップデートが適用されたシステムでは、NetIQ がそれらのアップデートをテストし認定するまで、Sentinel の実行をサポートしません。

NetIQ は、次のオペレーティングシステムおよびプラットフォームにおける Sentinel サーバ、コレクタマネージャ、および相関エンジンをサポートしています。

カテゴリ	要件
オペレーティングシステム	次のオペレーティングシステムにおいて、Sentinel がサポートされています。 ◆ SUSE Linux Enterprise Server (SLES) 11 SP2 64 ビット * ◆ Red Hat Enterprise Linux for Servers (RHEL) 6 64 ビット * Sentinel は、SLES の Open Enterprise Server インストールではサポートされません。 **重要 :** 従来のインストールの場合は、オペレーティングシステムでインターネットプロトコルバージョン 6 (IPv6) がご使用の環境で有効になっていることを確認してください。IPv6 が有効になっていないと、主要コンポーネントを動作させることができません。 アプライアンスインストールの場合は、IPv6 がデフォルトで有効になっています。

カテゴリ	要件
仮想プラットフォーム	NetIQ は、次の仮想プラットフォーム上に SLES 11 SP2 64 ビットサーバおよび Sentinel をインストールするアプライアンスを提供しています。 ◆ VMWare ESX 4.0 および 5.0 ◆ Xen 4.0
DVD ISO	NetIQ は、以下のプラットフォーム上に SLES 11 SP2 64 ビットおよび Sentinel をインストールする DVD ISO ファイルを提供しています。 ◆ Hyper-V Server 2008 R2 ◆ オペレーティングシステムがインストールされていないハードウェア
ファイルシステム	**従来型インストール :** ◆ **SLES システムの場合 :** Sentinel は ext3 および XFS ファイルシステムをサポートします。 ◆ **RHEL システムの場合 :** Sentinel は ext4 および XFS ファイルシステムをサポートします。 **アプライアンスインストール :** Sentinel 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、『*SLES 11 SP2: ストレージ管理ガイド*』の「Linux ファイルシステムの概要 (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html)」を参照してください。

5.2 サポートされるデータベースプラットフォーム

Sentinel には、埋め込みのファイルベースのストレージシステムおよび PostgreSQL データベースが含まれており、Sentinel の実行に必要なものはこれがすべてです。ただし、オプションのデータ同期機能を使用してデータをデータウェアハウスにコピーする場合、データウェアハウスとして PostgreSQL、Oracle バージョン 11g R2、または Microsoft SQL Server 2008 R2 の使用がサポートされています。

5.3 対応ブラウザ

Sentinel の Web インタフェースは、次の対応ブラウザを使用した、1280 x 1024 以上の解像度での表示用に最適化されています。

注 : Sentinel クライアントアプリケーションを正しくロードするには、システムに Java Web Start をインストールする必要があります。

プラットフォーム	ブラウザ
Windows 7	◆ Firefox バージョン 5 ～バージョン 18 ◆ Internet Explorer 8、9、および 10.* Internet Explorer 8 については、37 ページの 「Internet Explorer の前提条件」を参照してください。
SLES 11 SP2 および RHEL 6	◆ Firefox バージョン 5 ～バージョン 18

5.3.1 Internet Explorer の前提条件

インターネットの［セキュリティのレベル］が［高］に設定されている場合、Sentinel にログインしても、ファイルダウンロードのポップアップがブラウザによってブロックされることがあります。この問題を回避するには、次のようにしてセキュリティのレベルをいったん［中高］に設定した後、［カスタム］レベルに変更してください。

1. *［ツール］>［インターネットオプション］>［セキュリティ］*の順にクリックし、セキュリティのレベルを*［中高］*に設定します。
2. *［ツール］>［互換表示］*オプションが選択されていないことを確認します。
3. *［ツール］>［インターネットオプション］>［セキュリティ］タブ>［レベルのカスタマイズ］*の順にクリックし、*［ダウンロード］*セクションまで下にスクロールし、*［ファイルのダウンロード時に自動的にダイアログを表示］*オプションの*［有効にする］*を選択します。

5.4 システムサイズ設定情報

Sentinel の実装は環境の必要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、NetIQ コンサルティングサービスまたは NetIQ Sentinel パートナーにご相談ください。

このセクションでは、当社においてテスト時に入手可能であったハードウェアを使って行ったテストに基づく、サイズ設定情報を提供します。より大きな負荷を処理できる、より大規模で強力なハードウェア設定もあり得ます。

オールインワン設定の場合、処理の負荷をリモートコレクタマネージャとリモート相関エンジンに分散させるのではなく、すべてを Sentinel サーバに集中させます。少数の機能を限られた方法で使用するシンプルなシナリオでは、オールインワン設定で十分機能しますが、多数の機能を使用したり、機能を拡張して使用したりする場合には、そのスケールに十分対応できません。たとえば、インストール時より多い数の相関ルールを使用するなら、相関エンジンのリソース使用量が増加するために、システムにかかる負荷が非常に大きくなり、結果的に同じサーバ上の他の機能に障害が出る可能性があります。

- 使用するコレクタの数が多い場合は、リモートコレクタマネージャに負荷を分散させる必要があります。
- 使用する相関ルールの数がインストール時より多い場合は、リモート相関エンジンに負荷を分散することが必要です。
- 使用する機能の数や使用する機能の拡張性を増やすことを計画する際には、負荷を分散させるのが賢明です。

CPU のハイパースレッディングには、システムが処理できる負荷にかなりのプラス効果があることが分かっています。したがって、購入する CPU を決める際に、下に示すリファレンステストでハイパースレッディングが有効になっていたかに注意し、選択する CPU が十分なハイパースレッディングを備えていることを必ず確認してください。

カテゴリ	説明	デモオールインワン 運用向けではない	中規模オールインワン	中規模エージェントベースのデータ収集	大規模オールインワン	大規模分散エージェントベースのデータ収集	超大規模
EPS 保持能力	リアルタイムコンポーネントによって処理され、システムによってストレージに保持される 1 秒あたりのイベント数。	100 EPS	2500 EPS	2500 EPS	9000 EPS	11000 EPS	11000 EPS 以上
EPS 運用能力	システムがイベントソースから受信する 1 秒あたりの合計イベント数。これには保管される前にシステムのインテリジェントフィルタリング機能によってドロップされるデータが含まれます。この数値は EPS ベースのライセンスコンプライアンスのために使用されます。	100 EPS	2500 EPS 以上	2500 EPS 以上	9000 EPS	16000 EPS	16000 EPS 以上
Sentinel サーバのハードウェア							

カテゴリ	説明	デモオールインワン 運用向けではない	中規模オールインワン	中規模エージェントベースのデータ収集	大規模オールインワン	大規模分散エージェントベースのデータ収集	超大規模
CPU		インテル Xeon プロセッサー E5420 (2.50GHz 4 コア)、ハイパースレッディングなし	2 基のインテル Xeon プロセッサー E5450 (3.00GHz 4 コア、合計 8 コア)、ハイパースレッディングなし	2 基の AMD Opteron 2431 (2.40GHz 6 コア、合計 12 コア)	2 基のインテル Xeon プロセッサー E5-2680 (2.70GHz 8 コア、合計 16 コア)、ハイパースレッディングあり		NetIQ Services にお問い合わせください
ローカルストレージ	検索のパフォーマンスを上げるために、データはローカルにキャッシュされます。	500GB 7,200RPM ハードドライブ	5 台の 300GB SAS 15,000RPM ハードドライブ (ハードウェア RAID 0)	3 台の 146GB SAS 10,000RPM ハードドライブ (RAID 0、ストライプサイズ 128k)	5TB、8 台の 600GB SAS 15,000RPM ハードドライブ (ハードウェア RAID 0、ストライプサイズ 128k)		
ネットワークストレージ	ローカルストレージのデータのコピーを含みます。	使用しない	使用しない	使用しない	使用しない		
メモリ		4GB	24GB	16GB	64GB		
リモートコレクタマネージャ #1 のハードウェア							
CPU		該当なし (ローカル埋め込みコレクタマネージャのみ)				2 基のインテル Xeon プロセッサー E5-2680 (2.70GHz 8 コア、合計 16 コア)、ハイパースレッディングあり	NetIQ Services にお問い合わせください

カテゴリ	説明	デモオールインワン 運用向けではない	中規模オールインワン	中規模エージェントベースのデータ収集	大規模オールインワン	大規模分散エージェントベースのデータ収集	超大規模
ストレージ						20GB の空き領域	NetIQ Services にお問い合わせください
メモリ						24GB	
リモートコレクタマネージャ #2 のハードウェア							
CPU		該当なし (ローカル埋め込みコレクタマネージャのみ)				8 コア インテル Xeon プロセッサー X5570 2.93GHz (仮想マシン)	NetIQ Services にお問い合わせください
ストレージ						50GB	
メモリ						8GB	
エージェントマネージャのハードウェア							
CPU		該当なし (エージェントレス収集のみ)		2 基のインテル Xeon プロセッサー 5140 (2.33GHz 2 コア、合計 4 コア)	該当なし (エージェントレス収集のみ)		NetIQ Services にお問い合わせください
ストレージ				2 台の 300GB SAS 10,000RPM ハードドライブ (RAID 0、ストライプサイズ 128k)			
メモリ				16GB			
リモート相関エンジンのハードウェア							

カテゴリ	説明	デモオールインワン 運用向けではない	中規模オールインワン	中規模エージェントベースのデータ収集	大規模オールインワン	大規模分散エージェントベースのデータ収集	超大規模
CPU		該当なし (ローカル埋め込み相関エンジンのみ)					NetIQ Services にお問い合わせください
ストレージ							
メモリ							
データ収集							
コレクタマネージャの分散	各コレクタマネージャに配置されるイベントソースの数と 1 秒あたりのイベント数の負荷。 フィルタ率は、正規化されたイベントが収集直後に保管されも分析エンジンに渡されもせずにフィルタによってどれくらい除去されたかを示します。正規化されたイベントの元になっている正規化されていない生ログデータは、フィルタリングの影響を受けることなく、常に保管されます。 ローカル埋め込みコレクタマネージャは、Sentinel サーバマシンにあります。	**ローカル埋め込みコレクタマネージャ** イベントソース : 101 EPS: 100 フィルタ率 : 0%	**ローカル埋め込みコレクタマネージャ** イベントソース : 2500 EPS: 2500 フィルタ率 : 0%	**ローカル埋め込みコレクタマネージャ** イベントソース : 5000 EPS: 2500 フィルタ率 : 0%	**ローカル埋め込みコレクタマネージャ** イベントソース : 500 EPS: 9000 フィルタ率 : 0%	**ローカル埋め込みコレクタマネージャ** 使用しない **リモートコレクタマネージャ #1** イベントソース : 110 EPS: 9500 フィルタ率 : 21% 生データ無効 **リモートコレクタマネージャ #2** イベントソース : 20 EPS: 6500 フィルタ率 : 54% 生データ無効	NetIQ Services にお問い合わせください

カテゴリ	説明	デモオールインワン 運用向けではない	中規模オールインワン	中規模エージェントベースのデータ収集	大規模オールインワン	大規模分散エージェントベースのデータ収集	超大規模
使用するコレクタ		**IBM AIX 6.1r3** ソース 100 EPS: 99 **NetIQ Universal Event 2011.1r1** ソース : 1 EPS: 1	各コレクタには独自の Syslog サーバがあります。 **Oracle Solaris 6.1r3** ソース : 1000 EPS: 1000 **IBM AIX 6.1r3** ソース : 1000 EPS: 1000 **Sourcefire Snort 2011.1r1** ソース : 500 EPS: 500	カスタムテストコレクタ (解析なし) **エージェントマネージャコネクタサーバ 1** ソース : 5000 EPS: 2500	次の各コレクタには独自の Syslog サーバがあり、以下の EPS レートで解析します。 **Oracle Solaris 6.1r3** EPS: 2000 **Sourcefire Snort 2011.1r1** EPS: 1500 **NetIQ Universal Event 2011.1r1** EPS: 2000 **Juniper Netscreen Series 2011.1r1** EPS: 1500 **IBM AIX 6.1r3: 2000** EPS: 2000	次の各コレクタには独自の Syslog サーバがあり、以下の EPS レートで解析します。 **Oracle Solaris 6.1r3** RCM #1: 2000 RCM #2: 2000 **Sourcefire Snort 2011.1r1** RCM #1: 2000 RCM #2: 1000 **NetIQ Universal Event 2011.1r1** RCM #1: 2000 RCM #2: 0 **Juniper Netscreen Series 2011.1r1** RCM #1: 2000 RCM #2: 1500	NetIQ Services にお問い合わせください

カテゴリ	説明	デモオールインワン 運用向けではない	中規模オールインワン	中規模エージェントベースのデータ収集	大規模オールインワン	大規模分散エージェントベースのデータ収集	超大規模
						IBM AIX 6.1r3 RCM #1: 1500 RCM #2: 0 **IBM iSeries 2011.1r3** RCM #1: 0 RCM #2: 2000	NetIQ Services にお問い合わせください
合計		イベントソース : 101 EPS: 100 フィルタ率 : 0%	イベントソース : 2500 EPS: 2500 フィルタ率 : 0%	イベントソース : 5000 EPS: 2500 フィルタ率 : 0%	イベントソース : 500 EPS: 9000 フィルタ率 : 0%	イベントソース : 130 運用 EPS: 16000 保持 EPS: 11000 フィルタ率 : 25%	
データストレージ							

カテゴリ	説明	デモオールインワン 運用向けではない	中規模オールインワン	中規模エージェントベースのデータ収集	大規模オールインワン	大規模分散エージェントベースのデータ収集	超大規模
ユーザは過去何日までのデータを定期的に検索しますか？	検索のパフォーマンスを上げるために、ローカルにキャッシュされるデータの量。	7 日					NetIQ Services にお問い合わせください
検索全体の何パーセントが上記の日数より古いデータを検索していますか？	ローカルストレージまたはネットワークストレージの 1 秒あたりの入出力操作 (IOPS) の量に影響します。	10%					
過去何日までのデータを保持する必要がありますか？	すべてのデータを保持するための必要なディスク容量に影響します。ネットワークストレージが有効である場合は、必要なネットワークストレージのサイズに影響します。ネットワークストレージが無効である場合は、必要なローカルストレージのサイズに影響します。	14 日					

カテゴリ	説明	デモオールインワン 運用向けではない	中規模オールインワン	中規模エージェントベースのデータ収集	大規模オールインワン	大規模分散エージェントベースのデータ収集	超大規模
ネットワークストレージデバイスは使用可能になり接続されますか？	すべてのデータがローカルに保管されるか、または低価格で長期間利用可能なオンラインストレージをネットワークストレージとして使用可能かに影響します。ネットワークストレージのデータは常にオンラインです。	×					NetIQ Services にお問い合わせください
サマリや他のデータ同期ポリシーを使用して、いくつのレポートが最適化されますか？	ローカルストレージのサイズと IOPS を左右するデータ同期ポリシーの数に影響します。	5 (設定変更前)			4 (設定変更前、ただしソースサマリ RDD を除く)		
ユーザアクティビティ							
平均して同時に何人のユーザがアクティブになりますか？	ローカルストレージとネットワークストレージの IOPS の量および他の項目に影響します。	1					NetIQ Services にお問い合わせください
平均して 1 人のアクティブなユーザが同時に何件の検索を実行しますか？	ローカルストレージとネットワークストレージの IOPS の量に影響します。	検索またはレポート 1 件 (ただし両方を同時ではない)、1 件のレポートにつき 20,000 イベント、1 件の検索につき 100M イベント		検索またはレポートの負荷テストなし	1 1 件の検索につき 80M イベント	1 1 件の検索につき 20M イベント	
平均して 1 人のアクティブなユーザが同時に何件のレポートを実行しますか？	ローカルストレージとネットワークストレージの IOPS の量に影響します。	検索またはレポート 1 件 (ただし両方を同時ではない)、1 件のレポートにつき 20,000 イベント、1 件の検索につき 100M イベント		検索またはレポートの負荷テストなし	1 1 件のレポートにつき 1k イベント	1 1 件のレポートにつき 60k イベントおよび 5k ページ	

カテゴリ	説明	デモオールインワン 運用向けではない	中規模オールインワン	中規模エージェントベースのデータ収集	大規模オールインワン	大規模分散エージェントベースのデータ収集	超大規模
分析機能							
何パーセントのイベントデータが相関ルールに関係していますか？	相関エンジンが処理するデータの量。	100% (設定変更前) (1 秒あたり 3 個の相関)		100% (設定変更前) (1 秒あたり 0 個の相関)	0%	0% (一部のデータは遅すぎてリアルタイム相関で処理できません)	NetIQ Services にお問い合わせください
いくつのシンプルな相関ルール (フィルタやトリガのみ) が使用されますか？	相関エンジンの CPU 使用量に影響します。	84 (設定変更前)			0		NetIQ Services にお問い合わせください
いくつの複雑な相関ルールが使用されますか？	相関エンジンの CPU およびメモリ使用量に影響します。	0 (設定変更前)					
相関エンジン分散		ローカル埋め込み相関エンジン (すべてのルール)					
いくつのデータセットに対してアノマリー検出が実行されますか？	セキュリティインテリジェンスダッシュボードの数。これは CPU、ローカルストレージサイズ、およびメモリ使用量に影響します。	1 (各イベントストリームの 1%)		0			

カテゴリ	説明	デモオールインワン 運用向けではない	中規模オールインワン	中規模エージェントベースのデータ収集	大規模オールインワン	大規模分散エージェントベースのデータ収集	超大規模
高可用性							
メモ	上記のシステム負荷を超過すると、重要な機能が無効になるか、または起きる事柄の警告が出されます。				生データ無効 相関およびセキュリティインテリジェンスは使用されない レポート対象のイベントが 30k を超えると不安定になる	生データ無効 相関およびセキュリティインテリジェンスは使用されない レポート対象のイベントが一定の数を超えると不安定になる このシステム設定では、保持 EPS が増えると結果的に不安定になる	NetIQ Services にお問い合わせください

5.5 データストレージのパーティション計画

Sentinel をインストールする際には、Sentinel のインストール先 (デフォルトでは /var/opt/novell ディレクトリ) と同じ場所に、ローカルストレージ用のディスクパーティションをマウントする必要があります。

ディスク使用量が正しく計算されるように、/var/opt/novell/sentinel ディレクトリ下のディレクトリ構造全体が 1 つのディスクパーティションに置かれていなければなりません。そうしないと、自動データ管理機能がイベントデータを早まって削除してしまう可能性があります。Sentinel ディレクトリ構造の詳細については、99 ページの第 15 章「Sentinel のディレクトリ構造」を参照してください。

ベストプラクティスとして、このデータディレクトリが実行可能ファイル、環境設定ファイル、オペレーティングシステムファイルとは別のディスクパーティションに保管されるようにしてください。可変データを別個に保管することには、ファイルセットのバックアップがより簡単にでき、破損が生じた場合の回復がさらにシンプルになるという利点があります。そして、ディスクパーティションが満杯になった場合の堅牢性が強化されます。また、容量の小さいファイルシステムのほうが効率的であるため、システム全体のパフォーマンスも向上します。詳細については、「Disk Partitioning (パーティション)」を参照してください。

5.5.1 従来型インストールでのパーティションの使用

従来型インストールの場合、Sentinel をインストールする前にオペレーティングシステムのディスクパーティションレイアウトを変更できます。管理者は 99 ページのセクション 15「Sentinel のディレクトリ構造」で説明されているディレクトリ構造に基づいて、適切なディレクトリに目的のパーティションを作成およびマウントする必要があります。インストーラを実行すると Sentinel は事前に作成されたディレクトリにインストールされ、複数のパーティションにわたるインストール環境が構築されます。

注 :

- インストーラの実行中に --location オプションを使用して、ファイルを格納する場所としてデフォルトのディレクトリ以外の最上位の場所を指定できます。--location オプションに渡す値は、ディレクトリパスの前に付加されます。たとえば、「--location=/foo」を指定すると data ディレクトリは /foo/var/opt/novell/sentinel/data、config ディレクトリは /foo/etc/opt/novell/sentinel/config となります。
- --location オプションには、ファイルシステムリンク (ソフトリンクなど) は使用しないでください。

5.5.2 アプライアンスインストールでのパーティションの使用

DVD ISO アプライアンスフォーマットを使用して、インストール中にアプライアンスファイルシステムのパーティション作成を設定することができます。たとえば、/var/opt/novell/sentinel マウントポイント用に別のパーティションを作成して、すべてのデータを別のパーティションに置くことができます。ただし、他のアプライアンスフォーマットの場合は、インストール後にのみパーティション作成を設定することができます。SuSE YaST システム環境設定ツールを使用して、パーティションを追加し、その新しいパーティションにディレクトリを移動することができます。インストール後のパーティション作成の詳細については、90 ページのセクション 12.4.2「パーティションの作成」を参照してください。

5.6 コネクタおよびコレクタのシステム要件

各コネクタおよびコレクタには、それぞれ独自のシステム要件およびサポートされるプラットフォームがあります。Sentinel プラグインの Web ページ (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) にある、コネクタおよびコレクタのマニュアルを参照してください。

5.7 仮想環境

Sentinel は、広範にわたるテストが実施されており、VMware ESX サーバで完全にサポートされています。仮想環境を設定する場合、仮想マシンには CPU が少なくとも 2 基必要です。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。

物理マシンで推奨される内容については、35 ページの第 5 章「システム要件を満たす」を参照してください。

6 FIPS140-2 モードで Sentinel を運用する場合の展開に関する考慮事項

オプションとして、内部暗号化やその他の機能で、FIPS 140-2 認定暗号プロバイダである Mozilla ネットワークセキュリティサービス (NSS) を使用するように、Sentinel を設定することができます。この目的は、Sentinel を「FIPS 140-2 実装」にして、米国連邦購入ポリシーおよび標準に準拠させることです。

Sentinel の FIPS 140-2 モードを有効にすると、Sentinel サーバ、Sentinel リモートコレクタマネージャ、Sentinel リモート相関エンジン、Sentinel Web UI、Sentinel コントロールセンター、Sentinel Advisor サービスとの通信に FIPS 140-2 認定暗号が使用されます。

6.1 Sentinel における FIPS 実装

Sentinel は、オペレーティングシステムによって提供される Mozilla NSS ライブラリを使用します。Red Hat Enterprise Linux (RHEL) と SUSE Linux Enterprise Server (SLES) とでは、付属する NSS パッケージセットが異なります。

RHEL 6.2 によって提供される NSS 暗号化モジュールは、FIPS 140-2 認定です。SLES 11 SP2 によって提供される NSS 暗号化モジュールは、まだ公式には FIPS 140-2 認定ではありませんが、SUSE モジュールを FIPS 140-2 認定にするための作業が進行中です。認定が取得されれば、SUSE プラットフォームで「FIPS 140-2 実装」にするために Sentinel に変更を加える必要はありません。

RHEL 6.2 FIPS 140-2 証明書の詳細については、『*Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules*』を参照してください。

6.1.1 RHEL NSS パッケージ

FIPS 140-2 モードに対応するために、Sentinel には次の 64 ビット NSS パッケージが必要です。

- nspr-4.9-1.el6.x86_64
- nss-sysinit-3.13.3-6.el6.x86_64
- nss-util-3.13.3-2.el6.x86_64
- nss-softokn-freebl-3.12.9-11.el6.x86_64
- nss-softokn-3.12.9-11.el6.x86_64

- nss-3.13.3-6.el6.x86_64
- nss-tools-3.13.3-6.el6.x86_64

上記のパッケージでインストールされていないものがあれば、それらをインストールしてから Sentinel の FIPS 140-2 モードを有効にする必要があります。

6.1.2 SLES NSS パッケージ

FIPS 140-2 モードに対応するために、Sentinel には次の 64 ビット NSS パッケージが必要です。

- libfreebl3-3.13.1-0.2.1
- mozilla-nspr-4.8.9-1.2.2.1
- mozilla-nss-3.13.1-0.2.1
- mozilla-nss-tools-3.13.1-0.2.1

上記のパッケージでインストールされていないものがあれば、それらをインストールしてから Sentinel の FIPS 140-2 モードを有効にする必要があります。

6.2 Sentinel の FIPS 実装コンポーネント

次の Sentinel コンポーネントは FIPS 140-2 に対応しています。

- すべての Sentinel プラットフォームコンポーネントは、FIPS 140-2 モードをサポートするように更新されています。
- 暗号化をサポートする以下の Sentinel プラグインは、FIPS 140-2 モードをサポートするように更新されています。
  - エージェントマネージャコネクタ 2011.1r1 以降
  - データベース (JDBC) コネクタ 2011.1r2 以降
  - ファイルコネクタ 2011.1r1 以降 (イベントソースタイプがローカルまたは NFS である場合のみ)。
  - LDAP インテグレータ 2011.1r1 以降
  - Sentinel Link コネクタ 2011.1r3 以降
  - Sentinel Link インテグレータ 2011.1r2 以降
  - SMTP インテグレータ 2011.1r1 以降
  - Syslog コネクタ 2011.1r2 以降
  - Windows イベント (WMI) コネクタ 2011.1r2 以降

  上記の Sentinel プラグインを FIPS 140-2 モードで実行するための環境設定については、114 ページの 「Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する」を参照してください。

本書のリリース時点で、オプションの暗号化をサポートする以下の Sentinel コネクタは、まだ FIPS 140-2 モードをサポートするように更新されていません。ただし、これらのコネクタを使用したイベントの収集は引き続き実行することができます。これらのコネクタを FIPS 140-2 モードの Sentinel で使用する場合の手順については、119 ページの 「FIPS 140-2 モードの Sentinel で FIPS 非対応コネクタを使用する」を参照してください。

