Sentinel™
インストールと設定ガイド

2021 年 8 月

保証と著作権

Micro Focus、関連会社、およびライセンサ (「Micro Focus」) の製品およびサービスに対する保証は、当該製品およびサービスに付属する保証書に明示的に規定されたものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。Micro Focus は、本書に技術的または編集上の誤りまたは不備があっても責任を負わないものとします。本書の内容は、将来予告なしに変更されることがあります。

証明書関連の通知および商標などの追加情報については、http://www.microfocus.com/about/legal/ を参照してください。

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、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ているその他の情報

ライブラリには次の情報リソースが含まれています。

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。

Sentinel について

このセクションでは、Sentinel の概要と 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。

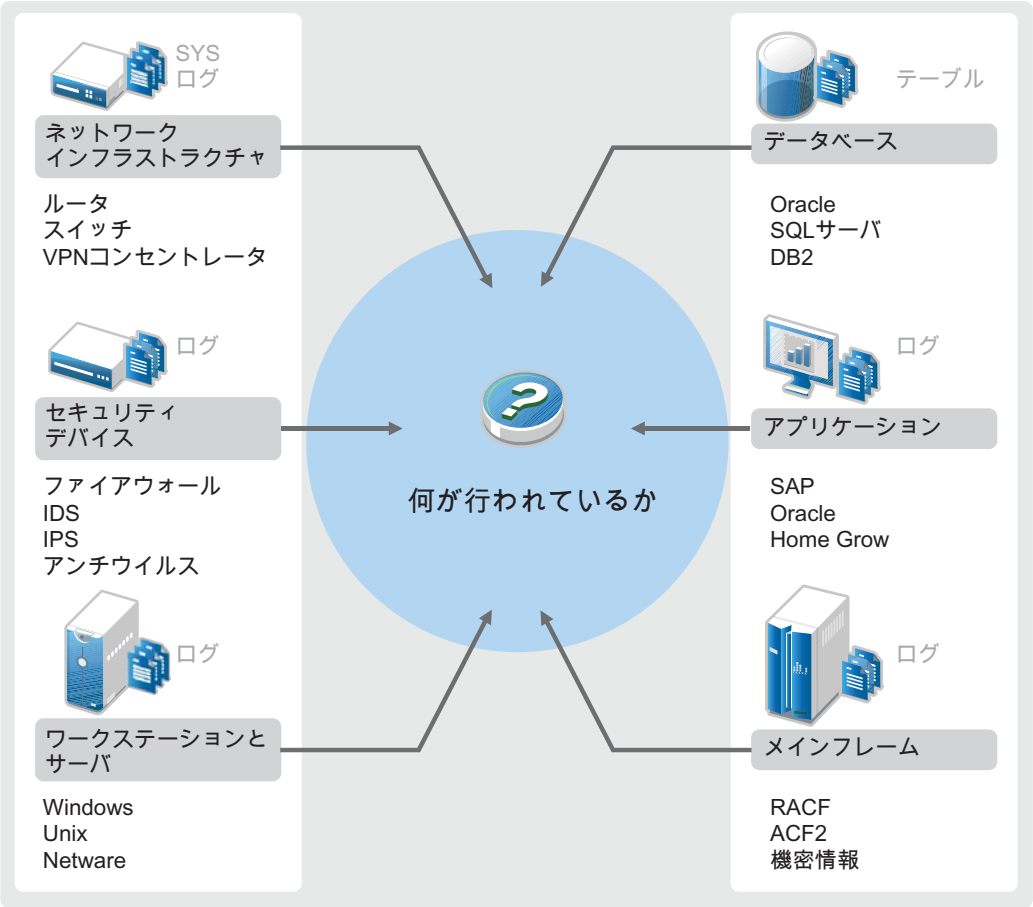
1 Sentinel の概要

Sentinel は、セキュリティ情報およびイベント管理 (SIEM) ソリューションであると同時に、コンプライアンスモニタリングソリューションでもあります。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。

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、その環境が複雑であるため容易ではありません。一般に、IT 環境には多数のアプリケーション、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存在し、それらすべてのエンティティがイベントのログを生成します。さらに、IT 環境にはセキュリティデバイスやネットワークインフラストラクチャデバイスもあり、それらのデバイスもイベントのログを生成する場合があります。

図1-1 環境で発生していること



次の要因が、困難を生み出します。

- IT 環境にデバイスがたくさんある
- ログの形式が異なる
- さまざまな場所にログが保存される
- ログファイルに大量の情報が取り込まれる
- ログファイルを手動で分析しないとイベントのトリガを判断できない

ログファイルの情報を活用するには、次の作業を実行できる必要があります。

- 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
- データが基準から外れたときには通知を送信する

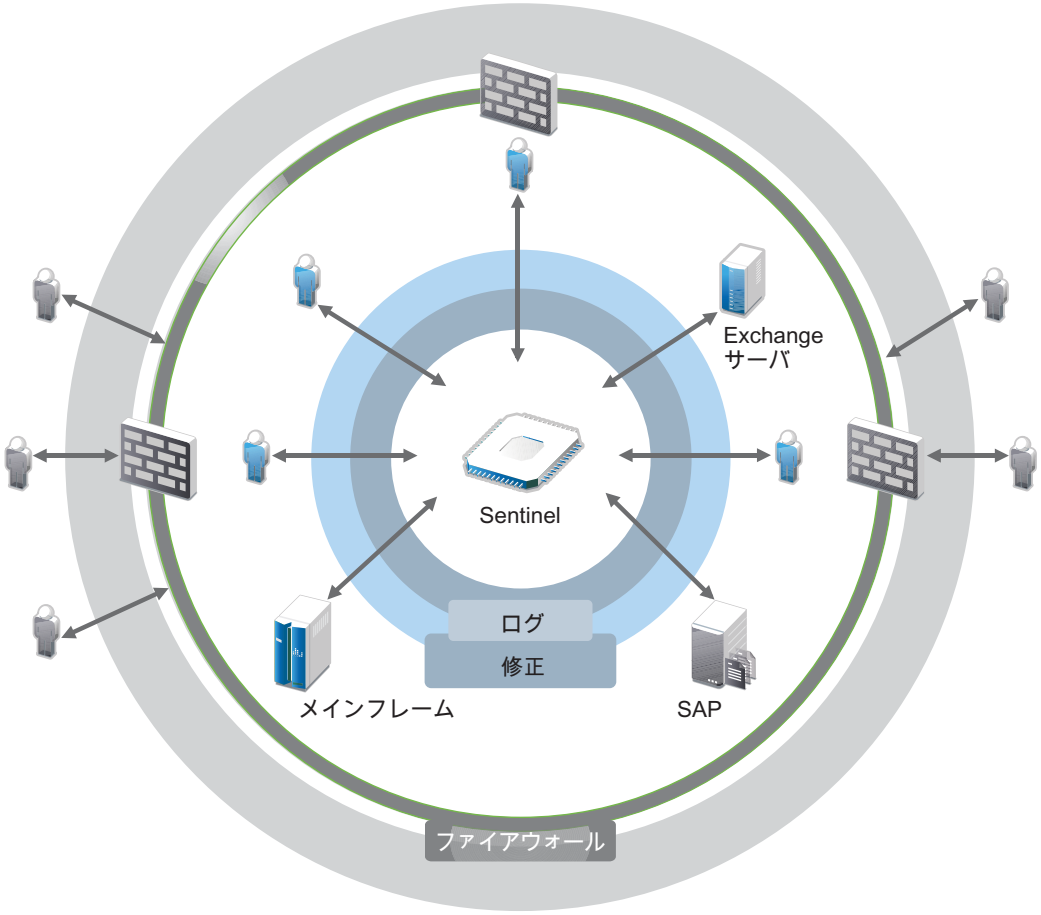
- ビジネスポリシーに従って通知に対する行動をとる
- コンプライアンスの証明のためにレポートを生成する

IT 環境のセキュリティ保護に関する課題について理解したら、ユーザエクスペリエンスを損なうことなく、ユーザのために企業のセキュリティを確保する方法と、ユーザから企業のセキュリティを保護する方法について判断することが必要になります。Sentinel がソリューションを提供します。

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収集します。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*



Sentinel では、IT 環境内にどの時点で発生した事態についても把握することができ、リソースに対して行われたアクションと、そのアクションを行った人物を結び付けることができます。これにより、ユーザの行動を特定し、アクティビティを能率的に監視して、悪意のあるアクティビティを防止することができます。

Sentinel では、次のようにして、これを実現しています。

- 複数のセキュリティ標準に及ぶ IT 制御に対応する単一のソリューションを提供する
- IT 環境内で発生するべき事象と実際に発生した事象の間にあるギャップを処理する
- セキュリティ標準への準拠を支援する
- 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

Sentinel では、ログコレクション、分析、およびレポーティングプロセスを自動化することで、IT 制御により効果的に脅威の検出と監査要件に対応します。Sentinel は、セキュリティイベント、コンプライアンスイベント、および IT コントロールの自動モニタリングを提供します。これにより、セキュリティ違反または準拠違反のイベントが発生している場合に、すぐに対処できます。さらに、Sentinel を使用すると、自社環境についてのサマリ情報を収集することもできます。この情報は、主要な利害関係者と共有できます。

2 Sentinel の動作原理

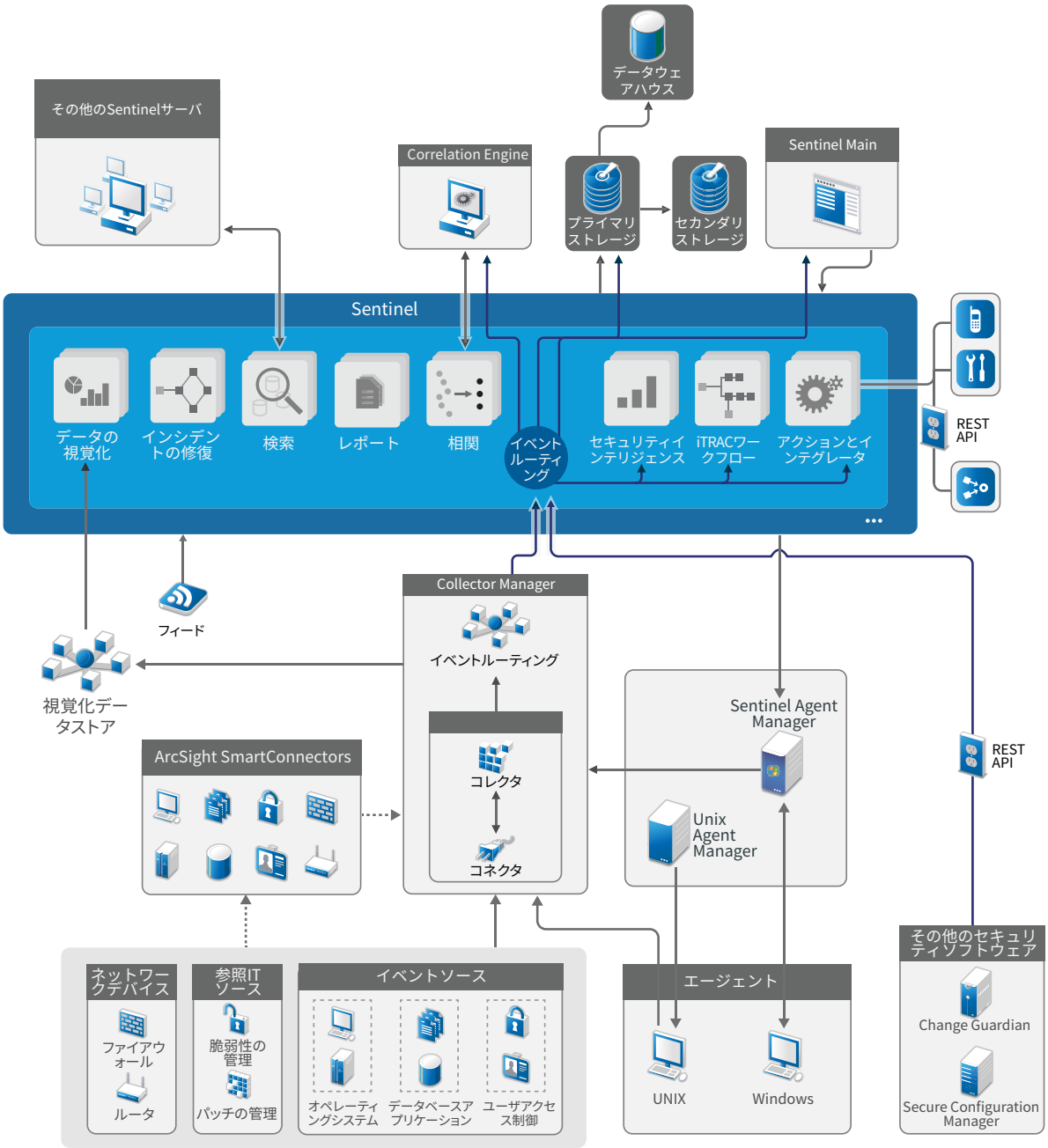
Sentinel は、IT 環境全体のセキュリティ情報とイベントを継続的に管理することで、完全なモニタリングソリューションを提供します。

Sentinel は次の処理を行います。

- IT 環境内のさまざまなソースからログ、イベント、およびセキュリティの情報を収集します。
- 収集したログ、イベント、およびセキュリティの情報を標準 Sentinel フォーマットに正規化します。
- 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レージにイベントを格納します。
- IP フローデータを収集し、ネットワークの動作を詳しく監視するのを支援します。
- 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 サーバ上のイベントに加えて、世界中に分散している Sentinel サーバ上のイベントも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、そのベースラインと発生中の事象を比較して、未知の問題が発生していないかどうかを判断します。
- 特定の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、データストレージオプションとして従来のストレージを使用する場合に、Sentinel がどのように機能するかを示しています。

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。

イベントソース

Sentinel は、IT 環境内のさまざまな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。一般に、次のものがネットワーク上のイベントソースになります。

セキュリティの境界 : 環境にセキュリティ境界を作成するために使用される、ハードウェアとソフトウェアが組み込まれているセキュリティデバイス。ファイアウォール、侵入検知システム (IDS)、VPN (仮想プライベートネットワーク) などがあります。

オペレーティングシステム : ネットワーク内で実行されている各種オペレーティングシステム。

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 : ネットワーク内にインストールされている各種アプリケーション。

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。

イベントソースからイベントを収集する方法の詳細については、『「Sentinel Administration Guide」』の「*Collecting and Routing Event Data*」を参照してください。

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。

イベントとは、サードパーティのセキュリティデバイスや、ネットワーク、アプリケーションデバイス、あるいは内部の Sentinel ソースから Sentinel に報告された、正規化されたログレコードです。イベントにはいくつかのタイプがあります。

- 次のような外部イベント (セキュリティデバイスから受信したイベント)
  - 侵入検知システム (IDS) が検出した攻撃
  - オペレーティングシステムによって報告された、正常なログイン
  - ユーザによるファイルへのアクセスなど、顧客が定義した状況
- 次を含む内部イベント (Sentinel によって生成されたイベント)
  - 無効化されている相関ルール
  - データベースの空きがなくなる

Sentinel は、カテゴリ情報 (taxonomy) をイベントに追加します。これにより、異なる方法でイベントをレポートするシステム全体でイベントを容易に比較できます。イベントは、リアルタイム表示、Correlation Engine、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。

1 つのイベントは、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、深刻性、宛先 IP アドレス、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。

設定可能なフィールドのセットが 2 つあります。

- 予約済みフィールド : 将来の機能拡張を可能にするために、Sentinel 内部で使用します。
- カスタマフィールド : カスタマイズのために、お客様が使用します。

フィールドのソースは、外部または参照のどちらかになります。

- 外部フィールドの値は、デバイスまたは対応するコレクタにより明示的に設定されます。たとえば、イベントの宛先 IP アドレス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。
- 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、イベントから得られる宛先 IP アドレスを使用して定義したマップを使用するマッピングサービスでフィールドを計算することができます。

- 23 ページの 「マッピングサービス」
- 23 ページの 「マップのストリーミング」

マッピングサービス

マッピングサービスにより、ビジネス関連のデータがシステム全体に伝播されます。このデータは、参照情報によってイベントを補足できます。

ソースデバイスからの着信イベントにホストや識別情報などの情報を追加するマップを使用することで、イベントデータを補足できます。Sentinel は、高度な相関とレポーティングに、この追加情報を使用できます。Sentinel は、複数の組み込みマップに加えて、カスタマイズされたユーザ定義のマップもサポートします。

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、内部で更新されて、自動的にマッピングサービス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］ユーザインタフェース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 Collector Manager 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。

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ないようにしています。これは、システムの一時的な負荷によって低下せず、安定して予測可能な素早いデータ移動を必要とする、Sentinel のようなミッションクリティカルなリアルタイムシステムにとって重要なことです。

Collector Manager

Collector Manager 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、イベントフィルタリングを実行します。Collector Manager の主要な機能は次のとおりです。

- コネクタの使用によるデータの収集。
- コレクタの使用によるデータの解析と正規化。

コレクタ

コレクタは、コネクタから情報を収集して、その情報を正規化します。コレクタは、次の機能を実行します。

- 生データをコネクタから受信する。
- データの解析と正規化を実行する。
    - イベントソース固有のデータを Sentinel 固有のデータに変換する。

- イベントに含まれる情報を Sentinel が読み込めるフォーマットに変更してイベントを補強する。
- イベントにイベントソース固有のフィルタリングを行う。

- 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 :
  - イベントを識別情報にマッピングする。
  - イベントをアセットにマッピングする。
- イベントをルーティングする
- 正規化、解析、および形式設定を行ったデータを Collector Manager に渡す。
- ヘルスメッセージを Sentinel サーバに送信する

コレクタの詳細については、Sentinel プラグイン Web サイトを参照してください。

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。

コネクタが提供する機能は、次のとおりです。

- 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。

ArcSight SmartConnectors

Sentinel では、ArcSight SmartConnector を利用して、Sentinel が直接にはサポートしていないさまざまな種類のイベントソースからイベントを収集します。SmartConnector は、サポートされているデバイスからイベントを収集し、イベントを CEF (Common Event Format) に正規化し、Syslog コネクタを経由して Sentinel に転送します。その後、コネクタは、解析するためにイベントを Universal Common Event Format Collector に転送します。

Sentinel で SmartConnector を構成する方法について詳しくは、Sentinel プラグインの Web サイトで Universal Common Event Format Collector のドキュメントを参照してください。

Agent Manager

Agent Manager により、ホストベースのデータ収集が可能になります。これは、ユーザが次のタスクを実行できるようにすることで、エージェントを使用しないデータ収集を補完するものです。

- ネットワーク経由では利用できないログへのアクセス。
- 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。.

Agent Manager を使用すると、エージェントの展開とエージェント設定の管理ができるようになります。また、Agent Manager は、Sentinel に流れ込むイベントの収集ポイントとしても機能します。Agent Manager の詳細については、Agent Manager の資料を参照してください。

Sentinel データのルーティングとデータストレージ

Sentinel は、収集したデータをルーティング、保存、および抽出するためのさまざまなオプションを備えています。デフォルトでは、Sentinel は解析済みイベントデータと生データを Collector Manager instances から受信します。Sentinel は、セキュアなエビデンスチェーンを提供するために生データを保存し、解析済みイベントデータをユーザ定義のルールに従ってルーティングします。解析済みイベントデータはフィルタ処理することで、ストレージやリアルタイム分析に送信することも、外部システムにルーティングすることもできます。Sentinel は、ストレージに送信されたすべてのイベントデータをユーザ定義の保持ポリシーに一致させます。保持ポリシーは、イベントデータをシステムから削除する必要がある場合に制御します。

1 秒あたりのイベント数 (EPS) レートと展開の要件に応じて、データストレージのオプションとして、従来のファイルベースのデータストレージを使用するかを選択できます。詳細については、39 ページの 「データストレージの考慮事項」を参照してください。

イベント視覚化

Sentinel には、データをチャート、テーブル、およびマップで表すイベント視覚化機能が備わっています。これらの視覚化機能では、IP フローイベントなどの大量のイベントを簡単に視覚化および分析できます。また、独自の視覚化とダッシュボードも作成できます。

従来のストレージセットアップでイベント視覚化を利用できるのは、データの保存とインデックス作成を行うために視覚化データストア (Elasticsearch) を有効にした場合のみです。Elasticsearch を有効にする方法については、「42 ページの 「視覚化データストアの設定」」を参照してください。

相関

単一のイベントでは取るに足りないように思えても、別のイベントと組み合わさると潜在的な問題の警告になることがあります。Sentinel では、ユーザが作成して Correlation Engine に展開したルールを使用して、このようなイベントを相関させ、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。さらに、相関ルールが MITRE ATT&CK ID に関連付けられるようになりました。詳細については、『「Sentinel 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 Correlation Engine に展開する必要があります。ルールの条件と一致するイベントが発生すると、Correlation Engine 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、『*Sentinel User Guide (Sentinel ユーザガイド)*』の「「Correlating Event Data(イベント相関データ)」」を参照してください。

セキュリティインテリジェンス

Sentinel の相関機能により、アクティビティの既知のパターンを見つけられるようになります。このパターンは、セキュリティ、コンプライアンス、またはその他の理由を目的として分析できます。セキュリティインテリジェンス機能は、通常のアクティビティから外れていて、悪意の可能性があるが、既知のパターンとは一致しないアクティビティを検出します。

Sentinel のセキュリティインテリジェンス機能は、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、分析者が異常を識別して分析できるようにします。詳細については、『「Sentinel User Guide」』の「*Analyzing Trends in Data*」を参照してください。

インシデントの修復

Sentinel は、自動インシデント応答管理システムを備えているため、インシデントやポリシー違反の追跡、エスカレート、対応について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、トラブルチケット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、『「Sentinel User Guide」』の「*Configuring Incidents*」を参照してください。

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します。iTRAC 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始まり解決に至るまで、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。iTrac のワークフローでは、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、『「Sentinel User Guide」』の「*Configuring iTRAC Workflows*」を参照してください。

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、何らかのタイプのアクションを手動または自動で実行します。アクションは、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、および相関ルールでトリガできます。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、『「Sentinel Administration Guide」』の「*Configuring Actions*」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、『「Sentinel Administration Guide」』の「*Configuring Integrators*」を参照してください。

検索

Sentinel は、イベントに対して検索を実行するオプションを提供しています。必要な環境設定により、Sentinel によって生成されたシステムイベントを検索して、イベントごとに生データを表示することもできます。詳細については、『「Sentinel User Guide」』の「*Searching Events*」を参照してください。

複数の地理的場所に分散した Sentinel サーバを検索することもできます。詳細については、『「Sentinel Administration Guide」』の「*Configuring Data Federation*」を参照してください。

Reports (レポート)

Sentinel では、収集したデータについてのレポートを実行できます。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パッケージとして含まれています。結果に表示するカラムを指定できる、構成可能なレポートもあります。

PDF フォーマットのレポートを実行することも、スケジュールすることも、電子メールで送信することもできます。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操作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、『「Sentinel User Guide」』の「*Reporting*」を参照してください。

ID トラッキング

Sentinel は、ID 管理システムに、各ユーザアカウントの ID とそれらの ID が実行するイベントを追跡するのための統合フレームワークを提供します。また、連絡先情報、ユーザアカウント、最近の認証イベント、最近のアクセスイベント、パーミッション変更などのユーザ情報も提供します。特定のアクションを開始した人物やアクションの影響を受ける人物に関する情報を表示することで、Sentinel はインシデント対応時間を短縮し、振る舞いベースの分析を可能にします。詳細については、『「Sentinel User Guide」』の「*Leveraging Identity Information*」を参照してください。

イベント分析

Sentinel には、重大なイベントデータの検索と分析を簡単にする強力なツールのセットが用意されています。Sentinel は、あらゆるタイプの分析で効率が最大になるようにシステムを最適化し、あるタイプの分析から別のタイプの分析へのシームレスで簡単な移行方法を提供しています。

Sentinel でのイベントの調査は、ほぼリアルタイムのイベント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、イベントビューにはフィルタされたイベントストリームとサマリチャートが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手早い分析や、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合わせて調整したフィルタを構築できるようになります。イベントビューは、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、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アクティビティなど、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でも、Sentinel のレポーティング機能に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用意されているため、大量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し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、この移行が簡単になります。これにより、多数のイベントにより適したフォーマットで同じデータを表示するレポートをすぐに作成できます。

Sentinel には、これを目的としたレポーティングテンプレートが多数含まれています。レポーティングテンプレートには、2 つのタイプがあります。

- 特定のタイプの情報 (認証データやユーザ作成など) の表示に合わせて微調整されたテンプレート。
- レポート上のグループと列を対話的にカスタマイズできる汎用テンプレート。

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サポートされています。詳細については、『*Sentinel User Guide*』を参照してください。

Sentinel のインストール計画

次に示す各章では、Sentinel のインストール計画について順を追って説明しています。以降の章で特定されていない構成をインストールする場合や質問がある場合は、テクニカルサポートまでお問い合わせください。

注 : Sentinel サーバに使用されるホストとそのコンポーネントはすべて、ホスト名から IP、IP からホスト名の 2 つの方法での DNS 解決が可能な環境で設定する必要があります。

---

3 実装チェックリスト

Sentinel の計画、インストール、および環境設定を実行する場合は、次に示すチェックリストを使用してください。

以前のバージョンの Sentinel からアップグレードする場合は、このチェックリストを使用しないでください。アップグレードの詳細については、155 ページのパート V「Sentinel のアップグレード」を参照してください。

❒	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 のライセンス情報を確認して、Sentinel の評価ライセンスとエンタープライズライセンスの、どちらのライセンスを使用する必要があるかを判断します。	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。	37 ページの第 5 章「システム要件を満たす」。
❒	イベント数 / 秒 (EPS) に基づいて、環境に適した展開の種類を決定します。 パフォーマンスおよび負荷分散を向上させるためにインストールする必要がある、Collector Manager インスタンス、Correlation Engine インスタンスの数を決定します。	39 ページの第 6 章「展開に関する考慮事項」。
❒	最新の Sentinel リリースノートで、新機能と既知の問題を確認します。	Sentinel リリースノート
❒	Sentinel をインストールします。	67 ページのパート III「Sentinel のインストール」。
❒	Sentinel を設定します。	103 ページのパート IV「Sentinel の環境設定」。
❒	Sentinel には、すぐに使える相関ルールが付属しています。一部の相関ルールは、ルールの起動時に電子メールを送信するアクション (［Notify Security Admin］アクションなど) を実行するようデフォルトで設定されています。そのため、SMTP インテグレータと Send Email アクションを設定することで、Sentinel サーバのメールサーバ設定を構成する必要があります。	SMTP インテグレータと Send Email アクションの資料は、Sentinel プラグイン Web サイトにあります。

❒	タスク	参照先
❒	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。	99 ページの第 15 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、Collector Manager instances と Correlation Engine instances を追加インストールします。	67 ページのパート III「Sentinel のインストール」。

4 ライセンス情報について

Sentinel には、お客様の多様なニーズに応えるための多彩な機能が含まれています。目的に合ったライセンスモデルを選択してください。

Sentinel プラットフォームでは、次の 2 つのライセンスモデルを提供しています。

- **Sentinel Enterprise:** フル機能のソリューションで、すべての主要なリアルタイムのビジュアル分析機能と、他の多くの機能を使用できます。Sentinel Enterprise は、リアルタイムの脅威の検出、アラート、修正など、SIEM のユースケースに重点を置いています。
- **Sentinel for Log Management:** データの収集、保存、検索、およびレポートなど、ログ管理用のソリューションです。

  Sentinel for Log Management は、Sentinel Log Manager 1.2.2 の機能の大幅なアップグレードで、設計の大部分が変更されているものもあります。Sentinel for Log Management へのアップグレードを計画している場合は、Sentinel FAQ ページを参照してください。

購入されたソリューションとアドオンに応じて、Sentinel の正当な機能を使用できるようにする、適切なライセンスキーとエンタイトルメントを購入できます。ライセンスキーとエンタイトルメントにより、製品の機能とダウンロードへの基本的なアクセスが管理されますが、追加の条項については購入契約とエンドユーザ使用許諾契約を参照する必要があります。

次の表では、各ソリューションで使用できる具体的なサービスや機能について説明します。

表 4-1 Sentinel のサービスと機能

サービスと機能	Sentinel Enterprise	Sentinel for Log Management
主要な機能 ◆ イベントの収集、解析、正規化、および分類学的分類 ◆ イベント以外のデータ収集 (アセットデータ、脆弱性データ、およびユーザ識別情報データ) ◆ インライン文脈マッピング ◆ 保持ポリシーと否認防止を備えたイベントストレージ ◆ 従来のストレージ (内部および外部) へのイベントルーティング ◆ イベントの検索と視覚化 ◆ IP フローの収集、保存、および視覚化 ◆ レポーティング ◆ 連邦情報処理標準刊行物 140-2 (FIPS 140-2) イネーブルメント ◆ 手動でトリガされるアクション ◆ 手動によるインシデントの作成と管理	対応	対応
Sentinel Link	対応	対応
データ同期	対応	対応
アーカイブからのイベントデータの復元	対応	対応
データフェデレーション (分散検索)	対応	対応
相関 ◆ リアルタイムのイベントパターン相関 ◆ 相関ルールによってトリガされるアクション ◆ アラートの選別 ◆ アラートの視覚化	対応	非対応
セキュリティインテリジェンス ◆ アノマリールール ◆ リアルタイムの統計分析	対応	非対応

Sentinel ライセンス

このセクションでは、Sentinel のライセンスの種類に関する情報を提供します。

評価ライセンス

デフォルトの評価ライセンスでは、一定の評価期間中に Sentinel Enterprise のすべての機能を、ハードウェアの容量に応じて EPS 制限なしで使用できます。Sentinel Enterprise で使用できる機能については、34 ページの 表 4-1 「Sentinel のサービスと機能」を参照してください。

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に復元すると、Sentinel はそれに応じて有効期限を更新します。

評価ライセンスの期限が切れると、Sentinel は基本の、無償ライセンスで実行されます。このライセンスで使用できる機能は一部のみに制限され、イベント数も 25EPS に制限されます。これは、Sentinel が従来のストレージで設定されている場合にのみ適用されます。

エンタープライズライセンスにアップグレードすると、Sentinel にすべての機能が戻ります。機能の中断を防ぐには、評価ライセンスが切れる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。

無償ライセンス

無償ライセンスでは、一部の機能のみが使用でき、イベント数が 25EPS に制限されます。無償ライセンスは、従来のストレージの Sentinel にのみ適用されます。

無償ライセンスでは、イベントを収集したり保管したりできます。EPS 数が 25 を超えると、Sentinel は受信したイベントを保管しますが、それらのイベントの詳細は検索結果やレポートには表示されません。Sentinel は、これらのイベントに OverEPSLimit タグを付けます。

無償ライセンスには、リアルタイム機能はありません。ライセンスをエンタープライスライセンスにアップグレードすることで、すべての機能を戻すことができます。

注 : テクニカルサポートおよび製品アップデートは、無償版の Sentinel では利用できません。

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た機能、データ収集レート、およびイベントソースがライセンスキーで有効になります。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ことがあるため、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。

エンタープライズライセンスキーは、インストール時またはそれ以降いつでも追加できます。ライセンスキーを追加するには、『「Sentinel Administration Guide」』の「*Adding a License Key*」を参照してください。

5 システム要件を満たす

Sentinel の実装は IT 環境のニーズに応じて異なるため、目的の環境に適った Sentinel のアーキテクチャを最終決定する前に、コンサルティングサービスまたは Sentinel パートナーにお問い合わせください。

注

- Sentinel サーバに使用されるホストとそのコンポーネントはすべて、ホスト名から IP、IP からホスト名の 2 つの方法での DNS 解決が可能な環境で設定する必要があります。
- Sentinel をインストールする前に、使用している環境がセキュリティ保護されており、最新のセキュリティアップデートを使用して最新の状態になっていることを確認してください。

推奨されるハードウェア、サポートされるオペレーティングシステム、アプライアンスのプラットフォーム、およびブラウザについて詳しくは、Sentinel 技術情報の Web サイトを参照してください。

- 37 ページの 「コネクタおよびコレクタのシステム要件」
- 37 ページの 「仮想環境」

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 Web サイトで、コネクタとコレクタのマニュアルを参照してください。

仮想環境

Sentinel は、VMware ESX サーバでサポートされています。仮想環境を設定する場合、仮想マシンには複数の CPU が必要です。ESX 上の物理マシンや、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。

物理マシンの推奨事項については、Sentinel システム要件の確認を参照してください。

6 展開に関する考慮事項

Sentinel は、必要な負荷に応じて拡張する、スケーラブルなアーキテクチャを備えています。この章では、Sentinel 展開のスケーリング時に考慮すべき重要な事項について簡単に説明します。テクニカルサポートまたは Partner Services の専門家が、目的の IT 環境に適した Sentinel システムの設計を支援します。