- チェックポイント (LEA) コネクタ 2011.1r2
- Cisco SDEE コネクタ 2011.1r1
- ファイルコネクタ 2011.1r1 (CIFS および SCP 機能には暗号化が含まれていますが、FIPS 140-2 モードでは動作しません)。
- NetIQ Audit Connector 2011.1r1
- SNMP Connector 2011.1r1

本書のリリース時点で、SSL をサポートする以下の Sentinel インテグレータは、FIPS 140-2 モードをサポートするように更新されていません。しかし、これらのインテグレータを FIPS 140-2 モードの Sentinel で使用している場合でも、引き続き非暗号化接続を使用することができます。

- Remedy インテグレータ 2011.1r1 以降
- SOAP インテグレータ 2011.1r1 以降

上記のリストに含まれていない Sentinel プラグインはどれも暗号化を使用せず、Sentinel を FIPS 140-2 モードにしたことによる影響を受けません。それらを FIPS 140-2 モードの Sentinel で使用するために、追加ステップを実行する必要はありません。

Sentinel プラグインの詳細については、Sentinel プラグイン Web サイトをご覧ください。まだ更新されていないプラグインを FIPS に対応させたい場合は、Bugzilla を使用してリクエストを送信してください。

6.3 実装チェックリスト

次の表は、Sentinel を FIPS 140-2 モードで運用するために必要なタスクの概要を示しています。

タスク	詳細の参照先
展開を計画する。	52 ページのセクション 6.4「導入シナリオ」
FIPS 140-2 モードを、Sentinel のインストール中に有効にするか、後から有効にするかを決める。 インストール中に Sentinel の FIPS 140-2 モードを有効にする場合、インストールの処理中にカスタムインストールかサイレントインストールを選択する必要があります。	73 ページのセクション 11.2.2「カスタムインストール」 75 ページのセクション 11.3「サイレントインストールの実行」 109 ページの第 18 章「既存の Sentinel インストール環境を FIPS 140 – 2 モードにする」
Sentinel プラグインを FIPS 140-2 モードで実行するように設定する。	114 ページのセクション 19.5「Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する」
証明書を Sentinel FIPS キーストアにインポートする。	120 ページのセクション 19.6「証明書を FIPS キーストアデータベースにインポートする」

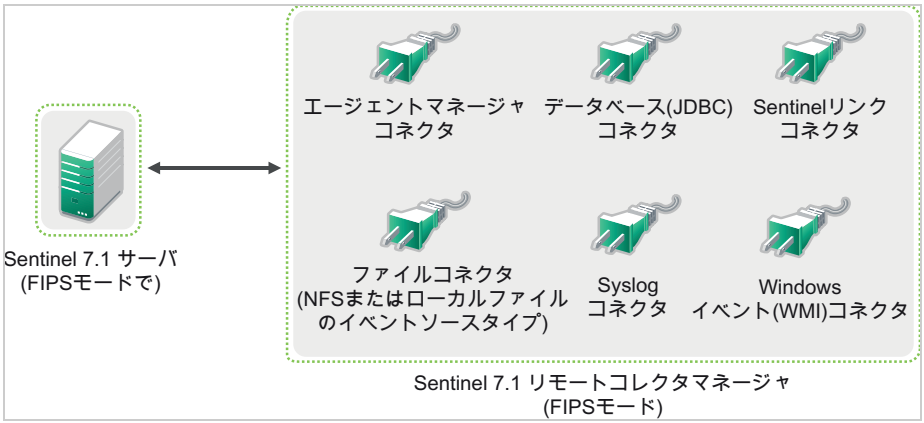
注 : FIPS モードへの変換を開始する前に、Sentinel システムのバックアップを取ることを強くお勧めします。何らかの理由でサーバを非 FIPS モードに戻す必要がある場合、そのためのサポートされている方法はバックアップからの復元のみです。非 FIPS モードに戻す場合の詳細については、120 ページの 「Sentinel を非 FIPS モードに戻す」を参照してください。

6.4 導入シナリオ

このセクションでは、Sentinel の FIPS 140-2 モードの導入シナリオについて説明します。

6.4.1 シナリオ 1: 完全 FIPS 140-2 モードでのデータ収集

このシナリオの場合、データ収集は FIPS 140-2 モードをサポートするコネクタによってのみ実行されます。Sentinel サーバがあり、リモートコレクタマネージャによってデータが収集されている環境を前提としています。リモートコレクタマネージャは、1 つまたは複数を使用することができます。



ご使用の環境で FIPS 140-2 モードをサポートするコネクタのみを使用してイベントソースからデータ収集が行われている場合は、以下の手順を実行する必要があります。

1 FIPS 140-2 モードの Sentinel 7.1 サーバが必要です。

   注 : 新規インストールまたはアップグレードされた Sentinel サーバが非 FIPS モードである場合は、Sentinel サーバの FIPS を有効にする必要があります。詳細については、109 ページの 「Sentinel サーバを FIPS 140-2 モードで実行する」を参照してください。

2 Sentinel 7.1 リモートコレクタマネージャを FIPS 140-2 モードで実行させておく必要があります。

   注 : 新規インストールまたはアップグレードされたリモートコレクタマネージャが非 FIPS モードで実行中である場合は、リモートコレクタマネージャの FIPS を有効にする必要があります。詳細については、109 ページの 「リモートコレクタマネージャおよび相関エンジンで FIPS 140-2 モードを有効にする」を参照してください。

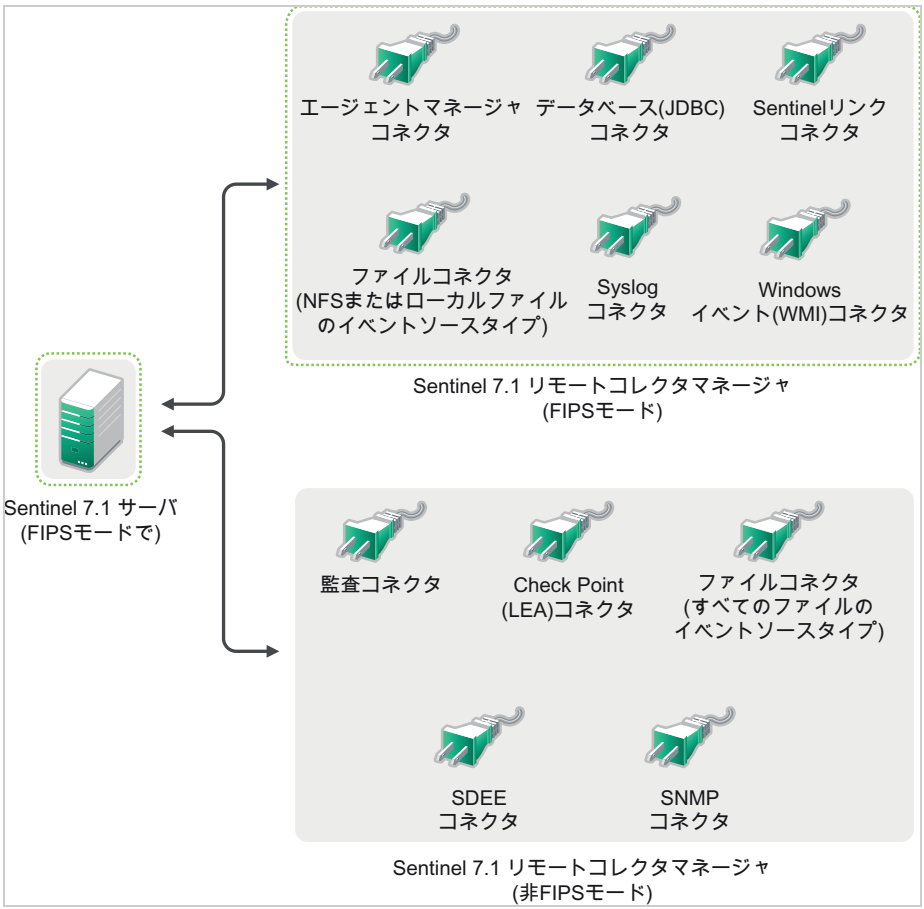
3 FIPS サーバとリモートコレクタマネージャが相互に通信していることを確認します。

4 リモート相関エンジンがあれば、それらを FIPS モードで実行するように変換します。詳細については、109 ページの 「リモートコレクタマネージャおよび相関エンジンで FIPS 140-2 モードを有効にする」を参照してください。

5 Sentinel プラグインを FIPS 140-2 モードで実行されるように環境設定します。詳細については、114 ページの 「Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する」を参照してください。

6.4.2 シナリオ 2: 部分 FIPS 140-2 モードでのデータ収集

このシナリオの場合、データ収集は FIPS 140-2 モードをサポートするコネクタと FIPS 140-2 モードをサポートしないコネクタを使用して実行されます。Sentinel サーバがあり、リモートコレクタマネージャによってデータが収集されている環境を前提としています。リモートコレクタマネージャは、1 つまたは複数を使用することができます。



FIPS 140-2 モードをサポートするコネクタとサポートしないコネクタを使用してデータ収集を処理する場合、2 つのリモートコレクタマネージャを使用することが推奨されています。1 つは FIPS をサポートするコネクタ用に FIPS 140-2 モードで実行し、もう 1 つは FIPS をサポートしないコネクタ用に非 FIPS 140-2(通常) モードで実行します。

ご使用の環境で FIPS 140-2 モードをサポートするコネクタと FIPS 140-2 モードをまだサポートしていないコネクタを使用してイベントソースからデータ収集が行われている場合には、以下の手順を実行する必要があります。

1 FIPS 140-2 モードの Sentinel 7.1 サーバが必要です。

注 : 新規インストールまたはアップグレードされた Sentinel サーバが非 FIPS モードである場合は、Sentinel サーバの FIPS を有効にする必要があります。詳細については、109 ページの「Sentinel サーバを FIPS 140-2 モードで実行する」を参照してください。

2 1 つのリモートコレクタマネージャは FIPS 140-2 モードで実行し、もう 1 つのリモートコレクタマネージャは引き続き非 FIPS モードで実行してください。

   2a FIPS 140-2 モード有効のリモートコレクタマネージャがない場合は、リモートコレクタマネージャで FIPS モードを有効にする必要があります。詳細については、109 ページの「リモートコレクタマネージャおよび相関エンジンで FIPS 140-2 モードを有効にする」を参照してください。

   2b FIPS 非対応リモートコレクタマネージャのサーバ証明書を更新します。詳細については、113 ページの 「リモートコレクタマネージャおよび相関エンジンのサーバ証明書の更新」を参照してください。

3 2 つのリモートコレクタマネージャが FIPS 140-2 有効の Sentinel サーバと通信していることを確認します。

4 リモート相関エンジンがあれば、それらを FIPS モードで実行するように変換します。詳細については、109 ページの 「リモートコレクタマネージャおよび相関エンジンで FIPS 140-2 モードを有効にする」を参照してください。

5 Sentinel プラグインを FIPS 140-2 モードで実行されるように環境設定します。詳細については、114 ページの 「Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する」を参照してください。

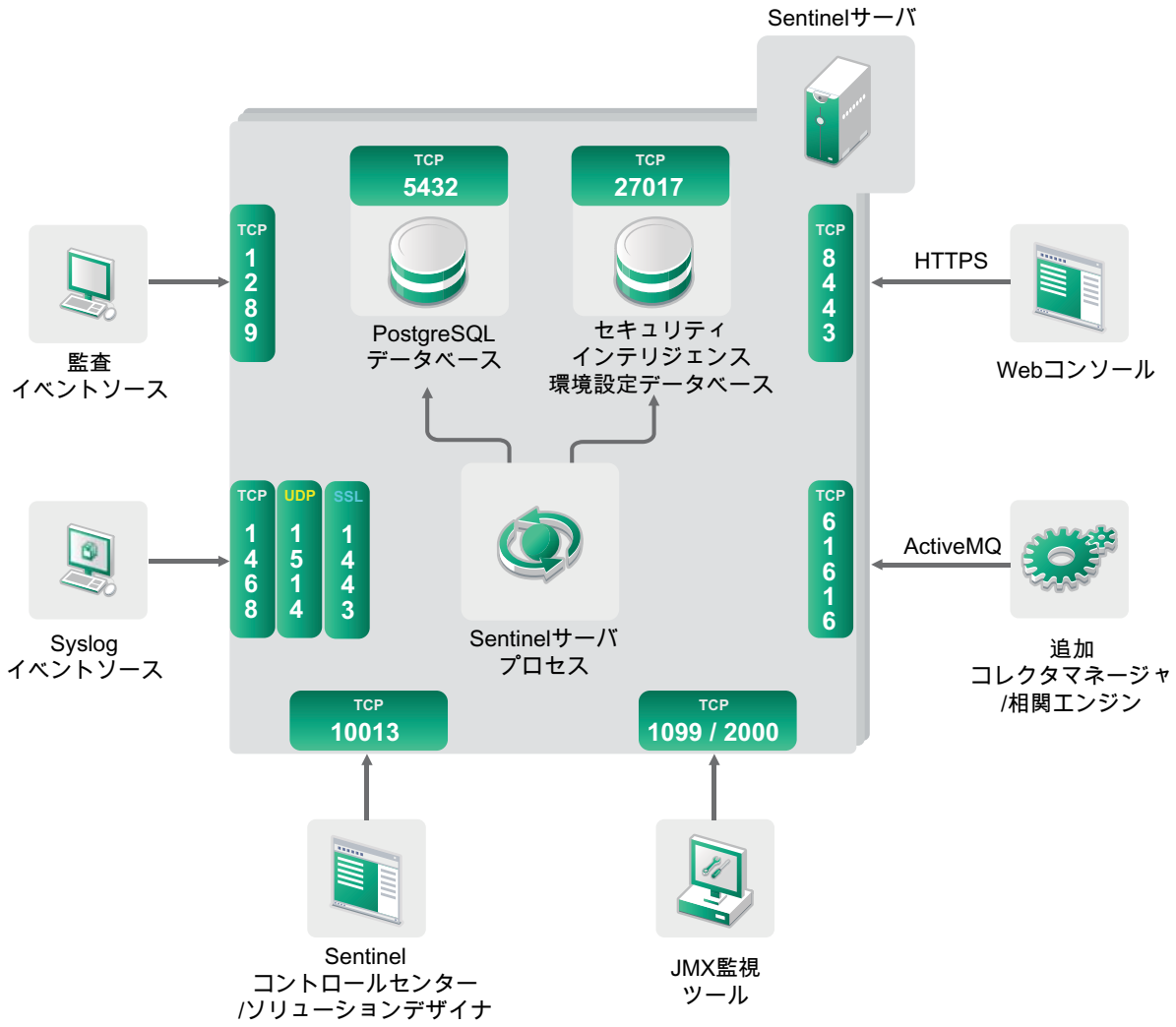
   5a FIPS 140-2 モードをサポートするコネクタを、FIPS モードで実行するリモートコレクタマネージャに展開します。

   5b FIPS 140-2 モードをサポートしないコネクタを、非 FIPS のリモートコレクタマネージャに展開します。

7 使用するポート

Sentinel は、他のコンポーネントとの外部通信には異なるポートを使用します。アプライアンスをインストールするため、ポートはファイアウォール上でデフォルトで開かれています。ただし、従来型インストールでは、Sentinel のインストール先となるオペレーティングシステムで、ファイアウォールのポートを開く設定を行う必要がありあます。Sentinel で使用するポートを次の図に示します。

図 7-1 Sentinel で使用するポート



- 56 ページのセクション 7.1「Sentinel サーバのポート」
- 59 ページのセクション 7.2「コレクタマネージャのポート」
- 60 ページのセクション 7.3「相関エンジンのポート」

7.1 Sentinel サーバのポート

Sentinel サーバは、内部通信と外部通信に次のポートを使用します。

7.1.1 ローカルポート

Sentinel は、データベースや他の内部プロセスとの内部通信に次のポートを使用します。

ポート	説明
TCP 27017	セキュリティインテリジェンス環境設定データベースで使用されます。

ポート	説明
TCP 28017	セキュリティインテリジェンスデータベースの Web インタフェースで使用されます。
TCP 32000	ラッパープロセスとサーバプロセス間の内部通信で使用されます。

7.1.2 ネットワークポート

Sentinel が正常に動作するよう、次のポートがファイアウォール上で開かれていることを確認してください。

ポート	方向	必須 / オプション	説明
TCP 5432	INBOUND	オプション。デフォルトでは、このポートはループバックインタフェースのみをリスンします。	PostgreSQL データベースで使用されます。デフォルトでこのポートを開く必要はありません。しかし、Sentinel SDK を使用してレポートを作成するときにはこのポートを開く必要があります。詳細については、「Sentinel Plug-in SDK」を参照してください。
TCP 1099 および 2000	INBOUND	オプション	監視ツールが Java Management Extensions (JMX) を利用して Sentinel サーバプロセスに接続するのに使用されます。
TCP 1289	INBOUND	オプション	Audit の接続用に使用されます。
UDP 1514	INBOUND	オプション	Syslog メッセージ用に使用されます。
TCP 8443	INBOUND	必須	HTTPS 通信に使用されます。
TCP 1443	INBOUND	オプション	SSL で暗号化された Syslog メッセージに使用されます。
TCP 61616	INBOUND	オプション	コレクタマネージャおよび相関エンジンからの着信接続に使用されます。
TCP 10013	INBOUND	必須	Sentinel コントロールセンターおよびソリューションデザイナが使用します。
TCP 1468	INBOUND	オプション	Syslog メッセージ用に使用されます。
TCP 10014	INBOUND	オプション	リモートのコレクタマネージャにより、SSL プロキシを介してサーバに接続するのに使用されます。ただし、これは一般的ではありません。デフォルトでは、リモートのコレクタマネージャは SSL ポート 61616 を使用してサーバに接続します。
TCP 443	OUTBOUND	オプション	Advisor が使用されると、このポートがインターネットを経由して Advisor サービス (Advisor Updates URL (https://secure-www.novell.com/sentinel/download/advisor/)) への接続を開始します。
TCP 8443	OUTBOUND	オプション	分散検索が使用されると、このポートが分散検索を実行するために他の Sentinel システムへの接続を開始します。

ポート	方向	必須 / オプション	説明
TCP 389 または 636	OUTBOUND	オプション	LDAP 認証が使用されると、このポートが LDAP サーバへの接続を開始します。
TCP/UDP 111 および TCP/UDP 2049	OUTBOUND	オプション	ネットワークストレージが NFS を使用するように設定されている場合。
TCP 137、138、139、445	OUTBOUND	オプション	ネットワークストレージが CIFS を使用するように設定されている場合。
TCP JDBC (データベース依存)	OUTBOUND	オプション	データ同期が使用されると、このポートが JDBC を使用するターゲットデータベースへの接続を開始します。使用されるポートはターゲットデータベースによって異なります。
TCP 25	OUTBOUND	オプション	電子メールサーバへの接続を開始します。
TCP 1290	OUTBOUND	オプション	Sentinel がイベントを別の Sentinel システムに転送すると、このポートがそのシステムへの Sentinel Link 接続を開始します。
UDP 162	OUTBOUND	オプション	Sentinel が SNMP トラップを受信するシステムにイベントを転送すると、このポートがパケットを受信者に送信します。
UDP 514 または TCP 1468	OUTBOUND	オプション	このポートは、Sentinel が Syslog メッセージを受信するシステムにイベントを転送するときに使用されます。このポートが UDP である場合は、パケットを受信者に送信します。このポートが TCP である場合は、受信者への接続を開始します。

7.1.3 Sentinel サーバアプライアンス固有のポート

上記のポートに加えて、アプライアンス用に次のポートが開いています。

ポート	方向	必須 / オプション	説明
TCP 22	INBOUND	必須	シェルが Sentinel アプライアンスに安全にアクセスできるようにするために使用されます。
TCP 54984	INBOUND	必須	Sentinel アプライアンスの管理コンソール (WebYaST) で使用されます。Sentinel アプライアンスのアップデートサービスにも使用されます。
TCP 289	INBOUND	オプション	Audit の接続用に 1289 に転送されます。
UDP 443	INBOUND	オプション	HTTPS 通信用に 8443 に転送されます。
UDP 514	INBOUND	オプション	Syslog メッセージ用に 1514 に転送されます。
TCP 1290	INBOUND	オプション	SuSE Firewall を抜けて接続することが許可されている Sentinel Link ポート。

ポート	方向	必須 / オプション	説明
UDP および TCP 40000 - 41000	INBOUND	オプション	syslog などのデータ収集サーバの設定に使用可能なポートです。Sentinel は、これらのポートをデフォルトではリスンしません。
TCP 443 または 80	OUTBOUND	必須	インターネット上の NetIQ アプライアンスソフトウェアアップデートリポジトリ、またはネットワーク内の Subscription Management Tool サービスへの接続を開始します。
TCP 80	OUTBOUND	オプション	Subscription Management Tool への接続を開始します。

7.2 コレクタマネージャのポート

コレクタマネージャは、以下のポートを使用して他のコンポーネントと通信します。

7.2.1 ネットワークポート

Sentinel コレクタマネージャが正常に動作できるよう、ファイアウォール上で次のポートが開かれていることを確認してください。

ポート	方向	必須 / オプション	説明
TCP 1289	INBOUND	オプション	Audit の接続用に使用されます。
UDP 1514	INBOUND	オプション	Syslog メッセージ用に使用されます。
TCP 1443	INBOUND	オプション	SSL で暗号化された Syslog メッセージに使用されます。
TCP 1468	INBOUND	オプション	Syslog メッセージ用に使用されます。
TCP 1099 および 2000	INBOUND	オプション	監視ツールが Java Management Extensions (JMX) を利用して Sentinel サーバプロセスに接続するのに使用されます。
TCP 61616	OUTBOUND	必須	Sentinel サーバへの接続を開始します。

7.2.2 コレクタマネージャアプライアンス固有のポート

上記のポートに加えて、Sentinel コレクタマネージャアプライアンス用に次のポートが開いています。

ポート	方向	必須 / オプション	説明
TCP 22	INBOUND	必須	シェルが Sentinel アプライアンスに安全にアクセスできるようにするために使用されます。

ポート	方向	必須 / オプション	説明
TCP 54984	INBOUND	必須	Sentinel アプライアンスの管理コンソール (WebYaST) で使用されます。Sentinel アプライアンスのアップデートサービスにも使用されます。
TCP 289	INBOUND	オプション	Audit の接続用に 1289 に転送されます。
UDP 514	INBOUND	オプション	Syslog メッセージ用に 1514 に転送されます。
TCP 1290	INBOUND	オプション	SuSE Firewall を介した接続が許可される Sentinel リンクポートです。
UDP および TCP 40000 - 41000	INBOUND	オプション	syslog などのデータ収集サーバの設定に使用可能なポートです。Sentinel は、これらのポートをデフォルトではリスンしません。
TCP 443	OUTBOUND	必須	インターネット上の NetIQ アプライアンスソフトウェアアップデートリポジトリ、またはネットワーク内の Subscription Management Tool サービスへの接続を開始します。
TCP 80	OUTBOUND	オプション	Subscription Management Tool への接続を開始します。

7.3 相関エンジンのポート

相関エンジンは、以下のポートを使用して他のコンポーネントと通信します。

7.3.1 ネットワークポート

Sentinel 相関エンジンが正常に動作するよう、ファイアウォール上で次のポートが開かれていることを確認してください。

ポート	方向	必須 / オプション	説明
TCP 1099 および 2000	INBOUND	オプション	監視ツールが Java Management Extensions (JMX) を利用して Sentinel サーバプロセスに接続するのに使用されます。
TCP 61616	OUTBOUND	必須	Sentinel サーバへの接続を開始します。

7.3.2 相関エンジンアプライアンス固有のポート

Sentinel 相関エンジンアプライアンスでは、上記のポートに加えて次のポートが開いています。

ポート	方向	必須 / オプション	説明
TCP 22	INBOUND	必須	シェルが Sentinel アプライアンスに安全にアクセスできるようにするために使用されます。

ポート	方向	必須 / オプション	説明
TCP 54984	INBOUND	必須	Sentinel アプライアンスの管理コンソール (WebYaST) で使用されます。Sentinel アプライアンスのアップデートサービスにも使用されます。
TCP 443	OUTBOUND	必須	インターネット上の NetIQ アプライアンスソフトウェアアップデートリポジトリ、またはネットワーク内の Subscription Management Tool サービスへの接続を開始します。
TCP 80	OUTBOUND	オプション	Subscription Management Tool への接続を開始します。

8 インストールオプション

Sentinel の従来型インストールを実行するか、アプライアンスをインストールできます。この章では、次の 2 つのインストールオプションについて説明します。

8.1 従来型インストール

従来型インストールは、アプリケーションインストーラを使用して、Sentinel を既存の SUSE Linux Enterprise Server (SLES) 11 または Red Hat Enterprise Linux (RHEL) 6 オペレーティングシステムにインストールします。次の方法で Sentinel をインストールすることができます。

- **Interactive:** ユーザの入力によってインストールを進行します。インストール中に、インストールオプション (ユーザ入力またはデフォルト値) をファイルに記録し、それを後でサイレントインストールに使用することができます。標準インストールまたはカスタムインストールのどちらかを実行できます。

標準インストール	カスタムインストール
環境設定にデフォルト値を使用します。ユーザ入力は、パスワードについてのみ必要です。	環境設定セットアップの値を指定するようプロンプトが表示されます。ユーザはデフォルト値を選択するか、または必要な値を指定できます。
デフォルトの 90 日間の評価版キーを使用してインストールします。	90 日間有効のライセンスキーまたは有効なライセンスキーを使用してインストールできます。
管理者パスワードを指定し、その管理者パスワードを dbauser と appuser の両方に対するデフォルトパスワードとして使用できます。	管理者パスワードを指定できます。dbauser と appuser については、新しいパスワードを指定することも、管理者パスワードを使用することもできます。
すべてのコンポーネントに対してデフォルトポートをインストールします。	コンポーネント別にポートを指定できます。
Sentinel を非 FIPS モードでインストールします。	Sentinel を FIPS 140-2 モードでインストールできます。
内部データベースでユーザを認証します。	データベース認証に加えて、Sentinel の LDAP 認証を設定するオプションが提供されます。Sentinel の LDAP 認証の環境設定を行うと、ユーザは Novell eDirectory または Microsoft Active Directory の資格情報を使用してサーバにログインすることができます。

インタラクティブインストールの詳細については、72 ページのセクション 11.2「インタラクティブインストールの実行」を参照してください。

- **サイレント :** 複数の Sentinel サーバをインストールして展開する場合は、標準またはカスタムインストール中に、環境設定ファイルにインストールオプションを記録し、そのファイルを使用して無人インストールを実行することができます。サイレントインストールの詳細については、75 ページのセクション 11.3「サイレントインストールの実行」を参照してください。

8.2 アプライアンスインストール

アプライアンスインストールは、SLES 11 SP2 64 ビットオペレーションシステムと Sentinel の両方をインストールします。

Sentinel アプライアンスは、次のフォーマットで使用できます。

- VMWare アプライアンスイメージ
- Xen アプライアンスイメージ
- ハードウェアサーバに直接展開できるハードウェアアプライアンスのライブ DVD イメージ

アプライアンスインストールの詳細については、81 ページの第 12 章「アプライアンスインストール」を参照してください。

Sentinel のインストール

このセクションでは、Sentinel および追加コンポーネントのインストールについて説明します。

9 インストールの概要

Sentinel をインストールすると、Sentinel サーバに次のコンポーネントがインストールされます。

- **Sentinel サーバプロセス :** Sentinel の主要コンポーネントです。Sentinel サーバプロセスは Sentinel の他のコンポーネントからの要求を処理し、システムのシームレスな機能を実現します。Sentinel サーバプロセスは、データのフィルタリング、検索クエリの処理、およびユーザ認証や権限付与などの管理タスクの管理といった要求を処理します。
- **Web サーバ :** Sentinel は、Sentinel 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 Jetty を採用しています。
- **PostgreSQL データベース :** Sentinel には組み込みデータベースが備わっており、Sentinel 設定情報、アセットおよび脆弱性データ、識別情報、インシデントおよびワークフローステータスなどはそこに格納されます。
- **MongoDB データベース :** セキュリティインテリジェンスデータを格納します。
- **コレクタマネージャ :** コレクタマネージャは、Sentinel に柔軟なデータ収集ポイントを提供します。Sentinel インストーラは、インストール時にデフォルトでコレクタマネージャをインストールします。
- **相関エンジン :** 相関エンジンは、リアルタイムイベントストリームからのイベントを処理して、イベントが何らかの相関ルールをトリガするべきかどうかを判別します。
- **アドバイザ :** Security Nexus を搭載したアドバイザは、オプションのデータサブスクリプションサービスです。侵入検出と防止システムから、および企業脆弱性スキャン結果から、リアルタイムイベント間のデバイスレベルの相関関係を提供します。アドバイザの詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「「Configuring Advisor」」を参照してください。
- **Sentinel のプラグイン :** 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。追加のプラグインおよびアップデートは、Sentinel Plug-ins Web サイトからダウンロードできます。Sentinel のプラグインには以下のものがあります。
  - コレクタ
  - コネクタ
  - 相関ルールとアクション
  - Reports
  - iTRAC ワークフロー
  - ソリューションパック

Sentinel のアーキテクチャは高度なスケーラビリティを備えており、高いイベント発生率が予想される場合は、コンポーネントを複数のマシンに分散し、そのシステムにとってベストなパフォーマンスを実現することができます。コンポーネントの独立したスケーリングは、コスト効率に優れたスケーラビリティとパフォーマンスを可能にしています。

9.1 追加のコレクタマネージャの利点

追加のコレクタマネージャをネットワーク内の適切な場所にインストールすることができます。これらのリモートコレクタマネージャはコネクタやコレクタを実行し、収集したデータは Sentinel サーバに転送されて保管、処理されます。追加のコレクタマネージャのインストールについては、78 ページのセクション 11.6「追加のコレクタマネージャのインストールおよび相関エンジンのインストール」を参照してください。

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

- **システムのパフォーマンスの向上 :** コレクタマネージャを追加すると、分散環境でイベントデータを解析および処理できるため、システムのパフォーマンスが向上します。
- **データのセキュリティの強化およびネットワーク帯域幅要件の低下 :** コレクタマネージャがイベントソースと同じ場所にあると、フィルタ、暗号化、およびデータの圧縮を同じソースで実行できます。
- **ファイルキャッシング :** イベントのアーカイブやイベントの大量発生の処理でサーバの負荷が一時的に上がったときに、追加のコレクタマネージャで大量のデータをキャッシュすることができます。この機能は、イベントキャッシングをネイティブでサポートしない Syslog などのプロトコルの場合に役立ちます。

注 : 1 つのシステムに複数のコレクタマネージャをインストールすることはできません。リモートシステムに追加のコレクタマネージャをインストールして、それらを Sentinel サーバに接続することはできます。

9.2 相関エンジンを追加することの利点

環境設定を複製したり、データベースを追加したりすることなく、複数の相関エンジンをそれぞれ独自のサーバに展開できます。多数の相関ルールがある環境、またはイベント発生率が極端に高い環境では、複数の相関エンジンをインストールして新しい相関エンジンにルールを再展開することが有効な場合があります。相関エンジンが複数あれば、Sentinel システムにデータソースが追加された場合やイベント発生率が増大した場合に、それに対応するスケーラビリティが得られます。追加の相関エンジンのインストールについては、78 ページのセクション 11.6「追加のコレクタマネージャのインストールおよび相関エンジンのインストール」を参照してください。

注 : 1 つのシステムに複数の相関エンジンをインストールすることはできません。リモートシステムに追加の相関エンジンをインストールして、それらを Sentinel サーバに接続することはできます。

---

10 インストールのチェックリスト

インストールを開始する前に、次の作業を完了していることを確認してください。

- ハードウェアおよびソフトウェアが、35 ページの第 5 章「システム要件を満たす」に示されているシステム要件を満たしていることを確認します。
- 以前に Sentinel がインストールされていた環境の場合は、以前のインストール環境のファイルやシステム設定が残っていないことを確認します。詳細については、155 ページの付録 C「アンインストール中」を参照してください。
- ライセンス版のインストールを計画している場合は、Novell Customer Care Center からライセンスキーを取得してください。
- 55 ページの第 7 章「使用するポート」に示されているポートがファイアウォールで開かれていることを確認します。
- Sentinel インストーラが正常に動作するためには、システムがホスト名や有効な IP アドレスを返すことができなければなりません。そのためには、/etc/hosts ファイル内の IP アドレスを含む行にホスト名を追加し、それから「hostname -f」と入力してホスト名が正しく表示されるようにします。
- Network Time Protocol (NTP) を使用して時刻を同期します。
- **RHEL システムの場合 :** パフォーマンスを最適化するには、PostgreSQL データベースに適したメモリ設定にする必要があります。SHMMAX パラメータは、1073741824 以上に設定する必要があります。

  適切な値を設定するには、次の情報を /etc/sysctl.conf ファイルに追加してください。

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```

- **従来型インストールの場合 :**
  - オペレーティングシステムで IPv6 が有効になっていることを確認してください。IPv6 が有効になっていないと、主要コンポーネントを動作させることができません。
  - Sentinel サーバのオペレーティングシステムに、少なくとも SLES サーバか RHEL 6 サーバの Base Server コンポーネントが含まれている必要があります。Sentinel では、次の RPM の 64 ビットバージョンが必要です。
    - bash
    - bc
    - coreutils
    - gettext
    - glibc
    - grep
    - libgcc
    - libstdc

- lsof
- net-tools
- openssl
- python-libs
- sed
- zlib

11 従来型インストール

本章では、Sentinel をインストールするさまざまな方法について説明します。

11.1 インストールオプションについて

./install-sentinel --help は、次のオプションを示します。

オプション	値	説明
--location	ディレクトリ	Sentinel をインストールする、root (/) 以外のディレクトリを指定します。
-m、--manifest	ファイル名	デフォルトのマニフェストファイルの代わりに使用する製品マニフェストファイルを指定します。
--no-configure		インストール後に製品を設定しないことを指定します。
-n、--no-start		インストールまたは設定後に Sentinel を起動または再起動しないことを指定します。
-r、--recordunattended	ファイル名	無人インストールで使用するパラメータを記録するファイルを指定します。
-u、--unattended	ファイル名	指定されたファイルにあるパラメータを使用して、無人のシステム上に Sentinel をインストールします。
-h、--help		Sentinel のインストール中に使用できるオプションを表示します。
-l、--log-file	ファイル名	ログメッセージをファイルに記録します。
--no-banner		バナーメッセージの表示を抑制します。
-q、--quiet		メッセージ数を減らします。
-v、--verbose		インストール時にすべてのメッセージを表示します。

11.2 インタラクティブインストールの実行

本セクションでは、標準インストールおよびカスタムインストールについて説明します。

- 72 ページのセクション 11.2.1「標準インストール」
- 73 ページのセクション 11.2.2「カスタムインストール」

11.2.1 標準インストール

次の手順に従って、標準インストールを実行します。

1. ノベル製品ダウンロード Web ページ (http://download.novell.com/index.jsp) から Sentinel インストールファイルをダウンロードします。
   - **1a** ［*製品または技術*］フィールドで［*SIEM-Sentinel*］をブラウズして選択します。
   - **1b** ［*検索*］をクリックします。
   - **1c** ［*Sentinel 7.1 Evaluation*］の［*ダウンロード*］列のボタンをクリックします。
   - **1d** ［*ダウンロードに進む*］をクリックし、お客様名とパスワードを入力します。
   - **1e** お使いのプラットフォーム用のインストールバージョンに該当する［*ダウンロード*］をクリックします。
2. コマンドラインで次のコマンドを指定して、インストールファイルを抽出します。

   ```
   tar zxvf <install_filename>
   ```

   <*install_filename*> は、実際のインストールファイル名に置き換えます。
3. インストーラを抽出したディレクトリに移動します。

   ```
   cd <directory_name>
   ```
4. 次のコマンドを指定して、Sentinel をインストールします。

   ```
   ./install-sentinel
   ```

   または

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

   ```
   ./install-sentinel -r <response_filename>
   ```
5. インストールに使用する言語の番号を指定してから、<Enter> を押します。

   エンドユーザの使用許諾契約が、選択した言語で表示されます。
6. スペースキーを押して使用許諾契約を確認します。
7. 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

   インストールパッケージをロードして環境設定のタイプの選択が求められるまで数秒かかることがあります。
8. 選択を求められたら、「1」を指定して標準環境設定に進みます。

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

9 管理者ユーザ admin のパスワードを指定します。

10 パスワードを再度確認します。

このパスワードは、admin、dbauser、および appuser が使用します。

Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

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

`https://<IP_Address_Sentinel_server>:8443.`

<*IP_Address_Sentinel_server*> は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

11.2.2 カスタムインストール

カスタム環境設定で Sentinel をインストールする場合、ライセンスキーを指定したり、ユーザごとにパスワードを変更したり、内部コンポーネントとのやり取りに使用されるポートごとに値を指定したりすることができます。

1 ノベル製品ダウンロード Web ページから Sentinel インストールファイルをダウンロードします。

1a ［*製品または技術*］フィールドで［*SIEM-Sentinel*］をブラウズして選択します。

1b ［*検索*］をクリックします。

1c ［*Sentinel 7.1 Evaluation*］の［*ダウンロード*］列のボタンをクリックします。

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

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

2 コマンドラインで次のコマンドを指定して、インストールファイルを抽出します。

`tar zxvf <install_filename>`

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

3 抽出されたディレクトリのルートで次のコマンドを指定して、Sentinel をインストールします。

`./install-sentinel`

または

このカスタム環境設定を使用して複数のシステムに Sentinel をインストールする場合は、インストールオプションをファイルに記録しておくことができます。このファイルを、他のシステムに対する Sentinel の無人インストールに使用できます。インストールオプションを記録するには、次のコマンドを指定します。

`./install-sentinel -r <response_filename>`

4 インストールに使用する言語の番号を指定してから、<Enter> を押します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

5 スペースキーを押して使用許諾契約を確認します。

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

インストールパッケージをロードして環境設定のタイプの選択が求められるまで数秒かかることがあります。

7 Sentinel のカスタム環境設定を実行する場合は、「2」を指定します。

8 デフォルトの 90 日間の評価版ライセンスキーを使用するには、「1」を入力します。

または

購入した Sentinel ライセンスキーを入力するには、「2」を入力します。

9 管理者ユーザ admin のパスワードを指定し、パスワードを再度確認します。

10 データベースユーザ dbauser のパスワードを指定し、パスワードを再度確認します。

dbauser アカウントは、Sentinel がデータベースとのやり取りに使用する ID です。ここで入力するパスワードは、管理者パスワードを忘れた場合や紛失した場合の管理者パスワードのリセット操作を含む、データベース保守タスクの実行に使用します。

11 アプリケーションユーザ appuser のパスワードを指定し、パスワードを再度確認します。

12 目的の番号を入力してから新しいポート番号を指定して、Sentinel サービスのポート割り当てを変更します。

13 ポートを変更してから「7」を指定し、完了します。

14 内部データベースのみを使用してユーザを認証するには、「1」を入力します。

または

ドメインで LDAP ディレクトリを設定している場合に、LDAP ディレクトリ認証を使用してユーザを認証するには、「2」を入力します。

デフォルト値は 1 です。

15 ***Sentinel を FIPS 140-2 モードにする場合は、***「y」を押します。

15a キーストアデータベース用の強化パスワードを指定し、そのパスワードを再確認します。

注 : パスワードは 7 文字以上にする必要があります。パスワードには、数字、ASCII 小文字、ASCII 大文字、ASCII 非英数字、および非 ASCII 文字の中から少なくとも 3 種類が含まれていなければなりません。

ASCII 大文字が最初の文字の場合、または数字が最後の文字の場合、それらは文字数にカウントされません。

15b 外部証明書をキーストアデータベースに挿入してトラストを確立する場合は、「y」を押して証明書ファイルのパスを指定します。そうしない場合は、「n」を押します。

15c 111 ページの第 19 章「FIPS 140-2 モードでの Sentinel の運用」に示されているタスクを行って、FIPS 140-2 モード設定を完了します。

Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

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

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_Sentinel_server> は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

11.3 サイレントインストールの実行

複数の Sentinel サーバをインストールして展開する必要がある場合は、サイレントインストール (無人インストール) が便利です。そのような場合には、インタラクティブインストール中にインストールパラメータを記録し、記録したファイルをその他のサーバで実行します。標準環境設定またはカスタム環境設定による Sentinel のインストール中に、インストールパラメータを記録できます。

サイレントインストールを実行する場合、インストールパラメータをファイルに記録してあることを確認してください。レスポンスファイルの作成については、72 ページのセクション 11.2.1「標準インストール」または73 ページのセクション 11.2.2「カスタムインストール」を参照してください。

Sentinel を FIPS 140－2 モードにする場合、レスポンスファイルに以下のパラメータが含まれていることを確認してください。

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

サイレントインストールを実行するには、以下のステップを行います。

1. ノベル製品ダウンロード Web ページからインストールファイルをダウンロードします。
2. Sentinel をインストールするサーバに roo t としてログインします。
3. 次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

   ```
   tar -zxvf <install_filename>
   ```

   <*install_filename*> は、実際のインストールファイル名に置き換えます。
4. 次のコマンドを指定して、Sentinel をサイレントモードでインストールします。

   ```
   ./install-sentinel -u <response_file>
   ```

   インストールは、レスポンスファイルに格納された値を使用して進行します。
5. **FIPS 140-2 モードを使用可能にする場合 ,** 111 ページの第 19 章「FIPS 140-2 モードでの Sentinel の運用」に示されているタスクを行って、FIPS 140-2 モード設定を完了します。

Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

11.4 非 root ユーザとして Sentinel をインストール

組織のポリシーによって、root として Sentinel の完全なインストールを実行することができない場合は、他のユーザとして Sentinel をインストールできます。このインストール手順では、いくつかの手順は root ユーザとして実行し、その後、root ユーザが作成した他のユーザとして Sentinel のインストールを続行します。最後に、root ユーザでインストールを完了します。

1. ノベル製品ダウンロード Web ページからインストールファイルをダウンロードします。
2. コマンドラインで次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

   ```
   tar -zxvf <install_filename>
   ```

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

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

4 次のコマンドを指定します。

```
./bin/root_install_prepare
```

root 権限で実行するコマンドの一覧が表示されます。非 root ユーザにデフォルト以外の場所に Sentinel をインストールさせたい場合は、コマンドに加えて --location オプションも指定します。例 :

```
./bin/root_install_prepare --location=/foo
```

--location オプションに渡す値 foo は、ディレクトリパスの前に付加されます。

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

5 コマンドリストを受け入れます。

表示されたコマンドが実行されます。

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

```
su novell
```

7 (条件による) インタラクティブインストールを実行するには :

7a 次のコマンドを指定します。

```
./install-sentinel
```

デフォルト以外の場所に Sentinel をインストールするには、コマンドに加えて --location オプションを指定します。例 :.

```
./install-sentinel --location=/foo
```

7b ステップ 9 に進みます。

8 (条件による) サイレントインストールを実行するには :

8a 次のコマンドを指定します。

```
./install-sentinel -u <response_file>
```

インストールは、レスポンスファイルに格納された値を使用して進行します。

8b ステップ 12 に進みます。

9 インストールに使用する言語の番号を指定します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

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

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

11 インストールのモードを指定するように求められます。

- 標準環境設定で続行する場合は、72 ページのセクション 11.2.1「標準インストール」のステップ 8 からステップ 10 に従って手順を進めます。
- カスタム環境設定で続行する場合は、73 ページのセクション 11.2.2「カスタムインストール」のステップ 7 からステップ 14 に従って手順を進めます。

12 root ユーザとしてログインし、次のコマンドを指定してインストールを完了します。

```
./bin/root_install_finish
```

Sentinel のインストールが終了し、サーバが起動します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

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

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_Sentinel_server> は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

11.5 インストール後の環境設定の変更

Sentinel のインストール後に、有効なライセンスキーを入力したり、パスワードを変更したり、割り当てられたポートを変更したりする場合は、configure.sh スクリプトを実行してこれらの変更を行います。スクリプトは /opt/novell/sentinel/setup フォルダにあります。

1. コマンドラインで次のコマンドを指定して、configure.sh スクリプトを実行します。

   ```
   ./configure.sh
   ```

2. Sentinel の標準環境設定を実行するには、「1」を指定します。カスタム環境設定を実行する場合は、「2」を指定します。
3. スペースキーを押して使用許諾契約を確認します。
4. 「yes」または「y」と入力して使用許諾契約に同意し、インストールを続行します。

   インストールパッケージをロードするのに数秒かかることがあります。
5. デフォルトの 90 日間の評価版ライセンスキーを使用するには、「1」を入力します。

   または

   購入した Sentinel ライセンスキーを入力するには、「2」を入力します。
6. 管理者ユーザ admin の既存のパスワードをそのまま使用するかどうか決定します。
   - 既存のパスワードをそのまま使用するには、「1」を入力してからステップ 7 に進みます。
   - 既存のパスワードを変更するには「2」を入力し、新しいパスワードを指定して確認してから、ステップ 7 に進みます。
7. データベースユーザ dbauser の既存のパスワードをそのまま使用するかどうか決定します。
   - 既存のパスワードをそのまま使用するには、「1」を入力してからステップ 8 に進みます。
   - 既存のパスワードを変更するには「2」を入力し、新しいパスワードを指定して確認してから、ステップ 8 に進みます。

   dbauser アカウントは、Sentinel がデータベースとのやり取りに使用する ID です。ここで入力するパスワードは、管理者パスワードを忘れた場合や紛失した場合の管理者パスワードのリセット操作を含む、データベース保守タスクの実行に使用します。
8. アプリケーションユーザ appuser の既存のパスワードをそのまま使用するかどうか決定します。
   - 既存のパスワードをそのまま使用するには、「1」を入力してからステップ 9 に進みます。
   - 既存のパスワードを変更するには「2」を入力し、新しいパスワードを指定して確認してから、ステップ 9 に進みます。

9 目的の番号を入力してから新しいポート番号を指定して、Sentinel サービスのポート割り当てを変更します。

10 ポートを変更してから「7」を指定し、完了します。

11 内部データベースのみを使用してユーザを認証するには、「1」を入力します。

または

ドメインで LDAP ディレクトリを設定している場合に、LDAP ディレクトリ認証を使用してユーザを認証するには、「2」を入力します。

デフォルト値は 1 です。

11.6 追加のコレクタマネージャのインストールおよび相関エンジンのインストール

デフォルトでは、Sentinel と一緒にコレクタマネージャと相関エンジンが 1 つずつインストールされます。ご使用の環境によっては、コレクタマネージャと相関エンジンを追加でインストールすることが必要かもしれません。コレクタマネージャと相関エンジンを追加することの利点については、68 ページのセクション 9.1「追加のコレクタマネージャの利点」および68 ページのセクション 9.2「相関エンジンを追加することの利点」を参照してください。

重要 : 追加のコレクタマネージャまたは相関エンジンは別個のシステムにインストールする必要があります。リモートコレクタマネージャまたはリモート相関エンジンを、Sentinel サーバがインストールされているのと同じシステムにインストールすることはできません。

11.6.1 インストールのチェックリスト

インストールを開始する前に、次のタスクを完了していることを確認してください。

- ❒ ハードウェアとソフトウェアが最低要件を満たしていることを確認します。詳細については、35 ページの第 5 章「システム要件を満たす」を参照してください。
- ❒ Network Time Protocol (NTP) を使用して時刻を同期します。
- ❒ コレクタマネージャは、Sentinel サーバ上のメッセージバスポート (61616) にネットワーク接続する必要があります。コレクタマネージャのインストールを開始する前に、すべてのファイアウォールおよびネットワーク設定で、このポートでの通信が許可されていることを確認します。

11.6.2 コレクタマネージャおよび相関エンジンの追加インストール

1 Web ブラウザに次の URL を入力して、Sentinel Web インタフェースを起動します。

```
https://<IP_Address_Sentinel_server>:8443.
```

<IP_Address_Sentinel_server> は Sentinel サーバの IP アドレスまたは DNS 名であり、8443 は Sentinel サーバのデフォルトポートです。

Sentinel サーバのインストール時に指定したユーザ名およびパスワードでログインします。

2 ツールバーで［*ダウンロード*］をクリックします。

3 ［コレクタマネージャ］の下の［*インストーラのダウンロード*］をクリックします。

4 ［*ファイルの保存*］をクリックして、目的の場所にインストーラを保存します。

5 次のコマンドを指定して、インストールファイルを抽出します。

```
tar zxvf <install_filename>
```

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

6 インストーラを抽出したディレクトリに移動します。

7 次のコマンドを指定して、コレクタマネージャまたは相関エンジンをインストールします。

コレクタマネージャの場合 :

```
./install-cm
```

相関エンジンの場合 :

```
./install-ce
```

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 1.5GB 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。

8 インストールに使用する言語の番号を指定します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

9 スペースキーを押して使用許諾契約を確認します。

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

環境設定のタイプの選択が求められるまで数秒かかることがあります。

11 選択を求められたら、「1」を指定して標準環境設定に進みます。

12 デフォルトの Communication Server ホスト名または、Sentinel がインストールされているマシンの IP アドレスを入力します。

13 コレクタマネージャまたは相関エンジンのユーザ名およびパスワードを指定します。

ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

14 証明書に同意するよう求められたら常に同意します。

15 「yes」または「y」を入力して、Sentinel の FIPS 140-2 モードを有効にし、FIPS 環境設定を続けます。

16 インストールが完了するまで、プロンプトの指示に従ってインストールを続行します。

11.6.3 コレクタマネージャまたは相関エンジンのカスタムユーザの追加

Sentinel では、リモートのコレクタマネージャと相関エンジンにはデフォルトのユーザ名を使用することを推奨しています。ただし、リモートのコレクタマネージャを複数インストールしており、それぞれを個別に識別する必要がある場合は、新しいユーザを作成できます。

1 Sentinel のインストールファイルにアクセスできるユーザとしてサーバにログインします。

2 activemqgroups.properties ファイルを開きます。

このファイルは /<*install_dir*>/etc/opt/novell/sentinel/config/ ディレクトリにあります。

3 次のようにコンマで区切って、新規ユーザ名を追加します。

コレクタマネージャの場合は、cm セクションに新規ユーザを追加します。たとえば、

```
cm=collectormanager,cmuser1,cmuser2,...
```

相関エンジンの場合は、admins セクションに新規ユーザを追加します。例 :

```
admins=system,correlationengine,ceuser1,ceuser2,...
```

4 ファイルを保存して閉じます。

5 activemqusers.properties ファイルを開きます。

このファイルは /<*install_dir*>/etc/opt/novell/sentinel/config/ ディレクトリにあります。

6 ステップ 3 で作成したユーザのパスワードを追加します。

このパスワードには任意のランダムな文字列を指定できます。たとえば、

コレクタマネージャユーザの場合 :

```
system=c7f34372ecd20d831cceb29e754e5ac9
collectormanager=1c51ae56
cmuser1=1b51de55
cmuser2=1a51ce57
```