データストレージの考慮事項

EPS レートに応じて、Sentinel データの保存とインデックス作成に、従来のストレージを使用するかを選択できます。

表 6-1 *従来のストレージ*

従来のストレージ
デフォルトでは、データはファイルベースの従来のストレージに保存されますが、インデックス作成は Sentinel サーバでローカルに実行されます。 ファイルベースのデータストレージに加えて、イベントの保存とインデックス作成を視覚化データストアで行ってデータ視覚化機能を利用する選択もできます。詳細については、42 ページの「視覚化データストアの設定」を参照してください。 約 20000 EPS までシームレスに拡張できます。それを超えてはるかに高い EPS までスケールアップするには、Sentinel サーバを追加する必要があります。 データ収集は複数の Sentinel サーバの間で負荷分散されます。したがって、データは複数の異なる Sentinel サーバに分散され、それぞれ個別に管理されます。 データはテナント別にラベルが付けられますが、ディスク上ではテナント別に分離されません。 データのレプリケーションや可用性は手動、または SAN ディスクなどの高価なストレージメカニズムを使用して処理されなければなりません。

従来のストレージのプラニング

ファイルベース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	プライマリストレージ (以前の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。最後に収集されたイベントデータと最も頻繁に検索されたイベントデータを保存します。
	セカンダリストレージ (以前のネットワークストレージ)。(オプション)	高速データ取得をサポートしながら、安価なストレージ上の領域使用量を削減するよう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、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存在するか、あるいは両方存在するかにかかわらず、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	アーカイバルストレージ	パーティションが閉じられているときには、そのパーティションを任意のファイルストレージサービス (Amazon Glacier など) にバックアップできます。そのパーティションは、長期的なフォレンジック分析に使用するために、いつでも一時的に再インポートできます。

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、『「Sentinel Administration Guide (NetIQ Sentinel 7.0.1 管理ガイド)」』の「*Configuring Data Synchronization (データ同期の設定)*」を参照してください。

Sentinel をインストールするときに、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) に、プライマリ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 ディレクトリの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る必要があります。そうしないと、自動データ管理機能がイベントデータを途中で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、43 ページの 「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配置されるようにしてください。可変データを別に保存することには、一連のファイルのバックアップが容易になり、破損した場合の回復が簡単になるというメリットがあるうえ、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向上します。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」を参照してください。

注 : ファイルストレージとしての ext3 ファイルシステムには制限があります。32000 を超えるファイルまたはサブディレクトリを、1 つのディレクトリで保持することはできません。多数の保持ポリシーを用意する予定がある場合や、データを長期間 (たとえば、1 年間) 保持する予定がある場合は、XFS ファイルシステムを使用できます。

- 41 ページの 「従来型インストールでのパーティションの使用」
- 41 ページの 「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」
- 42 ページの 「パーティションレイアウトのベストプラクティス」
- 42 ページの 「視覚化データストアの設定」

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は、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 43 ページの 「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。

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いる場合、YaST 画面の指示に従って、インストール中にアプライアンスのファイルシステムのパーティション化を設定できます。たとえば、/var/opt/novell/sentinel マウントポイント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、96 ページの 「従来のストレージのパーティションの作成」を参照してください。

パーティションレイアウトのベストプラクティス

多くの組織が、独自に、インストールしたシステムに関するベストプラクティスパーティションレイアウトスキームを文書化しています。以下のパーティション提案の目的は、定義済みのポリシーを持たない組織をガイドし、Sentinel 固有のファイルシステムの使い方を考慮することです。概して、Sentinel は可能な範囲でファイルシステム階層基準に準拠しています。

パーティション	マウントポイント	サイズ	備考
ルート	/	100GB	オペレーティングシステムファイルと Sentinel バイナリ / 環境設定が保存されます。
ブート	/boot	150MB	ブートパーティション
プライマリストレージ	/var/opt/novell/sentinel	System Sizing Information を使用して計算します。	この領域には、プライマリ Sentinel 収集データと、その他の可変データ (ログファイルなど) が保存されます。このパーティションは他のシステムと共有できます。
セカンダリストレージ	ストレージのタイプ (NFS、CIFS、または SAN) に基づく場所。	System Sizing Information を使用して計算します。	これはセカンダリストレージ領域で、前述のようにローカルにマウントすることも、リモートでマウントすることもできます。
アーカイバルストレージ	リモートシステム	System Sizing Information を使用して計算します。	このストレージはアーカイブしたデータ用です。

視覚化データストアの設定

Sentinel には、データをチャート、テーブル、およびマップで表すイベント視覚化機能が備わっています。これらの視覚化機能では、大量のイベントの分析を簡単に視覚化および分析できます。また、独自の視覚化とダッシュボードも作成できます。

Sentinel では、ブラウザベースの分析および検索ダッシュボードである Kibana を使用しており、イベントの検索と視覚化に役立ちます。Kibana は、ダッシュボードにイベントを表示するため、視覚化データストア (Elasticsearch) のデータにアクセスします。デフォルトで、Sentinel には、アラートのみを保存およびインデックス作成する Elasticsearch ノードが含まれています。Elasticsearch でイベントの保存とインデックス作成を行うには、イベント視覚化を有効にする必要があります。

Elasticsearch を有効にしてデータの保存とインデックス作成を行う場合、Sentinel は視覚化に必要な特定のイベントフィールドのみにインデックスを作成し、インデックスが付けられたフィールドを Elasticsearch に保存します。Sentinel では、それぞれの日付に対して専用のインデックスを作成し、インデックス日の計算に UTC タイムゾーン (午前 0 時から午前 0 時まで) を使用します。インデックス名の形式は security.events.normalized_yyyyMMdd です。たとえば、security.events.normalized_20160101 のインデックスには、2016 年 1 月 1 日のイベント時刻を持つすべてのイベントが含まれます。

視覚化データストアの設定には、以下の操作が含まれます。

- **クラスタモードでの Elasticsearch ノードのインストール :** デフォルトでは、Sentinel には Elasticsearch ノードが 1 つ含まれています。Sentinel サーバの最適なパフォーマンスと安定性のためには、追加の Elasticsearch ノードをクラスタモードでインストールすることが必須です。詳細については、73 ページの第 12 章「Elasticsearch のインストール」を参照してください。
- **イベント視覚化の有効化 :** デフォルトでは、イベント視覚化は無効です。イベント視覚化を有効にする方法については、「111 ページの第 18 章「イベント視覚化用の Elasticsearch の設定」」を参照してください。
- **パフォーマンスの調整 :** Sentinel では、最適なパフォーマンスのために特定の Elasticsearch 設定が自動的に設定されます。必要に応じて、これらの設定をカスタマイズできます。たとえば、Elasticsearch でインデックスを作成するイベントフィールドは変更できます。詳細については、74 ページの 「Elasticsearch のパフォーマンスチューニング」を参照してください。

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。
- 実行ファイルおよびライブラリは /opt/novell/sentinel ディレクトリに保存されています。.
- ログファイルは、/var/opt/novell/sentinel/log ディレクトリにあります。
- 一時ファイルは、/var/opt/novell/sentinel/tmp 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、/home/novell/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。

分散展開の利点

Sentinel サーバには、デフォルトで以下のコンポーネントが含まれます。

- **Collector Manager:** Collector Manager は、Sentinel に柔軟なデータ収集ポイントを提供します。

- **Correlation Engine:** Correlation Engine 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。
- **Elasticsearch:** データを保存およびインデックス作成するための、オプションのデータストレージコンポーネント。デフォルトでは、Sentinel には Elasticsearch ノードが 1 つ含まれています。EPS が大きくなること (2500 を超える) が予想される場合、追加の Elasticsearch ノードをクラスタに展開する必要があります。

重要 : 運用環境では、分散展開を設定して、データ収集コンポーネントを別のコンピュータに分離する必要があります。これは、システムの安定性を最大限に保ちながら、スパイクや他の異常を処理する上で重要になります。

このセクションでは、分散展開の利点について説明します。

- 44 ページの 「追加の Collector Manager instances の利点」
- 45 ページの 「Correlation Engine instances を追加することの利点」

追加の Collector Manager instances の利点

Sentinel サーバには、デフォルトで Collector Manager が含まれています。ただし運用環境では、Collector Manager instances を分散させることにより、大量のデータを受け取る場合に一層優れた分離を実現できます。こうした状態では、分散された Collector Manager のオーバーロードが生じる可能性があるものの、Sentinel サーバは途切れることなくユーザ要求に応じることができます。

分散ネットワークに複数の Collector Manager 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 :** Collector Manager instances 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 :** Collector Manager instances 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 Collector Manager instances 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。

追加の Collector Manager instances 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 Collector Manager instances 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 Collector Manager instances のインストールについては、67 ページのパート III「Sentinel 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 Collector Manager 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 Collector Manager 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。

Correlation Engine instances 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 Correlation Engine instances をそれぞれ独自のサーバに展開できます。相関ルールが多数ある環境やイベント発生率が極端に高い環境では、複数の Correlation Engine をインストールして、新しい Correlation Engine にルールを再展開するほうが効率的です。Correlation Engine instances を複数使用すると、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 Correlation Engine instances のインストールについては、67 ページのパート III「Sentinel のインストール」を参照してください。

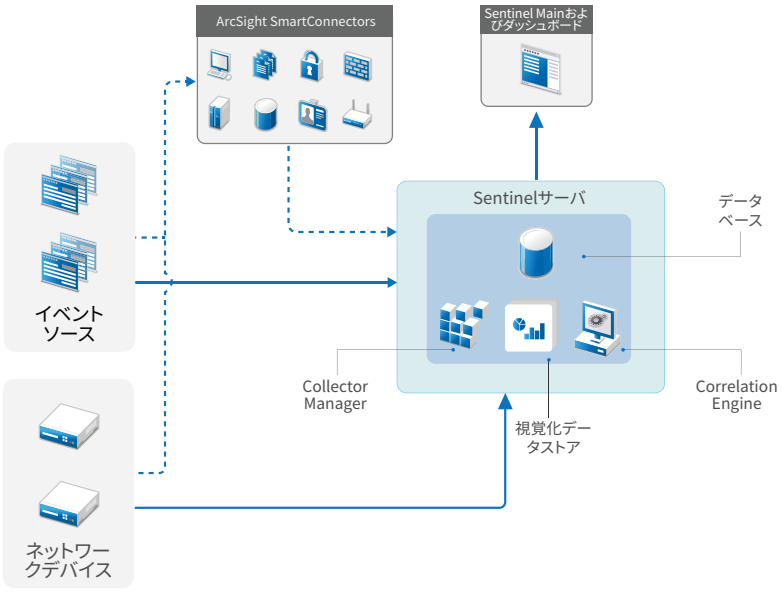
注 : 1 つのシステムに複数の Correlation Engine をインストールすることはできません。リモートシステムに追加の Correlation Engine instances をインストールして、それらを Sentinel サーバに接続することはできます。

オールインワン展開

最も基本的な展開オプションは、単一のコンピュータ上にすべての Sentinel コンポーネントをインストールするオールインワンシステムです。オールインワン展開は、システムの負荷が小さく、Windows マシンを監視する必要がない場合にのみ適しています。多くの環境では、予測が困難で流動的な負荷や、コンポーネント間のリソースの競合が原因で、パフォーマンスの問題が発生する可能性があります。

重要 : 運用環境では、分散展開を設定して、データ収集コンポーネントを別のコンピュータに分離する必要があります。これは、システムの安定性を最大限に保ちながら、スパイクや他の異常を処理する上で重要になります。

図 6-1 オールインワン展開

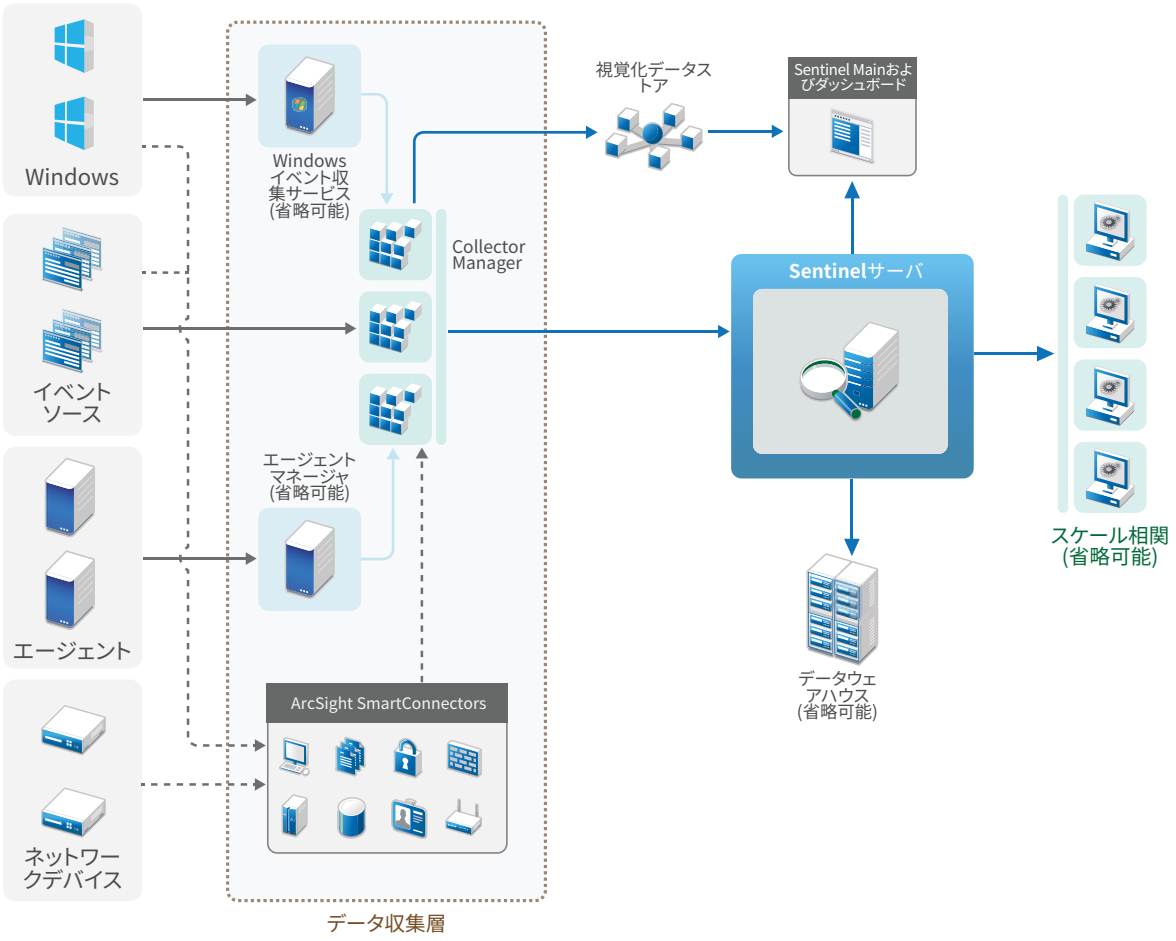


1 層分散展開

1 層展開は、Windows コンピュータを監視できるだけでなく、オールインワン展開よりも大きな負荷を処理できます。Collector Manager および Correlation Engine のコンピュータを追加して、中央 Sentinel サーバの処理をオフロードすることで、データの収集と相関をスケールアウトできます。また、イベントルールと相関ルールの負荷の処理に加えて、リモート Collector Manager インスタンスとリモート Correlation Engine インスタンスは、イベントの保存や検索などの他の要求に対処するために中央 Sentinel サーバ上のリソースを解放します。システムの負荷が増えるにつれ、中央 Sentinel サーバが最終的にボトルネックになってきたら、展開の階層を増やしてさらにスケールアウトする必要があります。

オプションで、イベントデータをデータウェアハウスにコピーするように Sentinel を構成できます。この方法は、カスタムレポーティング、分析、およびその他の処理を別のシステムにオフロードする場合に便利です。

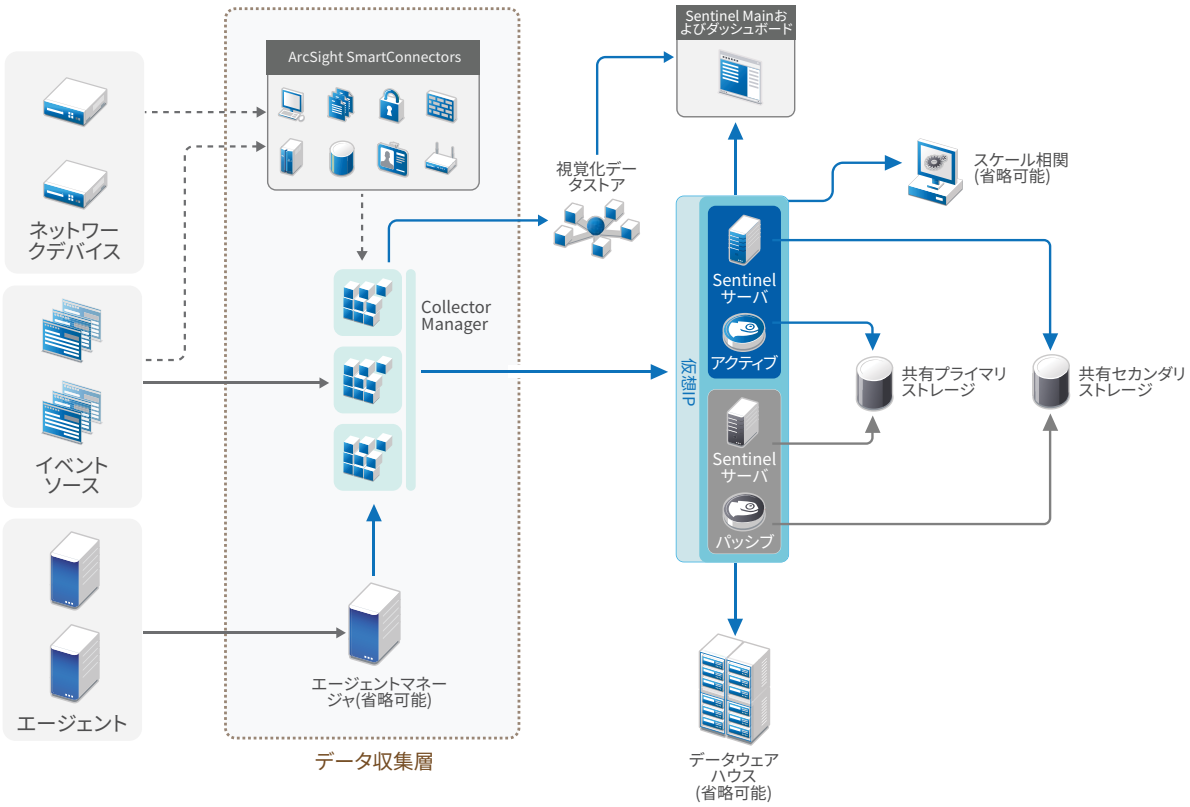
図 6-2 1 層分散展開



高可用性を備えた 1 層分散展開

この 1 層分散展開は、いかにフェールオーバー冗長性を備えた高可用性システムに変化できるかを示しています。高可用性での Sentinel の展開について詳しくは、207 ページのパート VII「高可用性のための Sentinel の展開」を参照してください。

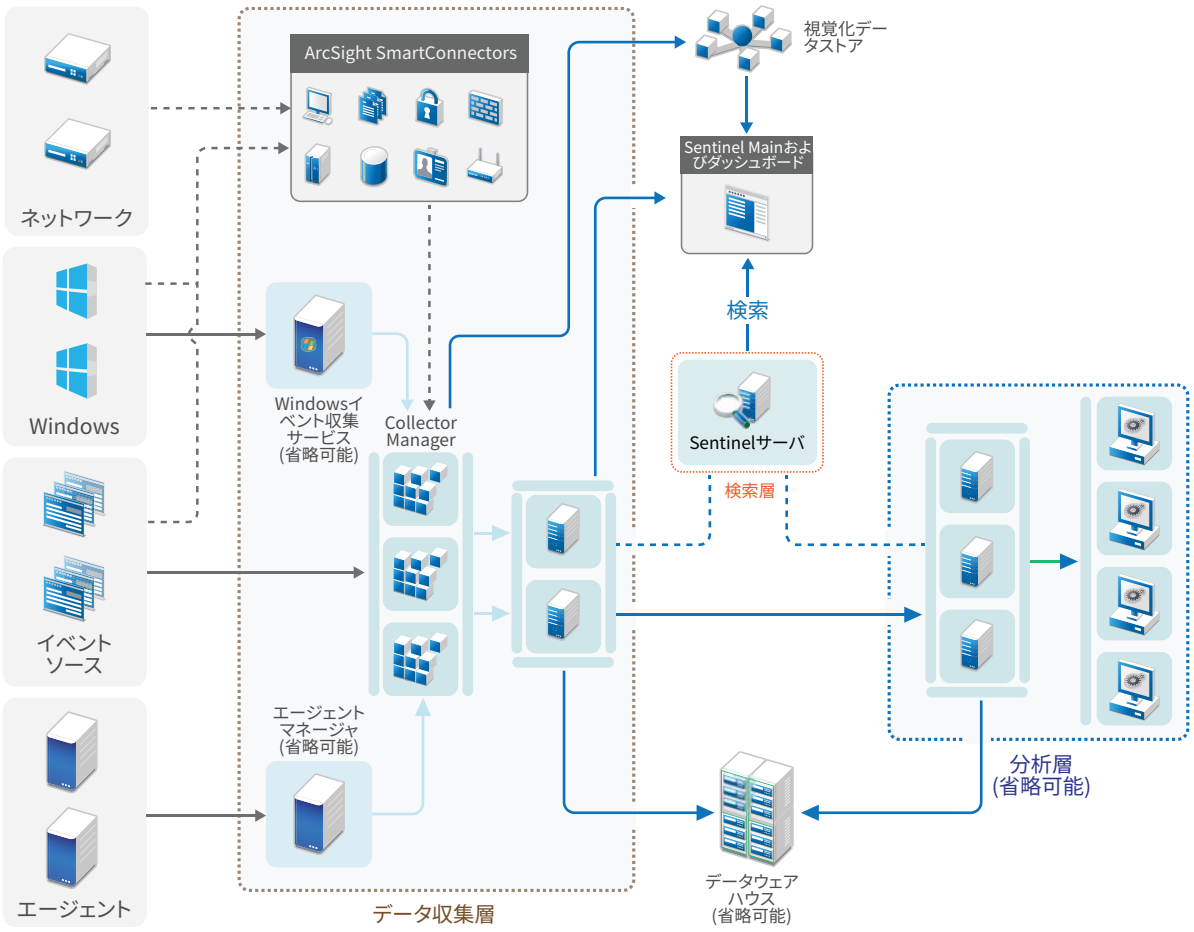
図6-3 高可用性を備えた 1 層分散展開



2 層および 3 層分散展開

この展開では、Sentinel リンク機能と Sentinel データフェデレーション機能を活用することで、単一の中央 Sentinel サーバの負荷処理能力を超えて、処理負荷を複数の Sentinel インスタンスで共有できるようになります。データ収集層で示したように、データ収集はそれぞれで複数の Collector Manager instances が動作する複数の Sentinel サーバによって負荷分散されています。イベント相関またはセキュリティインテリジェンスを実現したい場合は、オプションで、Sentinel Link を使ってデータを分析層に転送できます。検索層は Sentinel データフェデレーションを使用することで、すべての別階層にあるシステムをすべて検索できる、便利な単一アクセスポイントを提供します。検索要求が Sentinel の複数のインスタンスで共有されるため、この展開は検索負荷分散特性も備えています。この特性は、大規模な検索負荷を処理するためのスケーリングに役立ちます。

図6-4 2 層および3 層分散展開



7 FIPS140-2 モードでの展開に関する考慮事項

オプションとして、内部暗号化などの機能に 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インスタンス、Sentinel リモート相関エンジンインスタンス、Sentinel メインインタフェース、Sentinel コントロールセンターとの通信に、FIPS 140-2 認定暗号が使用されます。

重要 : FIPS モードは Sentinel でのみサポートされています。オペレーティングシステムが FIPS モードの場合、Sentinel はサポートされません。

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 6.3 以降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 に組み込まれている 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 モジュールの FIPS 140-2 認定を取得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 FIPS 140-2 証明書の詳細については、https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2711 および https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1837 を参照してください。

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-*
- nss-sysinit-*
- nss-util-*
- nss-softokn-freebl-*
- nss-softokn-*
- nss-*
- nss-tools-*

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。

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-*
- mozilla-nspr-*
- mozilla-nss-*
- mozilla-nss-tools-*

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。

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。
  - Agent Manager 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 の場合のみ)
  - 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
- チェックポイント (LEA) コネクタ 2011.1r2 以降
- Syslog インテグレータ 2011.1r1 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、136 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 で使用する方法の詳細については、143 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。

- 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)。
- 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。ただし、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、非暗号化接続は継続して使用できます。

- 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 サイトを参照してください。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。

FIPS モードの影響を受けるデータ接続

Sentinel が FIPS 140-2 モードの場合、Microsoft SQL Server に暗号化接続を行うことはできません。この点は、次のタイプの Sentinel 操作に影響します。

- SQL Server へのデータの同期ポリシー

- Agent Manager データベースと通信する Sentinel サーバ
- SQL Server のデータを収集するデータベースコネクタ

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。	54 ページの 「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。	78 ページの 「Sentinel サーバのカスタムインストール」。 83 ページの 「サイレントインストールの実行」 129 ページの第 22 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。	136 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」。
証明書を Sentinel FIPS キーストアにインポートする。	143 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」

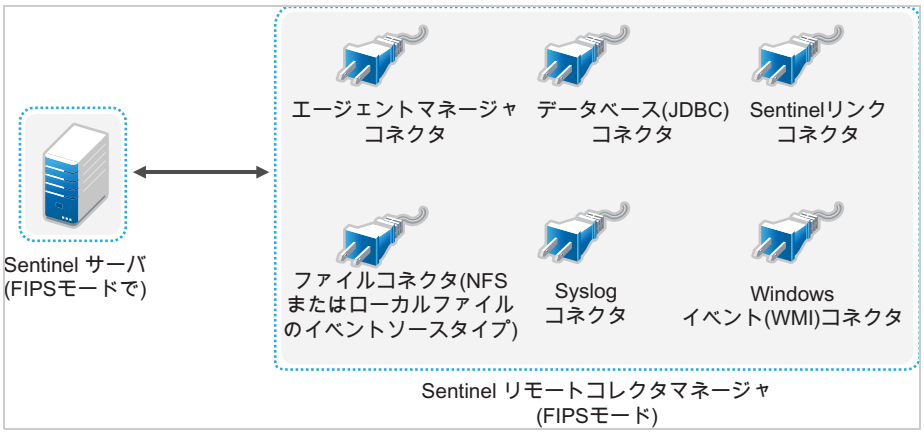
注 : FIPS モードへの変換を開始する前に、Sentinel システムをバックアップします。後でサーバを非 FIPS モードに戻す必要がある場合、サポートされている方法はバックアップからの復元のみになります。非 FIPS モードへ戻す方法について詳しくは、144 ページの「Sentinel を非 FIPS モードに戻す」を参照してください。

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。

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 Collector Manager 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 Collector Manager instances 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 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、129 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 リモート Collector Manager 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 Collector Manager が非 FIPS モードで実行中である場合は、リモート Collector Manager の FIPS を有効にする必要があります。詳細については、131 ページの 「リモート Collector Manager instances および Correlation Engine instances で FIPS 140-2 モードを有効にする」を参照してください。

---

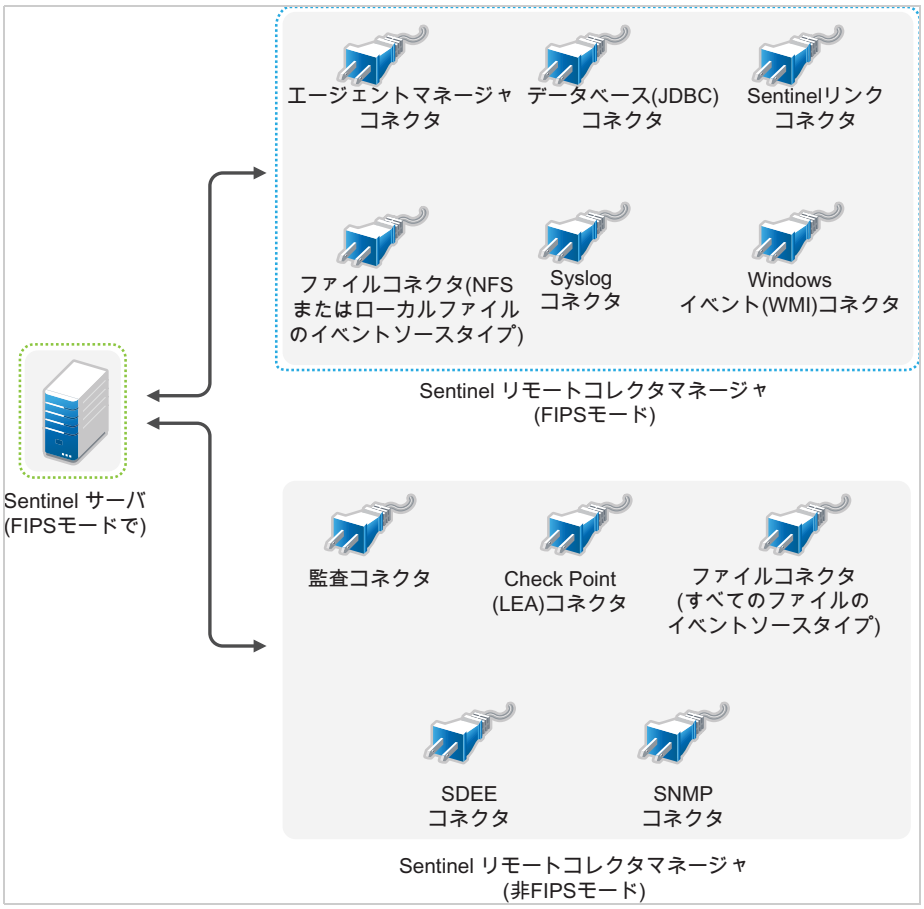
3 FIPS サーバとリモート Collector Manager instances が相互に通信していることを確認します。

4 リモート Correlation Engine instances がある場合は、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、131 ページの 「リモート Collector Manager instances および Correlation Engine instances 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 モードで実行するように設定します。詳細については、136 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。

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。ここでは、データはリモート Collector Manager によって収集されると仮定します。リモート Collector Manager instances 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必要があります。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 140-2 モードをサポートしないコネクタ用に非 FIPS (通常) モードで実行します。

FIPS 140-2 モードをサポートしているコネクタと、FIPS 140-2 モードを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を収集している環境では、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 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、129 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 Collector Manager は FIPS 140-2 モードで実行し、もう 1 つのリモート Collector Manager 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 Collector Manager がない場合は、リモート Collector Manager 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、131 ページの 「リモート Collector Manager instances および Correlation Engine instances 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 Collector Manager のサーバ証明書を更新します。詳細については、135 ページの「リモート Collector Manager instances および Correlation Engine instances 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 Collector Manager instances が FIPS 140-2 対応の Sentinel サーバと通信していることを確認します。

4 リモート Correlation Engine instances がある場合は、それらを FIPS 140-2 モードで実行するように設定します。詳細については、131 ページの 「リモート Collector Manager instances および Correlation Engine instances 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、136 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 Collector Manager 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 Collector Manager に展開します。

8 使用するポート

Sentinel は、さまざまなポートを使用して、他のコンポーネントとの外部通信を行います。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ます。

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。

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。
TCP 28017	セキュリティインテリジェンスデータベースの Web コンソールで使用されます。
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。
TCP 9200	REST を使用したアラートのインデックス作成サービスとの通信で使用されます。
TCP 9300	ネイティブプロトコルを使用したアラートのインデックス作成サービスとの通信で使用されます。

ネットワークポート

Sentinel が正常に動作するように、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	必須	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	Collector Manager instances および Correlation Engine instances からの着信接続に使用されます。
TCP 10013	INBOUND	必須	Sentinel Control Center および Solution Designer 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 Collector Manager instances 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 Collector Manager instances は SSL ポート 61616 を使用してサーバに接続します。
TCP 8443	OUTBOUND	オプション	データフェデレーションが使用されている場合は、分散検索を実行するために、このポートが別の Sentinel システムへの接続を開始します。
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	セカンダリストレージが 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	セカンダリストレージが CIFS を使用するように設定されている場合。

ポート	方向	必須 / オプション	説明
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、このポートから受信者にパケットが送信されます。
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。
TCP 7443	INBOUND	オプション	このポートで Sentinel システムは、Change Guardian および Secure Configuration Manager など他の SIEM ソフトウェアのイベントを受信できます。

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 4984	INBOUND	必須	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 接続用の 1289 に転送されます。
TCP 443	インバウンド	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。
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。

ポート	方向	必須 / オプション	説明
TCP 443 または 80	OUTBOUND	必須	インターネット上の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。
TCP 7630	INBOUND	必須	Hawk (High Availability Web Konsole) で使用されます。
TCP 9443	INBOUND	必須	Sentinel アプライアンス管理コンソールで使用されます。
TCP 1098 および 2000	INBOUND	必須	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 7443	INBOUND	必須	HTTP サーバコネクタによって使用されます。

Collector Manager のポート

Collector Manager 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。

ネットワークポート

SentinelCollector Manager 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	必須	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。

ポート	方向	必須 / オプション	説明
TCP 8443	OUTBOUND	必須	Sentinel Web サーバポートへの接続を開始します。 このポートを開いたままにしておくのは、Collector Manager のインストール中と設定中のみです。
TCP 7443	INBOUND	必須	HTTP サーバコネクタによって使用されます。