相関エンジンユーザの場合 :

```
system=c7f34372ecd20d831cceb29e754e5ac9
correlationengine=68790d7a
ceuser1=69700c6d
ceuser2=70701b5c
```

7 ファイルを保存して閉じます。

8 Sentinel サーバを再起動します。

12 アプライアンスインストール

Sentinel アプライアンスは SUSE Studio で構築された、すぐに実行可能なソフトウェアアプライアンスです。このアプライアンスは、強化された SUSE Linux Enterprise Server (SLES) 11 SP 2 オペレーティングシステムと、Sentinel ソフトウェアの統合されたアップデートサービスを組み合わせて、お客様が既存の投資を活用できるよう、簡単でシームレスなユーザエクスペリエンスを提供します。ソフトウェアアプライアンスは、ハードウェアまたは仮想環境にインストールできます。

12.1 VMware アプライアンスのインストール

このセクションでは、Sentinel、コレクタマネージャ、および相関エンジンの VMware ESX サーバへのインストールについて説明します。

12.1.1 Sentinel のインストール

以下の手順を行って、Sentinel を VMware ESX サーバにインストールします。

1. ノベル製品ダウンロードのサイトから VMware アプライアンスのインストールファイルをダウンロードします。

   VMware アプライアンスの正しいファイル名には vmx が含まれますたとえば、sentinel_server_7.1.0.0.x86_64.vmx.tar.gz などです。
2. アプライアンスイメージのインストール先となる ESX データストアを確立します。
3. アプライアンスをインストールするサーバに Administrator としてログインします。
4. 次のコマンドを指定して、VM Converter がインストールされているマシンから圧縮されたアプライアンスイメージを抽出します。

   ```
   tar zxvf <install_file>
   ```

   <*install_filename*> は、実際のファイル名に置き換えます。

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

6 ESX サーバマシンにログインします。

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

8 使用する言語を選択して、［*次へ*］をクリックします。

9 キーボードのレイアウトを選択して、［*次へ*］をクリックします。

10 SUSE Linux Enterprise Server (SLES) 11 SP2 ソフトウェア使用許諾契約書の条項を確認して同意します。

11 NetIQ Sentinel の使用許諾契約の条項を確認して同意します。

12 ［ホスト名］および［ドメイン名］ページで、ホスト名とドメイン名を指定してから、［*ホスト名をループバック IP に割り当てる*］オプションが選択されていることを確認します。

13 ［*次へ*］をクリックします。ホスト名の環境設定が保存されます。

14 次のいずれかの操作を行います。

- 現在のネットワーク接続設定を使用するには、［ネットワーク環境設定 II］ページで［*次の環境設定を使用する*］を選択して、［*次へ*］をクリックます。
- ネットワーク接続設定を変更するには、［*変更*］を選択して目的の変更を行ってから、［*次へ*］をクリックします。

ネットワーク接続設定が保存されます。

15 日付と時刻を設定して、［*次へ*］をクリックします。

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

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

```
rcntp restart
```

16 root のパスワードを設定して、［*次へ*］をクリックします。

使用可能なメモリとディスク領域がチェックされます。使用可能なメモリが 2.5GB よりも少ない場合、インストールは続行できません。［*次へ*］ボタンはグレー表示となり、使用できません。

使用可能なメモリが 2.5GB 以上 6.7GB 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表示されます。このメッセージが表示されたら、［*次へ*］をクリックしてインストールを続行します。

17 Sentinel 管理者のパスワードを設定してから、［*次へ*］をクリックします。

システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

18 コンソールに表示されたアプライアンスの IP アドレスをメモします。

19 90 ページのセクション 12.4「アプライアンスのインストール後の環境設定」に従って手順を進めます。

12.1.2 コレクタマネージャおよび相関エンジンの追加インストール

最初のコレクタマネージャ、相関エンジンのインストール手順と同じですが、Novell ダウンロード Web サイトから該当するファイルをダウンロードする必要があります。

1. ノベル製品ダウンロードのサイト (http://download.novell.com/index.jsp) から VMware アプライアンスのインストールファイルをダウンロードします。

   VMware アプライアンスの正しいファイル名には vmx が含まれますたとえば、sentinel_collector_manager_7.1.0.0.x86_64.vmx.tar.gz などです。
2. アプライアンスイメージのインストール先となる ESX データストアを確立します。
3. アプライアンスをインストールするサーバに Administrator としてログインします。
4. 次のコマンドを指定して、VM Converter がインストールされているマシンから圧縮されたアプライアンスイメージを抽出します。

   ```
   tar zxvf <install_file>
   ```

   <*install_filename*> は、実際のファイル名に置き換えます。
5. VMware イメージを ESX サーバにインポートするには、VMware Converter を使用して、インストールウィザードの画面の指示に従います。
6. ESX サーバマシンにログインします。
7. インポートしたアプライアンスの VMware イメージを選択して、［*電源オン*］アイコンをクリックします。
8. コレクタマネージャが接続する Sentinel サーバのホスト名または IP アドレスを指定します。
9. Communication Server のポート番号を指定します。デフォルトのメッセージバスのポートは 61616 です。
10. JMS ユーザ名を指定します。これは、コレクタマネージャまたは相関エンジンのユーザ名です。コレクタマネージャのデフォルトユーザ名は collectormanager で、相関エンジンのデフォルトユーザ名は correlationengine です。
11. JMS ユーザのパスワードを指定します。

    ユーザ名とパスワードは、Sentinel サーバの /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。
12. (オプション) パスワードを確認するには、activemqusers.properties 内の次の行を確認します。

    コレクタマネージャの場合 :

    ```
    collectormanager=<password>
    ```

    この例では、collectormanager はユーザ名であり、対応する値はパスワードです。

    相関エンジンの場合 :

    ```
    correlationengine=<password>
    ```

    この例では、correlationengine はユーザ名であり、対応する値はパスワードです。
13. *［次へ］* をクリックします。
14. 証明書を受け入れます。

15 [*次へ*] をクリックしてインストールを完了します。

インストールが完了すると、どちらをインストールしたかに応じて、インストーラはこのアプライアンスが Sentinel コレクタマネージャまたは Sentinel 相関エンジンであることを示すメッセージと、その IP アドレスを表示します。また、Sentinel サーバのユーザインタフェース IP アドレスも表示します。

12.1.3 VMware Tools のインストール

Sentinel を VMware サーバ上で効果的に動作させるには、VMware Tools をインストールする必要があります。VMware Tools は、仮想マシンのオペレーティングシステムのパフォーマンスを向上させるユーティリティスイートです。仮想マシンの管理も改善されます。VMware Tools のインストールの詳細については、「VMware Tools for Linux Guests (https://www.vmware.com/support/ws55/doc/ws_newguest_tools_linux.html#wp1127177)」を参照してください。

VMware のマニュアルについての詳細は、『Workstation User's Manual (http://www.vmware.com/pdf/ws71_manual.pdf)』を参照してください。.

12.2 Xen アプライアンスのインストール

このセクションでは、Sentinel、コレクタマネージャ、および相関エンジンの Xen アプライアンスイメージへのインストールについて説明します。

- 84 ページのセクション 12.2.1「Sentinel のインストール」
- 86 ページのセクション 12.2.2「コレクタマネージャおよび相関エンジンの追加インストール」

12.2.1 Sentinel のインストール

以下の手順を行って、Sentinel を Xen アプライアンスイメージにインストールします。

1 Xen 仮想アプライアンスのインストールファイルをノベル製品ダウンロードのサイト (http://download.novell.com/index.jsp) から /var/lib/xen/images にダウンロードします。

Xen 仮想アプライアンスの正しいファイル名には xen が付いています。たとえば、Sentinel_7.1.0.0.x86_64.xen.tar.gz などです。

2 次のコマンドを指定して、ファイルをアンパックします。

```
tar -zxvf <install_file>
```

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

3 新しいインストールディレクトリに移動します。このディレクトリには、次のファイルがあります。

- <*file_name*>.raw
- <*file_name*>.xenconfig

4 テキストエディタを使用して <*file_name*>.xenconfig ファイルを開きます。

5 このファイルを次のように変更します。

- disk 設定の .raw ファイルのフルパスを指定します。
- ネットワーク環境設定のブリッジ設定を指定します (例 : "bridge=br0" または "bridge=xenbr0")。

- name および memory の設定値を指定します。

  たとえば、

  ```
  # -*- mode: python; -*-
  name="Sentinel_7.1.0.0.x86_64"
  memory=4096
  ```

- 次の行をコメントにします。

  ```
  vfb=["type=vnc,vncunused=1,vnclisten=0.0.0.0"]
  ```

- 次の行を追加します。

  ```
  extra = "console=hvc0 xencons=tty"
  ```

更新後の xenconfig ファイルは、次のようになります。

```
# -*- mode: python; -*-
name=install_file_name
memory=4096
disk=["tap:aio:/var/lib/xen/images/install_directory/install_filename]
vif=[ "bridge=br0" ]
#vfb=["type=vnc,vncunused=1,vnclisten=0.0.0.0"]
extra = "console=hvc0 xencons=tty"
```

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

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

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

xm list

生成されるリストに VM が表示されます。

たとえば、.xenconfig ファイルに name="Sentinel_7.1.0.0.x86_64" と環境設定した場合、その名前に VM が付されます。

8 インストールを実行するには、次のコマンドを指定します。

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

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

xm console Sentinel_7.1.0.0.x86_64

最初に使用可能なメモリとディスク領域がチェックされます。使用可能なメモリが 2.5GB よりも少ない場合、インストールは自動的に終了します。使用可能なメモリが 2.5GB 以上 6.7GB 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表示されます。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。

9 使用する言語を選択して、[*次へ*] をクリックします。

10 キーボードのレイアウトを選択して、[*次へ*] をクリックします。

11 SUSE Linux Enterprise Server (SLES) 11 SP2 ソフトウェア使用許諾契約書の条項を確認して同意します。

12 NetIQ Sentinel の使用許諾契約の条項を確認して同意します。

13 [ホスト名] および [ドメイン名] ページで、ホスト名とドメイン名を指定してから、[*ホスト名をループバック IP に割り当てる*] オプションが選択されていることを確認します。

14 *[次へ]* を選択します。ホスト名の環境設定が保存されます。

15 次のいずれかの操作を行います。

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

16 *［次へ］* を選択します。ネットワーク接続設定が保存されます。

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

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

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

```
rcntp restart
```

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

19 Sentinel 管理者のパスワードを設定してから、［*次へ*］をクリックします。

Sentinel のインストールが続行されて完了します。システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

コンソールに表示されたアプライアンスの IP アドレスをメモします。

20 90 ページのセクション 12.4「アプライアンスのインストール後の環境設定」に従って手順を進めます。

12.2.2 コレクタマネージャおよび相関エンジンの追加インストール

最初のコレクタマネージャ、相関エンジンのインストール手順と同じですが、Novell ダウンロード Web サイトから該当するファイルをダウンロードする必要があります。

1 84 ページのセクション 12.2.1「Sentinel のインストール」のステップ 1 からステップ 14 を実行します。

2 ［ネットワーク環境設定 II］画面で［*変更*］を選択して、追加のコレクタマネージャまたは相関エンジンのインストール先となる仮想マシンの IP アドレスを指定します。

3 指定した IP アドレスのサブネットマスクを指定します。

4 *［次へ］* を選択します。ネットワーク接続設定が保存されます。

5 日付と時刻を設定して、［*次へ*］を選択します。

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

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

```
rcntp restart
```

6 SUSE Enterprise Server の root のパスワードを設定して、［*次へ*］を選択します。

7 コレクタマネージャまたは相関エンジンの接続先となる Sentinel サーバのホスト名または IP アドレスを指定します。

8 Communication Server のポート番号を指定します。デフォルトのメッセージバスのポートは 61616 です。

9 JMS ユーザ名を指定します。これは、コレクタマネージャまたは相関エンジンのユーザ名です。

10 JMS ユーザのパスワードを指定します。

ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

11 (オプション) パスワードを確認するには、activemqusers.properties ファイル内の次の行を確認します。

コレクタマネージャの場合 :

```
collectormanager=<password>
```

この例では、collectormanager はユーザ名であり、対応する値はパスワードです。

相関エンジンの場合 :

```
correlationengine=<password>
```

この例では、correlationengine はユーザ名であり、対応する値はパスワードです。

12 [*次へ*] を選択してインストールを完了します。

インストールが完了すると、どちらをインストールしたかに応じて、このアプライアンスが Sentinel コレクタマネージャまたは Sentinel 相関エンジンであることを示すメッセージとその IP アドレスが表示されます。

12.3 ISO アプライアンスのインストール

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

重要 : ISO ディスクイメージを使用してハードウェア (ベアメタルおよび Hyper-V) にインストールする場合は、最低 4.5GB のメモリが必要です。

- 87 ページのセクション 12.3.1「Sentinel のインストール」
- 89 ページのセクション 12.3.2「コレクタマネージャおよび相関エンジンの追加インストール」

12.3.1 Sentinel のインストール

以下の手順を実行して、Sentinel アプライアンスをハードウェアにインストールします。

1 DVD ドライブからその DVD を使用して物理マシンをブートします。

2 インストールウィザードの画面の指示に従います。

3 ブートメニューの一番上のエントリを選択して、ライブ DVD のアプライアンスイメージを実行します。

最初に使用可能なメモリとディスク領域がチェックされます。使用可能なメモリが 2.5GB よりも少ない場合、インストールは自動的に終了します。使用可能なメモリが 2.5GB 以上 6.7GB 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表示されます。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。

4 使用する言語を選択して、［*次へ*］をクリックします。

5 キーボードのレイアウトを選択して、［*次へ*］をクリックします。

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

7 NetIQ Sentinel の使用許諾契約の条項を確認して同意します。

8 ［*次へ*］を選択します。

9 ［ホスト名］および［ドメイン名］ページで、ホスト名とドメイン名を指定してから、［*ホスト名をループバック IP に割り当てる*］オプションが選択されていることを確認します。

10 ［*次へ*］を選択します。ホスト名の環境設定が保存されます。

11 次のいずれかの操作を行います。

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

12 *［次へ］*を選択します。ネットワーク接続設定が保存されます。

13 日付と時刻を設定して、［*次へ*］をクリックします。

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

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

```
rcntp restart
```

14 root のパスワードを設定して、［*次へ*］をクリックします。

15 Sentinel 管理者のパスワードを設定してから、［*次へ*］をクリックします。

16 コンソールでユーザ名とパスワードを入力して、アプライアンスにログインします。

ユーザ名のデフォルト値は root で、パスワードはステップ 14 で設定されたものです。

17 Sentinel サーバを停止します。

```
service sentinel stop
```

18 次のコマンドを入力して UI をリセットし、YaST での表示を整頓します。

```
reset
```

19 アプライアンスを物理サーバにインストールする場合は、［*Install Sentinel appliance to hard drive (for Live DVD image only)*］チェックボックスが選択されていることを確認してください。

デフォルトではこのオプションが選択されています。このチェックボックスのチェックを外すと、アプライアンスは物理サーバにインストールされず、LIVE DVD モードのみで実行されます。

システムが一度初期化を実行するため、インストール後にすべてのサービスを起動するのに数分かかることがあります。インストールが完了してから、サーバにログインしてください。

20 コンソールに表示されたアプライアンスの IP アドレスをメモします。

21 90 ページのセクション 12.4「アプライアンスのインストール後の環境設定」に従って手順を進めます。

12.3.2 コレクタマネージャおよび相関エンジンの追加インストール

最初のコレクタマネージャ、相関エンジンのインストール手順と同じですが、Novell ダウンロード Web サイトから該当するファイルをダウンロードする必要があります。

1 87 ページのセクション 12.3.1「Sentinel のインストール」のステップ 1 からステップ 14 を実行します。

2 コレクタマネージャが接続する Sentinel サーバのホスト名または IP アドレスを指定します。

3 Communication Server のポート番号を指定します。デフォルトのメッセージバスのポートは 61616 です。

4 JMS ユーザ名を指定します。これは、コレクタマネージャまたは相関エンジンのユーザ名です。

5 JMS ユーザのパスワードを指定します。

6 *[次へ]* をクリックします。

ユーザ名とパスワードは、Sentinel サーバにある /<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ファイルに保存されます。

7 パスワードを確認するには、activemqusers.properties ファイル内の次の行を確認します。

コレクタマネージャの場合 :

```
collectormanager=<password>
```

この例では、collectormanager はユーザ名であり、対応する値はパスワードです。

相関エンジンの場合 :

```
correlationengine=<password>
```

この例では、correlationengine はユーザ名であり、対応する値はパスワードです。

8 アプライアンスを物理サーバにインストールする場合は、[*Install Sentinel appliance to hard drive (for Live DVD image only)*] チェックボックスが選択されていることを確認してください。

デフォルトではこのオプションが選択されています。このチェックボックスの選択を解除すると、アプライアンスは物理サーバにインストールされず、LIVE DVD モードでのみ実行されます。

9 同意を求められたら、証明書に同意します。

10 「yes」または「y」を入力して、Sentinel の FIPS 140-2 モードを有効にし、FIPS 環境設定を続けます。

11 インストールが完了するまで、プロンプトの指示に従ってインストールを続行します。

インストールが完了すると、どちらをインストールしたかに応じて、このアプライアンスが Sentinel コレクタマネージャまたは Sentinel 相関エンジンであることを示すメッセージとその IP アドレスが表示されます。また、Sentinel サーバのユーザインタフェース IP アドレスも表示します。

12.4 アプライアンスのインストール後の環境設定

Sentinel をインストールした後、アプライアンスが正常に動作するように環境設定をさらに行う必要があります。

12.4.1 WebYaST の環境設定

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

1. Sentinel アプライアンスにログインします。
2. ［*アプライアンス*］をクリックします。
3. 91 ページのセクション 12.4.3「アップデートの登録」の説明にあるように、アップデートを受信する Sentinel サーバの環境設定を行います。
4. ［*次へ*］をクリックして、初期設定を完了します。

12.4.2 パーティションの作成

YaST ツールを使用して、アプライアンスにパーティションを追加し、新しいパーティションにディレクトリを移動させることができます。

次の手順で新しいパーティションを作成し、データファイルを元のディレクトリから新しく作成したパーティションに移動させます。

1. Sentinel に root としてログインします。
2. 次のコマンドを実行して、アプライアンス上の Sentinel を停止させます。

   /etc/init.d/sentinel stop
3. 次のコマンドを指定して、novell ユーザに変更します。

   su -novell
4. /var/opt/novell/sentinel のディレクトリの内容を一時的にどこかの場所に移動します。
5. root ユーザに変更します。
6. 次のコマンドを入力して、YaST2 コントロールセンターにアクセスします。

   ```
   yast
   ```
7. *［システム］* > *［パーティショナ］* の順に選択します。
8. 警告を確認して［*はい*］を選択し、新しい未使用パーティションを追加します。
9. /var/opt/novell/sentinel に新しいパーティションをマウントします。

10 次のコマンドを指定して、novell ユーザに変更します。

su -novell

11 ディレクトリの内容を一時保存先 (ステップ 4 で保存した場所) から、新しいパーティション内の /var/opt/novell/sentinel に戻します。

12 次のコマンドを実行して、Sentinel アプライアンスを再起動します。

/etc/init.d/sentinel start

12.4.3 アップデートの登録

Sentinel アプライアンスをアプライアンス更新チャネルに登録して、パッチの更新を受信できるようにする必要があります。アプライアンスを登録するには、まずアプライアンス登録コードまたはアプライアンスアクティベーションキーを Novell Customer Care Center から取得する必要があります。

以下の手順を行って、更新できるようにアプライアンスを登録します。

1 Sentinel アプライアンスにログインします。

2 ［*アプライアンス*］をクリックして、WebYaST を起動します。

3 ［*登録*］をクリックします。

4 アップデートを受信する電子メール ID を指定してから、システム名およびアプライアンス登録コードを指定します。

5 *［保存］* をクリックします。

12.4.4 SMT でのアプライアンスの設定

インターネットに直接アクセスできない保護された環境でアプライアンスを実行する必要がある場合は、Subscription Management Tool (SMT) でアプライアンスを設定できます。これにより、Sentinel の最新バージョンが公開されると、アプライアンスを最新バージョンにアップグレードできます。SMT は、ノベルカスタマセンターと統合されたパッケージ代理システムで、主な Novell Customer Center 機能を提供します。

- 91 ページの 「前提条件」
- 92 ページの 「アプライアンスの設定」
- 92 ページの 「アプライアンスのアップグレード」

前提条件

- 更新する Sentinel 用の Novell Customer Center 資格情報を Novell から入手します。資格情報の取得の詳細については、Novell サポートに問い合わせてください。
- SMT をインストールするマシンに次のパッケージと共に SLES 11 SP2 がインストールされていることを確認します。
  - htmldoc
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - perl-DBIx-Migration-Director
  - perl-MIME-Lite

- perl-Text-ASCIITable
- yum-metadata-parser
- createrepo
- perl-DBI
- apache2-prefork
- libapr1
- perl-Data-ShowTable
- perl-Net-Daemon
- perl-Tie-IxHash
- fltk
- libapr-util1
- perl-PIRPC
- apache2-mod_perl
- apache2-utils
- apache2
- perl-DBD-mysql

- SMT をインストールし、SMT サーバを設定します。詳細については、SMT のマニュアルの以下に関するセクションを参照してください。
  - SMT のインストール
  - SMT サーバの設定
  - SMT でのインストールと更新リポジトリのミラーリング
- アプライアンスコンピュータに wget ユーティリティをインストールします。

アプライアンスの設定

SMT を使用したアプライアンスの環境設定については、『Subscription Management Tool (SMT) for SUSE Linux Enterprise 11』マニュアルを参照してください。

アプライアンスリポジトリを有効にするには、次のコマンドを実行します。

```
smt-repos -e Sentinel-Server-7.0-Updates sle-11-x86_64
```

```
smt-repos -e Sentinel-Collector-Manager-7.0-Updates sle-11-x86_64
```

```
smt-repos -e Sentinel-Correlation-Engine-7.0-Updates sle-11-x86_64
```

アプライアンスのアップグレード

アプライアンスのアップグレードについては、128 ページのセクション 21.3「SMT を使用したアプライアンスのアップグレード」を参照してください。

12.5 WebYaST を使用したサーバの起動と停止

次のように Web インタフェースを使用して、Sentinel サーバを起動および停止できます。

1. Sentinel アプライアンスにログインします。
2. ［*アプライアンス*］をクリックして、WebYaST を起動します。
3. ［*システムサービス*］をクリックします。
4. Sentinel サーバを停止するには、［*停止*］をクリックします。
5. Sentinel サーバを起動するには、［*開始*］をクリックします。

13 コレクタとコネクタの追加インストール

デフォルトでは、Sentinel をインストールすると、リリースされているすべてのコレクタおよびコネクタがインストールされます。Sentinel のリリース以後にリリースされた新しいコレクタまたはコネクタをインストールする場合は、以下のセクションにある情報を参考にしてください。

- 95 ページのセクション 13.1「コレクタのインストール」
- 95 ページのセクション 13.2「コネクタのインストール」

13.1 コレクタのインストール

次の手順に従って、コレクタをインストールします。

1. Sentinel プラグインの Web ページから、希望するコレクタをダウンロードします。
2. https://<*IP address*>:8443 で Sentinel Web インタフェースにログインします。8443 は、Sentinel サーバのデフォルトポートです。
3. ツールバーで［*アプリケーション*］をクリックしてから、［*アプリケーション*］をクリックします。
4. ［*コントロールセンターの起動*］をクリックして Sentinel コントロールセンターを起動します。
5. ツールバーで、［*イベントソースの管理*］>［*ライブビュー*］の順にクリックし、［*ツール*］>［*プラグインのインポート*］の順にクリックします。
6. ステップ 1 でダウンロードしたコレクタファイルをブラウズして選択してから、［*次へ*］をクリックします。
7. 残りのプロンプトに従った後、［*終了*］をクリックします。

コレクタを環境設定するには、Sentinel プラグイン Web サイトにある、特定のコレクタのマニュアルを参照してください。

13.2 コネクタのインストール

次の手順に従って、コネクタをインストールします。

1. Sentinel プラグイン Web サイトから、希望するコネクタをダウンロードします。
2. https://<*IP address*>:8443 で Sentinel Web インタフェースにログインします。8443 は、Sentinel サーバのデフォルトポートです。
3. ツールバーで［*アプリケーション*］をクリックしてから、［*アプリケーション*］をクリックします。
4. ［*コントロールセンターの起動*］をクリックして Sentinel コントロールセンターを起動します。
5. ツールバーで、［*イベントソースの管理*］>［*ライブビュー*］の順に選択し、［*ツール*］>［*プラグインのインポート*］の順にクリックします。

6 ステップ 1 でダウンロードしたコネクタファイルをブラウズして選択してから、［次へ］をクリックします。

7 残りのプロンプトに従った後、［終了］をクリックします。

コネクタを環境設定するには、Sentinel プラグイン Web サイトにある、特定のコネクタのマニュアルを参照してください。

14 インストールの検証

次のいずれかを実行することにより、インストールが成功したかどうかを判断することができます。

- Sentinel のバージョンを確認する：

  ```
  /etc/init.d/sentinel version
  ```

- Sentinel サービスが実行中であるかどうかを確認する：

  ```
  /etc/init.d/sentinel status
  ```

- Web サービスが実行中であるかどうかを確認する：

  ```
  netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
  ```

  デフォルトのポート番号は 8443 です。

- Sentinel Web インタフェースにアクセスする：

  1. サポートされている Web ブラウザを起動します。
  2. Sentinel Web インタフェースの URL を指定する：

     ```
     https://<IP_Address/DNS_Sentinel_server:8443>
     ```

     「IP_Address_Sentinel_server」は Sentinel サーバの IP アドレスまたは DNS 名であり、「8443」は Sentinel サーバのデフォルトポートです。
  3. インストール時に指定した管理者名とパスワードでログインします。デフォルトのユーザ名は admin です。

15 Sentinel のディレクトリ構造

デフォルトでは、Sentinel のディレクトリは次の場所にあります。

- データファイルは、/var/opt/novell/sentinel/data ディレクトリおよび /var/opt/novell/sentinel/3rdparty ディレクトリにあります。
- 実行可能ファイルとライブラリは、次の場所にあります。
  - /opt/novell/sentinel/bin
  - /opt/novell/sentinel/setup
  - /opt/novell/sentinel/3rdparty
- ログファイルは、/var/opt/novell/sentinel/log ディレクトリにあります。
- 環境設定ファイルは、/etc/opt/novell/sentinel ディレクトリにあります。
- プロセス ID (PID) ファイルは、/var/run/sentinel/server.pid ディレクトリにあります。

  PID を使用すると、管理者は Sentinel サーバの親プロセスを識別し、プロセスを監視または終了することができます。

IV Sentinel の環境設定

このセクションでは、Sentinel および付属プラグインの環境設定について説明します。

16 時刻の設定

イベントの時刻は、Sentinel におけるイベントの処理には不可欠のものです。これはリアルタイム処理だけでなく、レポートや監査のためにも重要です。このセクションでは、Sentinel における時刻の意味、時刻の設定方法、およびタイムゾーンの取り扱いについて説明します。

16.1 Sentinel における時刻について

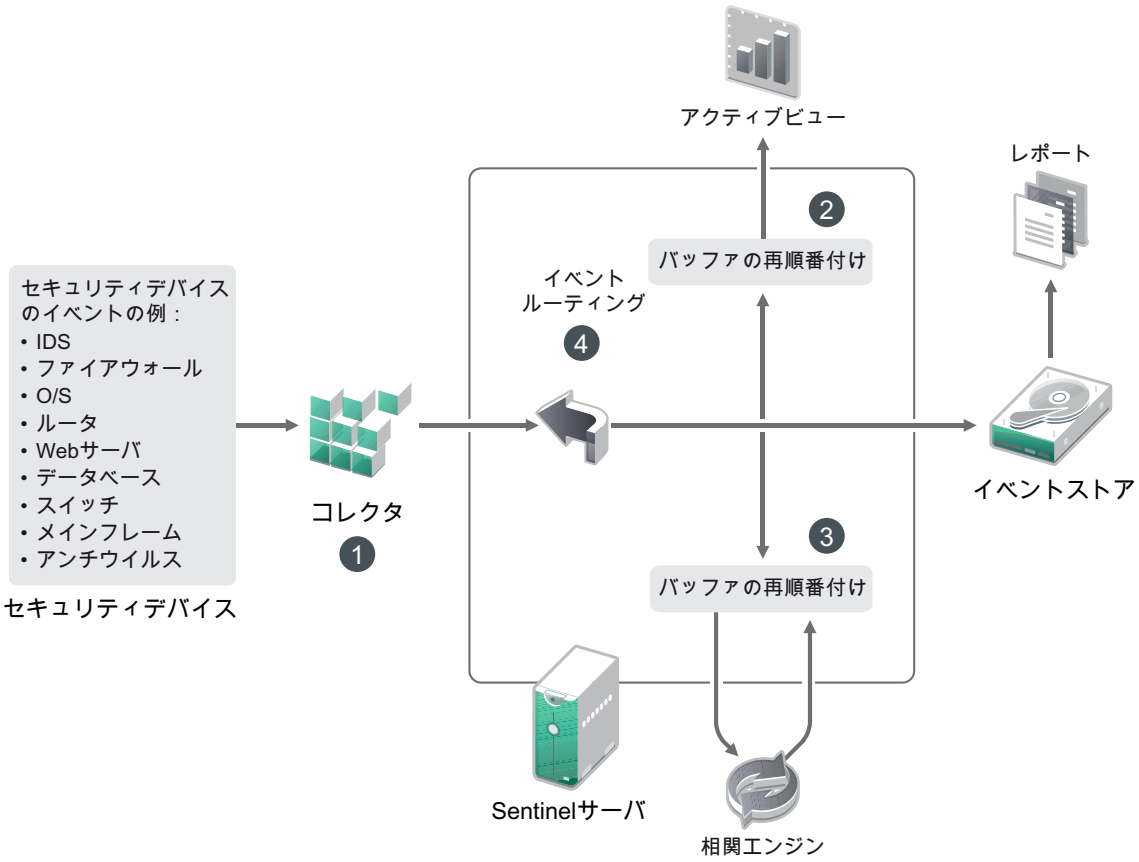
Sentinel は、ネットワーク全体に分散するいくつものプロセスで構成される分散システムです。また、イベントソースによって多少の遅延が発生する可能性があります。これに対応するために、Sentinel プロセスは、イベントを処理する前に、イベントを時間順に並び替えます。

どのイベントにも 3 つの時刻フィールドがあります。

- **イベント時刻 :** これは、すべての分析エンジン、検索、レポートなどで使用されるイベント時刻です。
- **Sentinel 処理時刻 :** Sentinel がデバイスからデータを収集した時刻で、この時刻はコレクタマネージャのシステム時間から取得されます。
- **オブザーバイベント時刻 :** デバイスがデータに書き込んだタイムスタンプ。データに書き込まれたタイムスタンプは必ずしも信頼できるとは限らず、Sentinel 処理時刻と大きく異なっていることもあります。たとえば、デバイスがデータをバッチ処理で送信するとします。

次の図は、Sentinel がこれをどのように処理するのかを示しています。

図 16-1 *Sentinel の時刻*



1. デフォルトでは、イベント時刻は Sentinel 処理時刻に設定されます。しかし、オブザーバイベント時刻を利用でき、それが信頼に値するのであれば、イベント時刻がオブザーバイベント時刻と一致するのが理想的です。デバイス時刻を利用でき、正確で、コレクタが正しく解析できるのであれば、データ収集を［**信頼イベントソース時刻**］に設定するのが最善です。コレクタは、オブザーバイベント時刻に合うようにイベント時刻を設定します。
2. イベント時刻がサーバ時刻の前後 5 分以内であるイベントは、アクティブビューによって普通に処理されます。イベント時刻が 5 分以上進んでいるイベントは、アクティブビューには表示されませんが、イベントストアには挿入されます。イベント時刻が 5 分以上進んでいるイベントと過去 24 時間以内のイベントは、チャートには表示されますが、チャートのイベントデータには表示されません。これらのイベントをイベントストアから取得するには、ドリルダウン操作が必要です。
3. 相関エンジンはイベントを時間順に処理することができるように、イベントは 30 秒間隔でソートされます。イベント時刻がサーバ時刻よりも 30 秒を超えて古い場合、相関エンジンはイベントを処理しません。
4. イベント時刻がコレクタマネージャシステム時刻より 5 分を超えて古い場合、Sentinel はイベントを直接イベントストアにルーティングし、相関、アクティブビュー、セキュリティインテリジェンスなどのリアルタイムシステムはバイパスします。

16.2 Sentinel における時刻の設定

相関エンジンは、時間順に並べられたイベントのストリームを処理し、イベント内のパターンおよびストリーム内の時系列パターンを検出します。しかし、時々、イベントを生成するデバイスについてログメッセージに時刻が組み込まれないことがあります。Sentinel で時刻を正しく取り扱えるように設定するには、次の 2 つの方法があります。

- コレクタマネージャで NTP を設定し、イベントソースマネージャのイベントソース上で［*信頼イベントソース時刻*］の選択を解除します。Sentinel は、イベント時刻のソースとしてコレクタマネージャを使用します。
- イベントソースマネージャのイベントソース上で［*信頼イベントソース時刻*］を選択します。Sentinel は、ログメッセージの時刻を正しい時刻として使用します。

この設定をイベントソース上で変更するには :

1 ［イベントソースの管理］にログインします。

詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「「Accessing Event Source Management」」を参照してください。

2 時刻の設定を変更するイベントソースを右クリックしてから、［*編集*］を選択します。

3 ［*全般*］タブの下の［*Trust Event Source*］オプションを選択または選択解除します。

4 ［OK］*をクリックして変更内容を保存します。*

16.3 タイムゾーンの処理

分散環境では、タイムゾーンの処理が複雑になる場合があります。たとえば、あるタイムゾーンにイベントソースがあり、別のタイムゾーンにコレクタマネージャがあり、また別のタイムゾーンにバックエンドの Sentinel サーバがあり、さらに別のタイムゾーンでクライアントがデータを表示している場合などです。さらに夏時間や、設定されているタイムゾーンをレポートしないイベントソース (すべての Syslog ソースなど) を考慮すると、処理を必要とする問題は多くあります。Sentinel は、イベントが実際に発生した時刻を正しく示し、これらのイベントを同じタイムゾーンまたは別のタイムゾーンの他のイベントと比較することを可能にする柔軟性を備えています。

一般的に、イベントソースがタイムスタンプをレポートする方法は 3 通りあります。

- イベントソースが UTC で時刻をレポートする場合。たとえば、Windows イベントログの標準的なイベントはすべて、常に UTC でレポートされます。
- イベントソースがローカル時刻でレポートを行い、タイムスタンプにタイムゾーン情報が含まれている場合。たとえば、RFC3339 に従ってタイムスタンプを構成するイベントソースはすべて、オフセットとしてタイムゾーンを含みます。他のソースはアメリカ / ニューヨークなどの長いタイムゾーン ID、または EST などの短いタイムゾーン ID をレポートするため、不一致や不適切な解決などによる問題が発生する場合があります。
- イベントソースがローカル時刻でレポートし、タイムゾーン情報を含まない場合。残念ながら、とてもよく使われる Syslog フォーマットはこの形です。

最初の方法では、イベントが発生した絶対 UTC 時刻を計算できるため (時刻同期プロトコルが使用されていると想定)、そのイベントの時刻を他の世界中のイベントソースと容易に比較できます。ただし、イベントが発生したときのローカル時刻は自動的には判断できません。このため、Sentinel では、イベントソースのタイムゾーンを手動で設定できるようになっています。これは、イベントソースマネージャでイベントソースノードを編集して、適切なタイムゾーンを指定することにより

可能です。この情報は［DeviceEventTime］や［EventTime］の計算には影響しませんが、［ObserverTZ］フィールドに取り込まれ、［ObserverTZHour］などの多様な［ObserverTZ］フィールドの計算に使用されます。これらのフィールドは、常にローカル時刻で示されます。

2 つめの方法では、長い形式のタイムゾーン ID またはオフセットが使用されている場合、UTC に変換して絶対的な標準 UTC 時刻 (［DeviceEventTime］に格納される) を取得できますが、ローカル時刻の［ObserverTZ］フィールドも計算できます。短い形式のタイムゾーン ID が使用されている場合、不一致が発生する可能性があります。

3 つめの方法では、Sentinel が UTC 時刻を正しく計算できるよう、影響を受けるすべてのソースのイベントソースタイムゾーンを管理者が手動で設定する必要があります。イベントソースマネージャでイベントソースノードを編集してタイムゾーンを正しく指定していない場合、［DeviceEventTime］(および、多くの場合は［EventTime］) が正しくない可能性があり、［ObserverTZ］および関連するフィールドも正しくない場合があります。

一般的に、特定のイベントソース (たとえば、Microsoft Windows など) 用のコレクタは、イベントソースからのタイムスタンプの形式が判明しているため、それに応じて調整を行います。イベントソースがローカル時刻でレポートし、タイムスタンプに常にタイムゾーンが含まれているのでない限り、イベントソースマネージャでイベントソースノードすべてに対して手動でタイムゾーンを設定することをお勧めします。

イベントソースからのタイムスタンプ情報は、コレクタおよびコレクタマネージャ上で処理されます。［DeviceEventTime］および［EventTime］は UTC として格納され、［ObserverTZ］フィールドはイベントソースのローカル時刻の文字列として格納されます。この情報はコレクタマネージャから Sentinel サーバに送信され、イベントストア内に格納されます。コレクタマネージャおよび Sentinel サーバが配置されたタイムゾーンは、このプロセスにも格納されるデータにも影響しません。ただし、クライアントが Web ブラウザでイベントを確認する場合、UTC の［EventTime］は Web ブラウザによってローカル時刻に変換されます。そのため、クライアントには、すべてのイベントがローカルのタイムゾーンで示されます。ユーザがソースのローカル時刻を知りたい場合は、［ObserverTZ］フィールドで詳細を確認できます。

17 付属プラグインの環境設定

デフォルトで、Sentinel にはいくつかのプラグインが付属しています。本章では、付属プラグインの環境設定を行う方法について説明します。

17.1 ソリューションパックの環境設定

Sentinel には、分析に関する多数のニーズに合わせて、導入後直ちに使用可能なさまざまなコンテンツが同梱されています。コンテンツの多くは、プリインストールされた Sentinel Core ソリューションパックおよび ISO 27000 Series のソリューションパックの一部です。詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「「Using Solution Packs」」を参照してください。

ソリューションパックによって、コンテンツを 1 つのユニットとして扱われるコントロールやポリシーセットに分類したり、グループにまとめたりすることができます。この導入後直ちに使用可能なコンテンツを提供するためにソリューションパックのコントロールがプリインストールされていますが、これらのコントロールは Sentinel Web コンソールを使用して、形式に沿って実装またはテストする必要があります。

Sentinel の実装が設計どおりに機能していることをある程度厳密に確認する場合は、ソリューションパックに組み込まれた形式的検証プロセスを使用できます。この検証プロセスでは、他のソリューションパックのコントロールの実装とテストを行う場合と全く同じように、ソリューションパックコントロールを実装およびテストします。このプロセスの一環として、実装担当者とテスト担当者が作業を完了したことを検証します。次に、これらの検証が監査証跡に含められ、特定のコントロールが正しく展開されたことを確認できます。

検証プロセスは、ソリューションマネージャを使用して実施できます。詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「「Installing and Managing Solution Packs」」を参照してください。

17.2 コレクタ、コネクタ、インテグレータ、およびアクションの環境設定

付属プラグインの環境設定については、Sentinel プラグイン Web サイトにある特定のプラグインマニュアルを参照してください。

18 既存の Sentinel インストール環境を FIPS 140 – 2 モードにする

本章では、Sentinel の既存インストール環境を FIPS 140 – 2 モードにする方法について説明します。

注 : Sentinel が /opt/novell/sentinel ディレクトリにインストールされていることを前提としています。コマンドは novell ユーザとして実行する必要があります。

18.1 Sentinel サーバを FIPS 140-2 モードで実行する

Sentinel サーバを FIPS 140-2 モードで実行できるようにするには :

1. Sentinel サーバにログインします。
2. novell ユーザ (su novell) に切り替えます。
3. Sentinel の bin ディレクトリを参照します。
4. convert_to_fips.sh スクリプトを実行して、画面の指示に従います。
5. 111 ページの第 19 章「FIPS 140-2 モードでの Sentinel の運用」に示されているタスクを行って、FIPS 140-2 モード設定を完了します。

18.2 リモートコレクタマネージャおよび相関エンジンで FIPS 140-2 モードを有効にする

FIPS 140-2 モードで実行している Sentinel サーバとの接続で FIPS 認定通信を使用する場合は、リモートのコレクタマネージャおよび相関エンジンで FIPS 140-2 モードを有効にする必要があります。

リモートのコレクタマネージャまたは相関エンジンを FIPS 140-2 モードで動作させるには :

1. リモートのコレクタマネージャまたは相関エンジンのシステムにログインします。
2. novell ユーザ (su novell) に切り替えます。
3. bin ディレクトリを参照します。デフォルトの場所は /opt/novell/sentinel/bin です。

4 convert_to_fips.sh スクリプトを実行して、画面の指示に従います。

5 111 ページの第 19 章「FIPS 140-2 モードでの Sentinel の運用」に示されているタスクを行って、FIPS 140-2 モード設定を完了します。

19 FIPS 140-2 モードでの Sentinel の運用

本章では、FIPS 140-2 モードの Sentinel の環境設定と運用について説明します。

19.1 Advisor サービスを FIPS 140-2 モードで実行するように環境設定する

Advisor サービスはセキュアな HTTPS 接続を使用して、Advisor サーバからフィードフォームをダウンロードします。サーバがセキュア通信に使用している証明書が、Sentinel FIPS キーストアデータベースに追加される必要があります。

リソース管理データベースに正常に登録されたことを検証するには :

1. Advisor サーバから証明書をダウンロードして、そのファイルに advisor.cer という名前を付けて保存します。
2. Advisor サーバ証明書を Sentinel FIPS キーストアにインポートします。

   証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

19.2 分散検索を FIPS 140-2 モードで実行するように環境設定する

このセクションでは、分散検索を FIPS 140-2 モードで実行するように環境設定する方法について説明します。

シナリオ 1: ソースとターゲットの両方の Sentinel サーバが FIPS 140-2 モードである

FIPS 140-2 モードで実行されている複数の Sentinel サーバにわたって分散検索を実行できるようにするには、セキュア通信で使用する証明書を FIPS キーストアに追加する必要があります。

1. 分散検索ソースコンピュータにログインします。
2. 証明書ディレクトリを参照します。

   ```
   cd <sentinel_install_directory>/config
   ```

3. ソース証明書 (sentinel.cer) をターゲットコンピュータの一時的な場所にコピーします。
4. ソース証明書をターゲットの Sentinel FIPS キーストアにインポートします。

   証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。
5. 分散検索ターゲットコンピュータにログインします。
6. 証明書ディレクトリを参照します。

   ```
   cd /etc/opt/novell/sentinel/config
   ```

7. ターゲット証明書 (sentinel.cer) をソースコンピュータの一時的な場所にコピーします。
8. ターゲットシステム証明書をソースの Sentinel FIPS キーストアにインポートします。
9. ソースコンピュータとターゲットコンピュータの両方で Sentinel サービスを再起動します。

シナリオ 2: ソース Sentinel サーバが非 FIPS モードであり、ターゲット Sentinel サーバが FIPS 140-2 モードである

ソースコンピュータの Web サーバキーストアを証明書フォーマットに変換してから、証明書をターゲットコンピュータにエクスポートする必要があります。

1. 分散検索ソースコンピュータにログインします。
2. 証明書 (.cer) 形式で、Web サーバキーストアを作成します。

   ```
   <sentinel_install_directory>/jre/bin/keytool -export -alias webserver -
   keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
   password -file <certificate_name.cer>
   ```

3. 分散検索ソース証明書 (Sentinel.cer) を分散検索ターゲットコンピュータの一時的な場所にコピーします。
4. 分散検索ターゲットコンピュータにログインします。
5. ソース証明書をターゲットの Sentinel FIPS キーストアにインポートします。

   証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。
6. ターゲットコンピュータの Sentinel サービスを再起動します。

シナリオ 3: ソース Sentinel サーバが FIPS モードであり、ターゲット Sentinel サーバが非 FIPS モードである

1. 分散検索ターゲットコンピュータにログインします。
2. 証明書 (.cer) 形式で、Web サーバキーストアを作成します。

   ```
   <sentinel_install_directory>/jre/bin/keytool -export -alias webserver -
   keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
   password -file <certificate_name.cer>
   ```

3. 証明書を分散検索ソースコンピュータの一時的な場所にコピーします。

4 ターゲット証明書をソースの Sentinel FIPS キーストアにインポートします。

証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

5 ソースコンピュータの Sentinel サービスを再起動します。

19.3 LDAP 認証を FIPS 140-2 モードで実行するように環境設定する

FIPS 140-2 モードで実行している Sentinel サーバに対して LDAP 認証を設定するには :

1 LDAP 管理者から LDAP サーバ証明書を入手します。または、コマンドを使用することもできます。たとえば、

```
openssl s_client -connect <LDAP server IP>:636
```

コマンド実行後に返されるテキスト (BEGIN 行と END 行の間) をファイルにコピーします。

2 LDAP サーバ証明書を Sentinel FIPS キーストアにインポートします。

証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

3 Sentinel Web コンソールに管理者の役割のユーザとしてログインして、LDAP 認証の設定を続行します。

詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「*Configuring LDAP Authentication*」を参照してください。

注 : FIPS 140-2 モードで実行している Sentinel サーバの LDAP 認証の設定は、/opt/novell/sentinel/setup ディレクトリにある ldap_auth_config.sh スクリプトを実行することによっても行えます。

19.4 リモートコレクタマネージャおよび相関エンジンのサーバ証明書の更新

既存のリモートコレクタマネージャおよびリモート相関エンジンを FIPS 140-2 モードで実行している Sentinel サーバと通信するように設定するには、リモートシステムを FIPS 140-2 モードに変換するか、またはリモートシステムに対して Sentinel サーバ証明書を更新してコレクタマネージャまたは相関エンジンを非 FIPS モードのままにしておきます。FIPS モードのリモートコレクタマネージャは、FIPS モードをサポートしないイベントソース、またはまだ FIPS が使用可能になっていない Sentinel コネクタのうちのいずれかを必要とするイベントソースと連携できない可能性があります。

リモートのコレクタマネージャまたは相関エンジンで FIPS140-2 モードを有効にしない場合は、最新の Sentinel サーバ証明書をリモートシステムにコピーして、コレクタマネージャまたは相関エンジンが Sentinel サーバと通信できるようにする必要があります。

リモートのコレクタマネージャまたは相関エンジンの Sentinel サーバ証明書を更新するには :

1 リモートのコレクタマネージャまたは相関エンジンのコンピュータにログインします。

2 novell ユーザ (su novell) に切り替えます。

3 bin ディレクトリを参照します。デフォルトの場所は /opt/novell/sentinel/bin です。

4 updateServerCert.sh スクリプトを実行して、画面の指示に従います。

19.5 Sentinel プラグインを FIPS 140-2 モードで実行するように環境設定する

このセクションでは、さまざまな Sentinel プラグインを FIPS 140-2 モードで実行するための設定について説明します。

注 : Sentinel が /opt/novell/sentinel ディレクトリにインストールされていることを前提としています。コマンドは novell ユーザとして実行する必要があります。

19.5.1 エージェントマネージャコネクタ

エージェントマネージャイベントソースサーバのネットワーク設定時に［*暗号化 (HTTPS)*］オプションを選択した場合にのみ、以下の手順に従ってください。

エージェントマネージャコネクタを FIPS 140-2 モードで実行するように設定するには :

1 エージェントマネージャイベントソースサーバを追加または編集します。［セキュリティ］ウィンドウが表示されるまで、設定画面を進めていきます。詳細については、『*Agent Manager Connector Guide*』を参照してください。

2 ［*クライアント認証のタイプ*］フィールドでオプションを 1 つ選択します。クライアント認証タイプによって、SSL エージェントマネージャイベントソースサーバがデータの送信を試行しているエージェントマネージャイベントソースの ID をどの程度厳密に検証するかが決まります。

- **開く :** エージェントマネージャエージェントから着信するすべての SSL 接続を許可します。クライアント証明書の検証または認証は行いません。
- **厳密 :** 証明書が有効な X.509 証明書であるかを検証し、クライアント証明書がイベントソースサーバによって信頼されていることも確認します。新規ソースは Sentinel に明示的に追加する必要があります (そうすることで、不正なソースが認証されていないデータを送信できないようにします)。

［*厳密*］オプションの場合、各新規エージェントマネージャクライアントの証明書を Sentinel FIPS キーストアにインポートする必要があります。Sentinel が FIPS 140-2 モードで動作しているときは、イベントソース管理 (ESM) インタフェースを使用してクライアント証明書をインポートすることはできません。

証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

注 : FIPS 140-2 モードでは、エージェントマネージャイベントソースサーバは Sentinel サーバキーを使用するため、サーバキーペアのインポートは必須ではありません。

3 エージェントでサーバ認証が有効になっている場合、コネクタが展開されている場所に応じて、Sentinel サーバ証明書かリモートコレクタマネージャ証明書を信頼するようにエージェントも設定する必要があります。

Sentinel サーバ証明書がある場所 : /etc/opt/novell/sentinel/config/sentinel.cer

リモートコレクタマネージャ証明書がある場所 : /etc/opt/novell/sentinel/config/rcm.cer

注 : 認証局 (CA) によってデジタル署名されているカスタム証明書を使用している場合は、エージェントマネージャエージェントが適切な証明書ファイルを信頼していなければなりません。

19.5.2 データベース (JDBC) コネクタ

データベース接続の設定時に［*SSL*］オプションを選択した場合にのみ、以下の手順に従います。

データベースコネクタを FIPS 140-2 モードで実行するように設定するには :

1 コネクタを設定する前に、データベースサーバから証明書をダウンロードし、database.cert というファイル名にして、Sentinel サーバの /etc/opt/novell/sentinel/config ディレクトリに保存します。

詳細については、各データベースのマニュアルを参照してください。

2 証明書を Sentinel FIPS キーストアにインポートします。

証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

3 続けてコネクタの設定を行います。

19.5.3 Sentinel Link コネクタ

Sentinel Link イベントソースサーバのネットワーク設定時に「*暗号化 (HTTPS)*」オプションを選択している場合にのみ、以下の手順に従ってください。