Collector Manager アプライアンス固有のポート

上記のポートに加えて、SentinelCollector Manager 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 4984	INBOUND	必須	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 接続用の 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	データ収集サーバ (syslog など) を設定するときに使用します。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。
TCP 9443	INBOUND	必須	Sentinel アプライアンス管理コンソールで使用されます。
TCP 1098 および 2000	INBOUND	必須	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 7443	INBOUND	必須	HTTP サーバコネクタによって使用されます。

Correlation Engine のポート

Correlation Engine 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。

ネットワークポート

Sentinel Correlation Engine が正常に動作するように、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	必須	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。
TCP 8443	OUTBOUND	必須	Sentinel Web サーバポートへの接続を開始します。 このポートを開いたままにしておくのは、Correlation Engine のインストール中と設定中のみです。

Correlation Engine アプライアンス固有のポート

Sentinel Correlation Engine 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。
TCP 4984	INBOUND	必須	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。
TCP 9443	INBOUND	必須	Sentinel アプライアンス管理コンソールで使用されます。
TCP 1098 および 2000	INBOUND	必須	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。

9 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。

従来型インストール

従来型インストールでは、アプリケーションインストーラを使用して、既存のオペレーティングシステムに Sentinel がインストールされます。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。
デフォルトの評価版キーを使用してインストールします。	デフォルトの評価版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、77 ページの 「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、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て展開する場合は、標準またはカスタムのインストール中に、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サイレント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、83 ページの 「サイレントインストールの実行」を参照してください。

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 オペレーティングシステムと 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。

- OVF アプライアンスイメージ
- ISO アプライアンスイメージ

アプライアンスインストールの詳細については、89 ページの第 14 章「アプライアンスインストール」を参照してください。

III 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。

10 インストールの概要

デフォルトで 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 サーバと Web サーバのプロセス :** 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。

  Sentinel Web サーバでは、Sentinel Main インタフェースへのセキュリティ保護された接続が可能です。
- **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、セキュリティインテリジェンス、アラートデータなどはそこに格納されます。
- **Elasticsearch:** 検索と視覚化のためにイベントとアラートのインデックスを作成します。データを保存およびインデックス作成するための、オプションのデータストレージコンポーネント。デフォルトでは、Sentinel には Elasticsearch ノードが 1 つ含まれています。EPS が大きくなること (2500 を超える) が予想される場合、追加の Elasticsearch ノードをクラスタに展開する必要があります
- **Collector Manager:** Collector Manager 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 Collector Manager をインストールします。
- **Correlation Engine:** Correlation Engine 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。
- **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 プラグイン 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
  - レポート
  - iTRAC ワークフロー
  - ソリューションパック

11 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、37 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、263 ページの付録 B「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、Customer Care Center からライセンスキーを取得してください。
- 59 ページの第 8 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 :**
  - 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 サーバのベースサーバコンポーネントが含まれている必要があります。したがって、Sentinel をインストールする前に、次のパッケージがインストールされていることを確認してください。
    - bc
    - bash
    - coreutils
    - gettext
    - glibc
    - grep
    - libgcc
    - libstdc

- lsof
- openssl
- sed
- insserv
- net-tools
- libX (RHEL 7.x の場合)
- zlib (SLES 12.x および RHEL 7.x、8.x まで)
- python-libs (SLES 12.x および RHEL 7.x まで)
- netstat (SLES 12.x および RHEL 7.x まで) または ss (SLES 15 以降の場合)
- pam-modules (Legacy-Module を SLES 15.x にインストールした場合にのみ使用できます)

❒ **従来のストレージを使用する Sentinel:**

イベント視覚化を表示するには、root ユーザとして、/etc/sysctl.conf ファイルでプロパティ vm.max_map_count=262144 を設定します。プロパティを追加した後、sysctl -p を実行して変更を有効にします。

12 Elasticsearch のインストール

イベントのインデックス作成をスケーラブルかつ分散型で行うには、Elasticsearch をクラスタモードでインストールする必要があります。Sentinel 用にインストールする Elasticsearch クラスタは、Sentinel データのインデックス作成にのみ使用しなければなりません。

前提条件

外部 Elasticsearch ノードをインストールする前に、次の前提条件を満たしてください。

- Sentinel 8.3 以前のバージョンで外部ノード Elasticsearch 5.6.13 をインストールした場合は、Elasticsearch をアンインストールしてから、Elasticsearch 7.7.0 をインストールします。インストールの詳細については、Elasticsearch のインストールを参照してください。
- 現在の EPS レートに基づき、「Sentinel システム要件」で推奨されている数のノードとレプリカを持つ Elasticsearch をクラスタモードで展開します。

Elasticsearch のインストール

Elasticsearch と必要なプラグインを Elasticsearch クラスタの各外部ノードにインストールする必要があります。

Elasticsearch をインストールし、設定するには次のようにします。

1. Elasticsearch でサポートされている JDK バージョンをインストールします。
2. Elasticsearch ユーザが Java にアクセスできることを確認します。
3. Elasticsearch RPM の認定バージョンをダウンロードします。Elasticsearch の認定バージョンの詳細とダウンロード URL については、『Sentinel システム要件』ページを参照してください。
4. Elasticsearch をインストールします。

   ```
   rpm -ivh elasticsearch-<version>.rpm
   ```

5. RPM のインストール後の手順として画面で説明されているタスクを完了します。
6. /etc/security/limits.conf ファイルに次のプロパティを追加して、ファイル記述子を設定します。

elasticsearch hard nofile 65536

elasticsearch soft nofile 65536

elasticsearch soft as unlimited

注 : 上記の前提条件を完了した後、sysctl -p コマンドを実行して、ファイルへの変更を再ロードしてください。

7 /etc/elasticsearch/jvm.options ファイルにある Elasticsearch ヒープのデフォルトサイズを更新します。

ヒープサイズは、サーバメモリの 50% である必要があります。たとえば、24GB の Elasticsearch ノードの場合、12GB をヒープサイズとして割り当てると、最適なパフォーマンスが得られます。

8 Elasticsearch を再起動します。

9 Elasticsearch クラスタの各外部 Elasticsearch ノードで上記の手順をすべて繰り返します。

Elasticsearch のパフォーマンスチューニング

Sentinel は、次の表で説明する Elasticsearch 設定を自動的に構成します。必要に応じて、Elasticsearch 設定をカスタマイズできます。

デフォルトの設定をカスタマイズする方法 :

従来のストレージの場合 : <sentinel_installation_path>/etc/opt/novell/sentinel/config/elasticsearch-index.properties ファイルを開き、表に記されているプロパティを必要に応じて更新します。

表 12-1 *Elasticsearch プロパティ*

プロパティ	デフォルト値	備考
elasticsearch.events.lucenefilter (オプション)		インデックスを作成するため特定のイベントのみを Elasticsearch に送信するためのフィルタを指定します。たとえば、sev:[3-5] という値を指定すると、重大度値が 3 から 5 のイベントだけが Elasticsearch に送信されます。

プロパティ	デフォルト値	備考
index.fields	id、dt、rv171、msg、ei、evt、xdastaxname、xdasoutcomename、sev、vul、rv32、rv39、rv159、dhn、dip、rv98、dp、fn、rv199、dun、tufname、rv84、rv158、shn、sip、rv76、sun、iufname、sp、iudep、rv198、rv62、st、tid、srcgeo、destgeo、obsgeo、rv145、estz、estzmonth、estzdiy、estzdim、estzdiw、estzhour、estzmin、rv24、tudep、pn、xdasclass、xdasid、xdasreg、xdasprov、iuident、tuident	Elasticsearch でインデックスを作成するイベントフィールドを示します。
es.num.shards	6	インデックスごとのプライマリシャード数を示します。 シャードサイズが 50GB を超える場合は、このデフォルト値を大きくできます。
es.num.replicas	1	各プライマリシャードに含める必要があるレプリカシャード数を示します。 フェールオーバーと高可用性を考慮し、少なくとも 2 ノードのクラスタをお勧めします。

13 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。

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。

Sentinel サーバの標準インストール

次の手順に従って、標準インストールを実行します。

1. ダウンロード Web サイトから Sentinel 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、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デフォルト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。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に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 Main 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 を指定します。

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

ここで、*IP_AddressOrDNS_Sentinel_server* は Sentinel サーバの IP アドレスまたは DNS 名、*8443* は Sentinel サーバのデフォルトポートです。

Sentinel サーバの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には、ライセンスキーを指定し、別のパスワードを指定し、別のポートを設定するなどして、Sentinel のインストールをカスタマイズする必要があります。

1 ダウンロード Web サイトから Sentinel 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、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 モードで有効にする場合は、***「y」を入力します。

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信頼を確立し、y を押して証明書ファイルのパスを指定し、外部証明書を求めるプロンプトが表示されたら、Elasticsearch http 証明書 <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks のパスを追加します。

15c 133 ページの第 23 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 Main 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 を指定します。

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

ここで、*<IP_AddressOrDNS_Sentinel_server>* は Sentinel サーバの IP アドレスまたは DNS 名、*8443* は Sentinel サーバのデフォルトポートです。

Collector Manager と Correlation Engine のインストール

デフォルトでは、Sentinel をインストールすると、Collector Manager と Correlation Engine も 1 つずつインストールされます。運用環境では、分散展開を設定して、データ収集コンポーネントを別のマシンに分離する必要があります。これは、システムの安定性を最大限に保ちながら、スパイクや他の異常を処理する上で重要になります。追加コンポーネントのインストールの利点については、43 ページの 「分散展開の利点」を参照してください。

複数の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することができます。

重要 : 追加の Collector Manager または Correlation Engine は別個のシステムにインストールする必要があります。Collector Manager または Correlation Engine を、Sentinel サーバがインストールされている同じシステムにインストールすることはできません。

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、記録されたファイルを使用して他のシステムへの無人インストールを行うことができます。次のファイルを指定して、インストールを記録できます。

- *<Response_file>*: インストール時に指定したインストールパラメータを記録します。
- *<Configuration_file>*: 複数の Sentinel サーバがある場合にのみ、このファイルを指定します。このファイルを使用して、レスポンスファイルに記録されているものとは別の Sentinel サーバに、コレクタマネージャおよび相関エンジンを接続することができます。インタラクティブインストールでは、Sentinel サーバの詳細用にプレースホルダーが作成されます。このファイルに関連する Sentinel サーバの詳細を後で更新し、無人インストール時にレスポンスファイルと一緒に使用することができます。

  注 : このオプションは、Sentinel 8.2 SP3 以降でのみ使用できます。

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、37 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。
- Collector Manager 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。Collector Manager 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。

コレクタマネージャと相関エンジンをインストールするには、次の手順を実行します。

1. Web ブラウザに次の URL を指定して、Sentinel Main インタフェースを起動します。

   `https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

   ここで、*<IP_AddressOrDNS_Sentinel_server>* は Sentinel サーバの IP アドレスまたは DNS 名、*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. 必要なインストールで［**[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. (条件による) インストールを記録しないでインストールするには、次のコマンドを指定します。
   - **Collector Manager の場合 :**

     `./install-cm`
   - **Correlation Engine の場合 :**

     `./install-ce`
8. (条件による) インストールを実行し記録するには、次のいずれかの操作を行います。
   - (条件による)Sentinel サーバが 1 つのみの場合は、次のコマンドを指定します。
     - **Collector Manager の場合 :**

       `./install-cm -r <response_filename>`
     - **Correlation Engine の場合 :**

       `./install-ce -r <response_filename>`
   - (条件による)Sentinel サーバが複数ある場合は、次のコマンドを指定します。
     - **コレクタマネージャの場合 :**

       `./install-cm -r <response_filename> -c <configuration_filename>`

- **相関エンジンの場合 :**

  ```
  ./install-ce -r <response_filename> -c <configuration_filename>
  ```

レスポンスファイルまたは環境設定ファイルの使用の詳細については、83 ページの「サイレントインストールの実行」を参照してください。

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 スペースキーを押して使用許諾契約を確認します。

11 「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。

12 プロンプトが表示されたら、適切なオプションを指定して、標準またはカスタムの環境設定を進めます。

13 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。

14 (条件による) カスタム環境設定を選択した場合は、次の項目を指定します。

14a Sentinel サーバ通信チャネルのポート番号。

14b Sentinel Web サーバのポート番号。

15 証明書の受諾を求めるプロンプトが表示されたら、Sentinel サーバで次のコマンドを実行して、証明書を検証します。

FIPS モードの場合 :

```
<sentinel_installation_path>/opt/novell/sentinel/jdk/jre/bin/keytool -
list -keystore
<Sentinel_installation_path>/etc/opt/novell/sentinel/config/
.activemqkeystore.jks
```

非 FIPS モードの場合 :

```
<sentinel_installation_path>/opt/novell/sentinel/jdk/jre/bin/keytool -
list -keystore
<sentinel_installation_path>/etc/opt/novell/sentinel/config/
nonfips_backup/.activemqkeystore.jks
```

証明書の出力をステップ 13 で表示された Sentinel サーバ証明書と比較します。

注 : 証明書が一致しない場合は、インストールが停止します。インストールのセットアップを再実行して、証明書を確認してください。

---

16 証明書の出力が Sentinel サーバ証明書と一致しているなら、その証明書を受諾します。

17 管理者の役割には、任意のユーザの資格情報を指定します。ユーザ名とパスワードを入力します。

18 (条件による) サーバで証明書取り消しリストが有効になっている場合、プロンプトが表示されたら［はい］を選択して、次の手順を実行します。

18a サーバの *<CONFIG_HOME>*/config/ からコレクタマネージャまたは相関エンジンの *<CONFIG_HOME>*/config/ に証明書をコピーします。*<CONFIG_HOME>* のデフォルト値は /etc/opt/novell/sentinel です。

18b プロンプトが表示されたら［はい］をクリックします。

18c クライアント証明書のパスワードを指定します。

19 (条件による) カスタム設定を選択した場合は、「yes」または「y」を入力して、Sentinel で FIPS 140-2 モードを有効にし、外部証明書を求めるプロンプトが表示されたら、Elasticsearch http 証明書 <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks のパスを追加します。

20 (条件による) ご使用の環境で多要素認証または強力な認証を使用している場合は、Sentinel クライアント ID と Sentinel クライアントシークレットを提供する必要があります。認証方法の詳細については、『「Sentinel Administration Guide」』の「*Authentication Methods*」を参照してください。

Sentinel クライアント ID と Sentinel クライアントシークレットを取得するには、次の URL に移動します。

https://*Hostname*:*port*/SentinelAuthServices/oauth/clients

各要素の内容は次のとおりです。

- *Hostname* は、Sentinel サーバのホスト名です。
- *Port* は、Sentinel が使用するポートです (通常は 8443)。

指定した URL では、Sentinel の現在のセッションを使用して、Sentinel クライアント ID と Sentinel クライアントシークレットを取得します。

21 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。

サイレントインストールの実行

複数の Sentinel サーバ、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。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他のシステムで実行することができます。

- インストールパラメータがファイルに記録されていることを確認します。レスポンスファイルの作成については、次の情報を参照してください。
  - 77 ページの 「Sentinel サーバの標準インストール」
  - 78 ページの 「Sentinel サーバのカスタムインストール」
  - 80 ページの 「Collector Manager と Correlation Engine のインストール」。

注 : コレクタマネージャおよび相関エンジンの場合は、環境設定ファイルを使用して、コレクタマネージャと相関エンジンをレスポンスファイルに記録されているものとは別の Sentinel サーバに接続します。このファイルに関連する Sentinel サーバの詳細を更新し、無人インストール時にレスポンスファイルとともに使用します。

FIPS 140-2 モードを有効にする場合は、次のパラメータがレスポンスファイルに含まれていることを確認します。

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

サイレントインストールを実行するには :

1. ダウンロード Web サイトからインストールファイルをダウンロードします。
2. Sentinel、Collector Manager または Correlation Engine をインストールするサーバに、root としてログインします。
3. 次のコマンドを指定して、tar ファイルからインストールファイルを抽出します。

   ```
   tar -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. (条件による)Sentinel サーバをサイレントモードでインストールするには、次のコマンドを指定します。

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

   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。

   Sentinel サーバをインストールした場合は、インストール後にすべてのサービスが開始されるまでに数分かかることがあります。これは、システムが 1 回限りの初期化を実行するためです。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。
5. (条件による) コレクタマネージャをインストールするには、次のコマンドを指定します。
   - レスポンスファイルを使用するには :

     ```
     ./install-cm -u <response_filename>
     ```
   - レスポンスファイルと環境設定ファイルを使用するには :

     ```
     ./install-cm -u <response_filename> -i <configuration_filename>
     ```
6. (条件による) 相関エンジンをインストールするには、次のコマンドを指定します。
   - レスポンスファイルを使用するには :

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

- レスポンスファイルと環境設定ファイルを使用するには :

  ```
  ./install-ce -u <response_filename> -i <configuration_filename>
  ```

7 (条件による)133 ページの第 23 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。外部証明書を求めるプロンプトが表示されたら、Elasticsearch http 証明書のパス <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks を追加します。

非 root ユーザとして Sentinel をインストール

組織の方針として、root として Sentinel を完全インストールすることを許可されていない場合は、Sentinel を非 root ユーザ、つまり novell ユーザとしてインストールすることができます。この方法でインストールする場合、root ユーザとしていくつかのステップを実行した後、root ユーザによって作成された novell ユーザとして Sentinel をインストールします。最後に、root ユーザとしてインストールを完了します。

非 root ユーザとして Sentinel をインストールする場合は、novell ユーザとして Sentinel をインストールする必要があります。novell ユーザ以外の非 root インストールはサポートされていませんが、インストールは正常に行われます。

1 ダウンロード Web サイト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 (条件による) デフォルト以外のディレクトリの場所が 85 ページのステップ 4 以前に存在する場合は、novell ユーザがディレクトリに対する所有権を持っている必要があります。次のコマンドを実行して、所有権を割り当てます。

  ```
  chown novell:novell <non-default installation directory>
  ```

7 次のコマンドを指定して、新しく作成された非 root ユーザ (つまり novell) に変更します。

su novell

8 (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 :

8a インストールしているコンポーネントに応じて適切なコマンドを指定します。

コンポーネント	コマンド
Sentinel サーバ	**デフォルトの場所 :** ./install-sentinel
	デフォルト以外の場所 : ./install-sentinel --location=/foo
Collector Manager	**デフォルトの場所 :** ./install-cm
	デフォルト以外の場所 : ./install-cm --location=/foo
Correlation Engine	**デフォルトの場所 :** ./install-ce
	デフォルト以外の場所 : ./install-cm --location=/foo

8b ステップ 11 に進みます。

9 (条件による)Sentinel サーバの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、77 ページの 「Sentinel サーバの標準インストール」または 78 ページの 「Sentinel サーバのカスタムインストール」を参照してください。

9a インストールするには、次のコマンドを指定します。

デフォルトの場所 : ./install-sentinel -u <*response_file*name>

デフォルト以外の場所 : ./install-sentinel --location=/foo -u <*response_filename*>

9b ステップ 14 に進みます。

10 (条件による) コレクタマネージャまたは相関エンジンのサイレントインストールを実行するには、インストールパラメータがファイルに記録されていることを確認してください。

注 : 環境設定ファイルを使用して、レスポンスファイルに記録されているものとは別の Sentinel サーバにコレクタマネージャおよび相関エンジンを接続します。このファイルに関連する Sentinel サーバの詳細を更新し、無人インストール時にレスポンスファイルとともに使用します。

レスポンスファイルまたは環境設定ファイル作成の詳細については、80 ページの「Collector Manager と Correlation Engine のインストール」を参照してください。

10a インストールしているコンポーネントに応じて適切なコマンドを指定します。

コンポーネント	コマンド
コレクタマネージャ	◆ レスポンスファイルを使用するには : ◆ **デフォルトの場所 :** ./install-cm -u <*response_file*name> ◆ **デフォルト以外の場所 :** ./install-cm --location=/foo -u <*response_file*name> ◆ レスポンスファイルと環境設定ファイルを使用するには : ◆ **デフォルトの場所 :** 。/install-cm -u <*response_file*name> -i <*configuration_filename*> ◆ **デフォルト以外の場所 :** 。/install-cm --location=/foo -u <*response_file*name> -i <*configuration_file*name> インストールは、環境設定ファイルからの Sentinel サーバの値およびレスポンスファイルに格納されているその他のインストールパラメータ値に従って進行します。
相関エンジン	◆ レスポンスファイルを使用するには : ◆ **デフォルトの場所 :** ./install-ce -u <*response_file*name> ◆ **デフォルト以外の場所 :** ./install-ce --location=/foo -u <*response_file*name> ◆ レスポンスファイルと環境設定ファイルを使用するには : ◆ **デフォルトの場所 :** 。/install-ce -u <*response_file*name> -i <*configuration_filename*> ◆ デフォルト以外の場所 : ./install-ce --location=/foo -u <*response_file*name> -i <*configuration_file*name> インストールは、環境設定ファイルからの Sentinel サーバの値およびレスポンスファイルに格納されているその他のインストールパラメータ値に従って進行します。

10b ステップ 14 に進みます。

11 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。

12 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。

13 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、77 ページの 「Sentinel サーバの標準インストール」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、78 ページの 「Sentinel サーバの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。

14 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 Main 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 を指定します。

`https://`*`IP_AddressOrDNS_Sentinel_server`*`:`*`8443`*`/sentinel/views/main.html`

ここで、*IP_AddressOrDNS_Sentinel_server* は Sentinel サーバの IP アドレスまたは DNS 名、*8443* は Sentinel サーバのデフォルトポートです。

14 アプライアンスインストール

Sentinel アプライアンスは、Micro Focus 共通アプライアンスフレームワークに基づく、いつでも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 SLES オペレーティングシステムと Sentinel ソフトウェア統合アップデートサービスを組み合わせて、既存の投資を活用できるように、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。Sentinel アプライアンスには、アプライアンスの構成と監視を行うための Web ベースのユーザインタフェースが備わっています。

Sentinel のバージョンに応じて、アプライアンスインストーラは認定された SLES オペレーティングシステムをインストールします。

- 8.2 では、アプライアンスインストーラにより SLES 12 SP3 がインストールされます。
- 8.2 SP2 では、アプライアンスインストーラにより SLES 12 SP4 がインストールされます。
- 8.3 SP1 では、アプライアンスインストーラにより SLES 12 SP5 がインストールされます。

Sentinel のアプライアンスイメージが、ISO 形式と仮想環境にデプロイできる OVF 形式の両方でパッケージされています。サポートされている仮想化プラットフォームの詳細については、Sentinel のシステム要件を参照してください。

- 89 ページの 「前提条件」
- 90 ページの 「Sentinel ISO アプライアンスのインストール」
- 92 ページの 「Sentinel OVF アプライアンスのインストール」
- 95 ページの 「アプライアンスのインストール後の環境設定」

前提条件

Sentinel を ISO アプライアンスとしてインストールする環境が、以下の前提条件を満たしていることを確認します。

- Sentinel アプライアンスをインストールする前に、認定済みの SLES リリースノートで新しい機能と既知の問題を確認してください。
- (条件付き) Sentinel ISO アプライアンスをベアメタルハードウェアにインストールする場合、アプライアンス ISO のディスクイメージをサポートサイトからダウンロードし、DVD を作成します。
- インストーラが自動パーティション提案を作成するのに必要な 50GB 以上のハードディスク容量が存在することを確認します。
- インストールを完了するには、システムに 4GB 以上のメモリがあることを確認します。メモリが 4GB 未満の場合、インストールは失敗します。メモリが 4GB を超えているものの推奨サイズが 24GB 未満の場合、推奨よりもメモリ容量が少ないというメッセージがインストール時に表示されます。

Sentinel ISO アプライアンスのインストール

このセクションでは、ISO アプライアンスイメージを使用して Sentinel、Collector Manager instances、および Correlation Engine instances をインストールする方法について説明します。このイメージ形式では、ブート可能な ISO DVD イメージを使って物理 (ベアメタル) または仮想 (ハイパーバイザでアンインストールされた仮想マシン) のハードウェアに直接デプロイできる、完全なディスクイメージ形式を生成できます。

- 90 ページの 「Sentinel のインストール」
- 91 ページの 「Collector Manager instances と Correlation Engine instances のインストール」

Sentinel のインストール

Sentinel ISO アプライアンスをインストールするには、次のようにします。

1 ISO 仮想アプライアンスイメージをダウンロード Web サイトからダウンロードします。

2 (条件付き) ハイパーバイザを使用している場合は、次のようにします。

ISO 仮想アプライアンスイメージを使用する仮想マシンを設定し、起動します。

または

ISO イメージを DVD に書き込み、DVD を使用して仮想マシンを設定し、起動します。

3 (条件付き)Sentinel アプライアンスをベアメタルハードウェアにインストールする場合は、次のようにします。

3a 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。

3b インストールウィザードの画面上の指示に従います。

3c [**[sentinel サーバ < *バージョン* > *のインストール*]**] を選択します。

4 必要な言語を選択します。

5 キーボードレイアウトを選択します。

6 [**[次へ]**] をクリックします。

7 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。[**[次へ]**] をクリックします。

8 Sentinel サーバアプライアンスライセンス契約書を確認して同意します。[**[次へ]**] をクリックします。

9 Sentinel アプライアンスのパスワード、NTP 設定、およびタイムゾーンを設定します。

Sentinel アプライアンス管理コンソールにログインするための vaadmin ユーザ資格情報を設定します。

注 : インストール後、次のように NTP 設定とタイムゾーンを変更できます。

- コマンドプロンプトに移動し、yast->Network Services->NTP Configuration と入力します
- Sentinel アプライアンス管理コンソールに移動し、[**[時間]**] をクリックします。

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
```

10 Sentinel サーバアプライアンスのネットワーク設定のページで、ホスト名とドメイン名を指定します。[**[スタティック IP アドレス]**] または [**[DHCP IP アドレス]**] を選択します。

11 [**[次へ]**] をクリックします。

12 (状況によって実行) ステップ 10 で [**[スタティック IP アドレス]**] を選択した場合は、ネットワーク接続設定を指定します。

13 [**[次へ]**] をクリックします。

14 Sentinel ユーザ admin のパスワードを設定し、[**[次へ]**] をクリックします。

アプライアンスがインストールされます。

15 コンソールに表示されたアプライアンスの IP アドレスをメモします。

16 アプライアンスにログインするため、コンソールに root ユーザとしてログインします。

ユーザ名として root と入力し、ステップ 9 で設定したパスワードを入力します。

17 95 ページの 「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。

Collector Manager instances と Correlation Engine instances のインストール

Collector Manager や Correlation Engine のインストール手順も Sentinel のインストール手順と似ていますが、ダウンロード Web サイトから該当する ISO アプライアンスファイルをダウンロードする必要があります。

1 90 ページの 「Sentinel のインストール」の手順 1 から 13 を実行します。

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 1GB 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。

2 Collector Manager または Correlation Engine のために、次の環境設定を指定します。

- **Sentinel サーバのホスト名または IP アドレス :** Collector Manager または Correlation Engine 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。
- **Sentinel 通信チャネルポート :** Sentinel サーバ通信チャネルポートの番号を指定します。デフォルトのポート番号は 61616 です。
- **Sentinel Web サーバポート :** Sentinel Web サーバポートを指定します。デフォルトポートは 8443 です。
- **管理者の役割を持つユーザ名 :** 管理者の役割の任意のユーザ名を指定します。
- **管理者の役割を持つユーザのパスワード :** 上記のフィールドで指定したユーザ名に対するパスワードを指定します。

3 (条件による) ご使用の環境で多要素認証または強力な認証を使用している場合は、Sentinel クライアント ID と Sentinel クライアントシークレットを提供する必要があります。認証方法の詳細については、『「Sentinel Administration Guide」』の「*Authentication Methods*」を参照してください。

Sentinel クライアント ID と Sentinel クライアントシークレットを取得するには、次の URL に移動します。

https://*Hostname*:*port*/SentinelAuthServices/oauth/clients

各要素の内容は次のとおりです。

- *Hostname* は、Sentinel サーバのホスト名です。
- *Port* は、Sentinel が使用するポートです (通常は 8443)。

指定した URL では、Sentinel の現在のセッションを使用して、Sentinel クライアント ID と Sentinel クライアントシークレットを取得します。

4 [［次へ］] をクリックします。

5 同意を求められたら、証明書に同意します。

6 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。

何をインストールしたかに応じて、このアプライアンスが SentinelCollector Manager または Correlation Engine であることを示すメッセージとその IP アドレスがコンソールに表示されます。コンソールには、Sentinel サーバのユーザインタフェース IP アドレスも表示されます。

7 90 ページの 「Sentinel のインストール」のステップ 16 からステップ 17 を実行します。

Sentinel OVF アプライアンスのインストール

このセクションでは、Sentinel、Collector Manager、および Correlation Engine を、OVF アプライアンスイメージとしてインストールする場合について説明します。

OVF フォーマットは、ほとんどのハイパーバイザで、直接または単純変換によってサポートされている標準の仮想マシンフォーマットです。Sentinel は、OVF アプライアンスを 2 つの認定ハイパーバイザでサポートしていますが、それ以外のハイパーバイザでも使用できます。

- 92 ページの 「Sentinel のインストール」
- 94 ページの「Collector Manager instances と Correlation Engine instances のインストール」

Sentinel のインストール

Sentinel OVF アプライアンスをインストールするには、次のようにします。

1 OVF 仮想アプライアンスイメージをダウンロード Web サイトからダウンロードします。

2 ハイパーバイザの管理コンソールで、OVF イメージファイルを新規仮想マシンとしてインポートします。OVF イメージをネイティブフォーマットに変換するように要求された場合に、ハイパーバイザが変換できるようにします。

3 新規仮想マシンに割り当てられた仮想ハードウェアリソースが、Sentinel の要件を満たしているか確認します。

4 仮想マシンの電源をオンにします。

5 必要な言語を選択します。

6 キーボードレイアウトを選択します。

7 [**[次へ]**] をクリックします。

8 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。[**[次へ]**] をクリックします。.