Sentinel Link コネクタを FIPS 140-2 モードで実行するように設定するには :

1 Sentinel Link イベントソースサーバを追加または編集します。［セキュリティ］ウィンドウが表示されるまで、設定画面を進めていきます。詳細については、『*Sentinel Link Connector Guide*』を参照してください。

2 ［*クライアント認証のタイプ*］フィールドでオプションを 1 つ選択します。クライアント認証タイプによって、SSL Sentinel Link イベントソースサーバがデータの送信を試行している Sentinel Link イベントソース (Sentinel Link インテグレータ) の ID をどの程度厳密に検証するかが決まります。

- **開く :** クライアント (Sentinel Link インテグレータ) から着信するすべての SSL 接続を許可します。インテグレータ証明書の検証または認証は行いません。
- **厳密 :** インテグレータ証明書が有効な X.509 証明書であるかを検証し、インテグレータ証明書がイベントソースサーバによって信頼されているかも確認します。詳細については、各データベースのマニュアルを参照してください。

  ［*厳密*］オプションの場合 :

  - Sentinel Link インテグレータが FIPS 140-2 モードで動作しているときは、/etc/opt/novell/sentinel/config/sentinel.cer ファイルを送信側の Sentinel マシンから受信側の Sentinel マシンにコピーする必要があります。証明書を受信側の Sentinel FIPS キーストアにインポートします。

    注 : 認証局 (CA) によってデジタル署名されているカスタム証明書を使用している場合は、適切なカスタム証明書ファイルをインポートする必要があります。

  - Sentinel Link インテグレータが非 FIPS モードで動作しているときは、カスタムインテグレータ証明書を受信側の Sentinel FIPS キーストアにインポートする必要があります。

    注 : 送信者が Sentinel ログマネージャ (非 FIPS モード) であり、受信者が FIPS 140-2 モードの Sentinel である場合、送信者がインポートするサーバ証明書は受信者の Sentinel マシンの /etc/opt/novell/sentinel/config/sentinel.cer ファイルです。

  Sentinel が FIPS 140-2 モードで動作しているときは、イベントソース管理 (ESM) インタフェースを使用してクライアント証明書をインポートすることはできません。証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

注 : FIPS 140-2 モードでは、Sentinel Link イベントソースサーバは Sentinel サーバのキーペアを使用します。サーバのキーペアのインポートは必須ではありません。

19.5.4 Syslog コネクタ

Syslog イベントソースサーバのネットワーク設定時に「*SSL*」プロトコルを選択している場合にのみ、以下の手順に従ってください。

Syslog コネクタを FIPS 140-2 モードで実行するように設定するには :

1 Syslog イベントソースサーバを追加または編集します。［ネットワーク］ウィンドウが表示されるまで、設定画面での作業を進めていきます。詳細については、『*Syslog Connector Guide*』を参照してください。

2 ［*設定*］をクリックします。

3 ［*クライアント認証のタイプ*］フィールドでオプションを 1 つ選択します。クライアント認証タイプによって、SSL Syslog イベントソースサーバがデータの送信を試行している Syslog イベントソースの ID をどの程度厳密に検証するかが決まります。

- **開く :** クライアント (イベントソース) から着信するすべての SSL 接続を許可します。クライアント証明書の検証または認証は行いません。
- **厳密 :** 証明書が有効な X.509 証明書であるかを検証し、クライアント証明書がイベントソースサーバによって信頼されていることも確認します。新規ソースは Sentinel に明示的に追加する必要があります (そうすることで、不正なソースがデータを Sentinel に送信できないようにします)。

  ［*厳密*］オプションの場合、Syslog クライアントの証明書を Sentinel FIPS キーストアにインポートする必要があります。

  Sentinel が FIPS 140-2 モードで動作しているときは、イベントソース管理 (ESM) インタフェースを使用してクライアント証明書をインポートすることはできません。

  証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

注 : FIPS 140-2 モードでは、Syslog イベントソースサーバは Sentinel サーバのキーペアを使用します。サーバのキーペアのインポートは必須ではありません。

---

4 Syslog クライアントでサーバ認証が有効になっている場合、コネクタが展開されている場所に応じて、クライアントは Sentinel サーバ証明書かリモートコレクタマネージャ証明書を信頼する必要があります。

Sentinel サーバ証明書ファイルは /etc/opt/novell/sentinel/config/sentinel.cer にあります。

リモートコレクタマネージャ証明書ファイルは /etc/opt/novell/sentinel/config/rcm.cer にあります。

注 : 認証局 (CA) によってデジタル署名されているカスタム証明書を使用している場合は、クライアントが適切な証明書ファイルを信頼していなければなりません。

19.5.5 Windows イベント (WMI) コネクタ

Windows イベント (WMI) コネクタを FIPS 140-2 モードで実行するように設定するには :

1 Windows イベントコネクタを追加または編集します。［セキュリティ］ウィンドウが表示されるまで、設定画面を進めていきます。詳細については、『*Windows Event (WMI) Connector Guide*』を参照してください。

2 ［*設定*］をクリックします。

3 ［*クライアント認証のタイプ*］フィールドでオプションを 1 つ選択します。クライアント認証タイプによって、Windows イベントコネクタがデータの送信を試行しているクライアント Windows イベント収集サービス (WECS) の ID をどの程度厳密に検証するかが決まります。

- **開く :** クライアント WECS から着信するすべての SSL 接続を許可します。クライアント証明書の検証または認証は行いません。
- **厳密 :** 証明書が有効な X.509 証明書であるかを検証し、クライアント WECS 証明書が CA によって署名されているかも確認します。新規ソースは明示的に追加する必要があります (そうすることで、不正なソースがデータを Sentinel に送信できないようにします)。

［*厳密*］オプションの場合、クライアント WECS の証明書を Sentinel FIPS キーストアにインポートする必要があります。Sentinel が FIPS 140-2 モードで動作しているときは、イベントソース管理 (ESM) インタフェースを使用してクライアント証明書をインポートすることはできません。

証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

注 : FIPS 140-2 モードでは、Windows イベントソースサーバは Sentinel サーバのキーペアを使用します。サーバのキーペアのインポートは必須ではありません。

4 Windows クライアントでサーバ認証が有効になっている場合、コネクタが展開されている場所に応じて、クライアントは Sentinel サーバ証明書かリモートコレクタマネージャ証明書を信頼する必要があります。

Sentinel サーバ証明書ファイルは /etc/opt/novell/sentinel/config/sentinel.cer にあります。

リモートコレクタマネージャ証明書ファイルは /etc/opt/novell/sentinel/config/rcm.cer にあります。

注 : 認証局 (CA) によってデジタル署名されているカスタム証明書を使用している場合は、クライアントが適切な証明書ファイルを信頼していなければなりません。

5 イベントソースを自動的に同期する場合、または Active Directory 接続を使用しているイベントソースのリストを生成する場合は、Active Directory サーバ証明書を Sentinel FIPS キーストアにインポートする必要があります。

証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

19.5.6 Sentinel Link インテグレータ

Sentinel Link インテグレータのネットワーク設定時に「*暗号化 (HTTPS)*」オプションを選択している場合にのみ、以下の手順に従ってください。

Sentinel Link インテグレータを FIPS 140-2 モードで実行するように設定するには :

1 Sentinel Link インテグレータが FIPS 140-2 モードであるときは、サーバ認証が必須になります。インテグレータインスタンスを設定する前に、Sentinel Link サーバ証明書を Sentinel FIPS キーストアにインポートしてください。

- **Sentinel Link コネクタが FIPS 140-2 モードである場合** :

  コネクタが Sentinel サーバに展開されている場合、/etc/opt/novell/sentinel/config/sentinel.cer ファイルを受信側 Sentinel マシンから送信側 Sentinel マシンにコピーする必要があります。

  コネクタがリモートコレクタマネージャに展開されている場合は、/etc/opt/novell/sentinel/config/rcm.cer ファイルを受信側のリモートコレクタマネージャマシンから受信側の Sentinel マシンにコピーする必要があります。

  証明書を送信側の Sentinel FIPS キーストアにインポートします。

  注 : 認証局 (CA) によってデジタル署名されているカスタム証明書を使用している場合は、適切なカスタム証明書ファイルをインポートする必要があります。

- Sentinel Link コネクタが非 FIPS モードである場合 :

  カスタム Sentinel Link サーバ証明書を送信側の Sentinel FIPS キーストアにインポートします。

注 : Sentinel Link インテグレータが FIPS 140-2 モードであり、Sentinel Link コネクタが非 FIPS モードのときは、コネクタにあるカスタムサーバのキーペアを使用してください。内部サーバのキーペアは使用しないでください。

証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

2 続けてインテグレータインスタンスの設定を行います。

注 : FIPS 140-2 モードでは、Sentinel Link インテグレータは Sentinel サーバのキーペアを使用します。インテグレータのキーペアのインポートは必須ではありません。

19.5.7 LDAP インテグレータ

LDAP インテグレータを FIPS 140-2 モードで実行するように設定するには :

1 インテグレータインスタンスを設定する前に、LDAP サーバから証明書をダウンロードし、ldap.cert というファイル名にして、Sentinel サーバの /etc/opt/novell/sentinel/config ディレクトリに保存します。

たとえば、次のように入力します。

```
openssl s_client -connect <LDAP server IP>:636
```

コマンド実行後に返されるテキスト (BEGIN 行と END 行の間) をファイルにコピーします。

2 証明書を Sentinel FIPS キーストアにインポートします。

証明書のインポートについて詳しくは、120 ページの 「証明書を FIPS キーストアデータベースにインポートする」を参照してください。

3 続けてインテグレータインスタンスの設定を行います。

19.5.8 SMTP インテグレータ

SMTP インテグレータは、2011.1r2 以降のバージョンで FIPS 140-2 をサポートしています。設定の変更は必要ありません。

19.5.9 FIPS 140-2 モードの Sentinel で FIPS 非対応コネクタを使用する

このセクションでは、FIPS 非対応コネクタを FIPS 140-2 モードの Sentinel サーバで使用する方法について説明します。FIPS をサポートしないソースがある場合、またはご使用の環境で非 FIPS コネクタからイベントを収集する場合に、この方法をお勧めします。

FIPS 140-2 モードの Sentinel サーバで非 FIPS コネクタを使用するには :

1 非 FIPS モードのリモートコレクタマネージャをインストールして、FIPS 140-2 モードの Sentinel サーバに接続します。

詳細については、78 ページのセクション 11.6「追加のコレクタマネージャのインストールおよび相関エンジンのインストール」を参照してください。

2 非 FIPS コネクタを明確に非 FIPS リモートコレクタマネージャに展開します。

注 : 監査コネクタやファイルコネクタなどの非 FIPS コネクタを、FIPS 140-2 モードの Sentinel 7.1 サーバに接続している非 FIPS リモートコレクタマネージャ上で展開する場合に発生する、既知の問題があります。これらの既知の問題の詳細については、『「NetIQ Sentinel 7.0.1 Readme」』を参照してください。

19.6 証明書を FIPS キーストアデータベースにインポートする

証明書を Sentinel FIPS キーストアデータベースに挿入して、その証明書を所有するコンポーネントから Sentinel へのセキュア (SSL) 通信を確立する必要があります。FIPS 140-2 モードが Sentinel で有効になっている場合、通常どおり Sentinel ユーザインタフェースを使用して証明書をアップロードすることはできません。証明書を FIPS キーストアデータベースに手動でインポートする必要があります。

リモートコレクタマネージャに展開されたコネクタを使用しているイベントソースの場合、証明書を中央 Sentinel サーバではなく、リモートコレクタマネージャの FIPS キーストアデータベースにインポートする必要があります。

証明書を FIPS キーストアデータベースにインポートするには :

1. 証明書ファイルを Sentinel サーバまたはリモートコレクタマネージャの一時的な場所にコピーします。
2. Sentinel の bin ディレクトリを参照します。デフォルトの場所は /opt/novell/sentinel/bin です。
3. 次のコマンドを実行して、証明書を FIPS キーストアデータベースにインポートし、画面の指示に従ってください。

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```

4. Sentinel サーバまたはリモートコレクタマネージャを再起動するようプロンプトが表示されたら、「yes」または「y」と入力します。

19.7 Sentinel を非 FIPS モードに戻す

このセクションでは、Sentinel およびそのコンポーネントを非 FIPS モードに戻す方法について説明します。

- 120 ページのセクション 19.7.1「Sentinel サーバを非 FIPS モードに戻す」
- 121 ページのセクション 19.7.2「リモートコレクタマネージャまたはリモート相関エンジンを非 FIPS モードに戻す」

19.7.1 Sentinel サーバを非 FIPS モードに戻す

FIPS 140-2 モードで実行している Sentinel サーバを非 FIPS モードに戻すことができるのは、Sentinel サーバを FIPS 140-2 モードにする前に Sentinel サーバのバックアップを取ってある場合のみです。

注 : Sentinel サーバを非 FIPS モードに戻すと、FIPS 140-2 モード実行に変換した後のイベント、インシデントデータ、および Sentinel サーバに対して行われた設定変更は失われます。Sentinel システムは非 FIPS モードの最後の復元ポイントに復元されます。後で使用することを考えて、現在のシステムのバックアップを取ってから、非 FIPS モードに戻すようにしてください。

Sentinel サーバを非 FIPS モードに戻すには :

1. Sentinel サーバに root ユーザでログインします。
2. novell ユーザに切り替えます。
3. Sentinel の bin ディレクトリを参照します。デフォルトの場所は /opt/novell/sentinel/bin です。
4. 次のコマンドを実行して、Sentinel サーバを非 FIPS モードに戻し、画面の指示に従ってください。

   ```
   ./backup_util.sh -f <backup_file_name.tar.gz> -m 'restore'
   ```

   たとえば、non-fips201301241911135903 4887.tar.gz がバックアップファイルである場合は、次のコマンドを実行します。

   ```
   ./backup_util.sh -f non-fips201301241911135903 4887.tar.gz -m 'restore'
   ```

5. Sentinel サーバを再起動します。

19.7.2 リモートコレクタマネージャまたはリモート相関エンジンを非 FIPS モードに戻す

リモートコレクタマネージャまたはリモート相関エンジンを非 FIPS モードに戻すことができます。

リモートコレクタマネージャまたはリモート相関エンジンを非 FIPS モードに戻すには :

1. リモートコレクタマネージャまたはリモート相関エンジンのシステムにログインします。
2. novell ユーザ (su novell) に切り替えます。
3. bin ディレクトリを参照します。デフォルトの場所は /opt/novell/sentinel/bin です。
4. revert_to_nonfips.sh スクリプトを実行して、画面の指示に従います。
5. リモートコレクタマネージャまたはリモート相関エンジンを再起動します。

V Sentinel のアップグレード

このセクションでは、Sentinel およびコンポーネントのアップグレードについて説明します。

20 Sentinel サーバのアップグレード

重要 : Sentinel 7.1 以降では、オペレーティングシステムが IPv6 有効でなければなりません。ご使用のシステムを Sentinel 7.1 以降にアップグレードする前に、オペレーティングシステムで IPv6 が有効になっていることを確認してください。IPv6 が有効になっていないと、主要コンポーネントを動作させることができません。

次の手順に従って、Sentinel サーバをアップグレードします。

1. 環境設定のバックアップを行った後、ESM エクスポートを作成します。

   データのバックアップの詳細については、「「Backing Up and Restoring Data (データのバックアップと復元)」」を参照してください。これは『*NetIQ Sentinel 7.1 Administration Guide*』にあります。
2. ノベル製品ダウンロードのサイトから最新のインストーラをダウンロードします。
3. Sentinel をアップグレードするサーバに roo t としてログインします。
4. 次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

   ```
   tar xfz <install_filename>
   ```

   <*install_filename*> は、実際のインストールファイル名に置き換えます。
5. インストールファイルを抽出したディレクトリに移動します。
6. 次のコマンドを指定して、Sentinel をアップグレードします。

   ```
   ./install-sentinel
   ```
7. 指定の言語でインストールを進めるには、言語の横の番号を選択します。

   エンドユーザの使用許諾契約が、選択した言語で表示されます。
8. エンドユーザの使用許諾契約を読み、「yes」または「y」と入力して契約に同意し、インストールを続行します。
9. インストールスクリプトで、古いバージョンの製品が存在していることが検出され、製品をアップグレードするかどうかを指定するよう求められます。アップグレードを続行するには、「y」を押します。

   すべての RPM パッケージのインストールが開始されます。このインストールが完了するまで数秒かかることがあります。
10. Web ブラウザのキャッシュをクリアして、最新の Sentinel バージョンを表示します。
11. (条件による) コレクタマネージャシステムと相関エンジンシステムをアップグレードするには、129 ページの第 22 章「コレクタマネージャまたは相関エンジンのアップグレード」を参照してください。

21 Sentinel アプライアンスのアップグレード

本章では、Sentinel アプライアンス、およびコレクタマネージャアプライアンスと相関エンジンアプライアンスをアップグレードする手順について説明します。

21.1 Sentinel 7.0.2 以降のアプライアンスのアップグレード

1. Sentinel アプライアンスに管理者の役割を持つユーザとしてログインします。
2. **Sentinel アプライアンスをアップグレードする場合は**、［*アプライアンス*］をクリックして WebYaST を起動します。
3. **コレクタマネージャまたは相関エンジンアプライアンスをアップグレードする場合は**、ポート 54984 を使用しているコレクタマネージャか相関エンジンのコンピュータの URL を指定して、WebYaST を起動します。
4. 環境設定のバックアップを行った後、ESM エクスポートを作成します。

   データのバックアップの詳細については、「「Backing Up and Restoring Data (データのバックアップと復元)」」を参照してください。これは『*NetIQ Sentinel 7.1 Administration Guide*』にあります。
5. (条件による) アプライアンスの自動更新をまだ登録していない場合は、登録します。

   詳細については、91 ページのセクション 12.4.3「アップデートの登録」を参照してください。

   アプライアンスが登録されていない場合、Sentinel はアプライアンスが登録されていないことを示す黄色い警告を表示します。
6. アップデートがあるかどうかを確認するには、［*更新*］をクリックします。

   利用可能な更新が表示されます。
7. 更新を選択して適用します。

   更新が完了するまで数分かかる場合があります。更新が成功すると、WebYaST のログインページが表示されます。

   アプライアンスをアップグレードする前に、WebYaST は Sentinel サービスを自動的に停止します。アップグレードが完了した後で、このサービスを手動で再開する必要があります。
8. Web インタフェースを使用して Sentinel サービスを再開します。

   詳細については、93 ページのセクション 12.5「WebYaST を使用したサーバの起動と停止」を参照してください。
9. Web ブラウザのキャッシュをクリアして、最新の Sentinel バージョンを表示します。

21.2 Sentinel 7.0 および 7.0.1 アプライアンスのアップグレード

WebYaST で Sentinel7.0 および 7.0.1 アプライアンスをアップグレードすると、パッチのベンダ名が Novell から NetIQ に変更されているため失敗します。zypper patch を使用してアプライアンスをアップグレードする必要があります。

zypper patch を使用してアプライアンスをアップグレードするには :

1. 環境設定をバックアップしてから、ESM エクスポートを作成します。詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「「Backing Up and Restoring Data」」を参照してください。
2. アプライアンスコンソールに root ユーザでログインします。
3. 次のコマンドを実行します。

   ```
   /usr/bin/zypper patch
   ```

4. 「1」と入力して、Novell から NetIQ へのベンダの変更を受け入れます。
5. 「Y」と入力して続行します。
6. 使用許諾契約書の条項を確認し、「yes」と入力します。
7. Sentinel アプライアンスを再起動します。
8. Web ブラウザのキャッシュをクリアして、最新の Sentinel バージョンを表示します。

21.3 SMT を使用したアプライアンスのアップグレード

インターネットに直接アクセスできない保護された環境でアプライアンスを実行する必要がある場合は、Subscription Management Tool (SMT) でアプライアンスを設定することができます。これにより、アプライアンスを使用可能な最新のバージョンにアップグレードできます。

1. アプライアンスが SMT で設定されていることを確認します。

   詳細については、91 ページのセクション 12.4.4「SMT でのアプライアンスの設定」を参照してください。
2. アプライアンスコンソールに root ユーザでログインします。
3. アップグレード用にリポジトリを更新します。

   ```
   zypper ref -s
   ```

4. アプライアンスがアップグレードに対して有効であることを確認します。

   ```
   zypper lr
   ```

5. (オプション) アプライアンスの使用可能な更新を確認します。

   ```
   zypper lu
   ```

6. (オプション) アプライアンスの使用可能な更新を含むパッケージを確認します。

   ```
   zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
   ```

7. アプライアンスを更新します。

   ```
   zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
   ```

8. アプライアンスを再起動します。

   ```
   rcsentinel restart
   ```

22 コレクタマネージャまたは相関エンジンのアップグレード

次の手順に従って、コレクタマネージャおよび相関エンジンをアップグレードします :

1. 環境設定のバックアップを行い、ESM エクスポートを作成します。

   詳細については、『*NetIQ Sentinel 7.1 Administration Guide*』の「「Backing Up and Restoring Data」」を参照してください。
2. Sentinel の Web インタフェースに管理者の役割を持つユーザとしてログインします。
3. ［*ダウンロード*］を選択します。
4. コレクタマネージャのインストーラセクションで［*インストーラのダウンロード*］をクリックします。

   ウィンドウが表示されたら、インストーラファイルを実行するか、ローカルマシンに保存するかを選択します。
5. ファイルを保存します。
6. ファイルを一時的な場所にコピーします。
7. ファイルの内容を抽出します。
8. 次のスクリプトを実行します。

   コレクタマネージャの場合 :

   ```
   ./install-cm
   ```

   相関エンジンの場合 :

   ```
   ./install-ce
   ```
9. 画面の説明に従って、インストールを完了します。
10. Web ブラウザのキャッシュをクリアして、最新の Sentinel バージョンを表示します。

23 Sentinel プラグインのアップグレード

Sentinel のインストール環境をアップグレードしても、最新版の Sentinel との互換性がないプラグインはアップグレードされません。

新規および最新の Sentinel プラグインは、Sentinel プラグインの Web サイトに頻繁にアップロードされています。最新のバグフィックス、マニュアルの更新、およびプラグインの拡張機能を取得するには、プラグインの最新バージョンをダウンロードしてインストールしてください。プラグインのインストールについては、それぞれのプラグインのマニュアルを参照してください。

VI 付録

A 高可用性のためのSentinelの環境設定

重要なエンタープライズイベントデータをできるだけ安定して収集できるようにするために、Sentinel を高可用性環境にインストールすることを希望するお客様が多くおられます。数々のセキュリティおよびコンプライアンス要件は、その要件に厳密に適合して実行される広範囲にわたるデータ収集に依存しており、わずかなイベントを見逃したために脅威や違反を検出できず、許容できないリスクが組織に及ぶことにもなりかねません。NetIQ は、Sentinel が高可用性環境で動作するようテストおよび認定しており、障害復旧アーキテクチャをサポートします。

本付録では、Sentinel をアクティブ - パッシブ高可用性モードでインストールする方法を説明します。このモードでインストールすると、ハードウェアやソフトウェアの障害時に Sentinel を冗長クラスタノードにフェールオーバーすることができます。ただし、アクティブ - アクティブ構成は対象外で、どの稼働時間も保証の対象とはなりません。NetIQ コンサルティングおよび NetIQ パートナーは、Sentinel の高可用性および障害復旧の実装を支援します。

注 : NetIQ は Sentinel オールインワンインストールの高可用性構成のみをサポートします。分散インストールされたコレクタマネージャまたは相関エンジンの直接的なサポートは行いません。

A.1 概念

高可用性とは、システムを現実的な範囲でできる限り継続的に利用できるようにすることを目的とした一つの設計方法論です。システム障害やシステム保守といったダウンタイムの原因を極力排除し、実際に発生してしまったダウンタイムイベントの検出とそこからの回復にかかる時間を最小限に抑えることを意図しています。より高度な可用性を実現するために、具体的には、ダウンタイムイベントの検出とそこからの回復を迅速に行う自動化された処理方法が必要となります。

A.1.1 外部システム

Sentinel は、さまざまなサービスに依存しながらさまざまなサービスを提供する、複合的な多層アプリケーションです。また、複数の外部サードパーティシステムとも連動して、データ収集、データ共有、およびインシデント修正を行います。たいていの高可用性ソリューションでは高可用性を持たせるサービスとそれに依存するサービスとの間の依存関係を実装者が宣言できますが、それもクラスタ上で実行するサービスに対してのみ可能です。イベントソースなどの Sentinel 外部のシステムは、組織が必要とする可用性に合わせて別個に構成する必要があり、フェールオーバーなどのために Sentinel が一時的に利用不能になった場合でも状況を適切に処理できるように設定されている必要があります。アクセス権限が厳しく制限されている場合 (たとえばサードパーティシステムと Sentinel との間でのデータ送受信に認証済みセッションを使用する場合など)、どのクラスタノードからでもセッションを受け入れ、どのクラスタノードに対してもセッションを開始できるようにサードパーティシステムを設定する必要があります (そのためには Sentinel を仮想 IP で設定する必要があります)。NetIQ は、弊社製品と管轄対象外サードパーティシステムとの間のいかなるレベルの高可用性についても保証しておりません。

A.1.2 共有ストレージ

すべての高可用性クラスタには、ノードに障害が起きた場合でもアプリケーションデータを別のノードにすばやく移動できるような、何らかの形式の共有ストレージが必要です。ストレージそのものが高可用性を備えていなければならず、これは通常ファイバチャネルネットワークを使用してクラスタノードに接続するストレージエリアネットワーク (SAN) の技術を採用することによって実現されます。他のシステムは NAS(Network Attached Storage)、iSCSI、または共有ストレージのリモートマウントを可能にするその他のテクノロジを使用します。共有ストレージの最も重要な要件は、クラスタが障害の発生したクラスタノードから新しいクラスタノードへストレージをきちんと移動できるということです。

注 : iSCSI の場合は、ハードウェアがサポートする最大のメッセージ転送単位 (MTU) を使用してください。MTU を大きくすることで、ストレージのパフォーマンスが向上します。ストレージへの接続のレイテンシまたは帯域幅、あるいはその両方が推奨値より遅い場合は、Sentinel で問題が生じる可能性があります。

Sentinel で共有ストレージを利用する場合に、使用可能な 2 つの基本的な方法があります。ひとつは、アプリケーションバイナリ、設定、イベントデータなどすべてのコンポーネントを共有ストレージに置くという方法です。フェールオーバーになると、ストレージはプライマリノードからアンマウントされてバックアップノードに移動します。これで、共有ストレージから全体のアプリケーションと設定が読み込まれます。もう一つは、イベントデータを共有ストレージに保管し、アプリケーションバイナリと設定は各クラスタノードに配置するという方法です。フェールオーバーになると、イベントデータのみがバックアップノードに移動します。

どちらの方法にも長所と短所がありますが、2 番目の方法では、Sentinel インストール環境で標準 FHS 準拠のインストールパスを使用でき、RPM パッケージの検証、ダウンタイムを最小限にするウォームパッチや再設定を行うことが可能です。

iSCSI 共有ストレージを使用し、アプリケーションバイナリと設定を各クラスタノードに配置するクラスタのインストールプロセスを、サンプルとして説明していきます。

A.1.3 サービスの監視

高可用性環境の重要な要素は、高可用であるべきリソースとそれに依存するリソースを監視するための、信頼できる安定した方法を確立することです。SLE HAE はリソースエージェントというコンポーネントを使用してそのような監視を実行します。リソースエージェントの役目は、各リソースの状況を知らせ、そのリソースを (要求に応じて) 開始および停止することです。

リソースエージェントは監視対象のリソース状況を信頼できる情報として提供して、不要なダウンタイムが発生しないようにする必要があります。誤検出 (リソースに障害が発生したと思われたが、実際には自力で回復したという場合など) によって実際には行う必要のないサービスマイグレーション (および関連するダウンタイム) が始まったり、検出漏れ (リソースは機能しているとリソースエージェントが報告したが、そのリソースは実際には正常に動作していないという場合など) によってサービスを適正に利用できなくなったりすることがあります。一方、サービスに対して外部監視を行うことは非常に難しいでしょう。たとえば、Web サービスポートは 1 つの単純な ping には応答するかもしれませんが、実際のクエリが発行されたときに正しいデータを提供できるとは限りません。多くの場合、本当に正確な測定値を取得するには、サービス自体に自己診断機能を組み込む必要があります。

このソリューションでは、主要なハードウェア、オペレーティングシステム、または Sentinel システム障害を監視することができる、基本 OCF リソースエージェントが Sentinel に装備されます。現時点では、Sentinel の外部監視機能は IP ポート試験に基づいており、これには読み取りに誤検出や検出漏れの可能性があります。弊社では、このコンポーネントの正確性を改善するために、時間をかけて Sentinel およびリソースエージェントの両方を改良することを計画しています。

A.1.4 フェンシング

HA クラスタ内では、クリティカルサービスを常時監視しており、障害発生時には別のノードでそのサービスが自動的に再起動するようになっています。しかし、この自動化によって問題が生じる可能性もあります。たとえば、プライマリノードで何らかの通信の問題が発生し、そのノード上で実行中のサービスが一見ダウンしているようでも、実際には実行が継続され、データを共有ストレージに書き込んでいるという場合です。このような場合に、バックアップノードで新たにサービスのセットが開始されると、容易にデータ破損が発生しかねません。

そうならないように、クラスタではフェンシングという方法が採用されています。これは、スプリットブレイン検出 (SBD) および STONITH(Shoot The Other Node In The Head) を含むさまざまな技術の総称です。この主な目的は、共有ストレージにおけるデータ破損を防ぐことにあります。

A.2 サポート範囲

NetIQ はこのソリューションを、規定されたクラスタ特性、および本マニュアルに規定され、弊社ラボでテストされた予想される動作に基づいてサポートします。その他のクラスタ設定は、お客様の環境で生じる問題が弊社内のテスト環境で再現される場合にのみサポートします。ローカル実装環境の違いは問題の原因と見なされません。

A.3 システム要件

高可用性インストール環境に対応できるようにクラスタリソースを割り振る場合、以下の要件を考慮してください。

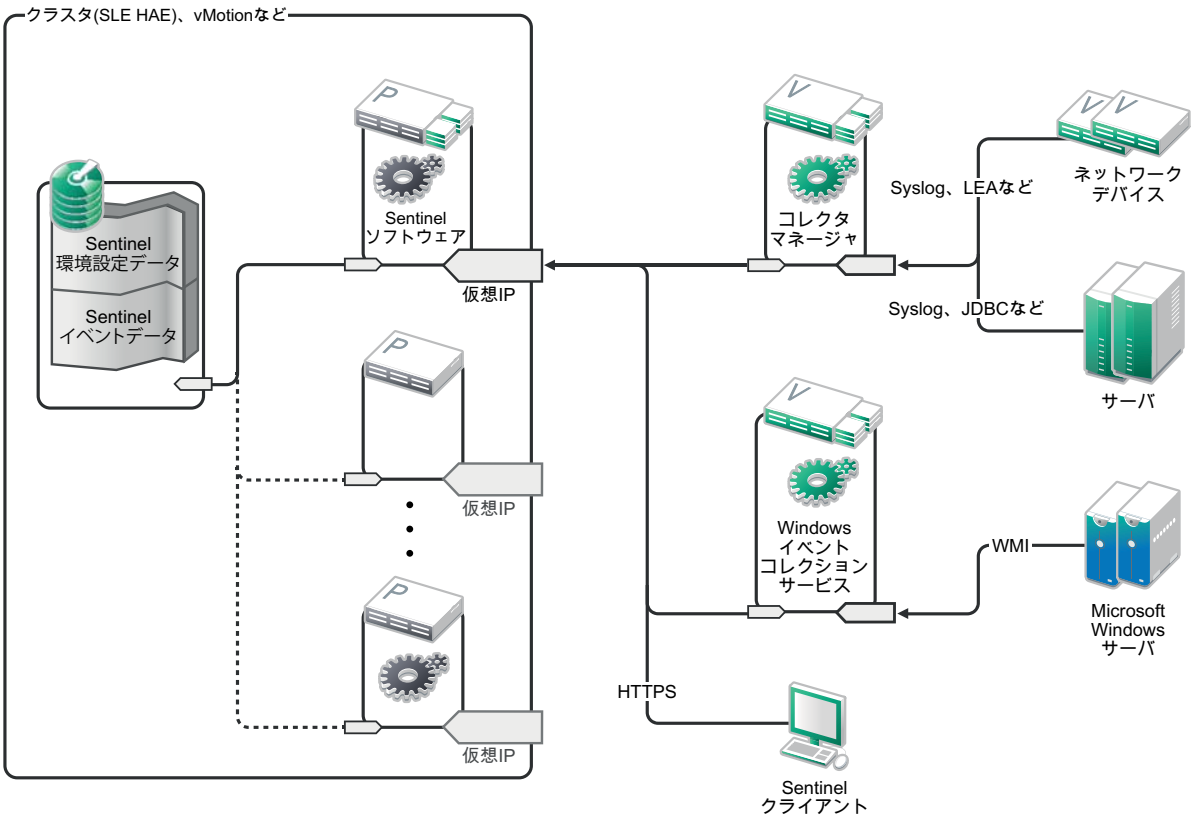
- Sentinel サービスをホストする各クラスタノードは、35 ページの第 5 章「システム要件を満たす」に指定されている要件を満たしている必要があります。

- Sentinelデータおよびアプリケーションが使用できる十分な共有ストレージが確保されていることを確認します。
- フェールオーバー時にノードからノードに移行可能なサービスの仮想 IP アドレス。
- Sentinel インストーラ (TAR ファイル、有効なライセンス付き)。
- SUSE Linux SUSE Linux High Availability Extension (ISO イメージ、有効なライセンス付き)。
- 35 ページの第 5 章「システム要件を満たす」に説明されているパフォーマンスおよびサイズ特性の条件を満たす共有ストレージデバイス。サンプルソリューションでは、標準 SUSE Linux VM を使用し、iSCSI Target を共有ストレージとして構成します。
- お客様の環境で Sentinel を実行するためのリソース要件を満たしたクラスタノードを最低 2 台。サンプルソリューションでは、2 台の Linux VM を使用します。
- クラスタノードが共有ストレージと通信する方式 (SAN 用の FibreChannel など)。サンプルソリューションでは、専用 IP アドレスを使用して、iSCSI Target に接続します。
- クラスタノードからクラスタノードに移行する際にSentinelの外部IPアドレスの役割を果たす仮想 IP。
- 各クラスタノードにつき最低1つのIPアドレス(内部クラスタ通信用)。サンプルソリューションでは単一のユニキャスト IP アドレスを使用しますが、運用環境ではマルチキャストが好まれます。

A.4 インストールと環境設定

このセクションでは、高可用性環境での Sentinel のインストールおよび設定の手順を説明します。各手順では、全般的な方法を説明した後、デモのセットアップを紹介してクラスタソリューション例を詳述します。本マニュアルにリストされていない他のオプションやテクノロジを使用することもできますが、137 ページのセクション A.2「サポート範囲」に説明されている制約が適用されます。

次の図は、アクティブ - パッシブ高可用性アーキテクチャを表しています。



- 139 ページのセクション A.4.1「初期セットアップ」
- 141 ページのセクション A.4.2「共有ストレージのセットアップ」
- 144 ページのセクション A.4.3「Sentinel のインストール」
- 145 ページのセクション A.4.4「クラスタインストール」
- 146 ページのセクション A.4.5「クラスタ環境設定」
- 149 ページのセクション A.4.6「リソースの設定」
- 150 ページのセクション A.4.7「ネットワークストレージの設定」

A.4.1 初期セットアップ

Sentinel 用に記述されている要件およびローカルカスタマ要件に従って、マシンハードウェア、ネットワークハードウェア、ストレージハードウェア、オペレーティングシステム、ユーザアカウント、およびその他の基本的なシステムリソースを設定します。システムをテストして、正常に機能し安定していることを確認します。

- ベストプラクティスとして、すべてのクラスタノードの時刻は同期されているべきです。そのために、NTP または同様の技術を使用します。
- クラスタには信頼できるホスト名解決が必要になります。ベストプラクティスとして、すべての内部クラスタホスト名を /etc/hosts ファイルに入力することで、DNS 障害が発生してもクラスタが継続して動作するようにできます。どのクラスタノードも他のすべてのノードを*名前で*解決できない場合、このセクションで説明されているクラスタ構成は失敗します。

- 各クラスタノードの CPU、RAM、およびディスク容量特性が、予期されるイベント発生率に基づいて、35 ページの第 5 章「システム要件を満たす」に定義されているシステム要件を満たしている必要があります。
- ストレージノードのディスク容量と入出力特性は、予想されるイベント発生率、ローカルおよびネットワークストレージに対するデータ保持ポリシーに基づいて、35 ページの第 5 章「システム要件を満たす」に定義されているシステム要件を満たしている必要があります。
- Sentinel およびクラスタへのアクセスを制限するためにオペレーティングシステムのファイアウォールを設定する場合は、55 ページの第 7 章「使用するポート」を参照してください。ローカル構成やイベントデータを送信する送信元に応じて、どのポートを使用可能にする必要があるのか詳しく説明されています。

サンプルソリューションでは以下の設定を使用します。

- 2 つの SUSE Linux 11 SP2 クラスタノード VM
  - OS インストールで X Windows をインストールする必要がありませんが、GUI 環境設定を希望する場合はインストールすることもできます。ブートスクリプトは X なしで起動するように設定できます (Runlevel 3)。これで、必要なときにのみ X を起動できるようになります。
  - ノードは 2 つの NIC を持つようになります。1 つは外部アクセス用で、もう 1 つは iSCSI 通信用です。
  - SSH または同様の機能を介してリモートアクセスできるように、外部 NIC に IP アドレスを設定します。このサンプルでは、172.16.0.1 (node01) と 172.16.0.2 (node02) を使用します。
  - 各ノードには、オペレーティングシステム、Sentinel のバイナリおよび設定データ、クラスタソフトウェア、一時スペースなどのために十分なディスク容量がなければなりません。SUSE Linux および SLE HAE のシステム要件、および Sentinel アプリケーション要件を参照してください。
- 1 つの SUSE Linux 11 SP2 VM(共有ストレージ用に iSCSI Target を設定済み)
  - OS インストールで X Windows をインストールする必要がありませんが、GUI 環境設定を希望する場合はインストールすることもできます。ブートスクリプトは X なしで起動するように設定できます (Runlevel 3)。これで、必要なときにのみ X を起動できるようになります。
  - システムは 2 つの NIC を持つようになります。1 つは外部アクセス用で、もう 1 つは iSCSI 通信用です。
  - SSH または同様の機能を介してリモートアクセスできるように、外部 NIC に IP アドレスを設定します。このサンプルでは、172.16.0.3 (storage03) を使用します。
  - システムには、オペレーティングシステム、一時スペース、共有ストレージが Sentinel データを保持できるような大容量スペース、そして SBD パーティションのためにいくらかのスペースが確保できる、十分なディスク容量がなければなりません。SUSE Linux システム要件および Sentinel イベントデータストレージ要件を参照してください。サンプルソリューションではすべてのデータ (ローカル、ネットワーク、SBD) を 1 つのディスクに書き込みますが、運用展開ではこれらのデータを別々のノードに割り振ることもできます。

注 : 運用クラスタでは、内部クラスタ通信用に、個々の NIC(おそらくは冗長性のために 2 個 1 組) でルーティング不可の内部 IP を使用できます。

A.4.2 共有ストレージのセットアップ

共有ストレージをセットアップして、そのストレージをクラスタノードごとにマウントします。FibreChannel と SAN を使用している場合は、この作業に物理的な接続とその他の設定が含まれる可能性があります。共有ストレージは Sentinel のデータベースおよびイベントデータを保持するために使用するので、予想されるイベント発生率およびデータ保持ポリシーに基づいて、お客様の環境に合った共有ストレージのサイズを決める必要があります。

一般的な実装では、FibreChannel ですべてのクラスタノードに接続された高速 SAN を使用し、ローカルイベントデータを保管するために大容量 RAID アレイを設置します。低速ネットワークストレージには、別個の NAS ノードや iSCSI ノードを使用することもできます。クラスタノードがローカルストレージを通常のブロックデバイスとしてマウントできるのであれば、この方法もソリューションに利用できます。ネットワークストレージもブロックデバイスとしてマウントできますが、NFS または CIFS ボリュームにすることも可能です。

注 : 共有ストレージを設定して、各クラスタノードで共有ストレージのマウントをテストしてください。しかし、実際の共有ストレージのマウントはクラスタ設定によって処理されます。

サンプルソリューションの場合、SUSE Linux VM によりホストされている iSCSI Target を使用します :

サンプルソリューションでは、SUSE Linux VM で設定されている iSCSI Target を使用します。初期セットアップにリストされているように、VM は storage03 です。iSCSI デバイスは任意のファイルまたはブロックデバイスを使用して作成できますが、ここでは分かりやすくするために、そのために作成したファイルを使用することにします。

storage03 に接続して、コンソールセッションを開始します。次の dd コマンドを使用して、Sentinel ローカルストレージ用に希望する任意のサイズのブランクファイルを作成します :

```
dd if=/dev/zero of=/localdata count=10240000 bs=1024
```

ここでは、(/dev/zero pseudo-device からコピーして) ゼロ (0) を埋め込んだ 10GB のファイルを作成します。コマンドラインオプションの詳細については、dd の情報ページまたはマニュアルページを参照してください。たとえば、異なるサイズの「ディスク」を複数作成する場合などです。iSCSI Target はこのファイルを 1 つのディスクであるかのように扱います。もちろん、実際のディスクを使用することもできます。

同様の手順を繰り返して、ネットワークストレージ用のファイルを作成します。

```
dd if=/dev/zero of=/networkdata count=10240000 bs=1024
```

このサンプルの場合、同じサイズとパフォーマンス特性を持つ 2 つのファイル (「ディスク」) を使用します。運用展開の場合、ローカルストレージを高速な SAN 上に置き、ネットワークストレージを低速な iSCSI、NFS、または CIFS ボリューム上に置くこともできます。

作成したファイルを iSCSI Target として設定する :

1. コマンドラインから YaST を実行します (または GUI を使用することもできます): /sbin/yast
2. ［**Network Devices (ネットワークデバイス)**］>［**Network Settings (ネットワーク設定)**］を選択します。
3. ［**概要**］タブが選択されていることを確認します。
4. 表示されているリストからセカンダリ NIC を選択して、タブで［編集］に進み、Enter を押します。

5 ［**アドレス**］タブで、静的 IP アドレス 10.0.0.3 を割り当てます。これが内部 iSCSI 通信 IP になります。

6 ［**次**］をクリックし、［**OK**］をクリックします。

7 メイン画面で、［**ネットワークサービス**］、［**iSCSI ターゲット**］の順に選択します。

8 プロンプト画面が表示されたら、SUSE Linux 11 SP2 メディアから必要なソフトウェア (iscsitarget RPM) をインストールします。

9 ［**サービス**］をクリックして、［**When Booting(ブート時)**］オプションを選択して、オペレーティングシステムのブート時にサービスが開始するようにします。

10 iSCSI 用の現行の OCF リソースエージェントが認証をサポートしていないため、［**Global(グローバル)**］をクリックしてから［**No Authentication(認証なし)**］を選択します。

11 ［**ターゲット**］、［**追加**］の順にクリックして、新規ターゲットを追加します。

iSCSI Target は ID を自動生成し、使用可能な LUN(ドライブ) の空のリストを表示します。

12 ［**追加**］をクリックして、新しい LUN を追加します。

13 LUN 番号は 0 のままで、［**パス**］ダイアログ (Type=fileio の下) を参照して、作成した /localdata ファイルを選択します。ストレージ専用のディスクがある場合は、/dev/sdc などのブロックデバイスを指定します。

14 12 と 13 の手順を繰り返して、今回は LUN 1 と /networkdata を追加します。

15 その他のオプションはデフォルトのままにしておきます。［**OK**］をクリックしてから［**次**］をクリックします。

16 ［**次**］をもう一度クリックしてデフォルト認証を選択してから、［**完了**］をクリックして設定を終了します。iSCSI の再起動を要求された場合は、それを受け入れます。

17 YaST の終了 .

上記の手順を行うことにより、IP アドレス 10.0.0.3 のサーバに 2 つの iSCSI Target が公開されます。各クラスタノードで、ローカルデータ共有ストレージデバイスをマウントできることを確認してください。デバイスのフォーマットも行う必要があります (1 回):

1 片方のクラスタノード (node1) に接続して、YaST を開始します。

2 ［**Network Devices (ネットワークデバイス)**］>［**Network Settings (ネットワーク設定)**］を選択します。

3 ［**概要**］タブが選択されていることを確認します。

4 表示されているリストからセカンダリ NIC を選択して、タブで［編集］に進み、Enter を押します。

5 ［**アドレス**］をクリックして、静的 IP アドレス 10.0.0.1 を割り当てます。これが内部 iSCSI 通信 IP になります。

6 ［**次**］を選択して、［**OK**］をクリックします。

7 ［**ネットワークサービス**］、［**iSCSI イニシエータ**］の順にクリックします。

8 プロンプト画面が表示されたら、SUSE Linux 11 SP2 メディアから必要なソフトウェア (open-iscsi RPM) をインストールします。

9 ［**サービス**］をクリックし、［**When Booting(ブート時)**］を選択して、ブート時に iSCSI サービスが開始するようにします。

10 ［**Discovered Targets(検出したターゲット)**］をクリックして、［**ディスカバリ**］を選択します。

11 iSCSI の IP アドレス (10.0.0.3) を指定し、［**No Authentication(認証なし)**］を選択して、［**次**］をクリックします。

12 IP アドレスが 10.0.0.3 である検出された iSCSI Target を選択して、［**ログイン**］を選択します。

13 ［**Startup(起動)**］ドロップダウンで自動に切り替えて、［**No Authentication(認証なし)**］を選択してから、［**次**］をクリックします。

14 ［**Connected Targets(接続済みターゲット)**］タブに切り替えて、ターゲットに接続していることを確認します。

15 環境設定を終了します。これで、iSCSI Target がクラスタノード上でブロックデバイスとしてマウントされました。

16 YaST メインメニューで、［**システム**］、［**パーティショナ**］の順に選択します。

17 ［System View(システムビュー)］で、リストに新しいハードディスク (/dev/sdb や /dev/sdc など) が表示されます。これらは IET-VIRTUAL-DISK タイプになります。リストの最初にタブを切り替えて (ローカルストレージが表示されます)、そのディスクを選択してから、Enter を押します。

18 ［**追加**］を選択して、空のディスクに新規パーティションを追加します。ディスクをプライマリ ex3 パーティションとしてフォーマットし、マウントはしないでおきます。［Do not mount partition(パーティションをマウントしない)］オプションが選択されていることを確認します。

19 ［**次**］を選択し、行われる変更内容を確認してから［**完了**］を選択します。この共有 iSCSI LUN に 1 つの大きなパーティションを作成することにした場合、最終的に /dev/sdb1 またはこれと同様のフォーマット済みディスク (以後 /dev/<SHARED1> と表記) が作成されているはずです。

20 パーティショナに戻り、/dev/sdc またはネットワークストレージに相当するブロックデバイスに対してパーティション作成 / フォーマットのプロセス (手順 16-19) を繰り返します。これにより、/dev/sdc1 パーティションまたはこれと同様のフォーマット済みディスク (以後 /dev/<NETWORK1> と表記) が作成されます。

21 YaST の終了 .

22 最後に、マウントポイントを作成し、ローカルパーティションのマウント処理を次の方法でテストします (実際のデバイス名は個別の実装によって異なります):

```
# mkdir /var/opt/novell
# mount /dev/<SHARED1> /var/opt/novell
```

23 新規パーティション上にファイルを作成でき、パーティションがマウントされているところでは必ずファイルが表示されるはずです。

アンマウントするには :

```
# umount /var/opt/novell
```

上記手順のステップ 1 ～ 15 を繰り返して、各クラスタノードがローカル共有ストレージをマウントできることを確認します。ただし、ステップ 5 のノード IP を別の IP に置き換えます (たとえば node02 > 10.0.0.2)。

A.4.3 Sentinel のインストール

Sentinel をインストールする方法には 2 つのオプションがあります。Sentinel のすべての部分を共有ストレージにインストールする方法 (--location オプションを使用して、Sentinel のインストールを共有ストレージのマウント先にリダイレクトする) と、アプリケーション変数データのみを共有ストレージに配置する方法です。

サンプルソリューションでは、後者の方法を採用し、Sentinel をホストする各クラスタノードに Sentinel をインストールします。初めて Sentinel をインストールする際には、アプリケーションバイナリ、環境設定、およびすべてのデータストアを含む完全インストールを行います。以後、他のクラスタノードにインストールする際にはアプリケーションのみをインストールし、実際の Sentinel データはその後 (共有ストレージがマウントされた後など) に利用可能になるものとします。

サンプルソリューション :

このサンプルソリューションでは、Sentinel を各クラスタノードにインストールし、アプリケーション可変データのみを共有ストレージに保管します。こうすることで、アプリケーションバイナリと環境設定が標準の場所に保管され、RPM の検証や特定のシナリオでのウォームパッチのサポートも可能になります。

最初のノードインストール

1. いずれかのクラスタノード (node01) に接続して、コンソールウィンドウを開きます。
2. Sentinel インストーラ (tar.gz ファイル) をダウンロードして、そのクラスタノードの /tmp に保管します。
3. 次のコマンドを実行します。

   ```
   mount /dev/<SHARED1> /var/opt/novell

   cd /tmp

   tar -xvzf sentinel_server*.tar.gz

   cd sentinel_server*

   ./install-sentinel --record-unattended=/tmp/install.props
   ```

1. 標準インストールを最後まで実行し、Sentinel の環境設定を適切に行います。インストーラはバイナリ、設定、データベースをインストールし、ユーザ名とパスワードおよびネットワークポートをセットアップします。
2. Sentinel を起動して、基本機能をテストします。標準の外部クラスタノード IP を使用して Sentinel にアクセスできます。
3. Sentinel をシャットダウンして、共有ストレージをマウント解除します。

   ```
   rcsentinel stop

   umount /var/opt/novell
   ```

   これにより、自動起動スクリプトが削除され、クラスタは Sentinel を管理できるようになります。

   ```
   cd /

   insserv -r sentinel
   ```

後続のノードインストール

その他のノードでインストールを繰り返します :

最初の Sentinel インストーラは Sentinel 自体が使用するユーザアカウントを作成します。そして、インストール時点から次に使用可能なユーザ ID を使用します。後続のインストールを無人モードで実行すると、アカウント作成時に使用したのと同じユーザ ID を使用しようとしますが、(クラスタノードがインストール時のノードと同じでない場合には) 競合が発生する可能性があります。以下のいずれかを行うことを強くお勧めします。