9 Sentinel サーバアプライアンスライセンス契約書を確認して同意します。[**[次へ]**] をクリックします。.

10 Sentinel アプライアンスのパスワード、NTP 設定、タイムゾーンを設定します。

Sentinel アプライアンス管理コンソールにログインするための vaadmin ユーザ資格情報を設定します。

注 : インストール後、次のように NTP 設定とタイムゾーンを変更できます。

- コマンドプロンプトに移動し、yast->Network Services->NTP Configuration と入力します
- Sentinel アプライアンス管理コンソールに移動し、[**[時間]**] をクリックします。

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
```

---

11 Sentinel サーバアプライアンスのネットワーク設定のページで、ホスト名とドメイン名を指定します。[**[スタティック IP アドレス]**] または [**[DHCP IP アドレス]**] を選択します。

12 [**[次へ]**] をクリックします。

13 (状況によって実行) ステップ 11 で [**[スタティック IP アドレス]**] を選択した場合は、ネットワーク接続設定を指定します。

14 [**[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、[**[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。

16 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。Sentinel Main インタフェースにアクセスする IP アドレスと同じものを使用します。

Collector Manager instances と Correlation Engine instances のインストール

Collector Manager または Correlation Engine を VMware ESX サーバに OVF アプライアンスイメージとしてインストールするには :

1. 92 ページの 「Sentinel のインストール」の手順 1 から 14 を実行します。

   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 1GB 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。
2. Collector Manager 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。デフォルトポートは 61616 です。
4. 管理者の役割には、任意のユーザの資格情報を指定します。ユーザ名とパスワードを入力します。
5. (条件による) ご使用の環境で多要素認証または強力な認証を使用している場合は、Sentinel クライアント ID と Sentinel クライアントシークレットを提供する必要があります。認証方法の詳細については、『「Sentinel Administration Guide」』の「*Authentication Methods*」を参照してください。

   Sentinel クライアント ID と Sentinel クライアントシークレットを取得するには、次の URL に移動します。

   https://*Hostname*:*port*/SentinelAuthServices/oauth/clients

   各要素の内容は次のとおりです。

   - *Hostname* は、Sentinel サーバのホスト名です。
   - *Port* は、Sentinel が使用するポートです (通常は 8443)。

   指定した URL では、Sentinel の現在のセッションを使用して、Sentinel クライアント ID と Sentinel クライアントシークレットを取得します。
6. [次へ] をクリックします。
7. 証明書を受け入れます。
8. [[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 SentinelCollector Manager または Sentinel Correlation Engine 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。

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。

- 95 ページの 「アップデートの登録」
- 96 ページの 「従来のストレージのパーティションの作成」
- 97 ページの 「SMT でのアプライアンスの設定」

アップデートの登録

Sentinel と最新のオペレーティングシステムの更新を受信するには、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カスタマーケアセンターから取得する必要があります。

インストールされているオペレーティングシステムに基づいて、次の方法でアップデートの登録を行うことができます。

- SLES 12 SP3 以降を使用している場合は、Sentinel アプライアンス管理コンソールを使用して登録できます。
- SLES 12 SP3 以降を使用している場合は、コマンドを使用して登録できます。

- 95 ページの 「Sentinel アプライアンス管理コンソールによる登録」
- 95 ページの 「コマンドによる登録」

Sentinel アプライアンス管理コンソールによる登録

Sentinel アプライアンス管理コンソールを使用して登録するには :

1. 次のいずれかの方法で、Sentinel アプライアンスを起動します。
   - Sentinel にログインします。[**[Sentinel メイン]**] > [**[アプライアンス]**] の順にクリックします。
   - Web ブラウザで次の URL を指定します : https://<IP_address>:9443。
2. vaadmin ユーザと root ユーザのいずれかでログインします。
3. [**[オンライン更新]**] > [**[今すぐ登録]**] をクリックします。
4. [**[電子メール]**] フィールドには、更新を受信する電子メール ID を指定します。
5. [**[アクティベーションキー]**] フィールドに登録コードを入力します。
6. [**[登録]**] をクリックして、登録を完了します。

コマンドによる登録

コマンドを使用して登録するには :

1. Sentinel サーバに root ユーザでログインします。

2 次のコマンドを指定します。

- サーバを登録する場合、次のように指定します : suse_register -a regcode-sentinel="<*registration_code*>" -a email="<*email_ID*>"
- Collector Manager を登録する場合、次のように指定します : suse_register -a regcode-sentinel-collector="<*registration_code*>" -a email="<*email_ID*>"
- Correlation Engine を登録する場合、次のように指定します : suse_register -a regcode-sentinel-correlation ="<*registration_code*>" -a email="<*email_ID*>"
- Sentinel を高可用性で登録する場合、次のように指定します : suse_register -a regcode-sentinel-ha ="<*registration_code*>" -a email="<*email_ID*>"

email パラメータには、更新を受信する電子メール ID を指定します。

従来のストレージのパーティションの作成

このセクションの情報は、データストレージオプションとして従来のストレージを使用する場合にのみ適用されます。

ベストプラクティスとして、別個のパーティションを作成して、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パーティションに Sentinel データを保存できるようにしてください。可変データを別に保存することには、一連のファイルのバックアップが容易になり、破損した場合の回復が簡単になるというメリットがあるうえ、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向上します。パーティションの計画については、40 ページの 「従来のストレージのプラニング」を参照してください。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 Control Center 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。

パーティションの作成について詳しくは、*SLES 11 のマニュアル*にある「Using the YaST Partitioner」を参照してください。

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
```

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、Customer Center に統合されたパッケージ代理システムで、主な Customer Center 機能を提供します。

前提条件

SMT でアプライアンスを設定する前に、次の前提条件を満たしていることを確認します。

- Sentinel の更新を取得するためにカスタマーセンターの資格情報を取得します。資格情報の入手方法の詳細については、テクニカルサポートにお問い合わせください。
- SMTをインストールするコンピュータに次のパッケージと共にSLES 11 SP3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

次の手順を実行して SMT でアプライアンスを設定します。

1 SMT サーバで次のコマンドを実行して、アプライアンスのリポジトリを有効にします。

```
smt-repos -e Sentinel-Server-8-OS-Updates sle-12-x86_64
smt-repos -e Sentinel-Server-8-Prod-Updates sle-12-x86_64
smt-repos -e Sentinel-Collector-Manager-8-OS-Updates sle-12-x86_64
smt-repos -e Sentinel-Collector-Manager-8-Prod-Updates sle-12-x86_64
smt-repos -e Sentinel-Correlation-Engine-8-OS-Updates sle-12-x86_64
smt-repos -e Sentinel-Correlation-Engine-8-Prod-Updates sle-12-x86_64
```

2 「SMT のマニュアル」の「Configuring Clients to Use SMT」セクションで説明されている手順を実行して、SMT でアプライアンスを設定します。

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、171 ページの 「Sentinel アプライアンスのアップグレード」を参照してください。

15 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。

- 99 ページの 「コレクタのインストール」
- 99 ページの 「コネクタのインストール」

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 Web サイトから、希望するコレクタをダウンロードします。
2. [Sentinel Main] から［ [admin]］ドロップダウンをクリックし、［ [アプリケーション]］をクリックします。
3. ［ [Control Center の起動]］をクリックして Sentinel Control Center を起動します。
4. 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。
5. 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。
6. 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。

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. [Sentinel Main] から［ [admin]］ドロップダウンをクリックし、［ [アプリケーション]］をクリックします。
3. ［ [Control Center の起動]］をクリックして Sentinel Control Center を起動します。
4. 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。

5 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。

6 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。

16 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 サービスが実行中かどうか、FIPS モードと非 FIPS モードのどちらで動作しているかを確認する :

  ```
  /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>
  ```

  注 : SLES15 以降では、次のコマンドを使用します。

  ```
  ss -tln |grep 'LISTEN' |grep <HTTPS_port_number>
  ```

  デフォルトのポート番号は 8443 です。

- Sentinel を起動します。

  1. サポートされている Web ブラウザを起動します。
  2. Sentinel の URL を指定します。

     ```
     https://IP_AddressOrDNS_Sentinel_server:8443
     ```

     ここで、*IP_AddressOrDNS_Sentinel_server* は Sentinel サーバの IP アドレスまたは DNS 名、*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。

  注 : Sentinel のメイン UI に着地するには、次の手順を実行します。

  1. <sentinel_installation_folder>/etc/opt/novell/sentinel/config/ ディレクトリに移動します。
  2. Configuration.properties ファイルの値を true に変更して、sentinel.sentinel.redirection を有効にします。
  3. Sentinel を再起動します : rcsentinel restart。
  4. URL を使用して、Sentinel にログインします。

     ```
     https://IP_AddressOrDNS_Sentinel_server:<port>/sentinel/
     ```

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。

17 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。

Sentinel における時刻について

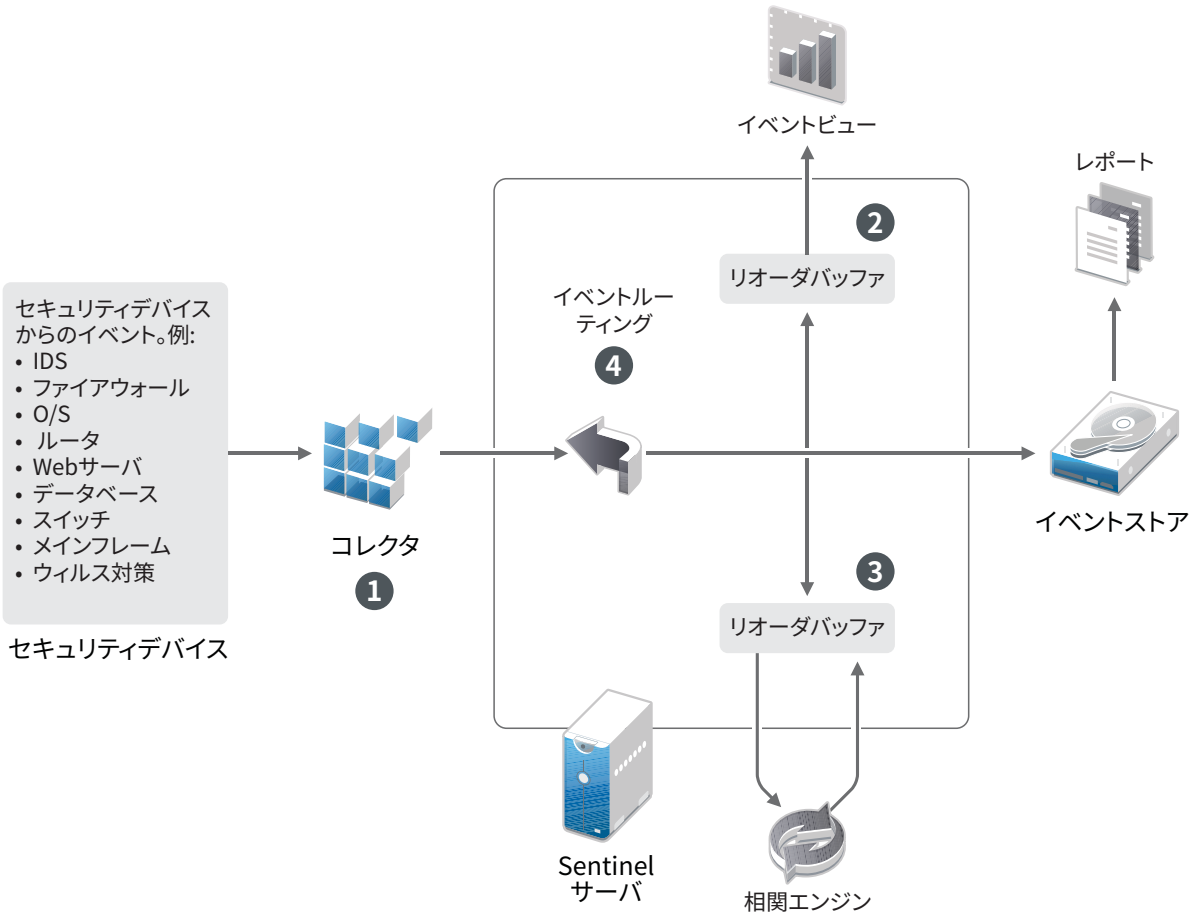
Sentinel は、ネットワーク全体に分散するいくつものプロセスで構成される分散システムです。また、イベントソースによって多少の遅延が発生する可能性があります。これに対応するために、Sentinel プロセスは、イベントを処理する前に、イベントを時間順に並び替えます。

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 Collector Manager 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、従来のストレージのセットアップで Sentinel がこれを処理する方法を説明します。

図 17-1 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、イベントビューによって普通に処理されます。イベント時刻が 5 分よりも先に進んでいるイベントは、イベント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. Correlation Engine 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、Correlation Engine はイベントを処理しません。
4. イベント時刻が Collector Manager システム時刻から 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、Correlation Engine および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。

Sentinel における時刻の設定

Correlation Engine 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。

- Collector Manager 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 Collector Manager 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、『「Sentinel 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]**。

イベントの遅延時間限度の環境設定

Sentinel がイベントソースからイベントを受け取るときに、イベントが生成された時間と Sentinel がそれを処理した時間の間で遅延が生じる場合があります。Sentinel は大きな遅延が生じたイベントを別個のパーティションに保存します。多くのイベントで長時間の遅延が生じている場合、それはイベントソースが正しく環境設定されていないことを示している場合があります。Sentinel は遅延が生じているイベントを処理しようとするため、Sentinel のパフォーマンスが低下することもあります。遅延が生じているイベントが正しくない環境設定の結果である可能性があるため、保存が望ましくない場合があります。そのため、Sentinel では、着信イベントでの受け入れ可能な遅延限度を設定できます。イベントルータはこの遅延限度を超えたイベントをドロップします。configuration.properties ファイル内の以下のプロパティで遅延限度を指定します。

```
esecurity.router.event.delayacceptthreshold = <time in milliseconds>
```

リストを定期的に Sentinel サーバログファイルに記録することもできます。このファイルには、指定したしきい値を超えたイベントの受信元のイベントソースが示されます。この情報をログ記録するには、configuration.properties ファイル内の以下のプロパティでしきい値を指定します。

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

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 Collector Manager 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 Collector Manager 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 Collector Manager 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。Collector Manager 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［イベント時刻］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。

18 イベント視覚化用の Elasticsearch の設定

Elasticsearch はほとんど環境設定を必要としませんが、実稼働環境に入る前に考慮する必要のある設定がいくつかあります。

注 : Elasticsearch クラスタ環境設定セットアップでは、接続されているノードまたは使用可能なノードのヘルスに基づいて、いずれかのノードが最初に kibana.yml ファイルで更新されます。この方法で設計されているのは、Sentinel サーバノードの負荷を減らす (パフォーマンスを向上させる) ためです。この kibana.yml ファイルは、最初に接続するノードのヘルスに基づいて、Sentinel を介して更新されます。

Sentinel でのイベント視覚化の有効化

1 novell ユーザに切り替えます。

```
su novell
```

Java バージョンが 292 の場合は、手順 2 と 3 を実行します。OS レベルで java バージョンを見つけるには、コマンドプロンプトで java -version を実行します。

2 (条件による)JAVA_HOME を Sentinel JDK バンドルに設定します。

```
JAVA_HOME=/opt/novell/sentinel/jdk
```

3 (条件による)java の PATH を、Sentinel JDK の場所に設定します。

```
PATH=$JAVA_HOME/bin:$PATH
```

4 Sentinel ノードでクラスタの認証局 (CA) を生成します。Sentinel の Elasticsearch ホームディレクトリ <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch で次のコマンドを実行します。

```
./bin/elasticsearch-certutil ca
```

CA 証明書のファイル名とパスワードの入力を求められます。デフォルトのファイル名は elastic-stack-ca.p12 です。

5 Sentinel の事前バンドルされた Elasticsearch ノードの証明書と秘密鍵を生成します。この場合、Sentinel の Elasticsearch ホームディレクトリ <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch で次のコマンドを実行します。

```
./bin/elasticsearch-certutil cert --ca <CA certificate filename>.p12 --out config/certs/node-1.p12
```

CA 証明書のパスワードを入力するように求められます。また、生成された証明書のパスワードを作成するよう求めるプロンプトも表示されます。

6 Sentinel ノードの <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.yml ファイルに次の設定を追加します。

- xpack.security.transport.ssl.enabled: true
- xpack.security.transport.ssl.keystore.path: certs/node-1.p12
- xpack.security.transport.ssl.truststore.path: certs/node-1.p12
- xpack.security.transport.ssl.verification_mode: 証明書

7 上記で生成された Truststore およびキーストア証明書ファイルのパスワードを、Elasticsearch キーストアに保存します。この場合、Elasticsearch ホームディレクトリで、次のコマンドを実行します : Sentinel の <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch:

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.truststore.secure_password
```

8 Sentinel サーバに novell ユーザでログインします。

9 /etc/opt/novell/sentinel/config/configuration.properties ファイルを開きます。

10 (条件による)Sentinel で高可用性 (HA) モードを使用している場合は、クラスタのすべてのノードに対して、sentinel.ha.cluster プロパティが true に設定されていることを確認してください。

11 eventvisualization.traditionalstorage.enabled を true に設定します。

12 数分後にユーザインタフェースを更新して、イベント視覚化機能を表示します。

[[マイ Sentinel]] ユーザインタフェースで有効にしたすべてのダッシュボードが表示されます。脅威ハンティングダッシュボードなど任意のダッシュボードを起動して、[[検索]] をクリックします。ダッシュボードには、過去 1 時間に生成されたすべてのイベントが表示されます。

13 (オプション) イベント視覚化ダッシュボードには、イベントの視覚化を有効にした後に処理されたイベントのみが表示されます。ファイルベースのストレージに存在する既存のイベントを表示するには、ファイルベースのストレージのデータを Elasticsearch に移行する必要があります。詳細については、203 ページの第 35 章「Elasticsearch へのデータの移行」を参照してください。

注 : イベント視覚化を有効または無効にすると、Sentinel インデックス作成サービスが再開されるため例外が生成されます。この例外は予想どおりで、無視できます。

クラスタモードの Elasticsearch

1 セクション 111 ページの 「Sentinel でのイベント視覚化の有効化」に表示される手順を実行します。

2 次の情報を更新または追加して、各外部 Elasticsearch ノード上の /etc/elasticsearch/elasticsearch.yml ファイルを設定します。

プロパティと値	備考
discovery.seed_hosts: ［< クラスタ内のマスタ適格な Elasticsearch ノードの IP>,< クラスタ内のマスタ適格な Elasticsearch ノードの IP>,< クラスタ内のマスタ適格な Elasticsearch ノードの IP> など］	
cluster.name: <*Elasticsearch _cluster_name*>	指定するクラスタ名は、すべてのノードで同じである必要があります。
node.name: <*node_name*>	ノード名は、各ノードで固有である必要があります。
network.host: _<*networkInterface*>:ipv4_	IP アドレスの代わりにホスト名を使用する場合は、Elasticsearch クラスタと Sentinel サーバのすべてのノードがホスト名を解決可能にしてください。
thread_pool.write.queue_size: 300	
thread_pool.search.queue_size: 10000	検索キューのサイズがその制限に達すると、Elasticsearch ではキュー内で保留中の検索要求が破棄されます。 次の計算に基づき、検索キューのサイズを増やすことができます。 threadpool.search.queue_size = 1 ダッシュボードのユーザごとのウィジェットクエリの平均数 x1 日のインデックスごとのシャード数 x 日数 (検索期間)
index.codec: best_compression	

プロパティと値	備考
path.data: ["/<*es1*>", "/<*es2*>"]	データを複数の独立したディスクまたは場所に分散させ、ディスク I/O のレイテンシを短縮します。 Elasticsearch データを格納するための複数のパスを設定します。たとえば、/es1、/es2 などです。 最高のパフォーマンスと管理性を得るため、それぞれのパスを個別の物理ディスク (JBOD) にマウントします。

3 Elasticsearch クラスタの各外部 Elasticsearch ノードで上記の手順をすべて繰り返します。

4 Sentinel サーバの Elasticsearch ノードで、<sentinel_installation_path>/opt/novell/sentinel/3drparty/elasticsearch/config/elasticsearch.yml を次のように設定します。

4a elasticsearch.yml ファイル内の cluster.name 値と discovery.seed_hosts 値が、外部 Elasticsearch ノードの elasticsearch.yml ファイルと同じであることを確認します。

5 (条件による) 従来のストレージを使用する Sentinel の場合、<sentinel_installation_path>/etc/opt/novell/sentinel/config/elasticsearch-index.properties ファイルの ServerList プロパティに、外部 Elasticsearch ノードの IP アドレスを追加します。

例 : ServerList=<*Elasticsearch_IP1*>:< *ポート* >,<*Elasticsearch IP2*>:< *ポート* >

6 **外部の Elasticsearch クラスタセットアップがある場合に、外部の Elasticsearch ノード間および Sentinel クラスタと Elasticsearch クラスタ間の安全な通信を有効にする**

Sentinel の最新リリースでは、Sentinel サーバと外部の Elasticsearch クラスタ間、および Elasticsearch クラスタの異なるノード間の安全な通信が可能です。このセクションでは、Sentinel サーバに外部の Elasticsearch クラスタが接続されている場合に、これらの安全な設定を有効にする手順について説明します。

Elasticsearch ノード間のクラスタ内通信をセキュリティ保護するための手順は、次のとおりです。

1. クラスタ内のすべての外部 Elasticsearch ノードの証明書を生成します。最初に、Sentinel ノード自体ですべての外部 Elasticsearch 証明書を作成し、それぞれの Elasticsearch ノードにコピーできます。この場合、まずは Sentinel の Elasticsearch ホームディレクトリ <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch で次のコマンドを実行します。

   ```
   ./bin/elasticsearch-certutil cert --ca <CA certificate
   filename>.p12 --out config/certs/newNode.p12
   ```

   CA 証明書のパスワードを入力するように求められます。また、生成された証明書のパスワードを作成するよう求めるプロンプトも表示されます。

2. 証明書をそれぞれの外部 Elasticsearch ノードにコピーします。たとえば、newNode.p12 ファイルを外部 Elasticsearch クラスタの newNode の /etc/elasticsearch/certs/ ディレクトリにコピーします。chmod コマンドを使用して、新しいマシン上の証明書に対する読み書き可能許可を提供します。

   注 : certs ディレクトリが存在しない場合は、同じディレクトリを作成する必要があります。

3. すべての外部 Elasticsearch ノードに証明書を生成してコピーした後、すべての外部 Elasticsearch ノードの /etc/elasticsearch/elasticsearch.yml ファイルに次の設定を追加します。
   - xpack.security.enabled: true
   - xpack.security.transport.ssl.enabled: true
   - xpack.security.transport.ssl.keystore.path: certs/newNode.p12
   - xpack.security.transport.ssl.truststore.path: certs/newNode.p12
   - xpack.security.transport.ssl.verification_mode: 証明書
4. 外部の Elasticsearch ノードごとに、生成されたキーストアおよび Truststore 証明書ファイルのパスワードを Elasticsearch キーストアに保存します。この場合、すべての外部 Elasticsearch ノードの Elasticsearch ホームディレクトリ /usr/share/elasticsearch で次のコマンドを実行します。

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.transport.ssl.keystore.secure_password
   ```

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.transport.ssl.truststore.secure_password
   ```

Sentinel からの Elasticsearch クラスタ通信をセキュリティ保護するために従う手順は次のとおりです。

1. novell ユーザに切り替えます。

   ```
   su novell
   ```

2. 次のコマンドを実行して、Sentinel マシンから外部の Elasticsearch ノード用の http 証明書を生成します。

   ```
   <sentinel_installation_path>/opt/novell/sentinel/bin/javacert.sh --
   generateES <provide path where the http certificate should be
   generated, example /opt/http.pks> <http certificate password>
   <keyalias>
   ```

3. http 証明書を Elasticsearch ノードにコピーします。たとえば、http.pks ファイルを Elasticsearch ノードの ES_PATH_CONF/certs/ ディレクトリにコピーします。新しいマシン上の証明書に対する読み書き可能許可を提供します。

   注 : certs ディレクトリが存在しない場合は、同じディレクトリを作成する必要があります。

4. すべての外部 Elasticsearch ノードの ES_PATH_CONF/elasticsearch.yml ファイルに次の設定を追加します。
   - xpack.security.http.ssl.enabled: true
   - xpack.security.http.ssl.keystore.path: certs/http.pks
5. すべての外部 Elasticsearch ノードの Elasticsearch ホームディレクトリ /usr/share/elasticsearch で次のコマンドを実行して、http 証明書のパスワードを Elasticsearch キーストアに保存します。

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.http.ssl.keystore.secure_password
   ```

7 Sentinel を再起動します。

```
rcsentinel restart
```

8 各外部 Elasticsearch ノードを再起動します。

```
/etc/init.d/elasticsearch restart
```

9 次のコマンドを実行して、Elasticsearch クラスタが作成された状態を確認します。

```
cd <sentinel_installation_path>/opt/novell/sentinel/bin
```

```
./elasticsearchRestClient.sh <sentinel_ip> <Port used for the
Elasticsearch> GET _cat/nodes
```

10 すべての既存のアラートデータとイベントデータ (存在する場合) が外部の Elasticsearch ノードに移動されていることを確認してください。

11 Sentinel サーバの最適なパフォーマンスと安定性のため、Sentinel サーバの Elasticsearch ノードを専用のマスタ適格ノードとして設定し、すべてのイベント視覚化データが外部 Elasticsearch ノードでインデックス化されるようにします。

11a 内部ノード (Sentinel サーバ) を停止します

```
rcsentinel stopES
```

11b elasticsearch.yml ファイルに次の内部ノードを設定します。

```
node.master: true
node.data: false
node.ingest: false
```

11c elasticsearch-node repurpose を実行して、すべてのシャードをクリーンアップします。

```
<sentinel_installation_path>/opt/novell/sentinel/3rdparty/
elasticsearch/bin/elasticsearch-node -v repurpose
```

11d 内部 Elasticsearch ノードを起動します。

```
rcsentinel startES
```

11e 各外部 Elasticsearch ノードを再起動します。

```
/etc/init.d/elasticsearch restart
```

重要 : 外部の Elasticsearch ノードがダウンすると、Elasticsearch クラスタは自動的に再起動します。このため、Kibana およびアラート検索を使用してダッシュボードを起動する場合に一時的な問題が発生する可能性があります。

Sentinel サーバを再起動したら、外部の Elasticsearch ノードも再起動してください。

19 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 以下のコマンドを使用して、Sentinel をシャットダウンします。

rcsentinel stop

2 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
```

3 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。

4 スペースキーを押して使用許諾契約を確認します。

5 「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。

6 デフォルト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。

7 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 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。

  admin ユーザは、Sentinel Main インタフェースから管理タスク (他のユーザアカウントの作成など) を実行するために使用される ID です。

8 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 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。

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。

9 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 10 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 10 に進みます。

  appuser アカウントは、Sentinel java プロセスがデータベースと接続を確立し、データをやり取りするために使用する内部 ID です。ここで入力したパスワードはデータベースタスクの実行に使用されます。

10 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。

11 ポートを変更してから「7」を指定し、完了します。

12 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。

20 付属プラグインの環境設定

Sentinel には、Sentinel リリース時点で利用可能なデフォルトの Sentinel プラグインがプリインストールされています。

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。

プリインストールプラグインの表示

Sentinel にプリインストールされているプラグインのリストを表示することができます。プラグインのバージョンや他のメタデータも見ることができ、利用可能なプラグインが最新バージョンかどうかを確認するのに役立ちます。

Sentinel サーバにインストールされているプラグインを表示するには :

1. https://*<IP アドレス>*:8443 で、Sentinel Main インタフェースに管理者としてログインします。8443 は Sentinel サーバのデフォルトポートです。
2. [**[プラグイン]**] > [**[カタログ]**] の順にクリックします。

データコレクションの環境設定

データコレクションに関する Sentinel の環境設定については、『Sentinel Administration Guide』の「*Collecting and Routing Event Data*」を参照してください。

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、『「Sentinel 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 Main インタフェースを使用して、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、『「Sentinel Administration Guide」』の「*Installing and Managing Solution Packs*」を参照してください。

アクションとインテグレータの環境設定

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。

21 既存の Sentinel インストールでの証明書取り消しリストの実装

Sentinel での相互 SSL 認証

Sentinel は、ネットワーク、サーバ、コンピュータ、および論理設計内のセキュリティプロトコルを標準化して、全体的なセキュリティを強化するために使用されます。

Sentinel は相互 SSL 認証をサポートし、証明書取り消しリスト (CRL) 機能を実装することで、取り消しデータのローカルキャッシュを提供します。CRL は、Sentinel がインターネットに接続されていない場合でも、侵害されたクライアントをブロックして、取り消されたクライアントの証明書資格情報を検証するのに役立ちます。

CRL は、発行元認証局（CA）によって予定された有効期限の前に取り消され、信頼されてはならないデジタル証明書のリストです。CRL はブラックリストの一種であり、証明書が有効で信頼できるかどうかを検証するために、Web ブラウザを含むさまざまなエンドポイントで使用されます。

本章では、次の事項について説明します。

相互 SSL 通信と証明書取り消しリストの有効化

Sentinel サーバで相互 SSL 通信と CRL を有効にするには、次の手順を実行します。

1. *<sentinel_installation_path>*/opt/novell/sentinel/bin ディレクトリに移動します。
2. novell ユーザとして、次のコマンドを実行します。

   ```
   ./createDefaultMutualCert.sh
   ```

3. (条件による) サーバを FIPS モードに変換する前にスクリプトを使用して証明書が作成された場合は、次の手順を実行します。

   3a *<sentinel_installation_path>*/opt/novell/sentinel/bin/ に移動します。

   3b 次のコマンドを実行します。

   ```
   ./convert_to_fips -i <sentinel_installation_path>
   /etc/opt/novell/sentinel/config/
   .defaultRestClient.p12
   ```

3c Sentinel を再起動します。

```
rcsentinel restart
```

4 コレクタマネージャと相関エンジン内の *<sentinel_installation_path>*/opt/novell/sentinel/setup directory に移動します。

5 次のコマンドを実行し、画面の指示に従って、コレクタマネージャおよび相関エンジンを Sentinel サーバと互換性を持たせます。

```
./configure.sh
```

注 : コレクタマネージャと相関エンジンが CRL モードにあり、サーバに接続できない場合は、マシン上の **[cURL バージョン]** を 7.60 以上にアップグレードします。

カスタム証明書の作成とインポート

カスタム証明書を作成してインポートするには、次の方法を実行します。

1 次のコマンドを使用して、公開鍵と秘密鍵を作成します。

```
openssl req -new -text -out <public_key_name> -keyout
<private_key_name>
```

2 次のコマンドを使用して、自己署名 X.509 認定を作成します。

```
openssl req -x509 -days 365 -in
 <public_key_name> -text -key
 <private_key_name> -out
 <certificate_name>
```

3 生成された証明書を Sentinel キーストアにインポートします。

```
<sentinel_installation_path>
/opt/novell/sentinel/bin/javacert.sh --import
 <sentinel_installation_path>
/etc/opt/novell/sentinel/config/.webserverkeystore.jks
 <password of the keystore>  <alias_name> <certificate_name>
```

4 生成された証明書を p12 形式に変換します。

```
openssl pkcs12 -inkey <private_key_name>  -in <certificate_name> -
export -out <certificate_name.p12>
```

5 キーストアにインポートされた証明書リストを表示するには、次のコマンドを実行します。

```
<sentinel_installation_path>
/opt/novell/sentinel/jdk/jre/bin/keytool -list -keystore
/etc/opt/novell/sentinel/config/.webserverkeystore.jks
```

6 Sentinel サーバを再起動します。

SSL 相互通信を使用した Sentinel の起動

SSL 相互通信で Sentinel を起動するには :

1. 123 ページの 「相互 SSL 通信と証明書取り消しリストの有効化」で作成した .defaultRestClient.p12 証明書ファイルをダウンロードします。

   また、独自のカスタマイズされた証明書も使用できます。カスタム証明書の作成方法の詳細については、124 ページの 「カスタム証明書の作成とインポート」を参照してください。
2. *<certificate name.p12>* 証明書をクライアントアプリケーションブラウザにインポートします。
3. クライアントアプリケーションブラウザを再ロードします。
4. 次の URL を使用して、Sentinel を起動します。

   https://*<sentinel_ipaddress>*:*<sentinel_port>*
5. 前の手順でインポートした証明書を選択し、[**[OK]**] をクリックします。

証明書の取り消しと CRL への追加

証明書を取り消して CRL に追加するには、

1. CRL のディレクトリを作成します。

   ```
   mkdir /etc/<CRL_directory>
   ```
2. 作成したディレクトリに切り替えます。

   ```
   cd /etc/<CRL_directory>
   ```
3. CRL のインデックスファイルを作成します。

   ```
   touch index.txt
   ```
4. 一時的な CRL 番号ファイルを作成します。

   ```
   echo 00 > pulp_crl_number
   ```
5. ディレクトリ /etc/ssl/(SLES の場合) または /etc/pki/tls/(RHEL の場合) に存在する openssl.cnf ファイルを編集します。

   注 : ファイルパスが分からない場合は、コマンド openssl version -a | grep OPENSSLDIR を実行して、openssl.cnf ファイルを含むディレクトリを検索します。

   ```
   database = /etc/<CRL_directory>/index.txt
   ```

   ```
   crlnumber = /etc/<CRL_directory>/pulp_crl_number
   ```

   (オプション)CRL に必要な設定を使用して、独自の設定ファイルを作成できます。
6. 取り消す証明書を crt 形式に変換します。

```
openssl pkcs12 -in <certificate in p12 format> -clcerts -nokeys -out
<certificate_name.crt>
```

7 証明書を取り消します。

```
openssl ca -revoke <certificate_name.crt>
-keyfile <private_key> -cert
<X.509 certificate>
```

8 取り消された証明書の CRL ファイルを生成します。

```
openssl ca -gencrl -keyfile <private_key>
-cert <X.509 certificate> -out /etc/
<CRL_directory>/crl.pem
```

9 取り消された証明書を既存の CRL ファイルに追加します。

9a 次のコマンドを実行します。

```
cat <sentinel_installation_path>/etc/opt/
novell/sentinel/config/<Sentinel CRL File Name>
/etc/<CRL_directory>/
crl.pem > temp.pem
```

9b 次のコマンドを実行します。

```
mv temp.pem <sentinel_installation_path>/etc/opt/
novell/sentinel/config/<Sentinel CRL File Name>
```

<Sentinel CRL File Name> は、プロパティ sentinel.webserver.crlfile キーから参照できます。このキーは、<sentinel_installation_path>/etc/opt/novell/sentinel/config/configuration.properties にあります。

10 (条件による) 複数の証明書を取り消す場合は、各証明書に対して手順 6 から手順 9 を繰り返します。

11 Sentinel サーバを再起動します。

CRL 機能の無効化

CRL 機能を無効にするには、次の手順を実行します。

1 該当するディレクトリに切り替えます。

```
<sentinel_installation_path>/etc/opt/novell/sentinel/3rdparty/jetty
```

2 次のコマンドを実行します。

```
mv jetty-ssl-context.xml.crl.bkp jetty-ssl-context.xml
```

3 <sentinel_installation_path>/etc/opt/novell/sentinel/config/configuration.properties ファイルで、次のプロパティを削除します。

- sentinel.client.cert.password=<cert.password>
- sentinel.validate.crl=true
- sentinel.webserver.crlfile=/config/pulp_crl.pem

4 Sentinel サーバを再起動します。

```
rcsentinel restart
```

5 コレクタマネージャと相関エンジン内の *<sentinel_installation_path>*/opt/novell/sentinel/setup directory に移動します。

6 次のコマンドを実行し、画面の指示に従って、コレクタマネージャおよび相関エンジンを Sentinel サーバと互換性を持たせます。

```
./configure.sh
```

注 : コレクタマネージャと相関エンジンが CRL モードにあり、サーバに接続できない場合は、マシン上の **[cURL バージョン]** を 7.60 以上にアップグレードします。

---

22 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。

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 ユーザに切り替えます。

   ```
   su novell
   ```

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。

   外部証明書を求めるプロンプトが表示されたら、Elasticsearch http 証明書 <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks のパスを追加します。

   (条件による)Elasticsearch がクラスタモードの場合は、188 ページの 「セキュアクラスタ通信用の Elasticsearch の設定」セクションで作成されたすべての外部の Elasticsearch ノード http 証明書を Sentinel サーバにコピーします。外部証明書を求めるプロンプトが表示されたら、上記でコピーした Elasticsearch http 証明書のパス < 上記でコピーした証明書パス >/< 証明書名 > を追加します。この手順を繰り返して、すべての外部 Elasticsearch 証明書が追加されていることを確認します。

   (条件による)CRL 機能を使用している場合は、外部証明書を求めるプロンプトが表示されたら、クライアント証明書 *<sentinel_installation_path>*/etc/opt/novell/sentinel/config/.defaultRestClient.p12 のパスを追加します。

デフォルトのクライアント証明書 (.defaultRestClient.p12) を使用するか、独自にカスタマイズした証明書を使用できます。カスタム証明書の作成方法の詳細については、124 ページの 「カスタム証明書の作成とインポート」を参照してください。

5 (条件による) ご使用の環境で多要素認証または強力な認証を使用している場合 :

5a create_mfa_fips_keys.sh スクリプトを実行し、画面の指示に従います。

注 : スクリプトには nss データベースのパスワードが必要です。

5b Sentinel クライアント ID と Sentinel クライアントシークレットを入力します。認証方法の詳細については、『「Sentinel Administration Guide」』の「Authentication Methods」を参照してください。

Sentinel クライアント ID と Sentinel クライアントシークレットを取得するには、次の URL に移動します。

https://*Hostname*:*port*/SentinelAuthServices/oauth/clients

各要素の内容は次のとおりです。

- *Hostname* は、Sentinel サーバのホスト名です。
- *Port* は、Sentinel が使用するポートです (通常は 8443)。

指定した URL では、Sentinel の現在のセッションを使用して、Sentinel クライアント ID と Sentinel クライアントシークレットを取得します。

6 Sentinel サーバを再起動します。

7 133 ページの第 23 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。

従来型 /Sentinel HA アプライアンスでの FIPS モードの有効化

1 アクティブノードの場合 :

1a 129 ページの 「Sentinel サーバを FIPS 140-2 モードで実行する」セクションで説明されている手順を完了します。

1b 次のコマンドを実行して、すべてのパッシブノードに設定プロパティを同期します。

- csync2 –x –v

1c フォルダがすべてのパッシブノードに同期済みか確認します。

- /etc/opt/novell/sentinel/3rdparty/nss

1d (条件による)/etc/opt/novell/sentinel/3rdparty/nss フォルダが同期されていない場合は、アクティブノードからクラスタ内の各パッシブノードに手動でフォルダをコピーします。

- scp –pr /etc/opt/novell/sentinel/3rdparty/nss <passivenode ip または passivenode 名 >:/etc/opt/novell/sentinel/3rdparty/

2 パッシブノードの場合 :

2a nss フォルダがパッシブノードに対する novell ユーザの許可を持っている必要があります。

2a1 パッシブノードにログインします。

2a2 フォルダの所有権を novell ユーザに変更します。

- chown –R novell:novell /etc/opt/novell/sentinel/3rdparty/nss

2a3 適切な権限をフォルダに設定します。

- chmod –R 600 /etc/opt/novell/sentinel/3rdparty/nss

2b クラスタ内のすべてのパッシブノードで手順 2a を繰り返します。

2c アクティブノードから次のコマンドを繰り返し実行して、すべてのパッシブノードですべての FIPS 関連ファイルが更新されていることを確認します。

- csync2 –x –v

リモート Collector Manager instances および Correlation Engine instances 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 Collector Manager および Correlation Engine 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 Collector Manager または Correlation Engine を FIPS 140-2 モードで動作させるには :

1 リモートの Collector Manager または Correlation Engine のシステムにログインします。

2 novell ユーザに切り替えます。

```
su novell
```

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。

Sentinel のインストール中に生成された内部の Elasticsearch http 証明書 (Sentinel サーバ内の <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks) をコピーし、外部証明書を求めるプロンプトが表示されたら、上記でコピーした Elasticsearch http 証明書 < 上記でコピーした証明書のパス >/< 証明書名 > のパスを追加します。

(条件による)Elasticsearch がクラスタモードの場合は、セクション「Settings in Elasticsearch for Secure Cluster Communication to the Remote Collector Manager(リモートコレクタマネージャへのセキュアクラスタ通信のための Elasticsearch の設定)」で作成されたすべての外部の Elasticsearch ノード http 証明書をコピーします。外部証明書を求めるプロンプトが表示されたら、上記でコピーした Elasticsearch http 証明書のパス < 上記でコピーした証明書パス >/< 証明書名 > を追加します。この手順を繰り返して、すべての外部 Elasticsearch 証明書が追加されていることを確認します。

5 Collector Manager または Correlation Engine を再起動します。

6 133 ページの第 23 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。

23 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。

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、143 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>/jdk/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、143 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>/jdk/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、143 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。

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、143 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 Main] インタフェースに管理者の役割のユーザとして移動して、LDAP 認証の設定を続行します。

詳しくは、『*Sentinel Administration Guide*』の「「LDAP Authentication Against a Single LDAP Server Or Domain」」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。

リモート Collector Manager instances および Correlation Engine instances のサーバ証明書の更新

既存のリモート Collector Manager instances およびリモート Correlation Engine instances 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 Collector Manager または Correlation Engine 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 Collector Manager instances 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 Collector Manager または Correlation Engine 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、Collector Manager または Correlation Engine 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 Collector Manager または Correlation Engine の Sentinel サーバ証明書を更新するには :

1 リモートの Collector Manager または Correlation Engine のコンピュータにログインします。

2 novell ユーザに切り替えます。

```
su novell
```

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。

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 : 以下の手順は、/opt/novell/sentinel ディレクトリに Sentinel をインストールしたと想定した場合のものです。すべてのコマンドを novell ユーザとして実行します。

Agent Manager コネクタ

Agent Manager 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。

Agent Manager 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. Agent Manager 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 Agent Manager イベントソースサーバがデータの送信を試行している Agent Manager 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 :** Agent Manager 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 Agent Manager 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、143 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、Agent Manager 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 Collector Manager 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 Collector Manager 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、Agent Manager 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。

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、143 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。

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、143 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。

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、143 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 Collector Manager 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 Collector Manager 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。

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、143 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 Collector Manager 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 Collector Manager 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、143 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。

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、143 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。

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、143 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。

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。

Syslog インテグレータ

Syslog インテグレータのネットワーク設定時に「暗号化 (SSL)」オプションを選択している場合にのみ、以下の手順を実行してください。

Syslog 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 Syslog 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、Syslog 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。

- **Syslog 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 サーバから送信側 Sentinel サーバにコピーする必要があります。

  コネクタがリモート Collector Manager 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 Collector Manager コンピュータから受信側の Sentinel コンピュータ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。

- **Syslog コネクタが非 FIPS モードである場合 :** カスタムの Syslog サーバ証明書を送信側の Sentinel FIPS キーストアにインポートする必要があります。

  注 : Syslog インテグレータが FIPS 140-2 モードであり、Syslog 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 Collector Manager の一時的な場所にコピーします。
2. /opt/novell/sentinel/bin ディレクトリに移動します。
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 Collector Manager 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。

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、Syslog 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をインポートする必要はありません。

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 Collector Manager 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、67 ページのパート III「Sentinel 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 Collector Manager 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 サーバに接続している非 FIPS リモート Collector Manager 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、Sentinel 8.5 リリースノートを参照してください。

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 モードが有効になっている場合、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 Collector Manager 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 Collector Manager 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 Collector Manager 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 Collector Manager 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。

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。

- 144 ページの 「Sentinel サーバを非 FIPS モードに戻す」
- 145 ページの 「リモート Collector Manager instances またはリモート Correlation Engine instances を非 FIPS モードに戻す」

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。

リモート Collector Manager instances またはリモート Correlation Engine instances を非 FIPS モードに戻す

リモート Collector Manager instances またはリモート Correlation Engine instances を非 FIPS モードに戻すことができます。

リモート Collector Manager instances またはリモート Correlation Engine を非 FIPS モードに戻すには :

1 リモート Collector Manager またはリモート Correlation Engine のシステムにログインします。

2 novell ユーザに切り替えます。

```
su novell
```

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 Collector Manager またはリモート Correlation Engine を再起動します。

24 同意バナーの追加

Sentinel では、ログインする前に同意バナーを表示できます。必要に応じて、バナーの内容を指定できます。同意バナーを追加した後は、Sentinel にログインするたびに同意バナーの条項に同意する必要があります。

同意バナーを追加する方法 :

1. Sentinel サーバに novell ユーザでログインします。
2. /<sentinel_installation_path>/var/opt/novell/sentinel/3rdparty/jetty/webapps/ROOT/siemdownloads にアクセスします。
3. USER_AGREEMENT.txt という名前のテキストファイルを追加します。
4. ユーザ契約テキストを入力します。
5. ファイルを保存します。
6. Sentinel を起動して同意バナーを表示します。

Sentinel のログイン画面に同意バナーが表示されるようになりました。

注 : Sentinel をアップグレードするには、その前に USER_AGREEMENT.txt ファイルを手動でバックアップする必要があります。

---

25 同時アクティブセッション数の制限

Sentinel 8.2 SP3 以降では、ユーザごと、テナントごと、またはその両方に許可する同時アクティブセッションの数を制限することができます。セッションの数を制限することによって、攻撃があった場合に、攻撃者が許可された制限を超えてセッションを起動することを防ぐことができます。

ユーザおよびテナントのセッション数を制限した場合、複数のユーザによって起動されたセッションの総数がテナントに許可された制限に達すると、ユーザはセッションを起動できなくなります。

Sentinel では、デフォルトでは同時セッションが制限されていません。この制限は手動で設定する必要があります。

注 : この機能は、非 MFA モードでのみ使用できます。

同時アクティブセッションの数を制限するには :

1. Sentinel サーバにログインします。
2. /*<sentinel_installation_path>*/etc/opt/novell/sentinel/config/configuration.properties ファイルを開きます。
3. (条件による) テナントごとの上限を設定するには、concurrent.overall.sessions プロパティを必要な値に設定します。
4. (条件による) ユーザごとの制限を設定するには、concurrent.per.user.sessions プロパティを必要な値に設定します。
5. ファイルを保存します。
6. Sentinel サーバを再起動します。

26 非アクティブなセッションの終了

Sentinel 8.2 SP3 以降では、指定された期間にユーザアクティビティがない場合に、セッションを終了するように Sentinel を設定できます。Sentinel は、指定された期間が終了する 1 分前に警告を表示します。ユーザがこの期間セッションで非アクティブ状態であると、Sentinel はユーザをセッションからログアウトします。

デフォルトでは、Sentinel はユーザの非アクティブ状態を追跡しません。非アクティブなセッションを終了させるには、Sentinel を手動で設定する必要があります。

非アクティブタイムアウト期間を設定するには :

1. Sentinel サーバにログインします。
2. /*<sentinel_installation_path>*/etc/opt/novell/sentinel/config/ui-configuration.properties ファイルを開きます。
3. user.inactivity.time プロパティの値をミリ秒単位で設定します。
4. Sentinel にログインしているブラウザを更新します。

27 IP フローデータ収集の設定

Sentinel は、IP フローデータを収集することによって、企業のネットワークの監視に役立つ、ArcSight SmartConnectors を活用します。SmartConnector は、IP フローデータをイベントとして収集します。これにより、以下のことが可能になります。

- 既存のコレクタマネージャインスタンスを使用して IP フローデータを収集します。
- 視覚化、イベントルーティング、データフェデレーション、レポート、および相関など、Sentinel のいくつかの領域で IP フローデータを利用します。
- データ保持ポリシーを IP フローデータに適用します。これにより、必要な期間、このデータを保存できます。

IP フローのデータ収集を設定するには、ArcSight SmartConnector をインストールして設定する必要があります。設定時に、IP フローデータを収集する関連 SmartConnector を忘れずに設定します。

SmartConnector の設定方法の詳細については、Sentinel プラグイン Web サイトの汎用 Universal CEF コレクタのマニュアルを参照してください。

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。

重要

- Sentinel 8.3 以前から Sentinel 8.4 にアップグレードした後、既存の Kibana カスタムダッシュボードは表示されません。Sentinel 8.4 にアップグレードした後に、カスタムダッシュボードを再作成してください。
- アップグレード前にパーティションに［Set to Expire］パラメータが設定されていない場合、Sentinel 8.4 へのアップグレード後に復元されたパーティションにオプションを設定することはできません。
- Sentinel 8.3.1 以前から Sentinel 8.4 にアップグレードした後は、アップグレードによって基礎となるデータ形式も更新されるため、既存のイベントデータは検索やレポート機能などの Sentinel 操作で使用できません。データを検索するには、アップグレード後にシステム内のすべてのイベントデータパーティションのインデックスを再設定する必要があります。詳細については、『Sentinel Administration Guide』の「Re-indexing Event Data Partitions(イベントデータパーティションのインデックスの再設定)」を参照してください。
- Sentinel サーバをアップグレードする場合は、コレクタマネージャシステム、相関エンジンシステム、Sentinel リンクインテグレータの宛先の Sentinel サーバ、および Syslog インテグレータの宛先の Sentinel サーバを同じバージョンの Sentinel サーバにアップグレードしてください。そうしないと、システムでいくつかの問題が発生する可能性があります。

28 実装チェックリスト

Sentinel をアップグレードする前に、以下のチェックリストを確認して、正しくアップグレードされるようにしてください。

表 28-1 *実装チェックリスト*

❒	タスク	参照先
❒	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所定の要件を満たしていることを確認します。	Sentinel 8.5 リリースノート
❒	サポートされているオペレーティングシステムのリリースノートで既知の問題を確認します。	SUSE リリースノート
❒	Sentinel リリースノートで新しい機能と既知の問題を確認します。	Sentinel リリースノート
❒	「前提条件」で説明されているタスクを完了します。	159 ページの第 29 章「前提条件」

29 前提条件

カスタム環境設定情報の保存

Server.conf ファイルの環境設定を保存する

カスタム環境設定パラメータの値を server.conf ファイルで設定している場合は、その値を別のファイルに保存してからアップグレードを実行します。

カスタム環境設定情報を保存するには、次の手順を実行します。

1. Sentinel サーバに novell ユーザでログインし、/etc/opt/novell/sentinel/config/ ディレクトリに移動します。
2. server-custom.conf という名前の設定ファイルを作成し、このファイルにカスタム設定パラメーターを追加します。

Sentinel は、アップグレード中にこれらの設定ファイル内の保存されたカスタム構成を適用します。

Jetty-ssl ファイルの環境設定を保存する

Sentinel の以前のバージョンで /etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml ファイルを修正した (たとえば、いずれかのサイファを除外した) 場合は、Sentinel をアップグレードする前に、それらの修正内容を別のファイルに保存しておいてください。

Sentinel のアップグレードが完了したら、それらの修正内容を /etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl-context.xml ファイルにコピーし、Sentinel を再起動します。

イベント関連付けデータの保持期間の延長

Sentinel 7.4.4 以降では、イベント関連付けデータのデフォルトの保持期間は 14 日間です。configuration.properties ファイルにプロパティを追加し、保持期間に必要な値を設定することができます。詳細については、『「Sentinel Administration Guide」』の「*Configuring the Retention Period for the Event Associations Data*」を参照してください。

Change Guardian の統合

Sentinel には、Change Guardian 4.2 以降との互換性があります。Change Guardian からイベントを受信するには、まず、Change Guardian サーバ、エージェント、および Policy エディタをバージョン 4.2 以降にアップグレードする必要があります。これにより、Sentinel はアップグレード後の Change Guardian からイベントを引き続き受信するようになります。

30 従来の Sentinel インストールのアップグレード

この章の手順では、Sentinel のアップグレードについて取り上げます。

Sentinel 8.2 以降からアップグレードすることができます。

重要 : Sentinel 8.3.0.0 の以前のバージョンからアップグレードする場合は、以下の手順が適用されます。

重要 : Sentinel サーバをアップグレードする場合は、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同じバージョンの Sentinel サーバにアップグレードしてください。そうしないと、システムでいくつかの問題が発生する可能性があります。

アップグレードプロセスでは、次の処理が実行されます。

- セキュリティインテリジェンスデータおよびアラートデータを MongoDB から PostgreSQL に移行します。

  Sentinel は、セキュリティインテリジェンスデータ、アラートデータなどを MongoDB ではなく PostgreSQL に保存するようになりました。アップグレードプロセスでは、まずこのデータを PostgreSQL に移行します。正常に終了した場合、アップグレードが自動的に実行されます。データマイグレーションに失敗した場合は、Sentinel をアップグレードできません。
- データおよび MongoDB 関連の RPM を削除するために使用できるクリーンアップスクリプトを生成します。
- MongoDB に格納されているデータはバックアップとして保持されます。

- 161 ページの 「Sentinel のアップグレード」
- 164 ページの 「非 root ユーザとしての Sentinel のアップグレード」
- 166 ページの 「Collector Manager または Correlation Engine のアップグレード」
- 167 ページの 「オペレーティングシステムのアップグレード」

Sentinel のアップグレード

次の手順に従って、Sentinel サーバをアップグレードします。

Sentinel サーバ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。

データのバックアップの詳細については、『「Sentinel Administration Guide」』の「*Backing Up and Restoring Data*」を参照してください。

2 (条件付き)server.xml、collector_mgr.xml、または correlation_engine.xml ファイルの構成設定をカスタマイズした場合、カスタマイズ内容がアップグレード後も保持されるように、obj コンポーネント ID の付いた名前の適切なプロパティファイルが作成されていることを確認します。詳しくは、『「Sentinel Administration Guide」』の「*Maintaining Custom Settings in XML Files*」を参照してください。

3 ダウンロード Web サイトから最新のインストーラをダウンロードします。

4 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。

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

```
tar 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。

6 インストーラの untar された場所に移動します。たとえば、

```
cd /opt/sentinel_server-<version>*
```

7 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
```

8 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。

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

---

10 **重要 :** Sentinel 8.3.0.0 の以前のバージョンからアップグレードする場合は、以下の手順が適用されます。

10a (条件による) 必要なマイグレーションオプションを選択します。セキュリティインテリジェンスデータおよびアラートデータを MongoDB から PostgreSQL に移行します。

[**[Only upgrade without migrating data(データを移行せずにアップグレードのみ実行)]**］オプションを選択した場合は、Sentinel サーバが起動されて稼働している必要があります。

警告 : アップグレードが正常に終了した後にこの手順を繰り返すことはできないため、適切なオプションを選択していることを確認してください。

データが正常に移行されると、MongoDB に保存されていたデータはバックアップとして保持され、Sentinel アップグレードプロセスが自動的に続行されます。

アップグレードの完了までに、数分かかることがあります。

10b (条件による) データマイグレーションに失敗した場合 :

10b1 部分的に移行されたデータをクリーンアップします。詳細については、183 ページの 「マイグレーションが失敗した場合の PostgreSQL 内のデータのクリーンアップ」を参照してください。

10b2 Sentinel をアップグレードするまで、上記のステップ 7 からステップ 10 の手順を繰り返します。

11 (条件による) アップグレードの前に、イベント視覚化が有効になっている場合、Sentinel 8.4.0.0 にアップグレードした後、Elasticsearch は X-Pack セキュリティプラグインで有効になっているため停止し、Elasticsearch を起動するには 188 ページの 「セキュアクラスタ通信用の Elasticsearch の設定」の手順に従います。

12 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。

13 (条件による)delete_old_cluster.sh ファイルが bin フォルダ (/opt/novell/sentinel/3rdparty/postgresql/bin) にある場合は、PostgreSQL データベースがメジャーバージョン (8.0 から 9.0 など) にアップグレードされたことを意味します。古い PostgreSQL ファイルを PostgreSQL データベースから消去します。カスタムパスのインストールでは、フォルダパスが異なる場合があります。

古い PostgreSQL ファイルをクリアするには、

13a novell ユーザに切り替えます。

```
su novell
```

13b bin フォルダを参照します。

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

13c 次のコマンドを使用して、古い PostgreSQL ファイルをすべて削除します。

```
./delete_old_cluster.sh
```

14 Sentinel にログインし、アラート、セキュリティインテリジェンスデータなどの移行されたデータを検証します。

15 Sentinel 8.3 以降では、データは PostgreSQL にのみ格納されるようになるため、MongoDB 内のデータは冗長になります。ディスク容量を空けるには、このデータを削除してください。詳細については、187 ページの 「MongoDB からデータを削除しています」を参照してください。

16 Collector Manager システムおよび Correlation Engine システムをアップグレードするには、166 ページの 「Collector Manager または Correlation Engine のアップグレード」を参照してください。

非 root ユーザとしての Sentinel のアップグレード

組織のポリシーによって、root としての Sentinel のフルアップグレードが実行できない場合は、別のユーザとして Sentinel をアップグレードできます。このアップグレードでは、いくつかの手順を root ユーザとして実行してから、root ユーザによって作成された別のユーザとして Sentinel をアップグレードします。

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。

データのバックアップ方法については、『「Sentinel Administration Guide」』の「*Backing Up and Restoring Data*」を参照してください。

2 (条件付き)server.xml、collector_mgr.xml、または correlation_engine.xml ファイルの構成設定をカスタマイズした場合、カスタマイズ内容がアップグレード後も保持されるように、obj コンポーネント ID の付いた名前の適切なプロパティファイルが作成されていることを確認します。詳細については、『「Sentinel Administration Guide」』の *Backing Up and Restoring Data* を参照してください。

3 ダウンロード Web サイトからインストールファイルをダウンロードします。

4 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。

5 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。

- インストーラの untar された場所に移動します。たとえば、

```
cd /opt/sentinel_server-8.4.0.0*
```

6 Sentinel インストールファイルから squashfs RPM を抽出します。

7 Sentinel サーバに squashfs をインストールします。

```
rpm -Uvh <install_filename>
```

8 novell ユーザに切り替えます。

```
su novell
```

9 (条件による) インタラクティブアップグレードを実行するには :

9a Sentinel インストールディレクトリに移動し、次のコマンドを実行します。

```
./bin/root_install_prepare
```

次のコマンドを指定します。

```
./install-sentinel
```

デフォルトの場所にない Sentinel をアップグレードするには、コマンドと一緒に --location オプションを指定します。例 :

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

9b ステップ 11 に進みます。

10 (条件による) サイレントアップグレードを実行するには、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。Sentinel のアップグレードが完了します。

11 アップグレード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。

12 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、アップグレードを続行します。

---

13 **重要 :** Sentinel 8.3.0.0 の以前のバージョンからアップグレードする場合は、以下の手順が適用されます。

13a (条件による) マイグレーションオプションを選択します。セキュリティインテリジェンスデータおよびアラートデータを MongoDB から PostgreSQL に移行します。

警告 : アップグレードが正常に終了した後にこの手順を繰り返すことはできないため、適切なオプションを選択していることを確認してください。

データが正常に移行されると、MongoDB に保存されていたデータはバックアップとして保持され、Sentinel アップグレードプロセスが自動的に続行されます。

アップグレードの完了までに、数分かかることがあります。

13b (条件による) データマイグレーションに失敗した場合 :

13b1 移行されたデータをクリーンアップします。詳細については、183 ページの「マイグレーションが失敗した場合の PostgreSQL 内のデータのクリーンアップ」を参照してください。

13b2 Sentinel をアップグレードするまで、上記のステップ 7 からステップ 13 の手順を繰り返します。

14 (条件による) アップグレードの前に、イベント視覚化が有効になっている場合、Sentinel 8.4.0.0 にアップグレードした後、Elasticsearch は X-Pack セキュリティプラグインで有効になっているため停止し、Elasticsearch を起動するには 188 ページの 「セキュアクラスタ通信用の Elasticsearch の設定」の手順に従います。

15 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。

16 (条件による)delete_old_cluster.sh ファイルが bin フォルダ (/opt/novell/sentinel/3rdparty/postgresql/bin) にある場合は、PostgreSQL データベースがメジャーバージョン (8.0 から 9.0 など) にアップグレードされたことを意味します。古い PostgreSQL ファイルを PostgreSQL データベースから消去します。カスタムパスのインストールでは、フォルダパスが異なる場合があります。

古い PostgreSQL ファイルをクリアするには、

16a novell ユーザに切り替えます。

```
su novell
```

16b bin フォルダを参照します。

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

16c 次のコマンドを使用して、古い PostgreSQL ファイルをすべて削除します。

```
./delete_old_cluster.sh
```

17 Sentinel にログインし、アラート、セキュリティインテリジェンスデータなどの移行されたデータを検証します。

18 Sentinel 8.3 以降では、データは PostgreSQL にのみ格納されるようになるため、MongoDB 内のデータは冗長になります。ディスク容量を空けるには、このデータを削除してください。詳細については、187 ページの 「MongoDB からデータを削除しています」を参照してください。

Collector Manager または Correlation Engine のアップグレード

次の手順に従って、Collector Manager および Correlation Engine をアップグレードします :

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、『「Sentinel Administration Guide」』の *Backing Up and Restoring Data* を参照してください。

2 管理者の役割を持つユーザとして **[Sentinel Main]** インタフェースに移動します。

3 [**[ダウンロード]**] を選択します。

4 Collector Manager 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。

5 それぞれのコレクタマネジャサーバまたは Correlation Engine サーバにインストーラ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。

Collector Manager の場合 :

```
./install-cm
```

Correlation Engine 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 (条件による) カスタムインストールの場合、次のコマンドを実行して、Sentinel サーバ、Collector Manager、および Correlation Engine の間で環境設定を同期します。

```
/opt/novell/sentinel/setup/configure.sh
```

オペレーティングシステムのアップグレード

この Sentinel のバージョンには、オペレーティングシステムのアップグレード手順で使用される一連のコマンドが含まれています。これらのコマンドは、オペレーティングシステムのアップグレード後、Sentinel が正しく動作するかどうかを確認するものです。Sentinel をアップグレードする前に、互換性のシステム要件を参照してください。詳細については、『Sentinel システム要件』を参照してください。

オペレーティングシステムをアップグレードするには、次の手順を使用します。

1. オペレーティングシステムをアップグレードする Sentinel サーバで、次のいずれかとしてログインします。
   - ルートユーザー
   - 非ルートユーザ
2. コマンドプロンプトを開き、Sentinel の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。
3. Sentinel サービスを停止します。

   rcsentinel stop
4. (条件による) オペレーティングシステムをアップグレードする前に Sentinel が FIPS モードだった場合は、NSS データベースのファイルを手動でアップグレードするために次のコマンドを実行する必要があります。

   certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X

   画面の指示に従って、NSS データベースをアップグレードしてください。

   novell ユーザに、次のファイルに対する完全な許可を付与します。

   ```
   cert9.db
   key4.db
   pkcs11.txt
   ```
5. オペレーティングシステムをアップグレードします。
6. root ユーザとして、/etc/sysctl.conf ファイルの vm.max_map_count=262144 プロパティを設定します。プロパティを追加した後、sysctl -p を実行して変更を有効にします。
7. (条件による)SLES 15 SP1 または SLES 15 SP 2 にアップグレードする場合、次の警告が表示されます。

   警告 : サポートされていないキーのバージョン : V3

   警告を無視するか、回避策を実行して警告が表示されないようにできます。この回避策の詳細については、SLES マニュアルを参照してください。
8. (条件による)Mozilla Network Security Services (NSS) を使用する場合、依存する 2 つの RPM ファイル libfreebl3-hmac と libsoftokn3-hmac はインストールされません。次の RPM ファイルを手動でインストールします : libfreebl3-hmac、libsoftokn3-hmac。
9. (条件による)SLES12SP4 を FIPS モードで SLES15SP1 または SLES15SP2 にアップグレードする場合は、まず SLES オペレーティングシステムをアップグレードし、最新のオペレーティングシステムパッチを適用してから、Sentinel を起動する必要があります。

10 (条件による) RHEL 7.*x* の場合は、RPM データベースにエラーがないかどうかをチェックするために、次のコマンドを実行します。

rpm -qa --dbpath <*install_location*>/rpm | grep novell

例 : # rpm -qa --dbpath /custom/rpm | grep novell

10a エラーがある場合は、次のコマンドを実行してエラーを修正します。

rpm --rebuilddb --dbpath <*install_location*>/rpm

例 : # rpm --rebuilddb --dbpath /custom/rpm

10b 手順 7 に示されているコマンドを実行して、エラーがなくなったことを確認します。

11 次についてこの手順を繰り返します。

- Collector Manager instances
- Correlation Engine instances

12 次のように Sentinel サービスを再起動します。

rcsentinel restart

この手順は Sentinel HA には当てはまりません。

Sentinel アップグレードの Python バージョンの依存関係

Sentinel では、アップグレードプロセスを正常に実行するために、互換性のあるバージョンの Python ライブラリを使用する必要があります。これは、古いバージョンの OS から新しいバージョンの OS にアップグレードする場合に非常に重要になります。たとえば、SLES 11 SP4 ベースの Sentinel から SLES 15 SP2 ベースの OS バージョンの Sentinel にアップグレードする場合。Sentinel アップグレードプロセスを開始する前に、Python のバージョンを確認してください。OS のアップグレード後に既存の Sentinel ボックスの Python バージョンが変更された場合は、次に示す手順に従う必要があります。

シナリオの例を考えてみましょう。

シナリオ : Sentinel 8.2 (SLES 11 SP4 ベース) から Sentinel 8.4 (SLES 15 SP2 ベース) へのアップグレード。

上のシナリオで、SLES 11 SP4 ボックスで python –V を実行すると、使用されている Python バージョンが 2.6.x であることが示されました。OS のアップグレード後、Python バージョンが 2.7.x にアップグレードされることを期待しています。この違いにより、以下に説明する互換性の問題が発生する可能性があります。

オペレーティングシステムのアップグレード後、および Sentinel バージョンのアップグレード前 :

アップグレードの最初のステップとして、SLES 11 SP4 から SLES 15 SP2 への OS のアップグレードに進みます。OS のアップグレード時に、Python 2.7.x など、より新しいバージョンの Python ライブラリがボックスにインストールされている可能性があります。これで、python –V コマンドを実行すると、Python バージョンが 2.7.x であることが示されます。ただし、このバージョンの Python が表示されているマシンにもかかわらず、以前のバージョンの Sentinel と一緒にインストールされた Python 共有オブジェクトファイル (plpython2.so) が 2.6.x バージョンの Python を指している可能性が高いです。

以下のコマンドを実行します。

```
ldd <sentinel_installation_path>/opt/novell/sentinel/3rdparty/postgresql/
lib/postgresql/plpython2.so
```

このコマンドの出力により、どのバージョンの Python で plpython2.so ファイルが作成されたのかを確認できます。たとえば、出力としての libpython2.6.so.1.0 => /usr/lib64/libpython2.6.so.1.0 は、この .so ファイルが 2.6.x バージョンの Python に基づいており、2.7.x バージョンでは動作しないことを示します。

この衝突により、アップグレードプロセスが失敗する可能性があります。これを解決するには、指定したシナリオに応じ、古いバージョンの plpython2.so ファイル (2.6.x に基づく) を削除し、新しいバージョンの plpython2.so ファイル (2.7.x に基づく) を使用する必要があります。これらの Python のバージョンがセットアップで異なる可能性が高く、これらのコマンドを使用する必要があります。

この場合、次の手順に従います。

1. 以下のコマンドを使用して、Sentinel を停止します。

   ```
   rcsentinel stop
   ```

2. plpython2.so ファイルが存在するディレクトリに切り替えます。

   ```
   cd <sentinel_installation_path>/opt/novell/sentinel/3rdparty/
   postgresql/lib/postgresql
   ```

3. 次のコマンドを使用して、2.6.x を指す既存の .so ファイルを削除します。

   ```
   rm plpython2.so
   ```

4. Python 2.7.x.so ファイルを untar します (これは <sentinel_installation_path>/opt/novell/sentinel/3rdparty/postgresql/lib/postgresql ディレクトリにあります)。

   ```
   tar zxf plpython2.7.so.tar.gz
   ```

5. ファイルに対する novell ユーザ許可を設定します。

   ```
   chown novell:novell plpython2.so
   ```

6. 以下のコマンドを使用して、ファイルが正しい Python バージョンを指していることを確認します (この時点で、出力は 2.7.x バージョンを指しているはずです)。

   ```
   ldd <sentinel_installation_path>/opt/novell/sentinel/3rdparty/
   postgresql/lib/postgresql/plpython2.so
   ```

   上記の手順を完了し、plpython2.so ファイルが正しいバージョンの Python を指していることを確認したら、Sentinel アップグレードプロセスを続行します。

31 Sentinel アプライアンスのアップグレード

この章の手順では、Sentinel アプライアンスのアップグレードについて取り上げます。

Sentinel 8.3.0.0 以降は、MongoDB ではなく PostgreSQL を使用してセキュリティインテリジェンスデータおよびアラートデータを保存するようになりました。アプライアンスのアップグレードは、データを MongoDB から PostgreSQL に正常に移行した後に実行できます。

MongoDB に格納されているデータはバックアップとして保持され、Sentinel をアップグレードした後に削除することができます。

重要 : Sentinel サーバをアップグレードする場合は、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同じバージョンの Sentinel サーバにアップグレードしてください。そうしないと、システムでいくつかの問題が発生する可能性があります。

アプライアンスをアップグレードするための前提条件

アップグレードを実行する前に、次の前提条件を満たしてください。

1. Sentinel 8.2 以降がインストールされている必要があります。
2. SLES 12 SP3 または SLES 12 SP4 がインストールされている必要があります。
    a. (条件による)Sentinel 8.2.0.0 で SLES 11 SP4 を使用している場合は、SLES 11 ですべてのチャネル更新を取得することが推奨されます。次に、OS を SLES 12 SP3 にアップグレードします。SLES オペレーティングシステムのアップグレードの詳細については、172 ページの 「オペレーティングシステムの SLES 12 SP3 へのアップグレード」を参照してください。Micro Focus Patch Finder Web サイトからアップグレード後のユーティリティをダウンロードして実行します。

b. (条件による)Sentinel 8.2.0.0 で SLES 12 SP3 を使用し、アップグレード後のユーティリティ sentinel_sles_iso_os_post_upgrade-release-73.tar.gz を実行している場合は、Micro Focus Patch Finder Web サイトからアップグレード後のユーティリティ sentinel_sles_iso_os_post_upgrade-release-85.tar.gz をダウンロードして実行する必要があります。

c. (条件による)Sentinel 8.2.0.0 で SLES 12 SP3 を使用し、Micro Focus Patch Finder Web サイトからアップグレード後のユーティリティ sentinel_sles_iso_os_post_upgrade-release-85.tar.gz を実行している場合は、175 ページの「アプライアンスのアップグレード」の手順に従います。

3. **重要 :** Sentinel 8.3.0.0 のアップグレードされたバージョンまたは 8.3.0.0 の最新インストールを実行している場合は、175 ページの 「アプライアンスのアップグレード」の手順に従います。

(条件による) セキュリティインテリジェンスデータ、アラートデータなどを MongoDB から PostgreSQL に移行します。これは、上記の前提条件を満たした後でのみ実行できます。データのマイグレーションの詳細については、174 ページの「MongoDB から PostgreSQL へのデータの移行」を参照してください。

マイグレーションスクリプトによってクリーンアップスクリプトが生成されるため、移行するデータがない場合でもマイグレーションスクリプトを実行する必要があります。クリーンアップスクリプトを使用して、Sentinel をアップグレードした後に冗長になる MongoDB データを削除することができます。

オペレーティングシステムの SLES 12 SP3 へのアップグレード

次の理由により、オペレーティングシステムをアップグレードする必要があります。

- Sentinel は、SLES 12 チャネルでのみ使用できるようになりました。したがって、Sentinel およびオペレーティングシステムのアップデートを引き続き受信するには、Sentinel をアップグレードする前に、まずオペレーティングシステムを SLES 12 SP3 にアップグレードする必要があります。
- Sentinel アプライアンスマネージャ機能を活用できます。Sentinel アプライアンスマネージャには、アプライアンスの構成および管理を行える Web ベースのシンプルなユーザインタフェースが備わっています。

オペレーティングシステムをアップグレードし、アプライアンスを設定する方法 :

1 Sentinel サービスを停止します。