- クラスタノード全体でユーザアカウントデータベースを (手動で LDAP からまたは同様の方法で) 同期して、後続のインストールを実行する前に同期を完了させておきます。この場合、インストーラはユーザアカウントの存在を検出して、既存のアカウントを使用します。
- 後続の無人インストールの結果を確認します。同じユーザ ID でユーザアカウントを作成できなかった場合、警告が出ている可能性があります。

1. 各追加クラスタノード (node02) に接続して、コンソールウィンドウを開きます。
2. 次のコマンドを実行します :

```
cd /tmp
scp root@node01:/tmp/sentinel_server*.tar.gz
scp root@node01:/tmp/install.props
tar -xvzf sentinel_server*.tar.gz
./install-sentinel --no-start --cluster-node --unattended=/tmp/install.props
cd /
insserv -r sentinel
```

この処理が終わると、Sentinel がすべてのノードにインストールされているはずです。しかし、各種キーが同期されるまで、最初のノード以外のノードでは Sentinel が正常に動作しない可能性があります。これは、クラスタリソースを設定した場合に発生します。

A.4.4 クラスタインストール

各ノードにクラスタソフトウェアをインストールし、各クラスタノードをクラスタマネージャに登録します。この操作の手順はクラスタ実装によって異なりますが、最終的には各クラスタノードがクラスタ管理コンソールに表示されている状態になります。

サンプルソリューションでは、SUSE Linux High Availability Extension をセットアップし、それに Sentinel 固有のリソースエージェントをオーバーレイします。:

Sentinel の監視に OCF リソースエージェントを使用しない場合は、ローカルクラスタ環境用に同様の監視ソリューションを開発する必要があるでしょう。Sentinel 用の OCF リソースエージェントはシンプルなシェルスクリプトで、さまざまな検査を実行して Sentinel が機能しているかどうかを検証します。独自に開発する場合は、既存のリソースエージェントを参考に調べることをお勧めします (リソースエージェントは Sentinel ダウンロードパッケージの sentinel-ha.rpm に含まれています)。

SLE HAE クラスタの設定の仕方は数多くありますが、ここでは単純なオプションを選ぶことにします。最初のステップとして、SLE HAE コアソフトウェアをインストールします。その手順については『SLE HAE Documentation』に詳しく説明されています。SLES アドオンのインストールについては、『Deployment Guide』を参照してください。

このサンプルソリューションの場合、SLE HAE をすべてのクラスタノード (node01 および node02) にインストールする必要があります。このアドオンをインストールすると、コアとなるクラスタ管理および通信ソフトウェアだけでなく、クラスタリソースの監視に使用される多数のリソースエージェントもインストールされます。

クラスタソフトウェアがインストールされたなら、さらに RPM をインストールして Sentinel 固有のクラスタリソースエージェントを追加する必要があります。この RPM は novell-Sentinel-ha-7.1*.rpm で、Sentinel をインストールする際にアンパックした通常の Sentinel ダウンロードに含まれています。

各クラスタノードで、novell-Sentinel-ha-7.1*.rpm を /tmp にコピーしてから、次のコマンドを実行します。

```
cd /tmp
```

```
rpm -i novell-Sentinel-ha-7.1*.rpm
```

A.4.5 クラスタ環境設定

クラスタソフトウェアを設定して、各クラスタノードをクラスタのメンバーとして登録する必要があります。この設定の一部として、フェンシングと STONITH リソースもセットアップすることで、クラスタの整合性を保つことができます。

サンプルソリューションでは、基本的に、追加の冗長性や高度な機能を含めない最もシンプルな構成を使用します。また、(一般に好まれるマルチキャストアドレスではなく) ユニキャストアドレスを使用します。ネットワーク管理者とのやり取りが少なく済み、かつテスト目的には十分であるからです。加えて、シンプルな SBD ベースのフェンシングリソースもセットアップします。

サンプルソリューション :

サンプルソリューションでは、内部クラスタ通信にプライベート IP アドレスを使用し、ネットワーク管理者へのマルチキャストアドレスの要求が最小限で済むようにユニキャストを使用します。ソリューションでは、iSCSI Target も使用します。これは、フェンシングのために SBD デバイスの役割を果たす共有ストレージをホストしているのと同じ SUSE Linux VM に設定されます。前述のように、iSCSI デバイスは任意のファイルまたはブロックデバイスを使用して作成できますが、ここでは分かりやすくするために専用のファイルを作成して使用することにします。

以下の設定ステップは、「共有ストレージのセットアップ」のステップと非常によく似ています :

SBD のセットアップ

storage03 に接続して、コンソールセッションを開始します。次の **dd** コマンドを使用して、希望する任意のサイズのブランクファイルを作成します :

```
dd if=/dev/zero of=/sbd count=1024 bs=1024
```

ここでは、(/dev/zero pseudo-device からコピーして) ゼロ (0) を埋め込んだ 1MB のファイルを作成します。

このファイルを iSCSI Target として設定します :

1. コマンドラインから YaST を実行します (または GUI を使用することもできます): /sbin/yast
2. ［**ネットワークサービス**］、［**iSCSI ターゲット**］の順に選択します。
3. ［**ターゲット**］をクリックして、既存のターゲットを選択します。
4. ［**編集**］を選択します。UI に使用可能な LUN(ドライブ) のリストが表示されます。

5 ［**追加**］を選択して、新しい LUN を追加します。

6 LUN 番号は 2 のままにしておきます。［**パス**］ダイアログを参照して、作成した /sbd ファイルを選択します。

7 その他のオプションはデフォルトのままにしておき、［**OK**］を選択してから［**次**］を選択し、もう一度［**次**］をクリックしてデフォルト認証オプションを選択します。

8 ［**完了**］をクリックして、設定を終了します。必要に応じてサービスを再起動します。YaST の終了 .

注 : 以下のステップでは、各クラスタノードが他のすべてのクラスタノードのホスト名を解決できなければなりません (それができないと、ファイル同期サービス csync2 が失敗します)。DNS がセットアップされていないまたは使用できない場合は、各ホストのエントリを /etc/hosts ファイルに追加します。このファイルには、hostname コマンドを実行して返されるような各 IP とそのホスト名がリストされています。

上記の手順を行うことにより、IP アドレス 10.0.0.3(storage03) のサーバに SBD デバイスの iSCSI Target が公開されます。

ノードの設定

クラスタノード (node01) に接続して、コンソールを開きます :

1 YaST を実行します。

2 ［**ネットワークサービス**］、［**iSCSI イニシエータ**］の順に開きます。

3 ［**Connected Targets(接続済みターゲット)**］を選択してから、上記の手順で設定した iSCSI Target を選択します。

4 ［**ログアウト**］オプションを選択して、Target をログアウトします。

5 ［**Discovered Targets(検出したターゲット)**］タブに切り替えて、［**Target(ターゲット)**］を選択し、もう一度ログインし直して、デバイスのリストを更新します (自動起動オプションと［No Authentication(認証なし)］はそのままにしておきます)。

6 ［**OK**］を選択して、iSCSI イニシエータツールを終了します。

7 ［**システム**］、［**Partitioner(パーティショナ)**］の順に開いて、SBD デバイスを 1MB IET-VIRTUAL-DISK として特定します。このデバイスは **/dev/sdd** または同様の形式でリストされます。どちらかを確認します。

8 YaST の終了 .

9 コマンド ls -l /dev/disk/by-id/ を実行して、上記の手順で特定したデバイス名にリンクされているデバイス ID を確認します。

10 コマンド sleha-init を実行します。

11 バインド先のネットワークアドレスの入力を要求されたら、外部 NIC IP (172.16.0.1) を指定します。

12 デフォルトのマルチキャストアドレスおよびポートを受け入れます。この設定は後で上書きします。

13 SBD の有効化に「y」と入力してから、/dev/disk/by-id/<device id> を指定します。<device id> は上記の手順で特定した ID です (Tab キーを使ってパスを自動補完することができます)。

14 ウィザードを最後まで進めて、エラーの報告がないことを確認します。

15 YaST を起動します。

16 ［**High Availability(高可用性)**］、［**Cluster(クラスタ)**］の順に選択します (一部のシステムでは［Cluster(クラスタ)］を選択するだけです)。

17 左のボックスで、［**Communication Channels(通信チャネル)**］が選択されていることを確認します。

18 設定の最上部行にタブで移動し、udp の選択を udpu に変更します (これで、マルチキャストを無効にし、ユニキャストを選択します)。

19 ［**Add a Member Address(メンバアドレスを追加)**］を選択して、このノード (172.16.0.1) を指定してから、この手順を繰り返して他のクラスタノード (172.16.0.2) を追加します。

20 ［**完了**］をクリックして設定を完了します。

21 YaST の終了 .

22 コマンド /etc/rc.d/openais restart を実行して、新しい同期プロトコルでクラスタサービスを再起動します。

各追加クラスタノード (node02) に接続して、コンソールを開きます :

1 次のコマンドを実行します : sleha-join

2 最初のクラスタノードの IP アドレスを入力します。

環境によっては、クラスタ通信が正しく初期化されないことがあります。クラスタが起動しない場合 (openais サービスが開始できない場合):

- corosync.conf を node1 から node02 に手動でコピーするか、ノード 1 で csync2 -x -v を実行する、または YaST を使用して node02 上にクラスタを手動で設定します。
- node02 で /etc/rc.d/openais start を実行します。

場合によっては、xinetd サービスが新規 csync2 サービスを正しく追加できないために、スクリプトが失敗する可能性があります。他方のノードがクラスタ設定ファイルをこのノードに同期できるようにするためには、このサービスが必須です。csync2 run failed (csync2 の実行が失敗しました) のようなエラーが表示されるときは、この問題である可能性があります。この問題を修復するには、kill -HUP `cat /var/run/xinetd.init.pid を実行してから、sleha-join スクリプトを再実行します。

この時点で、各クラスタノードで crm_mon を実行できるようになっており、クラスタが正常に実行していることを確認できるはずです。または、Web コンソール 'hawk' を使用することもできます。デフォルトのログイン資格情報は 'hacluster / linux' です。

この例では、さらに 2 つのパラメータを微調整する必要があります。この調整がお客様の運用クラスタに適用されるかどうかは、お客様のクラスタ設定により異なります。

1 グローバルクラスタオプション no-quorum-policy を ignore に設定します。このようにするのは、ノードが 2 つしかないクラスタで、どちらかのノードに障害が発生すると必要数が満たされなくなり、クラスタ全体がシャットダウンしてしまうからです : crm 設定プロパティ no-quorum-policy=ignore

注 : クラスタに 3 つ以上のノードがある場合は、このオプションを設定しないでください。

2 グローバルクラスタオプション default-resource-stickiness を 1 に設定します。このように設定することで、リソースマネージャはリソースを循環させるのではなく、一定の場所で実行したままにします : crm 設定プロパティ default-resource-stickiness=1。

A.4.6 リソースの設定

「クラスタのインストール」で説明したように、このソリューションでは SLE HAE で実行するコアサービスを監視するために OCF リソースエージェントが使用されていますが、必要に応じてその代わりになるものも作成できます。また、このソフトウェアは他のいくつかのリソースに依存しています。そのために、SLE HAE にはリソースエージェントがデフォルトで使用されるようになっています。SLE HAE を使用しない場合は、何か他のテクノロジを使用して以下の追加リソースを監視する必要があります。

- このソフトウェアが使用する共有ストレージに相当するファイルシステムリソース。
- サービスへのアクセスに使用する仮想 IP に相当する IP アドレスリソース。
- ソフトウェアが設定およびイベントメタデータを保管するために使用するPostgresデータベースソフトウェア。

他にもセキュリティインテリジェンス用に使用される MongoDB や ActiveMQ メッセージバスなどのリソースがあり、少なくとも現時点ではコアサービスの一部として監視されています。

サンプルソリューション

サンプルソリューションでは、シンプルなファイルシステムリソースエージェントなど、必須リソースは単純なものになっています。必要であれば、cLVM(論理ボリューム対応のファイルシステム) のようなより高性能なクラスタリソースを使用することもできます。

サンプルソリューションでは、クラスタ設定に役立つように crm スクリプトが提供されています。スクリプトは、Sentinel インストールの途中で生成される無人セットアップファイルから必要な設定変数を取り出します。セットアップファイルを生成していない場合、またはリソースの設定を変更する場合は、それに応じてスクリプトを編集できます。

Sentinel をインストールした元のノード (Sentinel の完全インストールを実行したノード) に接続し、次のコマンドを実行します (<SHARED1> は上記の作業で作成した共有ボリューム):

```
mount /dev/<SHARED1> /var/opt/novell
```

```
cd /usr/lib/ocf/resource.d/novell
```

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

クラスタ内に生成される新規リソースに問題がある可能性もあります。その場合は、node02 上で /etc/rc.d/openais restart を実行します。

install-resources.sh スクリプトは、2 つの値、すなわち一般ユーザが Sentinel にアクセスするときに使用する仮想 IP および共有ストレージのデバイス名の入力を要求し、その後必要なクラスタリソースを自動生成します。スクリプトに指定する共有ボリュームは既にマウント済みのものでなければならないこと、および Sentinel インストール時に作成された無人インストールファイル (/tmp/install.props) も必要であることに注意してください。このスクリプトは最初にインストールを実行したノードのみで実行すればよく、必要なすべての設定ファイルは他のノードに自動的に同期されます。

お客様の環境がこのサンプルソリューションとは異なる場合は、同一ディレクトリにある resources.cli ファイルを編集し、その中のプリミティブ定義を変更してください。たとえば、サンプルソリューションではシンプルなファイルシステムリソースを使用していますが、もっとクラスタ指向の cLVM リソースを望むお客様もおられるでしょう。

シェルスクリプトを実行した後、crm ステータスコマンドを実行することができます。出力は次のように表示されます。

```
crm status
```

```
Last updated: Thu Jul 26 16:34:34 2012
Last change: Thu Jul 26 16:28:52 2012 by hacluster via crmd on node01
Stack: openais
Current DC: node01 - partition with quorum
Version: 1.1.6-b988976485d15cb702c9307df55512d323831a5e
2 Nodes configured, 2 expected votes
5 Resources configured.
```

```
Online: [ node01, node02 ]
stonith-sbd    (stonith:external/sbd):    Started node01
 Resource Group: sentinelgrp
     sentinelip    (ocf::heartbeat:IPaddr2):    Started node01
     sentinelfs    (ocf::heartbeat:Filesystem):    Started node01
     sentineldb    (ocf::novell:pgsql):    Started node01
     sentinelserver    (ocf::novell:sentinel):    Started node01
```

この時点で、関係する Sentinel リソースがクラスタに設定されています。クラスタ管理ツールで crm status を実行するなどして、リソースがどのように設定およびグループ化されているかを確認できます。

A.4.7 ネットワークストレージの設定

一連の作業の最後のステップとして、ネットワークストレージを設定して、Sentinel がイベントパーティションを低コストなストレージに移行できるようにします。このステップは省略可能です。実際、ネットワークストレージに対してシステムの他の部分に行ったのと同じように高可用性を持たせる必要はありません。NFS ボリュームでも、CIFS ボリュームでも、どのディレクトリでも (SAN にマウントされているかどうかに係わりなく) 使用可能です。

上部メニューバーの［**ストレージ**］をクリックしてから［**環境設定**］を選択し、［Network storage(ネットワークストレージ)］から未設定のネットワークストレージのラジオボタンを 1 つ選択してセットアップします。

サンプルソリューション

サンプルソリューションでは、ネットワーク共有ストレージの場所としてシンプルな iSCSI Target を、ローカルストレージとほぼ同じ設定で使用します。運用実装では、これとは異なるストレージテクノロジを使用することもあり得ます。

以下の手順に従って、Sentinel が使用するネットワークストレージを設定します。

注 : このサンプルソリューションでは iSCSI Target を使用するので、ネットワークストレージとして使用するターゲットはディレクトリとしてマウントされます。そのため、このマウントを、ローカルストレージファイルシステムを設定するのと同様の方法で、ファイルシステムリソースとして設定する必要があります。セットアップには他にもいろいろな方法があり得るため、リソースインストールスクリプトの一部として自動的には設定されませんでした。ここで手動で設定します。

1. 上記のステップを確認して、ネットワークストレージ用にどのパーティションが作成されたかを判別します (/dev/<NETWORK1>、つまり /dev/sdc1 など)。必要であれば、パーティションをマウントできる空のディレクトリを作成します (/var/opt/netdata など)。
2. ネットワークファイルシステムをクラスタリソースとしてセットアップします。Web GUI を使用するかまたは次にコマンドを実行します :

   ```
   crm configure primitive sentinelnetfs ocf:heartbeat:Filesystem params device="/
   dev/<NETWORK1>" directory="<PATH>" fstype="ext3" op monitor interval=60s
   ```

   ここで、/dev/<NETWORK1> は前述の「共有ストレージのセットアップ」セクションで作成したパーティションで、<PATH> はストレージをマウントする任意のローカルディレクトリです。

3 管理対象リソースのグループに新規リソースを追加します :

```
crm resource stop sentinelgrp
crm configure delete sentinelgrp
crm configure group sentinelgrp sentinelip sentinelfs sentinelnetfs sentineldb
sentinelserver
crm resource start sentinelgrp
```

4 現在リソースをホストしているノードに接続して (crm status または Hawk を使用)、ネットワークストレージが正しくマウントされていることを確認します (mount コマンドを使用)。

5 Sentinel Web インタフェースにログインします。

6 ［**ストレージ**］を選択してから［**環境設定**］を選択し、未設定のネットワークストレージの［**SAN(ローカルにマウント)**］を選択します。

7 ネットワークストレージがマウントされるパスを、たとえば /var/opt/netdata のように入力します。

サンプルソリューションでは、シンプルなファイルシステムリソースエージェントなど、必要なリソースには単純なものを使用しています。お客様のご希望によっては、cLVM(論理ボリューム対応のファイルシステム) のようなより高性能なクラスタリソースを使用することも可能です。

A.5 バックアップと復元

本マニュアルに記述されている高可用性フェールオーバークラスタは一定レベルの冗長性を提供するので、クラスタ内のあるノードでサービスに障害が起きた場合でも、自動的にフェールオーバーして、クラスタ内の別のノード上に復元します。このようなイベントが生じたとき、障害が発生したノードを運用状態に戻して、システムの冗長性を回復し、再び障害が発生したときにシステムを保護できるようにすることが重要です。このセクションでは、さまざまなエラー条件で障害が発生したノードを復元する方法について説明します。

- 151 ページのセクション A.5.1「バックアップ」
- 151 ページのセクション A.5.2「回復」

A.5.1 バックアップ

本マニュアルに記述されているような高可用性フェールオーバークラスタは一定レベルの冗長性を提供していますが、環境設定やデータについては従来の方法でバックアップを定期的に取っておくことは重要です。これらは、一度失われたり壊れたりしても簡単には回復できない場合が多いからです。『*NetIQ Sentinel 7.1 Administration Guide*』のセクション「「Backing Up and Restoring Data」」では、Sentinel の組み込みツールを使用してバックアップを作成する方法が説明されています。クラスタ内のパッシブノードは共有ストレージデバイスに対する必要なアクセス権を持っていないため、これらのツールはクラスタ内のアクティブノードで使用します。他のバックアップツール製品を代わりに使用することもできますが、どのノードで使用できるかに関して異なる要件を持っている可能性があります。

A.5.2 回復

- 152 ページの 「一時的な障害」
- 152 ページの 「ノードの破損」
- 152 ページの 「クラスタデータの設定」

一時的な障害

障害が一時的であり、アプリケーション、オペレーティングシステムソフトウェア、および環境設定に明らかな破損がない場合は、ノードをリブートするなどして一時的な障害を解除するだけでノードを運用状態に復元できます。必要であれば、クラスタ管理ユーザインタフェースを使用して、実行中のサービスをフェールバックして元のクラスタノードに戻すことができます。

ノードの破損

障害によって、ノードのストレージシステム上にあるアプリケーション、オペレーティングシステムソフトウェア、または環境設定に破損が生じた場合は、破損したソフトウェアを再インストールする必要があります。本マニュアルで既に説明したクラスタのノードを追加するステップを繰り返すことで、ノードを運用状態に復元することができます。必要であれば、クラスタ管理ユーザインタフェースを使用して、実行中のサービスをフェールバックして元のクラスタノードに戻すことができます。

クラスタデータの設定

共有ストレージデバイス上でデータの破損が生じて共有ストレージデバイスが回復不能である場合は、その影響がクラスタ全体に及んでおり、本マニュアルで説明されている高可用性フェールオーバークラスタを使用しても自動的には回復できない状態になっていると考えられます。『*NetIQ Sentinel 7.1 Administration Guide*』のセクション「「Backing Up and Restoring Data」」では、Sentinel の組み込みツールを使用してバックアップから復元する方法が説明されています。クラスタ内のパッシブノードは共有ストレージデバイスに対する必要なアクセス権を持っていないため、これらのツールはクラスタ内のアクティブノードで使用します。他のバックアップ復元ツール製品を代わりに使用することもできますが、どのノードで使用できるかに関して異なる要件を持っている可能性があります。

B インストールのトラブルシューティング

このセクションでは、インストール時に発生する可能性があるいくつかの問題とその解決方法について説明します。

B.1 ネットワーク接続が不正なためにインストールが失敗する

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

この問題を解決するには、ネットワークを正しく設定します。環境設定を確認するには、有効な IP アドレスを返す ipconfig コマンドと、有効なホスト名を返す hostname -f コマンドを使用します。

B.2 イメージを作成したコレクタマネージャまたは相関エンジンの 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 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 が重複してい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で次の手順を実行し、新しい UUID を生成する必要があります。

1. /var/opt/novell/sentinel/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。

C アンインストール中

この付録では、Sentinel のアンインストールおよびアンインストール後の作業について説明します。

C.1 アンインストールのためのチェックリスト

次のチェックリストを使用して、Sentinel のアンインストールしてください :

- ❒ Sentinel サーバをアンインストールする。
- ❒ コレクタマネージャおよび相関エンジンをアンインストールする(インストールされている場合)。
- ❒ アンインストール後の作業を実行して、Sentinel のアンインストールを完了する。

C.2 Sentinel のアンインストール

Sentinel のインストールを削除するのに便利なアンインストーラスクリプトを使用できます。新規のインストールを実行する前に、以前のインストールのファイルまたはシステム設定が残らないようにするために、次の手順をすべて実行する必要があります。

警告 : これらの手順では、オペレーティングシステムの設定やファイルを変更します。システム設定やファイルの変更方法に精通したユーザでない場合は、システム管理者に問い合わせてください。

C.2.1 Sentinel サーバのアンインストール

次の手順に従って、Sentinel サーバをアンインストールします。

1. Sentinel サーバに root としてログインします。

   注 : root ユーザとしてインストールを実行している場合、root 以外のユーザで Sentinel サーバをアンインストールすることはできません。ただし、root 以外のユーザがインストールした場合は、root 以外のユーザで Sentinel サーバをアンインストールできます。

2. 次のディレクトリにアクセスします。

   `/opt/novell/sentinel/setup/`

3. 次のコマンドを実行します。

```
./uninstall-sentinel
```

4 アンインストールを続行するかどうか再確認を求められたら、「y」を押します。

スクリプトはまずサービスを停止し、その後に削除を実行します。

C.2.2 コレクタマネージャまたは相関エンジンのアンインストール

次の手順に従って、コレクタマネージャおよび相関エンジンをアンインストールします :

1 root としてログインします。

注 : root ユーザとしてインストールを実行している場合、root 以外のユーザでリモートコレクタマネージャまたはリモート相関エンジンをアンインストールすることはできません。ただし、root 以外のユーザがインストールしている場合は、root 以外のユーザでアンインストールできます。

---

2 次の場所に移動します。

```
/opt/novell/sentinel/setup
```

3 次のコマンドを実行します。

```
./uninstall-sentinel
```

スクリプトによって、コレクタマネージャまたは相関エンジンとすべての関連データが完全に削除されるという警告が表示されます。

4 「y」と入力して、コレクタマネージャまたは相関エンジンを削除します。

スクリプトはまずサービスを停止し、その後に削除を実行します。ただし、コレクタマネージャと相関エンジンのアイコンは、Web インタフェースにインアクティブな状態で表示されたままです。

5 次の追加の手順を行って、Web インタフェースのコレクタマネージャと相関エンジンを手動で削除します :

コレクタマネージャ :

1. *［イベントソースの管理］> ［ライブビュー］* にアクセスします。
2. 削除するコレクタマネージャを右クリックして、［*削除*］をクリックします。

相関エンジン :

1. 管理者として Sentinel Web インタフェースにログインします。
2. ［*相関関係*］を展開してから、削除する相関エンジンを選択します。
3. ［*削除*］ボタン (ごみ箱アイコン) をクリックします。

C.3 アンインストール後の作業

Sentinel サーバをアンインストールしても、Sentinel 管理者ユーザはオペレーティングシステムから削除されません。このユーザを手動で削除する必要があります。

Sentinel のアンインストール後も、特定のシステム設定が残ります。これらの設定は、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。特に、Sentinel のアンインストール時にエラーが発生した場合にその必要があります。

Sentinel のシステム設定を手動でクリーンアップするには :

1. root としてログインします。
2. すべての Sentinel プロセスを停止します。
3. /opt/novell/sentinel または Sentinel ソフトウェアがインストールされていた場所の内容を削除します。
4. Sentinel 管理者オペレーティングシステムユーザ (デフォルトでは novell) としてログインしているユーザがいないことを確認してから、ユーザ、ホームディレクトリ、およびグループを削除します。

   userdel -r novell

   groupdel novell
5. オペレーティングシステムを再起動します。