```
rcsentinel stop
```

2 (条件による) オペレーティングシステムをアップグレードする前に Sentinel が FIPS モードだった場合は、NSS データベースのファイルを手動でアップグレードするために次のコマンドを実行する必要があります。

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

画面の指示に従って、NSS データベースをアップグレードしてください。

novell ユーザに、次のファイルに対する完全な許可を付与します。

```
cert9.db
key4.db
pkcs11.txt
```

3 (条件による) Mozilla Network Security Services (NSS) 3.29 を使用している場合、依存する 2 つの RPM ファイル libfreebl3-hmac と libsoftokn3-hmac はインストールされません。次の RPM ファイルを手動でインストールします : libfreebl3-hmac、libsoftokn3-hmac。

4 Micro Focus Patch FinderWeb サイトから、SLES 12 SP3 インストーラおよびアップグレード後ユーティリティをダウンロードします。Sentinel HA では、SLES 12 SP3 HA ファイルもダウンロードします。

5 インストールで示される指示に従って、オペレーティングシステムをアップグレードします。Sentinel HA では、追加のアドオン製品をインストールするプロンプトが表示されたら、SLES 12 SP3 HA ファイルをダウンロードした場所を選択し、アップグレードを続行します。

SLES 12 SP3 にアップグレードする方法について詳しくは、SLES のマニュアルを参照してください。

重要 : アップグレード中に SLES 12 SP3 への登録を求めるメッセージが表示されます。ただし、登録をスキップしてください。この画面でアップデートの登録をすると、SUSE カスタマチャネルから SLES 12 SP3 アップデートのみが登録されますが、これはサポートされていません。また、Sentinel のアップデートを受信しなくなります。そのため、Sentinel アプライアンス更新チャネルから Sentinel と SLES 12 SP3 の両方のアップデートを受信するには、ステップ 9 を完了してからのみアップデートの登録をしてください。

---

6 アップグレードプロセスで、SLES によって /etc/sysctl.conf ファイルがバックアップとして /etc/sysctl.conf.rpmsave という名前に変更され、new /etc/sysctl.conf ファイルが作成されます。アップグレードの後、/etc/sysctl.conf.rpmsave ファイルを /etc/sysctl.conf ファイルにコピーします。sysctl.conf ファイルを開き、# Added by sentinel vm.max_map_count を検索します。次のように、この設定を次の行に移動します。

変更前 :

```
net.core.wmem_max = 67108864# Added by sentinel vm.max_map_count :
65530
vm.max_map_count = 262144
```

変更後 :

```
net.core.wmem_max = 67108864
# Added by sentinel vm.max_map_count : 65530
vm.max_map_count = 262144
```

7 (条件による) Sentinel HA の場合、次のセクションに示されている手順を実行します。

- 239 ページの 「iSCSI Target の環境設定」
- 241 ページの 「iSCSI イニシエータの環境設定」
- 242 ページの 「HA クラスタの設定」

8 アプライアンスを設定するには、コマンドプロンプトから、アップグレード後ユーティリティを次のように実行します。

8a ファイルを次のように untar します。

```
tar -xvf <post upgrade utility installer filename>.tar.gz
```

8b ユーティリティを抽出したディレクトリに次のように移動します。

```
cd <post upgrade utility installer filename>
```

8c アプライアンスを設定するには、次のスクリプトを実行します。

```
./appliance_SLESISO_post_upgrade.sh
```

注 : このスクリプトはネットワークの再設定を伴うため、リモートでは実行しないでください。

8d 画面の指示に従って、設定を完了します。

このスクリプトによって、インストールされたパッケージが再設定され、アプライアンスの管理用パッケージが設定されます。

9 Sentinel と最新のオペレーティングシステムの更新を受け取るためには、既存の登録コードを使用して更新に再登録します。詳細については、95 ページの 「アップデートの登録」を参照してください。

MongoDB から PostgreSQL へのデータの移行

マイグレーションスクリプトを実行して、セキュリティインテリジェンスデータ、アラートデータなどを MongoDB から PostgreSQL に移行する必要があります。

マイグレーションスクリプトは、次の処理を実行します。

- セキュリティインテリジェンスデータおよびアラートデータを PostgreSQL に移行します。
- MongoDB からデータおよび MongoDB 関連の RPM を削除するために使用できるクリーンアップスクリプトを生成します。

警告 : データを移行した後は、Sentinel を起動または再起動する前に、Sentinel をアップグレードする必要があります。これは、Sentinel に渡されるデータが失われないようにするためです。

データを移行する方法 :

1 Mongo_To_PostgreSQL_Migration_Utility_8.3.0.0-5575.tar.gz を Download Website(ダウンロード Web サイト)Web サイトからダウンロードします。

2 ファイルを解凍します。

3 アプライアンスコンソールに novell ユーザでログインします。

重要 : マシンの端末からマイグレーションスクリプトを実行します。PuTty や MobaXterm などのエミュレーション端末ソフトウェアを使用しないでください。

---

4 次のスクリプトを実行します :mongo_to_pgsql_migration.sh。

5 要件に従ってマイグレーションオプションを選択します。

警告 : マイグレーションが正常に終了した後でこの手順を繰り返すことはできないため、適切なオプションを選択していることを確認してください。

データが正常に移行されると、確認メッセージが画面に表示されます。これでアプライアンスをアップグレードできるようになりました。

6 (条件による) データマイグレーションに失敗した場合 :

6a 移行されたデータをクリーンアップします。詳細については、183 ページの 「マイグレーションが失敗した場合の PostgreSQL 内のデータのクリーンアップ」を参照してください。

6b この手順を繰り返してデータを移行します。

7 (条件による) マイグレーションスクリプトの実行時に次のエラーが表示される場合は、184 ページの 「マイグレーションスクリプトを実行できません」に記載されているタスクを実行してください。

```
 8101server:/opt # su novell
novell@8101server:/opt>
novell@8101server:/opt> ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as novell
novell@8101server:/opt>
novell@8101server:/opt> exit
exit
8101server:/opt #
8101server:/opt # ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as root
```

アプライアンスのアップグレード

Sentinel と SLES オペレーティングシステムの両方は、アプライアンス更新チャネル、または Subscription Management Tool (SMT) を使用してアップグレードできます。まず 171 ページの 「アプライアンスをアップグレードするための前提条件」に記載されている前提条件を完了してから、アプライアンスをアップグレードする必要があります。

- 176 ページの 「アプライアンス更新チャネルによるアップグレード」
- 178 ページの 「SMT を介したアップグレード」
- 180 ページの 「オフライン更新の実行」

アプライアンス更新チャネルによるアップグレード

Zypper を使用して、Sentinel をアップグレードできます。Zypper は、アプライアンスのインタラクティブアップグレードを実行できるコマンドラインのパッケージマネージャです。エンドユーザライセンス契約の更新など、アップグレードを完了するためにユーザの介入が必要な場合は、Zypper を使用して Sentinel アプライアンスをアップグレードする必要があります。

コマンドプロンプトからアプライアンスをアップグレードするには、次の手順に従います。

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、『「Sentinel Administration Guide」』の *Backing Up and Restoring Data* を参照してください。

2 (条件付き)server.xml、collector_mgr.xml、または correlation_engine.xml ファイルの構成設定をカスタマイズした場合、カスタマイズ内容がアップグレード後も保持されるように、obj コンポーネント ID の付いた名前の適切なプロパティファイルが作成されていることを確認します。詳しくは、『「Sentinel Administration Guide」』の「*Maintaining Custom Settings in XML Files*」を参照してください。

3 アプライアンスマシンにログインし、root ユーザとしてコマンドプロンプトを開きます。

4 コマンドプロンプトから次のコマンドを実行します。

重要 : 177 ページのステップ 6 まで再起動メッセージ / プロンプトを無視します。マシンを再起動する前に、Sentinel を起動する (手順 4c) ことが重要です。

4a zypper -v patch

4b zypper up

4b1「Y」と入力して続行します。

4c (条件による) アップグレードの前に、イベント視覚化が有効になっている場合、Sentinel 8.4.0.0 にアップグレードした後、Elasticsearch は X-Pack セキュリティプラグインで有効になっているため停止し、Elasticsearch を起動するには 188 ページの「セキュアクラスタ通信用の Elasticsearch の設定」の手順に従います。

4d rcsentinel start

5 /etc/sysctl.conf ファイルを開き、# Added by sentinel vm.max_map_count を検索します。次のように、この設定を次の行に移動します。

変更前 :

```
net.core.wmem_max = 67108864# Added by sentinel vm.max_map_count :
65530
vm.max_map_count = 262144
```

変更後 :

```
net.core.wmem_max = 67108864
# Added by sentinel vm.max_map_count : 65530
vm.max_map_count = 262144
```

6 アプライアンスを再起動します。

7 (条件による) Sentinel をカスタムポートにインストールした場合や、Collector Manager または Correlation Engine が FIPS モードの場合は、次のコマンドを実行します。

```
/opt/novell/sentinel/setup/configure.sh
```

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。

9 (条件による) PostgreSQL データベースがメジャーバージョンにアップグレードされた場合 (8.0 から 9.0 や 9.0 から 9.1 など)、PostgreSQL データベースから古い PostgreSQL ファイルを消去してください。PostgreSQL データベースがアップグレードされたかどうかについて詳しくは、『Sentinel リリースノート』を参照してください。

9a novell ユーザに切り替えます。

```
su novell
```

9b bin フォルダを参照します。

```
cd /opt/novell/sentinel/3rdparty/postgresql/bin
```

9c 次のコマンドを使用して、古い postgreSQL ファイルをすべて削除します。

```
./delete_old_cluster.sh
```

10 (条件による)Collector Manager または Correlation Engine をアップグレードするには、ステップ 3 からステップ 7 までを実行します。

11 (条件による) Sentinel を HA 環境で実行している場合は、クラスタ内のすべてのノードでこれらの手順を繰り返します。

12 Sentinel を再起動します。

13 Sentinel にログインし、アラート、セキュリティインテリジェンスデータなどの移行されたデータを表示できるかどうかを検証します。

14 Sentinel 8.3 以降では、データは PostgreSQL にのみ格納されるようになるため、MongoDB 内のデータは冗長になります。ディスク容量を空けるには、このデータを削除してください。詳細については、187 ページの 「MongoDB からデータを削除しています」を参照してください。

Sentinel アプライアンスマネージャを介してアプライアンスをアップグレードするには :

1 次のいずれかの方法で、Sentinel アプライアンスを起動します。

- Sentinel にログインします。[**[Sentinel メイン]**] > [**[アプライアンス]**] の順にクリックします。
- Web ブラウザで次の URL を指定します : https://<IP_address>:9443。

2 Vaadmin としてログインするか、root ユーザとしてログインします。

3 (条件による) これまでにアップデートを実行していない場合は、アップデートの登録をしてください。詳細については、95 ページの 「アップデートの登録」を参照してください。

注 : Sentinel 8.3.1 の場合は、手順 4 および手順 5 以外に、追加の手順 6 が必要です。

---

4 [[オンラインアップデート]] をクリックします。

注 : 以下のすべての手順が完了するまで、システムを再起動しないでください。

5 表示されたアップデートをインストールするには、[[今すぐ更新]] > [[OK]] をクリックします。

6 コマンドプロンプトで次のコマンドを実行します。

重要 : 手順 7 まで再起動メッセージ / プロンプトを無視します。マシンを再起動する前に、Sentinel を起動することが重要です。

- zypper up
- (条件による) アップグレードの前に、イベント視覚化が有効になっている場合、Sentinel 8.4.0.0 にアップグレードした後、Elasticsearch は X-Pack セキュリティプラグインで有効になっているため停止し、Elasticsearch を起動するには 188 ページの「セキュアクラスタ通信用の Elasticsearch の設定」の手順に従います。
- rcsentinel start

7 インストールされているアップデートを適用するには、[[再起動]] をクリックします。

8 Sentinel にログインし、アラート、セキュリティインテリジェンスデータなどの移行されたデータを表示できるかどうかを検証します。

9 Sentinel 8.3 以降では、データは PostgreSQL にのみ格納されるようになるため、MongoDB 内のデータは冗長になります。ディスク容量を空けるには、このデータを削除できます。詳細については、187 ページの 「MongoDB からデータを削除しています」を参照してください。

SMT を介したアップグレード

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。

SMT を介してアプライアンスをアップグレードするには :

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、97 ページの 「SMT でのアプライアンスの設定」を参照してください。

2 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、『「Sentinel Administration Guide」』の *Backing Up and Restoring Data* を参照してください。

3 (条件付き)server.xml、collector_mgr.xml、または correlation_engine.xml ファイルの構成設定をカスタマイズした場合、カスタマイズ内容がアップグレード後も保持されるように、obj コンポーネント ID の付いた名前の適切なプロパティファイルが作成されていることを確認します。詳しくは、『「Sentinel Administration Guide」』の「*Maintaining Custom Settings in XML Files*」を参照してください。

4 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。

5 アップグレード用にリポジトリを更新します。

```
zypper ref -s
```

6 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
```

7 (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
```

8 (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>
```

9 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>
```

10 (条件による) アップグレードの前に、イベント視覚化が有効になっている場合、Sentinel 8.4.0.0 にアップグレードした後、Elasticsearch は X-Pack セキュリティプラグインで有効になっているため停止し、Elasticsearch を起動するには 188 ページの 「セキュアクラスタ通信用の Elasticsearch の設定」の手順に従います。

11 /etc/sysctl.conf ファイルを開き、# Added by sentinel vm.max_map_count を検索します。次のように、この設定を次の行に移動します。

変更前 :

```
net.core.wmem_max = 67108864# Added by sentinel vm.max_map_count :
65530
vm.max_map_count = 262144
```

変更後 :

```
net.core.wmem_max = 67108864
# Added by sentinel vm.max_map_count : 65530
vm.max_map_count = 262144
```

12 アプライアンスを再起動します。

```
rcsentinel restart
```

13 (条件による) Sentinel をカスタムポートにインストールした場合や、Collector Manager または Correlation Engine が FIPS モードの場合は、次のコマンドを実行します。

```
/opt/novell/sentinel/setup/configure.sh
```

14 (条件による)Collector Manager または Correlation Engine をアップグレードするには、ステップ 4 からステップ 13 までを実行します。

15 (条件による) Sentinel を HA 環境で実行している場合は、クラスタ内のすべてのノードでこれらの手順を繰り返します。

16 Sentinel を再起動します。

17 Sentinel にログインし、アラート、セキュリティインテリジェンスデータなどの移行されたデータを表示できるかどうかを検証します。

18 Sentinel 8.3 以降では、データは PostgreSQL にのみ格納されるようになるため、MongoDB 内のデータは冗長になります。ディスク容量を空けるには、このデータを削除できます。詳細については、187 ページの 「MongoDB からデータを削除しています」を参照してください。

オフライン更新の実行

各アプライアンスのオフラインパッチ ISO をダウンロードすることで、オフラインアップデートを実行できます。

安全な環境でオフラインでアプライアンスを更新する

パッチを適用する際にレジストリ / リポジトリの問題が発生した場合、システム内のレジストリエントリとリポジトリエントリのクリアを試してみてください。

アプライアンスの登録とリポジトリの詳細をクリーンアップするには、次の手順を実行します。

1. レジストリエントリをクリアする前に、ファイルのバックアップを取ります :
   a. バックアップディレクトリを作成します。例 :

      ```
      mkdir /etc/zypp/backup
      ```

   b. 次のレジストリファイルをバックアップディレクトリにコピーします。例 :

      ```
      cp /etc/zypp/credentials.d /etc/zypp/backup
      cp /etc/zypp/repos.d/*     /etc/zypp/backup
      cp /etc/zypp/services.d/*  /etc/zypp/ backup
      ```

2. 次のレジストリファイルを削除します。

   ```
   rm -fr /etc/zypp/credentials.d
   rm -fr /etc/zypp/repos.d/*
   rm -fr /etc/zypp/services.d/*
   ```

ISO パッチの適用

次の手順を実行します。

1. パッチ ISO をディレクトリにダウンロードします。例 : <directoryname>/PatchCD-Sentinel-Server-<version-build number>-SLES12-SP5-<datetime>.iso
2. 次のコマンドを使用して、パッチ ISO をマウントするディレクトリを作成します。例 :

```
mkdir -p /opt/trial
```

3. 次のコマンドを使用して、パッチ ISO をローカルにマウントします。例 :

```
mount -o loop <directoryname>/PatchCD-Sentinel-Server-<version-build
number>-SLES12-SP5-<datetime>.iso /opt/trial
```

4. 製品およびオペレーティングシステムのリポジトリを追加します。例 :

```
zypper ar -c -t plaindir "/opt/trial/product-repo" "<product
repository>"

zypper ar -c -t plaindir "/opt/trial/osupdate-repo" "<operating system
repository>"
```

5. (オプション) 次のコマンドを使用して、リポジトリが正常に追加されたどうかを確認します。

```
zypper repos
```

6. 次のコマンドを使用して、パッチがパッチ ISO にバンドルされているのかを確認します。

```
zypper lp
```

7. 次のコマンドを使用して、すべての更新を適用します。

```
zypper -v patch

zypper -v update
```

8. 次のコマンドを使用して、リポジトリリストをクリーンアップします。

```
zypper rr "<product repository>"

zypper rr "<operating system repository>"
```

9. 更新が完了したら、次のコマンドを使用してマシンを再起動します。

```
reboot
```

オペレーティングシステムパッチの適用

オペレーティングシステムパッチを適用するには :

1 次のいずれかの方法で、Sentinel アプライアンスを起動します。

- Sentinel にログインします。[**[Sentinel メイン]**] > [**[アプライアンス]**] の順にクリックします。
- Web ブラウザで次の URL を指定します : https://<IP_address>:9443。

2 Vaadmin としてログインするか、root ユーザとしてログインします。

3 [[オンラインアップデート]] をクリックします。

3a (条件による) これまでにアップデートを実行していない場合は、アップデートの登録をしてください。詳細については、95 ページの 「アップデートの登録」を参照してください。

3b オペレーティングシステムの表示されたアップデートをインストールするには、[[今すぐ更新]] > [[OK]] をクリックします。

4 インストールされているアップデートを適用するには、[[再起動]] をクリックします。

32 トラブルシューティング

マイグレーションが失敗した場合の PostgreSQL 内のデータのクリーンアップ

マイグレーションが失敗した場合は、PostgreSQL データベースに部分的に移動されたデータを削除してから、マイグレーションスクリプトを再実行する必要があります。

警告 : マイグレーションが正常に終了した場合は、この手順を実行しないでください。このスクリプトは、移行されたすべてのデータを削除します。

部分的にマイグレートされたデータをクリーンアップするには、次の手順を実行します。

1. PostgreSQL データベースが稼動していることを確認します。
2. Sentinel サーバに novell ユーザでログインします。
3. Sentinel インストーラまたはマイグレーションユーティリティを抽出した場所に移動します。
4. ./db_migration_failure_cleanup.sh スクリプトを実行して、部分的に移行されたデータを削除します。
5. rm db_migration_failure_cleanup.sh コマンドを実行して、db_migration_failure_cleanup.sh ファイルを削除します。

   従来のアップグレードを続行するには、161 ページの第 30 章「従来の Sentinel インストールのアップグレード」を参照してください。

   アプライアンスのアップグレードを続行するには、MongoDB から PostgreSQL にデータを移行します。詳細については、「174 ページの 「MongoDB から PostgreSQL へのデータの移行」」を参照してください。

マイグレーションスクリプトを実行できません

マイグレーションスクリプトを実行してデータを PostgreSQL に移動するときに次のエラーが表示される場合があります。

```
8101server:/opt # su novell
novell@8101server:/opt>
novell@8101server:/opt> ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as novell
novell@8101server:/opt>
novell@8101server:/opt> exit
exit
8101server:/opt #
8101server:/opt # ./mongo_to_pgsql_migration.sh
./mongo_to_pgsql_migration.sh: line 25: /bin/setenv.sh: No such file or
directory
Cannot execute ./mongo_to_pgsql_migration.sh as root
```

このエラーは、以前のアップグレード中に bashrc が変更された可能性があるため、アプライアンスを前のバージョンから Sentinel 8.2 にアップグレードしている場合に発生することがあります。

このエラーを回避するには、bashrc ファイルを更新する必要があります。

Bashrc ファイルを更新するには :

1. bashrc ファイルを開きます。

   /home/novell/.bashrc

2. (条件による) ファイルに次のプロパティが含まれていない場合は、追加します。

   ```
   APP_HOME="/opt/novell/sentinel"
   export PATH="$APP_HOME/bin:$APP_HOME/bin/actions:$PATH"
   ```

3. マイグレーションスクリプトを再実行します。詳細については、174 ページの「MongoDB から PostgreSQL へのデータの移行」を参照してください。

アプライアンスを介してサーバまたは他のコンポーネントに接続できません

Sentinel を以前にインストールした場合は、IP が含まれている場合があります。インストール時に［[ホスト名をループバックアドレスに割り当てる]］オプションを選択した場合は、/etc/hosts ファイル内の 127.0.0.2 としてアドレス指定をします。これにより、他のサーバまたはコンポーネントとの通信に問題が発生する可能性があります。ファイルを編集して、この IP アドレスを削除する必要があります。

IP アドレスを削除するには :

1. /etc/hosts ファイルを開きます。

2 IP アドレス 127.0.0.2 のエントリにコメントを付けます。

3 ファイルを保存します。

アプライアンスのアップグレード時のエラー

アプライアンスをアップグレードする際に、以前のバージョンから 8.2 以降にアップグレードしている場合、次のエラーが発生する可能性があります。

```
(104/134) Installing: kernel-default-4.12.14-95.45.1.x86_64
.....................................................................
.............[error]
Installation of kernel-default-4.12.14-95.45.1.x86_64 failed:
Error: Subprocess failed. Error: RPM failed:    installing package kernel-
default-4.12.14-95.45.1.x86_64 needs 4MB on the /boot filesystem
```

これは、Sentinel ではなく SUSE オペレーティングシステムの既知の問題です。したがって、この問題を解決するには、SUSE マニュアルに記載されている解決方法に従ってください。

アップグレードセットアップ時に Elasticsearch キーストアにパスワードを追加する場合のエラー

アップグレードのセットアップ時に次のコマンドを実行すると、FileAlreadyExistsException エラーメッセージが表示されます。

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

解決策 :

1. novell ユーザに切り替えます。

   ```
   su novell
   ```

2. 次のファイル <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.keystore.tmp を削除します。

3. 証明書 <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks を削除し、次のコマンドを実行して証明書を再生成します。

   ```
   <sentinel_installation_path>/opt/novell/sentinel/bin/javacert.sh --
   generateES <sentinel_installation_path>/opt/novell/sentinel/3rdparty/
   elasticsearch/config/http.pks <password> <keyalias>
   ```

4. <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch で次のコマンドを実行して、上記の手順で作成した証明書のパスワードを Elasticsearch キーストアに追加します。

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.http.ssl.keystore.secure_password
   ```

5. Elasticsearch の設定については、111 ページの 「Sentinel でのイベント視覚化の有効化」を参照し、手順 5 ～ 11 を実行してください。
6. Sentinel を再起動します。

   ```
   rcsentinel restart
   ```

Elasticsearch の設定後にダッシュボードおよびアラートビューで古いアラートを表示できない

Elasticsearch を設定した後、アラートダッシュボードとアラートビューのチャートが更新されない、または古いアラートが表示されません。ただ、アラートビューの表には、新しく生成されたアラートが表示されます。この問題は、アラートインデックスが壊れているため発生する可能性があります。

解決策 : 次の手順を実行してください。

1. <Sentinel_installation_path>/var/opt/novell/sentinel/bin ディレクトリに移動します。
2. novell ユーザに切り替える場合は、次のコマンドを実行します。

   ```
   su novell
   ```

3. アラート同期プロセスを開始するには、次のコマンドを実行します。

   ```
   ./reSyncAlert.sh
   ```

33 アップグレード後の環境設定

この章では、アップグレード後の環境設定について説明します。

MongoDB からデータを削除しています

Sentinel をアップグレードすると、MongoDB に保存されているデータは必要なくなります。このデータを削除して、ディスク容量を解放することができます。

ストレージ容量をクリーンアップするには :

1. Sentinel サーバに root ユーザでログインします。
2. *<sentinel_installation_path>*/opt/novell/sentinel/bin に移動します。
3. 次のスクリプトを実行します。

   ./mongoDB_cleanup.sh

Postgresql.conf ファイルの同期

アップグレード時に、以前のバージョンの postgresql.conf ファイルの名前は postgresql.conf_old に変更されます。新しい postgresql.conf ファイルが 8.3 用に作成されます。新しい postgresql.conf ファイルには、セキュリティインテリジェンスダッシュボードのパフォーマンスを向上させるための環境設定が含まれています。そのため、このファイルを

保持する必要があります。万が一、新しいファイルにカスタマイズが含まれていない場合は、新しい postgres.sql ファイルを編集します。どちらのファイルも次の場所にあります。/var/opt/novell/sentinel/3rdparty/postgresql/data/

イベント視覚化の設定

Sentinel には、データをチャート、テーブル、およびマップで表すイベント視覚化機能が備わっています。これらの視覚化機能では、イベント、IP フローイベント、およびアラートなどの大量のデータを簡単に視覚化および分析できます。また、独自の視覚化とダッシュボードも作成できます。

Sentinel では、ブラウザベースの分析および検索ダッシュボードである Kibana を使用しており、イベントの検索と視覚化に役立ちます。Kibana は、ダッシュボードにイベントを表示するため、視覚化データストア (Elasticsearch) のデータにアクセスします。デフォルトでは、Sentinel には Elasticsearch ノードが 1 つ含まれています。Elasticsearch でイベントの保存とインデックス作成を行うには、イベント視覚化を有効にする必要があります。詳細については、42 ページの 「視覚化データストアの設定」を参照してください。

セキュアクラスタ通信用の Elasticsearch の設定

Sentinel 8.4.0.0 以降には、すぐに使用できる拡張セキュリティ機能が付属しており、一部はインストール後 / アップグレード後の構成が必要になります。8.4.0.0 より、Sentinel はセキュアな方法で (SSL を介して)Elasticsearch と通信し、Elasticsearch の X-Pack プラグインをデフォルトでバンドルしています。これにより、Sentinel 管理者は、すべての**ノード**から**ノード**への Elasticsearch 通信を SSL を介して安全に設定できます。これにより、地理的に Elasticsearch ノード全体にデータが保存され、Sentinel サーバがデータを安全に受け渡して表示できるようになる可能性が広がります。この機能を使用すると、ユーザは世界中に分散しているすべての Elasticsearch クラスタに参加できます。また、Sentinel の単一の検索コンソールから結果を安全に表示して累積することができます。

重要 : アップグレードプロセスを完了するには、次の手順を実行する必要があります。このページの詳細は、古いバージョンの Sentinel からバージョン Sentinel 8.4 または Sentinel 8.5 にアップグレードする前にイベント視覚化機能が有効になっている場合にのみ適用されます。

Sentinel 8.4 から Sentinel 8.5 にアップグレードする場合、次の手順は実行しないでください。

次の手順を実行しない場合、古いバージョンからの Sentinel 8.4.0.0 以降へのアップグレードは完了せず、次の問題が発生します。

- Elasticsearch が自動的に起動されない。
- Elasticsearch を手動で再起動しない場合、Sentinel で検索中に、その中に存在するアラートおよびイベントが正しく反映されない。

外部の Elasticsearch クラスタセットアップがない場合の、Sentinel サーバと事前バンドルされた Elasticsearch 間のセキュア通信の有効化

このセクションは、Sentinel に関連付けられている外部の Elasticsearch クラスタがない場合に必要です。このような場合は、Sentinel と事前バンドルされた Elasticsearch 間のセキュア通信を有効にする必要があります。

1 次のコマンドを使用して、内部の Elasticsearch サービスを停止します。

```
rcsentinel stopES
```

2 novell ユーザに切り替えます。

```
su novell
```

Java バージョンが 292 の場合は、手順 3 と 4 を実行します。OS レベルで java バージョンを見つけるには、コマンドプロンプトで java -version を実行します。

3 (条件による)JAVA_HOME を Sentinel JDK バンドルに設定します。

```
JAVA_HOME=/opt/novell/sentinel/jdk
```

4 (条件による)java の PATH を、Sentinel JDK の場所に設定します。

```
PATH=$JAVA_HOME/bin:$PATH
```

5 Sentinel ノードでクラスタの認証局 (CA) を生成します。Sentinel の Elasticsearch ホームディレクトリ <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch で次のコマンドを実行します。

```
./bin/elasticsearch-certutil ca
```

CA 証明書のファイル名とパスワードの入力を求められます。デフォルトのファイル名は elastic-stack-ca.p12 です。

6 Sentinel の事前バンドルされた Elasticsearch ノードの証明書と秘密鍵を生成します。この場合、Sentinel の Elasticsearch ホームディレクトリ <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch で次のコマンドを実行します。

```
./bin/elasticsearch-certutil cert --ca <CA certificate filename>.p12 --
out config/certs/node-1.p12
```

CA 証明書のパスワードを入力するように求められます。また、生成された証明書のパスワードを作成するよう求めるプロンプトも表示されます。

7 Sentinel ノードの <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.yml ファイルに次の設定を追加します。

- xpack.security.transport.ssl.enabled: true
- xpack.security.transport.ssl.keystore.path: certs/node-1.p12
- xpack.security.transport.ssl.truststore.path: certs/node-1.p12
- xpack.security.transport.ssl.verification_mode: 証明書

8 上記で生成された Truststore およびキーストア証明書ファイルのパスワードを、Elasticsearch キーストアに保存します。この場合、Elasticsearch ホームディレクトリで、次のコマンドを実行します : Sentinel の <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch:

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.truststore.secure_password
```

9 次のコマンドを使用して、Elasticsearch サービスを開始します。

```
rcsentinel startES
```

外部の Elasticsearch クラスタセットアップがある場合に、外部の Elasticsearch ノード間および Sentinel と Elasticsearch クラスタ間のセキュア通信を有効にする

Sentinel の最新リリースでは、Sentinel サーバと外部の Elasticsearch クラスタ間、および Elasticsearch クラスタの異なるノード間の安全な通信が可能です。このセクションでは、Sentinel サーバに外部の Elasticsearch クラスタが接続されている場合に、これらの安全な設定を有効にする手順について説明します。

1 **Elasticsearch ノード間のクラスタ内通信をセキュリティ保護するための手順は、次のとおりです。**

1. すべてのノードで Elasticsearch を停止します。
2. novell ユーザに切り替えます。

   ```
   su novell
   ```

   Java バージョンが 292 の場合は、手順 3 と 4 を実行します。OS レベルで java バージョンを見つけるには、コマンドプロンプトで java -version を実行します。
3. (条件による)JAVA_HOME を Sentinel JDK バンドルに設定します。

   ```
   JAVA_HOME=/opt/novell/sentinel/jdk
   ```
4. (条件による)java の PATH を、Sentinel JDK の場所に設定します。

   ```
   PATH=$JAVA_HOME/bin:$PATH
   ```
5. Sentinel ノードでクラスタの認証局 (CA) を生成します。Sentinel の Elasticsearch ホームディレクトリ <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch で次のコマンドを実行します。

   ```
   ./bin/elasticsearch-certutil ca
   ```

   CA 証明書のファイル名とパスワードの入力を求められます。デフォルトのファイル名は elastic-stack-ca.p12 です。
6. Sentinel の事前バンドルされた Elasticsearch ノードの証明書と秘密鍵を生成します。この場合、Sentinel の Elasticsearch ホームディレクトリ <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch で次のコマンドを実行します。

```
./bin/elasticsearch-certutil cert --ca <CA certificate
filename>.p12 --out config/certs/node-1.p12
```

CA 証明書のパスワードを入力するように求められます。また、生成された証明書のパスワードを作成するよう求めるプロンプトも表示されます。

7. Sentinel ノードの <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/elasticsearch.yml ファイルに次の設定を追加します。
   - xpack.security.transport.ssl.enabled: true
   - xpack.security.transport.ssl.keystore.path: certs/node-1.p12
   - xpack.security.transport.ssl.truststore.path: certs/node-1.p12
   - xpack.security.transport.ssl.verification_mode: 証明書
8. 上記で生成された Truststore およびキーストア証明書ファイルのパスワードを、Elasticsearch キーストアに保存します。この場合、Sentinel の Elasticsearch ホームディレクトリ <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch で次のコマンドを実行します。

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.transport.ssl.keystore.secure_password
   ```

   ```
   ./bin/elasticsearch-keystore add
   xpack.security.transport.ssl.truststore.secure_password
   ```

9. クラスタ内のすべての外部 Elasticsearch ノードの証明書を生成します。最初に、Sentinel ノード自体ですべての外部 Elasticsearch 証明書を作成し、それぞれの Elasticsearch ノードにコピーできます。この場合、まずは Sentinel の Elasticsearch ホームディレクトリ <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch で次のコマンドを実行します。

   ```
   ./bin/elasticsearch-certutil cert --ca <CA certificate
   filename>.p12 --out config/certs/newNode.p12
   ```

   CA 証明書のパスワードを入力するように求められます。また、生成された証明書のパスワードを作成するよう求めるプロンプトも表示されます。

10. 証明書をそれぞれの外部 Elasticsearch ノードにコピーします。たとえば、newNode.p12 ファイルを外部 Elasticsearch クラスタの newNode の /etc/elasticsearch/certs/ ディレクトリにコピーします。chmod コマンドを使用して、新しいマシン上の証明書に対する読み書き可能許可を提供します。

    注 : certs ディレクトリが存在しない場合は、同じディレクトリを作成する必要があります。

    ---

11. すべての外部 Elasticsearch ノードに証明書を生成してコピーした後、すべての外部 Elasticsearch ノードの /etc/elasticsearch/elasticsearch.yml ファイルに次の設定を追加します。
    - xpack.security.enabled: true
    - xpack.security.transport.ssl.enabled: true
    - xpack.security.transport.ssl.keystore.path: certs/newNode.p12

- xpack.security.transport.ssl.truststore.path: certs/newNode.p12
- xpack.security.transport.ssl.verification_mode: 証明書

12. 外部の Elasticsearch ノードごとに、生成されたキーストアおよび Truststore 証明書ファイルのパスワードを Elasticsearch キーストアに保存します。この場合、すべての外部 Elasticsearch ノードの Elasticsearch ホームディレクトリ /usr/share/elasticsearch で次のコマンドを実行します。

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.keystore.secure_password
```

```
./bin/elasticsearch-keystore add
xpack.security.transport.ssl.truststore.secure_password
```

2 Sentinel からの Elasticsearch クラスタ通信をセキュリティ保護するために従う手順は次のとおりです。

1. novell ユーザに切り替えます。

```
su novell
```

2. 次のコマンドを実行して、Sentinel マシンから外部の Elasticsearch ノード用の http 証明書を生成します。

```
<sentinel_installation_path>/opt/novell/sentinel/bin/javacert.sh --
generateES <provide path where the http certificate should be
generated, example /opt/http.pks> <http certificate password>
<keyalias>
```

3. http 証明書を Elasticsearch ノードにコピーします。たとえば、http.pks ファイルを Elasticsearch ノードの ES_PATH_CONF/certs/ ディレクトリにコピーします。新しいマシン上の証明書に対する読み書き可能許可を提供します。

注 : certs ディレクトリが存在しない場合は、同じディレクトリを作成する必要があります。

---

4. すべての外部 Elasticsearch ノードの ES_PATH_CONF/elasticsearch.yml ファイルに次の設定を追加します。
   - xpack.security.http.ssl.enabled: true
   - xpack.security.http.ssl.keystore.path: certs/http.pks
5. すべての外部 Elasticsearch ノードの Elasticsearch ホームディレクトリ /usr/share/elasticsearch で次のコマンドを実行して、http 証明書のパスワードを Elasticsearch キーストアに保存します。

```
./bin/elasticsearch-keystore add
xpack.security.http.ssl.keystore.secure_password
```

6. 各外部 Elasticsearch ノードで Elasticsearch サービスを開始します。

```
/etc/init.d/elasticsearch start
```

3 (条件による)FIPS モードの場合は、上記の 2 つの手順を実行した後で、次の手順を実行する必要があります。

1. 次のコマンドを使用して、Sentinel のインストール中に生成された内部の Elasticsearch http 証明書を Sentinel サーバの FIPS キーストアに追加します。

   ```
   ./convert_to_fips.sh -i <sentinel_installation_path>/opt/novell/
   sentinel/3rdparty/elasticsearch/config/http.pks
   ```

2. 上記の手順の後に、Sentinel を再起動するプロンプトが表示されます。[**[いいえ]**] を選択します。
3. 手順 2 で生成された外部の Elasticsearch ノードの http 証明書をコピーし、以下のコマンドを使用して Sentinel サーバの FIPS キーストアに追加します。

   ```
   ./convert_to_fips.sh -i <location of the copied http certificate>/
   <name of the certificate>
   ```

4. 次のコマンドを実行して、外部の Elasticsearch ノードのすべての http 証明書が、Sentinel サーバの FIPS キーストアに存在するようにします。

   ```
   certutil -L -d sql:<sentinel_installation_path>/etc/opt/novell/
   sentinel/3rdparty/nss
   ```

5. Sentinel のインストール中に生成された内部の Elasticsearch http 証明書 (Sentinel サーバ内の <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks) をコピーし、次のコマンドを使用して、すべてのリモートコレクタマネージャ (RCM) の FIPS キーストアに追加します。

   ```
   ./convert_to_fips.sh -i <location of the copied http certificate>/
   http.pks
   ```

6. 上記の手順の後に、Sentinel を再起動するプロンプトが表示されます。[**[いいえ]**] を選択します。
7. 手順 2 で生成された外部の Elasticsearch ノードの http 証明書をコピーし、次のコマンドを使用して、すべての RCM の FIPS キーストアに追加します。

   ```
   ./convert_to_fips.sh -i <location of the copied http certificate>/
   <name of the certificate>
   ```

8. 次のコマンドを実行して、外部 Elasticsearch ノードのすべての http 証明書が RCM の FIPS キーストアに存在するようにします。

   ```
   certutil -L -d sql:<rcm_installation_path>/etc/opt/novell/sentinel/
   3rdparty/nss
   ```

4 Sentinel とすべての RCM を再起動します。

```
rcsentinel restart
```

FIPS モードでの http.pks 証明書の追加

Sentinel 8.4.0.0 より、Elasticsearch と Sentinel 間の通信はセキュリティ保護されています。そのため、Sentinel サーバとリモートコレクタマネージャ (RCM) の FIPS キーストアに http 証明書を追加する必要があります。

イベント視覚化が有効になっていない場合は、次の手順を実行します。

1. 以下のコマンドを使用して、Sentinel のインストール中に生成された内部の Elasticsearch http 証明書を Sentinel サーバの FIPS キーストアに追加します。

   ```
   ./convert_to_fips.sh -i <sentinel_installation_path>/opt/novell/
   sentinel/3rdparty/elasticsearch/config/http.pks
   ```

2. 次のコマンドを使用して、内部の Elasticsearch http 証明書 (<sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks) をすべての RCM にコピーし、FIPS キーストアにインポートします。

   ```
   ./convert_to_fips.sh -i <path of the certificate copied above>/http.pks
   ```

IP フローデータ収集の設定

Sentinel は、IP フローデータを収集することによって、企業のネットワークの監視に役立つ、ArcSight SmartConnectors を活用します。SmartConnector は、IP フローデータをイベントとして収集するため、EPS 数と見なされます。これにより、次の作業が可能になります。

- 既存のコレクタマネージャインスタンスを使用して IP フローデータを収集します。
- 視覚化、イベントルーティング、データフェデレーション、レポート、および相関など、Sentinel のいくつかの領域で IP フローデータを利用します。
- データ保持ポリシーを IP フローデータに適用します。これにより、必要な期間、このデータを保存できます。

IP フロー機能がデフォルトで有効になりました。IP フローデータを収集するには、ArcSight SmartConnector をインストールして設定する必要があります。

Sentinel には、NetFlow ビューなどの NetFlow 機能が含まれなくなりました。IP フローデータをイベントとして収集する SmartConnector を使用すると、既存のコレクタマネージャを使用して NetFlow データを収集できます。したがって、NetFlow データを収集するために NetFlow コレクタマネージャインスタンスが不要になります。そのため、既存の NetFlow コレクタマネージャインスタンスはすべてアンインストールできます。

- 195 ページの 「IP フローデータを収集する SmartConnectors の設定」
- 195 ページの 「既存の NetFlow コレクタマネージャのアンインストール」

IP フローデータを収集する SmartConnectors の設定

ArcSight SmartConnector をインストールして設定します。設定時に、IP フローデータを収集する関連 SmartConnector を忘れずに設定します。

SmartConnector の設定方法の詳細については、Sentinel プラグイン Web サイトの汎用 Universal CEF コレクタのマニュアルを参照してください。

既存の NetFlow コレクタマネージャのアンインストール

既存の NetFlow コレクタマネージャをアンインストールするには :

1. NetFlow コレクタマネージャのインストールに使用したものと同じユーザ権限を使用して、NetFlow コレクタマネージャコンピュータにログインします。
2. 以下のディレクトリに変更します。

   `/opt/novell/sentinel/setup`
3. 次のコマンドを実行します。

   `./uninstall-sentinel`
4. [y] を入力して、Collector Manager をアンインストールします。

   スクリプトはまずサービスを停止してから、コレクタマネージャを完全にアンインストールします。

JDBC DB2 ドライバの追加

Sentinel のアップグレード後には、次の手順を実行して、正しい JDBC ドライバを追加し、データ収集とデータ同期が行われるように JDBC ドライバを設定します。

1. /opt/novell/sentinel/lib フォルダに、お使いの DB2 データベースのバージョンに適する IBM DB2 JDBC ドライバ (db2jcc-*.jar) のバージョンをコピーします。
2. ドライバファイルに必要な所有権およびアクセス権を設定してください。
3. データ収集用にこのドライバを構成します。詳細については、データベースコネクタのマニュアルを参照してください。

Sentinel アプライアンスのデータフェデレーションプロパティの設定

Sentinel アプライアンスのアップグレード後に、次の手順を実行して、複数の NIC が構成されている環境でデータフェデレーションがエラーを表示しないようにします。

1. 許可リクエスタサーバで、次のプロパティを /etc/opt/novell/sentinel/config/configuration.properties ファイルに追加します。

   sentinel.distsearch.console.ip=< 許可リクエスタの IP アドレスの 1 つ >

2 データソースサーバで、次のプロパティを /etc/opt/novell/sentinel/config/configuration.properties ファイルに追加します。

sentinel.distsearch.target.ip=< データソースの IP アドレスの 1 つ >

3 Sentinel を再起動します。

rcsentinel restart

4 許可リクエスタサーバにログインし、［統合］をクリックします。追加するデータソースが既に存在する場合、それを削除してから、ステップ 2 で指定した IP アドレスの 1 つを使用して追加しなおします。

同じように、許可リクエスタを、ステップ 1 で指定した IP アドレスを使用して追加します。

更新のための Sentinel アプライアンスの登録

オペレーティングシステムをアップグレードした場合に Sentinel と最新のオペレーティングシステムの更新を受信するには、Sentinel アプライアンスを再登録する必要があります。既存の登録キーを使用して、更新を再登録できます。アプライアンスを登録するには、「95 ページの 「アップデートの登録」」を参照してください。

データの同期のための外部データベースの更新

Sentinel 8.x 以降、メッセージ (msg) イベントフィールドのサイズは 4000 から 8000 文字に拡大され、フィールド内にさらに情報を追加できるようになりました。

Sentinel の以前のバージョンでメッセージ (msg) イベントフィールドを外部データベースと同期するデータの同期ポリシーを作成した場合は、それに合わせて外部データベースに適切にマッピングされた列のサイズも拡大する必要があります。

注 : 上記の手順は、Sentinel の以前のバージョンを 8.x にアップグレードする場合にのみ適用されます。

他の統合された製品から Sentinel にデータを送信するユーザの許可の更新

Sentinel 8.2 SP1 以降では、指定されたユーザのみが、Change Guardian または Secure Configuration Manager から Sentinel にイベントおよび添付ファイルを送信できるようにする新しい許可、イベントおよび添付ファイルの送信を提供しています。Sentinel 8.2 SP1 以降にアップグレードすると、Sentinel は自動的にこの権限を管理者の役割を持つユーザに割り当てます。Sentinel にイベントまたは添付ファイルを送信する管理者以外のユーザに対

しては、この許可を手動で割り当てる必要があります。この許可を割り当てない限り、Sentinel は Change Guardian または Secure Configure Manager からのイベントまたは添付ファイルを受信しなくなります。

この許可の更新は、Sentinel が Change Guardian または Secure Configuration Manager に統合されている場合にのみ適用されます。詳細については、『Sentinel Administration Guide』の「Creating Roles(役割の作成)」を参照してください。

キーストアパスワードの更新

chg_keystore_pass.sh スクリプトを使用すると、キーストアのパスワードを変更できます。セキュリティのベストプラクティスとして、Sentinel をアップグレードした直後にキーストアパスワードを変更します。

注 : Sentinel サーバが FIPS モードの場合は、この手順を実行しないでください。

キーストアのパスワードを変更するには、次の手順を実行します。

1. Sentinel サーバに root としてログインします。
2. ユーザを novell に切り替えます。
3. /opt/novell/sentinel/bin ディレクトリに移動します。
4. chg_keystore_pass.sh スクリプトを実行し、画面上に表示されるメッセージに従ってキーストアのパスワードを変更します。

34 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。

ソリューションパックを含め、新しい Sentinel プラグインや更新された Sentinel プラグインは、頻繁に Sentinel プラグイン Web サイトにアップロードされます。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入手するには、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 従来のストレージからのデータの移行

従来のストレージを使用する Sentinel からデータを移行すると、既存の Sentinel データとそれに注ぎ込んだ時間を無駄にせずに済みます。従来のストレージを使用する Sentinel からデータを移行するには、ソースとターゲット両方の Sentinel サーバ上の Sentinel バージョンを同じにする必要があります。たとえば、Sentinel 8.1(ソース) から Sentinel 8.2(ターゲット) にデータを移行する場合は、まず Sentinel 8.1 を Sentinel 8.2 にアップグレードしてから、データマイグレーションプロセスを開始する必要があります。

このセクションでは、既存のデータを目的のデータストアコンポーネントに移行することに関する情報を取り上げます。

35 Elasticsearch へのデータの移行

デフォルトで Sentinel は、ファイルベースの従来のストレージにデータを保存し、Sentinel サーバでローカルにデータのインデックス作成を行います。イベント視覚化を有効にすると、Sentinel は、ファイルベースの従来のストレージに加え、Elasticsearch でデータの保存とインデックスの作成を行います。ダッシュボードには、イベントの視覚化を有効にした後に処理されたイベントのみが表示されます。ファイルベースのストレージに存在する既存のイベントを表示するには、ファイルベースのストレージのデータを Elasticsearch に移行する必要があります。Elasticsearch にデータを移行する方法については、「205 ページの第 36 章「データの移行」」を参照してください。

36 データの移行

data_uploader.sh スクリプトを使用すると、データを次のいずれかのデータストレージコンポーネントに移行できます。

- **Kafka:** イベントと生データの両方を Kafka に移行できます。イベントデータと生データに対して、このスクリプトを別個に実行する必要があります。このスクリプトでは、データが Kafka トピックに移行されます。

  マイグレーション時のデータ圧縮や、データのバッチ送信など、カスタマイズ設定を指定することができます。こうしたカスタマイズ設定を指定するには、プロパティファイルを作成し、キーと値の形式で必要なプロパティを追加してください。たとえば、次のようにプロパティを追加することができます。

  compression.type=lz4

  batch.size=20000

  Kafka プロパティについては、Kafka のドキュメントを参照してください。スクリプトではこれらのプロパティが検証されないため、ユーザの判断でプロパティとその値を設定してください。

  注 : Sentinel サーバが Kafka クラスタ全体のすべての Kafka ブローカホスト名を有効な IP アドレスに解決できることを確認します。解決できるよう DNS がセットアップされていない場合、Kafka ブローカホスト名を Sentinel サーバの /etc/hosts ファイルに追加します。

- **Elasticsearch:** イベントデータだけを Elasticsearch に移行できます。データを移行する前に、イベント視覚化が有効になっていることを確認します。詳細については、111 ページの第 18 章「イベント視覚化用の Elasticsearch の設定」を参照してください。

このスクリプトでは、指定した日付範囲 (開始日と終了日) についてデータが転送されます。このスクリプトを実行すると、データマイグレーションを開始するために指定する必要がある必須およびオプションのパラメータ、および目的のデータストレージコンポーネントに使用する関連プロパティに関する情報が表示されます。

このスクリプトは、novell ユーザとして実行する必要があります。そのため、指定するデータディレクトリやファイルに対する適切な許可が novell ユーザに与えられていることを確認してください。デフォルトでは、スクリプトはプライマリストレージからデータを移行します。セカンダリストレージからデータを移行する場合は、スクリプトの実行時にセカンダリストレージの適切なパスを指定します。

データを移行する方法 :

1. Sentinel サーバに novell ユーザとしてログインします。
2. 次のスクリプトを実行します。

/opt/novell/sentinel/bin/data_uploader.sh

3 画面の指示に従い、必要なパラメータを指定してもう一度スクリプトを実行します。

移行したデータには、ターゲットサーバで設定した保持期間が割り当てられます。

データマイグレーションが完了すると、正常に移行されたパーティション、移行に失敗したパーティション、移行されたイベント数などのステータスがスクリプトによって記録されます。前日および当日の日付のパーティションについては、遅れて到着するイベントを考慮に入れて、データ転送のステータスが IN_PROGRESS になります。

データマイグレーションが正常に完了しなかった場合や、パーティションのデータマイグレーションステータスがまだ IN_PROGRESS を示している場合は、スクリプトを再度実行してください。スクリプトを再実行すると、まずステータスファイルを確認してすでに移行されたパーティションが把握され、残っているパーティションのみが移行されます。スクリプトは、トラブルシュートの目的で /var/opt/novell/sentinel/log/data_uploader.log ディレクトリにログを保持します。

VII 高可用性のための Sentinel の展開

このセクションでは、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。お客様の Sentinel 環境における高可用性と障害復旧の実装に関する詳しい情報は、テクニカルサポートにお問い合わせください。

注 : 高可用性 (HA) 環境設定は Sentinel サーバでのみサポートされています。しかし、Collector Manager instances と Correlation Engine instances は Sentinel HA サーバとも通信できます。

---

37 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。

高可用性の詳細については、『SUSE High Availability Guide』を参照してください。

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。ほとんどの HA ソリューションでは高可用性を持たせるサービス間の依存関係を実装者が宣言できますが、これはクラスタ自体で動作しているサービスにしか適用されません。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 との間でのデータの送信または受信 (あるいはその両方) 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 アドレスで設定する必要があります)。

共有ストレージ

すべての HA 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。

Sentinel における共有ストレージの使用には、2 つの基本的なアプローチがあります。1 つは、すべてのコンポーネント (アプリケーションバイナリ、環境設定、およびイベントデータ) 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。

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。

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。

38 システム要件

高可用性 (HA) 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。

- ❒ (条件による) HA アプライアンスインストールでは、有効なライセンス付きの Sentinel HA アプライアンスが使用可能であることを確認します。Sentinel HA アプライアンスは、以下のパッケージを含む ISO アプライアンスです。
  - オペレーティングシステム : SLES 12 SP5
  - SLES High Availability Extension (SLES HAE) パッケージ
  - Sentinel ソフトウェア (HA rpm を含む)
- ❒ (条件による) 従来の HA のインストールの場合は、以下のものが利用可能であることを確認します。
  - オペレーティングシステム : SLES 12 SP5 以降
  - 有効なライセンスを持つ SLES HAE の ISO イメージ
  - Sentinel インストーラ (TAR ファイル)
- ❒ (条件による) SLESオペレーティングシステム(カーネルバージョン3.0.101以降)を使用している場合、コンピュータにウォッチドッグドライバを手動でロードする必要があります。ご使用のコンピュータハードウェア用の適切なウォッチドッグドライバを見つけるには、ハードウェアベンダーに連絡してください。ウォッチドッグドライバをロードするには、以下を実行します。
  1. コマンドプロンプトで、以下のコマンドを実行し、現在のセッションでウォッチドッグドライバをロードします。

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

  2. /etc/init.d/boot.local ファイルに、次の行を追加して、毎ブート時にコンピュータが自動的にウォッチドッグドライバをロードするようにします :

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

- ❒ Sentinel サービスをホストする各クラスタノードが、37 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ことを確認します。
- ❒ 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動できるサービスに対して、仮想 IP アドレスが使用されていることを確認します。
- ❒ 共有ストレージデバイスが、37 ページの第 5 章「システム要件を満たす」に指定されているパフォーマンスおよびサイズ特性の要件を満たしていることを確認します。iSCSI Target を共有ストレージとして設定された標準 SLES 仮想マシンを使用します。

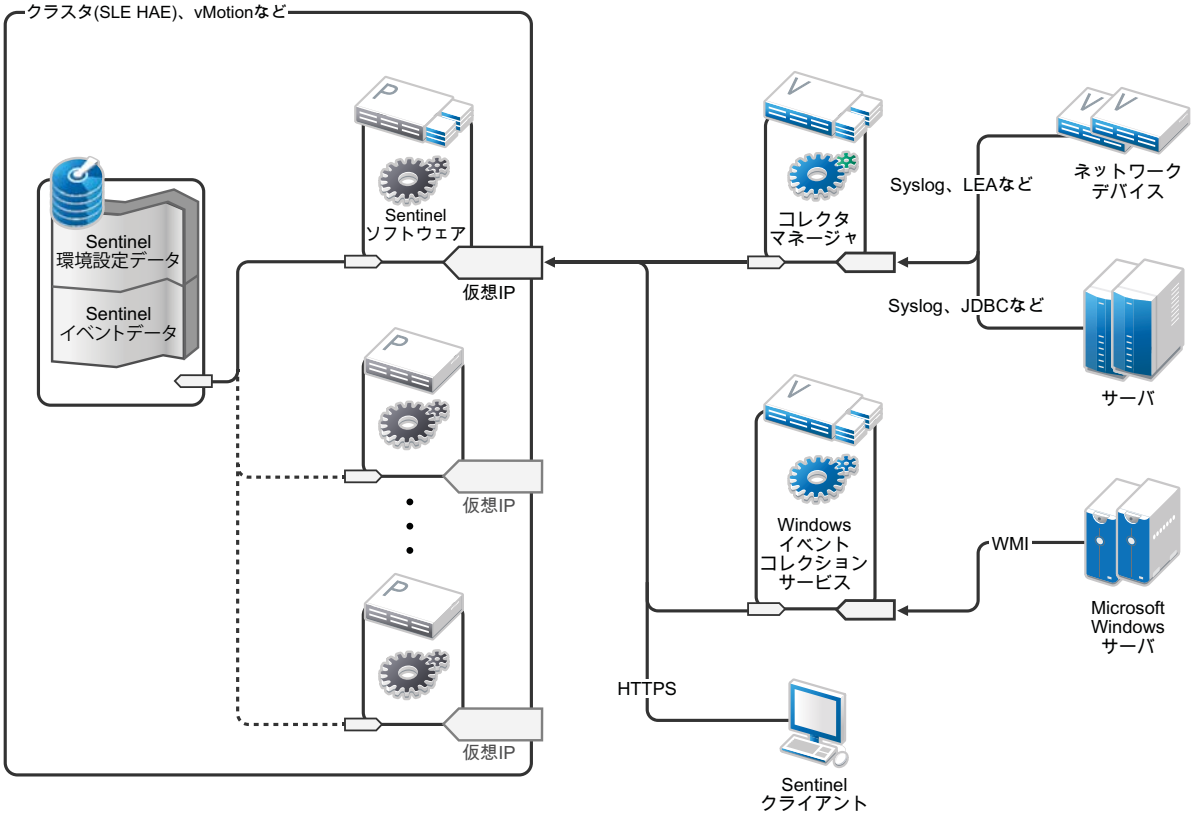
iSCSI の場合は、ハードウェアがサポートする最大のメッセージ転送単位 (MTU) を使用してください。MTU を大きくすることで、ストレージのパフォーマンスが向上します。ストレージのレイテンシと帯域幅が推奨値より遅いと、Sentinel で問題が生じる可能性があります。

- ❒ 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が少なくとも 2 つあるようにします。2 つの SLES 仮想マシンが推奨されています。
- ❒ 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) を作成しておきます。iSCSI Target に接続するために専用 IP アドレスを使用します。
- ❒ Sentinel の外部 IP アドレスの役割を果たす、クラスタ内のノード間で移行可能な仮想 IP アドレスがあることを確認します。
- ❒ 各クラスタノードにつき内部クラスタ通信用のIPアドレスが少なくとも1つあることを確認します。単一のユニキャスト IP アドレスを使用できますが、運用環境ではマルチキャストが好まれます。

39 インストールと環境設定

この章では、高可用性 (HA) 環境での Sentinel のインストールと環境設定の手順を説明します。

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。



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のお客様の要件に従って、コンピュータハードウェア、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。

次のチェックリストを使用して、初期セットアップと環境設定を行います。

	チェックリストの項目
❑	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、37 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、プライマリおよびセカンダリストレージのデータ保持ポリシーに基づいて、37 ページの第 5 章「システム要件を満たす」で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、59 ページの第 8 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。
❑	すべてのクラスタノードの時刻が同期されていることを確認します。NTP または類似のテクノロジを使って、確認することができます。
❑	◆ クラスタには、信頼できるホスト名解決が必要です。DNS 障害が発生してもクラスタが稼働を継続できるようにするために、すべての内部クラスタホスト名を /etc/hosts ファイルに入力しておきます。 ◆ ループバック IP アドレスにホスト名を割り当てることのないようにします。 ◆ オペレーティングシステムのインストール時にホスト名とドメイン名を設定する際に、[**[ホスト名をループバック IP に割り当てる]**] の選択を解除します。

次の設定を使用できます。

- (条件による) 従来の HA インストールの場合 :
  - SLES 11 SP4 または SLES 12 SP1 以降を実行する 2 つのクラスタノード VM。
  - (条件による) GUI 設定が必要な場合は、X Windows をインストールできます。X なしで起動するようにブートスクリプトを設定すると (実行レベル 3)、必要な場合にのみ起動させることができます。
- (条件による) HAアプライアンスのインストールの場合: クラスタノード仮想マシンに基づく 2 つの HA ISO アプライアンス。HA ISO アプライアンスのインストールについて詳しくは、90 ページの 「Sentinel のインストール」を参照してください。
- ノードには、外部アクセス用に 1 つの NIC、iSCSI 通信用にもう 1 つの NIC が設定されます。
- 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。SLES および SLES 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。
- 共有ストレージのために iSCSI Target を構成した、SLES 11 SP4 または SLES 12 SP1 以降を実行している 1 つの仮想マシン
  - (条件による) GUI 設定が必要な場合は、X Windows をインストールできます。X なしで起動するようにブートスクリプトを設定すると (実行レベル 3)、必要な場合にのみ起動させることができます。
  - システムには 2 つの NIC が設定されます。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使用してリモートアクセスできるような IP アドレスを外部 NIC に設定します。たとえば、「172.16.0.3 (storage03)」のように入力します。
  - オペレーティングシステム、一時スペース、Sentinel データを保持する大容量の共有ストレージのための十分なスペース、および SBD パーティションのためのいくらかのスペースを、システムに確保してください。SLES 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。

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 アドレスを使用できます。

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、物理的な接続と追加の環境設定を行うことが必要になることがあります。Sentinel はデータベースとイベントデータの格納にこの共有ストレージを使用します。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、共有ストレージのサイズが適切に設定されていることを確認します。

共有ストレージのセットアップについては、次の例を検討してください。

一般的な実装では、FibreChannel を使用して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存するために大容量 RAID アレイを設置する場合があります。低速セカンダリストレージには、別の NAS ノードまたは iSCSI ノードを使用することもできます。クラスタノードがプライマリ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。セカンダリ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、各クラスタノードでマウントをテストします。しかし、実際のストレージのマウントはクラスタ構成が処理します。

SLES 仮想マシンでホストされる iSCSI ターゲットを作成するには、次の手順を実行します。

1 storage03 (初期セットアップで作成した仮想マシン) に接続して、コンソールセッションを開始します。

2 次のコマンドを実行して、Sentinel プライマリストレージ用に、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=<file size> bs=<bit size>
```

たとえば、次のコマンドを実行して、/dev/zero 疑似デバイスからコピーしたゼロで埋めた 20GB のファイルを作成します。

```
dd if=/dev/zero of=/localdata count=20480000 bs=1024
```

3 手順 1 と 2 を繰り返し、セカンダリストレージ用のファイルを同様に作成します。

たとえば、セカンダリストレージに次のコマンドを実行します。

```
dd if=/dev/zero of=/networkdata count=20480000 bs=1024
```

注 : この例では、サイズとパフォーマンス特性が同じ 2 つのディスクを表す、2 つのファイルを作成しました。運用展開では、プライマリストレージを高速な SAN 上に作成し、セカンダリストレージを低速な iSCSI、NFS、または CIFS ボリューム上に作成することができます。

次のセクションに示す手順を実行して、iSCSI ターゲットおよびイニシエータデバイスを設定します。

- 218 ページの 「iSCSI Target の環境設定」
- 220 ページの 「iSCSI イニシエータの環境設定」

iSCSI Target の環境設定

次の手順を実行して、localdata および networkdata ファイルを iSCSI ターゲットとして設定します。

iSCSI ターゲットの設定方法の詳細については、SUSE のマニュアルの「Creating iSCSI Targets with YaST」を参照してください。

1 コマンドラインから YaST を実行します (またはグラフィカルユーザインタフェース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 アドレスになります。

6 [[次]] をクリックし、[[OK]] をクリックします。

7 (条件による) メイン画面で :

- SLES 12 SP1 以降を使用している場合は、[[ネットワークサービス]] > [[iSCSI LIO Target (iSCSI LIO ターゲット)]] を選択します。

注 : このオプションが見つからない場合は、[[Software(ソフトウェア)]] > [[Software Management(ソフトウェア管理)]] > [[iSCSI LIO Server(iSCSI LIO サーバ)]] の順に進み、iSCSI LIO パッケージをインストールします。

---

8 (条件による) 要求された場合は、必要なソフトウェアをインストールします。

- SLES 12 SP1 以降の場合 : iscsiliotarget RPM

9 (条件による)SLES 12 を使用する場合は、クラスタのすべてのノード上で次の手順を実行します。

9a iSCSI イニシエータ名を含むファイルを開くには、次のコマンドを実行します。

cat /etc/iscsi/initiatorname.iscsi

9b iSCSI イニシエータを設定するために使用されるイニシエータ名を確認します。

次に例を示します。

InitiatorName=iqn.1996-04.de.suse:01:441d6988994

これらのイニシエータ名は、iSCSI ターゲットのクライアントセットアップを設定するときに使用されます。

10 [[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。

11 [[Global (グローバル)]] タブを選択して [[認証なし]] の選択を解除して認証を有効化し、認証の送受信に必要な資格情報を指定します。

デフォルトでは [認証なし] のオプションが有効になっています。ただし、環境設定を確実にセキュリティ保護するため、認証を有効にする必要があります。

注 : Micro Focus では、iSCSI ターゲットとイニシエータに異なるパスワードを使用することをお勧めします。

---

12 [[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。

13 [[追加]] をクリックして、新しい LUN を追加します。

14 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。

15 13 と 14 の手順を繰り返して、今回は LUN 1 を追加し、/networkdata を選択します。

16 その他のオプションをデフォルトのままにし、[[次へ]] をクリックします。

17 (条件による)SLES 12 を使用している場合は、[[追加]] をクリックします。クライアント名を求められたら、手順 9 でコピーしたイニシエータ名を入力します。この手順を繰り返し、イニシエータ名を指定してすべてのクライアント名を追加します。

クライアント名のリストは、[Client List(クライアントリスト)] に表示されます。

SLES 15 以降のクライアントイニシエータ名を追加する必要はありません。

18 (条件による) 手順 11 で認証を有効にした場合は、認証の資格情報を指定します。

クライアントを選択し、[[Edit Auth (認証の編集)]] > [[Incoming Authentication (着信認証)]] の順に選択し、ユーザ名とパスワードを指定します。すべてのクライアントについて、この手順を繰り返します。

19 [[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。

20 YaST を終了します。

注 : 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。

---

iSCSI イニシエータの環境設定

iSCSI イニシエータデバイスをフォーマットするには、次の手順を実行します。

iSCSI イニシエータの設定の詳細については、SUSE マニュアルの「Configuring the iSCSI Initiator」を参照してください。

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 アドレスになります。

6 [[次]] を選択して、[[OK]] をクリックします。

7 [[Network Services (ネットワークサービス)]] > [[iSCSI Initiator]] の順にクリックします。

8 要求があれば、必要なソフトウェア (iscsiclient 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 ターゲット IP アドレス (10.0.0.3) を指定します。

(条件による) 218 ページの 「iSCSI Target の環境設定」 の手順 11 で認証を有効にした場合は、[[認証なし]] の選択を解除します。[[Outgoing Authentication (送信認証)]] フィールドで、iSCSI ターゲット環境設定で設定したユーザ名とパスワードを入力します。

[次へ] 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 次の手順を実行します。

13a [[スタートアップ]] ドロップダウンメニューで [Automatic(自動)] に切り替えます。

13b (条件による) 認証を有効にした場合は、[[認証なし]] の選択を解除します。

手順 11 で指定したユーザ名とパスワードが [[Outgoing Authentication (送信認証)]] セクションに表示されます。これらの資格情報が表示されない場合は、このセクションで資格情報を入力します。

13c [次へ] 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 [システム] ビューに、次のタイプ (/dev/sdb および /dev/sdc など) の新しいハードディスクがリストに表示されます。

- SLES 11 SP4 の場合 : IET-VIRTUAL-DISK
- SLES 12 SP1 以降の場合 : LIO-ORG-FILEIO

リストの先頭 (プライマリストレージのはずです) にタブを切り替えて、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。

フォーマット済みディスク (/dev/sdb1 など) の準備が完了します。これは、以下の手順では /dev/<SHARED1> と呼ばれます。

20 [[パーティショナ]] に戻り、/dev/sdc またはセカンダリストレージに対応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 を終了します。

22 (条件による) 従来の HA インストールを実行している場合、マウントポイントを作成し、以下のようにローカルパーティションのマウントをテストします (正確なデバイス名は、特定の実装によって異なります)。

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

新しいパーティション上でファイルを作成したり、パーティションがマウントされているファイルを表示したりできるはずです。

23 (条件による) 従来の HA インストールを実行している場合にアンマウントするには、以下を行います。

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

24 (条件による) HA アプライアンスのインストールの場合、手順 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ようにします。クラスタノードごとに、手順 5 のノード IP アドレスを異なる IP アドレスに置き換えます。

25 (条件による) 従来の HA インストールの場合、手順 1 ～ 15、22、23 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ようにします。クラスタノードごとに、手順 6 のノード IP アドレスを異なる IP アドレスに置き換えます。

Sentinel のインストール

Sentinel のインストールには 2 つのオプションがあります。1 つは、--location オプションを使用して、Sentinel のすべての部分を共有ストレージにインストールし、Sentinel インストール環境を共有ストレージがマウントされた場所にリダイレクトさせる方法です。もう 1 つは、可変アプリケーションデータのみを共有ストレージにインストールする方法です。

Sentinel をホスト可能な各クラスタノードにインストールします。Sentinel を初めてインストールした後に、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め、完全インストールを実行する必要があります。その他のクラスタノードへの後続のインストールでは、アプリケーションのみをインストールします。共有ストレージをマウントすると、Sentinel データが利用可能になります。

最初のノードインストール

- 222 ページの 「従来の HA インストール」
- 223 ページの 「Sentinel HA アプライアンスのインストール」

従来の HA 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 以下の各ステップを実行し、インストールを開始します。

3a 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
```

3b 環境設定の方法を選択するよう要求されたら、2 を指定してカスタム環境設定を選択します。

3c FIPS モードを有効にする場合は、外部証明書の入力を求めるプロンプトが表示されたら、Elasticsearch http 証明書 <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks のパスを追加します。

4 インストールを最後まで実行し、製品の環境設定を適切に行います。

5 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 アドレスを使用して製品にアクセスできます。

6 次のコマンドを使用して、Sentinel をシャットダウンし、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
```

Sentinel HA アプライアンスのインストール

Sentinel HA アプライアンスには、既にインストールされて環境設定されている Sentinel ソフトウェアが含まれています。HA 用に Sentinel ソフトウェアを環境設定するには、以下のステップを実行します。

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 以下のディレクトリを選択します。

```
cd /opt/novell/sentinel/setup
```

3 環境設定を記録します。

3a 次のコマンドを実行します :

```
./configure.sh --record-unattended=/tmp/install.props --no-start
```

このステップでは、install.props ファイルに環境設定を記録します。このファイルは、install-resources.sh スクリプトを使用してクラスタリソースを環境設定するのに必要です。

3b 環境設定の方法を選択するよう要求されたら、2 を指定してカスタム環境設定を選択します。

3c パスワードを要求されたら、2 を指定して新しいパスワードを入力します。

1 を指定すると、install.props ファイルにパスワードは保管されません。

3d FIPS モードを有効にする場合は、外部証明書の入力を求めるプロンプトが表示されたら、Elasticsearch http 証明書 <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/config/http.pks のパスを追加します。

4 以下のコマンドを使用して、Sentinel をシャットダウンします。

```
rcsentinel stop
```

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。

```
insserv -r sentinel
```

5 次のコマンドを使用して、Sentinel データフォルダを共有ストレージに移動します。この移動により、ノードは共有ストレージを介して Sentinel データフォルダを利用できます。

```
mkdir -p /tmp/new
```

```
mount /dev/<SHARED1> /tmp/new
```

```
mv /var/opt/novell/sentinel/* /tmp/new
```

```
umount /tmp/new/
```

6 次のコマンドを使用して、共有ストレージへの Sentinel データフォルダの移動を検証します。

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

```
umount /var/opt/novell/sentinel
```

SMT でのアプライアンスの設定

次の手順を実行して SMT でアプライアンスを設定します。

1 SMT サーバで次のコマンドを実行して、アプライアンスのリポジトリを有効にします。

```
smt-repos -e Sentinel-Server-HA-8-OS-Updates sle-12-x86_64
```

```
smt-repos -e Sentinel-Server-HA-8-Prod-Updates sle-12-x86_64
```

2 「SMT のマニュアル」の「Configuring Clients to Use SMT」セクションで説明されている手順を実行して、SMT でアプライアンスを設定します。

後続のノードインストール

- 225 ページの 「従来の HA インストール」
- 225 ページの 「Sentinel HA アプライアンスのインストール」

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。

従来の HA インストール

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

cd sentinel_server*

./install-sentinel --no-start --cluster-node --unattended=/tmp/
install.props

insserv -r sentinel
```

Sentinel HA アプライアンスのインストール

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 :

```
insserv -r sentinel
```

3. Sentinel サービスを停止します。

```
rcsentinel stop
```

4. Sentinel ディレクトリを削除します。

```
rm -rf /var/opt/novell/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。

HA モードでの RCM/RCE の接続

従来の HA

新しいセットアップと既存のセットアップの両方について、従来の HA モードで RCM/RCE を接続するには、次の手順を実行します。

1. RCM/RCE をインストール / 設定する前に、RCM/RCE ボックスの /etc/hosts ファイルに、以下のようなエントリを追加します。

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   例 : 164.99.87.27 first_active_host.dom.name first_active_host

   重要 : configure.sh を実行する前に、このエントリが /etc/hosts ファイルで指定された HA 環境で最初に正常に成功した適切なアクティブノードのホスト名と常に一致することを確認してください。

2. RCM/RCE をサーバに接続する時に、プロンプトで仮想 IP を指定します。

   重要 : 最初に成功したアクティブノードはダウンし、もう一方のノードは現在アクティブですが、/etc/hosts ファイル内の仮想 IP で最初に成功したアクティブノード名を使用します。

アプライアンス HA

新しいセットアップのためにアプライアンス HA モードで RCM/RCE を接続するには、次の手順を実行します。

- HA クラスタ内で最初に成功したアクティブノードのホスト名のみを使用します。

既存のセットアップのために RCM/RCE をアプライアンス HA モードで接続するには、次の手順を実行します。

1. RCM/RCE をインストール / 設定する前に、RCM/RCE ボックスの /etc/hosts ファイルに、以下のようなエントリを追加します。

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   例 : 164.99.87.27 first_active_host.dom.name first_active_host

   重要 : configure.sh を実行する前に、このエントリが /etc/hosts ファイルで指定された HA 環境で最初に正常に成功した適切なアクティブノードのホスト名と常に一致することを確認してください。

2. RCM/RCE をサーバに接続する時に、プロンプトで仮想 IP を指定します。

重要 : 最初に成功したアクティブノードはダウンし、もう一方のノードは現在アクティブですが、/etc/hosts ファイル内の仮想 IP で最初に成功したアクティブノード名を使用します。

クラスタインストール

クラスタソフトウェアは、従来の高可用性 (HA) インストール環境にのみインストールする必要があります。Sentinel HA アプライアンスにはクラスタソフトウェアが含まれており、手動でのインストールは必要ありません。

次の手順で、SLES High Availability Extension に Sentinel 固有のリソースエージェントオーバーレイを指定して設定します。

1. 各ノードにクラスタソフトウェアをインストールします。
2. 各ノードクラスタをクラスタマネージャに登録します。
3. クラスタ管理コンソールに各クラスタノードが表示されることを確認します。

注 : 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。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を監視する同様のソリューションを開発する必要があります。独自に開発する場合は、Sentinel ダウンロードパッケージの Sentinelha.rpm ファイルに格納されている既存のリソースエージェントを確認してください。

4. SLE HAE 資料に従って、コアとなる SLE HAE ソフトウェアをインストールします。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。
5. すべてのクラスタノードに対してステップ 4 を繰り返します。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。
6. 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します。この HA RPM は、Sentinel をインストールする際に解凍したデフォルトの Sentinel ダウンロードに保存されている、novell-Sentinelha-<*Sentinel_version*>*.rpm に含まれています。
7. 各クラスタノードで、novell-Sentinelha-<*Sentinel_version*>*.rpm ファイルを /tmp ディレクトリにコピーしてから、次のコマンドを実行します。

```
cd /tmp
rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

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。この環境設定の一環として、クラスタの整合性を確保するために、フェンシングと Shoot The Other Node In The Head (STONITH) リソースを設定することもできます。

重要 : このセクションで説明する手順には、rcopenais および openais コマンド (SLES 11 SP4 でのみ動作) を使用します。SLES 12 SP2 以降の場合は、systemctl pacemaker.service コマンドを使用してください。

たとえば、/etc/rc.d/openais start コマンドについては、systemctl start pacemaker.service コマンドを使用します。

次の手順でクラスタの設定を行います。

この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に対する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する必要があります。また、共有ストレージをホストしているのと同じ SLES 仮想マシンで、iSCSI ターゲットをフェンシングのための SBD デバイスとして機能するように設定して使用する必要もあります。

SBD のセットアップ

1. storage03 に接続して、コンソールセッションを開始します。次のコマンドを実行して、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=<*file size*> bs=<*bit size*>

   たとえば、次のコマンドを実行して、/dev/zero 疑似デバイスからコピーしたゼロで埋めた 1MB のファイルを作成します。

   ```
   dd if=/dev/zero of=/sbd count=1024 bs=1024
   ```

2. コマンドラインまたはグラフィカルユーザインタフェースから YaST を実行します : /sbin/yast
3. [**[ネットワークサービス]**]、[**[iSCSI ターゲット]**] の順に選択します。
4. [**[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。
5. [**[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。
6. [**[追加]**] を選択して、新しい LUN を追加します。
7. 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。
8. 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。
9. [**[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 を終了します。

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 アドレスとそのホスト名がリストされています。また、ループバック IP アドレスにホスト名を割り当てることのないようにします。

次の手順を行うことにより、IP アドレス 10.0.0.3 (storage03) のサーバの 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]** 起動オプションはそのままにし、[**[No Authentication(認証なし)]**] の選択は解除します)。
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 を終了します。
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. (条件による) 次のコマンドのいずれかを実行します。
    - SLES 11 SP4 を使用する場合 :

      sleha-init
    - SLES 12 SP1 以降を使用する場合 :

      ha-cluster-init
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 アドレス (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. (条件による) 次のプロンプトが表示されたら、N を入力します。

    ```
    Do you wish to configure an administration IP? [y/N]
    ```

    管理 IP アドレスを設定するには、「232 ページの 「リソースの環境設定」」の際に仮想 IP アドレスを指定します。
15. 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。
16. YaST を起動します。

17 [[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)。

18 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。

19 設定の最上部行に移動し、[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)。

20 [[Add a Member Address(メンバーアドレスを追加)]] 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。

21 (条件による) 認証を有効にしていない場合は、左側のパネルから [[セキュリティ]] を選択して、[[セキュリティ認証を有効にする]] をオフにします。

22 [[完了]] をクリックして設定を完了します。

23 YaST を終了します。

24 コマンドの /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 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] 起動オプションはそのままにし、[[No Authentication(認証なし)]] の選択は解除します)。

6 [[OK]] を選択して、iSCSI イニシエータツールを終了します。

7 (条件による) 次のコマンドのいずれかを実行します。

- SLES 11 SP4 を使用する場合 :

  sleha-join

- SLES 12 SP1 以降を使用する場合 :

  ha-cluster-join

8 最初のクラスタノードの IP アドレスを入力します。

(条件による) クラスタが正常に起動しない場合は、次の手順を実行します。

1 crm status コマンドを実行して、ノードが結合されているかどうかを確認します。ノードが結合されていない場合、クラスタ内のすべてのノードを再起動します。

2 /etc/corosync/corosync.conf ファイルを node01 から node02 に手動でコピーするか、node01 で csync2 -x -v を実行するか、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。

3 (条件による) 手順 1 で実行した csync2 -x -v コマンドですべてのファイルを同期できない場合、次の手順を実行します。

3a すべてのノードで、/var/lib/csync2 ディレクトリの csync2 データベースをクリアします。

3b 次のように、すべてのノード上で csync2 データベースがファイルシステムと一致するよう更新しますが、他のサーバとの同期が必要というマークは何にも付けません。

```
csync2 -cIr /
```

3c アクティブなノードで、次の手順に従います。

3c1 アクティブノードとパッシブノード間のすべての相違点を探し、それらの違いに同期のマークを付けます。

```
csync2 -TUXI
```

3c2 アクティブノードが衝突を強制的に上書きするため、データベースをリセットします。

```
csync2 -fr /
```

3c3 その他のすべてのノードで同期を開始します。

```
csync2 -xr /
```

3d すべてのノードで、すべてのファイルが同期されていることを検証します。

```
csync2 -T
```

このコマンドは、同期されていないファイルのみをリストします。

4 node02 上で次のコマンドを実行します。

Sles 11 SP4 の場合 :

```
/etc/rc.d/openais start
```

SLES 12 SP1 以降の場合 :

```
systemctl start pacemaker.service
```

(条件による) xinetd サービスが新しい csync2 サービスを正しく追加しないと、スクリプトは正常に機能しません。もう一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、xinetd サービスが必須です。csync2 run failed 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。

この問題を解決するには、kill -HUP `cat /var/run/xinetd.init.pid コマンドを実行してから、sleha-join スクリプトを再実行します。

5 各クラスタノードで crm_mon を実行して、クラスタが正常に稼働しているかどうかを確認します。「hawk」という Web コンソールを使用して、クラスタを確認することもできます。デフォルトのログイン名は hacluster で、パスワードは linux です。

(条件による) 環境に応じて、次のタスクを実行してさらにパラメータを変更します。

1 2 ノードクラスタの環境で起きた 1 つのノードの障害がクラスタ全体を予期せず停止させないように、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。

```
crm configure property 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。

リソースの環境設定

リソースエージェントはデフォルトで SLE HAE に付属しています。SLE HAE を使用しない場合は、代替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 アドレスに相当する IP アドレスリソース。
- 環境設定とイベントメタデータを保存する PostgresSQL データベースソフトウェア。

次の手順でリソースの設定を行います。

crm スクリプトは、クラスタ設定に役立ちます。このスクリプトは、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、またはリソースの環境設定を変更する場合は、それぞれに応じて次の手順でスクリプトを編集できます。

1 Sentinel をインストールした元のノードに接続します。

注 : このノードは、Sentinel の完全インストールを実行したノードである必要があります。

2 スクリプトの内容を次のように編集します。<SHARED1> は以前に作成した共有ボリュームです。

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

cd /usr/lib/ocf/resource.d/novell

./install-resources.sh
```

3 (条件による) クラスタに新しいリソースが加わった場合に、問題が起きることがあります。この問題が起きた場合は、node02 上で次のコマンドを実行します。

Sles 11 SP4 の場合 :

/etc/rc.d/openais start

Sles 12 SP1 の場合 :

systemctl start pacemaker.service

4 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 アドレス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。

5 ご使用の環境がこの推奨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型定義を変更してください。たとえば、推奨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 リソースを使用する場合もあります。

6 シェルスクリプトを実行した後、crm status 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
```

7 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。

セカンダリストレージ設定

Sentinel がイベントパーティションをより安価なストレージに移動できるようにセカンダリストレージを環境設定するには、次の手順を実行します。

注 : この手順はオプションであり、システムの他のストレージを設定したのと同じようにセカンダリストレージを高可用性にする必要はありません。SAN、非 SAN、NFS、または CIFS ボリュームからマウントされている任意のディレクトリを使用できます。

---

1 Sentinel Main インタフェースのトップメニューバーで、[**[ストレージ]**] をクリックします。

2 [**[環境設定]**] を選択します。

3 未設定のセカンダリストレージのラジオボタンを 1 つ選択します。

シンプルな iSCSI Target をネットワーク共有ストレージの場所として使用します。設定はプライマリストレージとほぼ同じです。運用環境では、ストレージテクノロジが異なる場合があります。

以下の手順に従って、Sentinel が使用するセカンダリストレージを設定します。

注 : iSCSI Target の場合、ターゲットはセカンダリストレージとして使用するディレクトリとしてマウントされます。プライマリストレージのファイルシステムを環境設定したような方法で、マウントをファイルシステムリソースとして環境設定する必要があります。異なる設定が指定される可能性もあるため、この設定がリソースインストールスクリプトの一部として自動で設定されることはありません。

1. 上記のステップを確認して、セカンダリ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>、または /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。Sentinel Main インタフェースを使用するかまたは次の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 Main 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、未設定のセカンダリストレージの [**[SAN (ローカルにマウント)]**] を選択します。
7. セカンダリストレージがマウントされているパスを、たとえば /var/opt/netdata のように入力します。

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、単純な必須リソースを使用します。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。

40 高可用性の Sentinel のアップグレード

HA 環境で Sentinel をアップグレードする場合は、まず、クラスタ内のパッシブノードをアップグレードしてから、アクティブクラスタノードをアップグレードする必要があります。

前提条件

- ダウンロード Web サイトから最新のインストーラをダウンロードします。
- SLESオペレーティングシステム(カーネルバージョン3.0.101以降)を使用している場合、コンピュータにウォッチドッグドライバを手動でロードする必要があります。ご使用のコンピュータハードウェア用の適切なウォッチドッグドライバを見つけるには、ハードウェアベンダーに連絡してください。ウォッチドッグドライバをロードするには、以下を実行します。
  1. コマンドプロンプトで、以下のコマンドを実行し、現在のセッションでウォッチドッグドライバをロードします。

     /sbin/modprobe -v --ignore-install <*watchdog driver name*>
  2. 以下の行を /etc/init.d/boot.local ファイルに追加し、コンピュータが各ブート時にウォッチドッグドライバを自動的にロードするようにします。

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

従来の Sentinel HA のアップグレード

このセクションの手順では、従来の Sentinel HA およびオペレーティングシステムのアップグレードについて説明します。

Sentinel 8.3.0.0 以降は、MongoDB ではなく PostgreSQL を使用してセキュリティインテリジェンスデータおよびアラートデータを保存するようになりました。

重要 : Sentinel 8.3.0.0 の以前のバージョンからアップグレードする場合は、以下の手順が適用されます。

アップグレードプロセスでは、アクティブノードで次の処理が実行されます。

- セキュリティインテリジェンスデータ、アラートデータなどを MongoDB から PostgreSQL に移行する。

Sentinel は、セキュリティインテリジェンスデータおよびアラートデータを MongoDB ではなく PostgreSQL に保存するようになりました。アップグレードプロセスでは、まずこのデータを PostgreSQL に移行します。正常に終了した場合、アップグレードが自動的に実行されます。データマイグレーションに失敗した場合は、Sentinel をアップグレードできません。

- データおよび MongoDB 関連の RPM を削除するために使用できるクリーンアップスクリプトを生成します。

MongoDB に格納されているデータはバックアップとして保持され、Sentinel をアップグレードした後に削除することができます。

- 236 ページの 「Sentinel HA のアップグレード」
- 238 ページの 「オペレーティングシステムのアップグレード」

Sentinel HA のアップグレード

1 クラスタの保守モードを有効にします。

crm configure property maintenance-mode=true

保守モードは、Sentinel をアップデートする際、稼働中のクラスタリソースに影響を与えないようにするのに役立ちます。このコマンドは、どのクラスタノードからでも実行することができます。

2 保守モードがアクティブかどうか確認します。

```
crm status
```

クラスタリソースは非管理状態と表示されるはずです。

3 パッシブクラスタノードをアップデートします。

3a クラスタスタックを停止します。

```
rcpacemaker stop
```

クラスタスタックを停止することで、クラスタリソースをアクセス可能に保ち、ノードのフェンシングを避けることができます。

3b 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。

3c 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>
```

3d インストールファイルを抽出したディレクトリで、次のコマンドを実行します。

```
./install-sentinel --cluster-node
```

3e アップグレード完了後、クラスタスタックを再起動します。

```
rcpacemaker start
```

すべてのパッシブクラスタノードに対して 236 ページのステップ 3a から 236 ページのステップ 3e を繰り返します。

3f 自動起動スクリプトを削除して、クラスタが製品を管理できるようにします。

```
cd /

insserv -r sentinel
```

4 アクティブなクラスタノードをアップグレードします。

4a 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。

データのバックアップの詳細については、『「Sentinel Administration Guide」』の「*Backing Up and Restoring Data*」を参照してください。

4b クラスタスタックを停止します。

```
rcpacemaker stop
```

クラスタスタックを停止することで、クラスタリソースをアクセス可能に保ち、ノードのフェンシングを避けることができます。

4c 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。

4d 次のコマンドを実行して、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>
```

4e インストールファイルを抽出したディレクトリで、次のコマンドを実行します。

```
./install-sentinel
```

4f **重要 :** Sentinel 8.3.0.0 の以前のバージョンからアップグレードする場合は、以下の手順が適用されます。

4f1 必要なマイグレーションオプションを選択します。

警告 : アップグレードが正常に終了した後にこの手順を繰り返すことはできないため、適切なオプションを選択していることを確認してください。

データが正常に移行されると、アップグレードプロセスは自動的にアップグレードを実行します。

アップグレードプロセスでは、MongoDB に格納されているデータをバックアップとして保持します。

4f2 (条件による) データマイグレーションに失敗した場合 :

4f2a 正常にマイグレートされなかったデータをクリーンアップします。詳細については、183 ページの 「マイグレーションが失敗した場合の PostgreSQL 内のデータのクリーンアップ」を参照してください。

4f2b (条件による)Sentinel が自動的に起動されない場合は、Sentinel を起動します。

```
rcsentinel start
```

4f2c (条件による) アップグレードの前に、イベント視覚化が有効になっている場合、Sentinel 8.4.0.0 にアップグレードした後、Elasticsearch は X-Pack セキュリティプラグインで有効になっているため停止し、Elasticsearch を起動するには 188 ページの 「セキュアクラスタ通信用の Elasticsearch の設定」の手順に従います。

4g アップグレード完了後、クラスタスタックを起動します。

```
rcpacemaker start
```

4h 自動起動スクリプトを削除して、クラスタが製品を管理できるようにします。

```
cd /
insserv -r sentinel
```

4i 次のコマンドを実行して、環境設定ファイルの変更を同期します。

```
csync2 -x -v
```

5 クラスタの保守モードを無効にします。

```
crm configure property maintenance-mode=false
```

このコマンドは、どのクラスタノードからでも実行することができます。

6 保守モードがアクティブではないことを確認します。

```
crm status
```

クラスタリソースは起動済みと表示されるはずです。

7 (任意)Sentinel のアップグレードが成功したかどうか確認します。

```
rcsentinel version
```

8 Sentinel にログインし、アラート、セキュリティインテリジェンスデータなどの移行されたデータを表示できるかどうかを検証します。

9 Sentinel 8.3 以降では、データは PostgreSQL にのみ格納されるようになるため、MongoDB 内のデータは冗長になります。ディスク容量を空けるには、このデータを削除してください。詳細については、187 ページの 「MongoDB からデータを削除しています」を参照してください。

オペレーティングシステムのアップグレード

このセクションでは、Sentinel HA クラスタ内で、SLES 11 から SLES 12 にアップグレードするなど、オペレーティングシステムを主要バージョンにアップグレードする方法について説明します。オペレーティングシステムをアップグレードする場合は、ごくわずかな設定タスクを実行して、オペレーティングシステムのアップグレード後に Sentinel HA が正しく動作することを確認する必要があります。

次のセクションで説明されている手順を実行します。

- 239 ページの 「オペレーティングシステムのアップグレード」
- 239 ページの 「iSCSI Target の環境設定」
- 241 ページの 「iSCSI イニシエータの環境設定」
- 242 ページの 「HA クラスタの設定」

オペレーティングシステムのアップグレード

オペレーティングシステムをアップグレードするには、次の手順を実行します。

1. root ユーザとして Sentinel HA クラスタの任意のノードにログインします。
2. 次のコマンドを実行して、クラスタで保守モードを有効にします。

   ```
   crm configure property maintenance-mode=true
   ```

   保守モードは、オペレーティングシステムをアップグレードする際、稼働中のクラスタリソースに影響を与えないようにするのに役立ちます。
3. 保守モードがアクティブかどうか検証するには、次のコマンドを実行します。

   ```
   crm status
   ```

   クラスタリソースは非管理状態と表示されるはずです。
4. すべてのクラスタノードで、Sentinel をバージョン 8.2 以降にアップグレードしたことを確認します。
5. クラスタ内のすべてのノードが SLES および SLESHA で登録されていることを確認します。
6. 次の手順を実行して、パッシブクラスタノード上のオペレーティングシステムをアップグレードします。
   - **6a** 次のコマンドを実行して、クラスタスタックを停止します。

     rcpacemaker 停止

     クラスタスタックを停止することで、クラスタリソースをアクセス不可のままに保ち、ノードのフェンシングを避けることができます。
   - **6b** オペレーティングシステムをアップグレードします。詳細については、オペレーティングシステムのアップグレードを参照してください。
7. すべてのパッシブノードで手順 6 を繰り返し、オペレーティングシステムをアップグレードします。
8. アクティブノード上で手順 6 を繰り返し、オペレーティングシステムをアップグレードします。
9. 手順 6b を繰り返し、共有ストレージ上のオペレーティングシステムをアップグレードします。
10. クラスタ内のすべてのノード上で、オペレーティングシステムが同じであることを確認します。

iSCSI Target の環境設定

次の手順を実行して、localdata および networkdata ファイルを iSCSI ターゲットとして設定します。

iSCSI ターゲットの設定方法の詳細については、SUSE のマニュアルの「Creating iSCSI Targets with YaST」を参照してください。

iSCSI ターゲットを設定するには、次のとおり実行します。

1 コマンドラインから YaST を実行します (またはグラフィカルユーザインタフェース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 アドレスになります。

6 [[次]] をクリックし、[[OK]] をクリックします。

7 (条件による) メイン画面で :

- [[ネットワークサービス]] > [[iSCSI LIO ターゲット]] を選択します。

  注 : このオプションが見つからない場合は、[[Software(ソフトウェア)]] > [[Software Management(ソフトウェア管理)]] > [[iSCSI LIO Server(iSCSI LIO サーバ)]] の順に進み、iSCSI LIO パッケージをインストールします。

8 (条件による) 要求された場合は、必要なソフトウェアをインストールします。

iscsiliotarget RPM

9 条件付き) クラスタ内のすべてのノード上で、次の手順を実行します。

9a iSCSI イニシエータ名を含むファイルを開くには、次のコマンドを実行します。

cat /etc/iscsi/initiatorname.iscsi

9b iSCSI イニシエータを設定するために使用されるイニシエータ名を確認します。

次に例を示します。

InitiatorName=iqn.1996-04.de.suse:01:441d6988994

これらのイニシエータ名は、iSCSI ターゲットのクライアントセットアップを設定するときに使用されます。

10 [[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。

11 [[Global(グローバル)]] タブを選択して [[認証なし]] の選択を解除して認証を有効化し、認証の送受信に必要なユーザ名とパスワードを指定します。

デフォルトでは [認証なし] のオプションが有効になっています。ただし、環境設定を確実にセキュリティ保護するため、認証を有効にする必要があります。

注 : Micro Focus では、iSCSI ターゲットとイニシエータに異なるパスワードを使用することをお勧めします。

12 [[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。

13 [[追加]] をクリックして、新しい LUN を追加します。

14 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。

15 13 と 14 の手順を繰り返して、今回は LUN 1 を追加し、/networkdata を選択します。

16 その他のオプションはデフォルト値のままにしておきます。[次へ] をクリックします。

17 (条件による)SLES 12 を使用している場合は、[追加] をクリックします。クライアント名を求められたら、手順 9 でコピーしたイニシエータ名を入力します。この手順を繰り返し、イニシエータ名を指定してすべてのクライアント名を追加します。

クライアント名のリストは、[Client List(クライアントリスト)] に表示されます。

SLES 15 以降のクライアントイニシエータ名を追加する必要はありません。

18 (条件による) 手順 11 で認証を有効にした場合は、認証の資格情報を指定します。

クライアントを選択し、[[Edit Auth (認証の編集)]] > [[Incoming Authentication (着信認証)]] の順に選択し、ユーザ名とパスワードを指定します。すべてのクライアントについて、この手順を繰り返します。

19 [[次]] をクリックしてデフォルト認証オプションを選択してから、[[完了]] をクリックして設定を終了します。要求された場合は、iSCSI を再起動します。

20 YaST を終了します。

iSCSI イニシエータの環境設定

iSCSI イニシエータを設定するには、次のとおり実行します。

1 片方のクラスタノード (node01) に接続して、YaST を開始します。

2 [[Network Services (ネットワークサービス)]] > [[iSCSI Initiator]] の順にクリックします。

3 要求があれば、必要なソフトウェア (iscsiclient RPM) をインストールします。

4 [[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。

5 [[Discovered Targets(検出したターゲット)]] をクリックします。

注 : 既存の iSCSI ターゲットが表示される場合は、これらのターゲットを削除します。

[[Discovery(検出)]] を選択して、新しい iSCSI ターゲットを追加します。

6 iSCSI ターゲット IP アドレス (10.0.0.3) を指定します。

(条件による) 239 ページの 「iSCSI Target の環境設定」 の手順 4 で認証を有効にした場合は、[[認証なし]] の選択を解除します。[[Outgoing Authentication(送信認証)]] セクションで、iSCSI ターゲットを設定する際に指定した認証の資格情報を入力します。

[次へ] をクリックします。

7 IP アドレスが 10.0.0.3 である検出された iSCSI ターゲットを選択して、[[ログイン]] を選択します。

8 次の手順を実行します。

8a［[スタートアップ]］ドロップダウンメニューで［Automatic(自動)］に切り替えます。

8b (条件による) 認証を有効にした場合は、［[認証なし]］の選択を解除します。

指定したユーザ名とパスワードが［[Outgoing Authentication(送信認証)]］セクションに表示されます。これらの資格情報が表示されない場合は、このセクションで資格情報を入力します。

8c [次へ] をクリックします。

9［[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。

10 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。

11 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。

12 システムビューのリストに、LIO-ORG-FILEIO タイプの新しいハードディスク (/dev/sdb および /dev/sdc など) が、フォーマット済みのディスク (/dev/sdb1 や /dev/<SHARED1 など) と合わせて表示されます。

13 すべてのノードで手順 1 から 12 を繰り返します。

HA クラスタの設定

HA クラスタを設定するには、次のとおり実行します。

1 YaST2 を起動し、［[High Availability(高可用性)]］>［[Cluster(クラスタ)]］の順に進みます。

2 要求されたら HA パッケージをインストールして、依存関係を解決します。

HA パッケージのインストール後にクラスタ通信チャネルが表示されます。

3 転送オプションとして Unicast が選択されていることを確認します。

4［[Add a Member Address(メンバーアドレスを追加)]］を選択してノード IP アドレスを指定してから、このアクションを繰り返し、その他すべてのクラスタノード IP アドレスを追加します。

5［[Auto Generate Node ID(自動ノード ID 生成)]］が選択されていることを確認します。

6 すべてのノードで、HAWK サービスが有効になっていることを確認します。有効でない場合は、次のコマンドを実行して有効にします。

service hawk start

7 次のコマンドを実行します。

ls -l /dev/disk/by-id/

SBD パーティション ID が表示されます。たとえば、scsi-1LIO-ORG_FILEIO:33caaa5a-a0bc-4d90-b21b-2ef33030cc53 です。

ID をコピーします。

8 sbd ファイル (/etc/sysconfig/sbd) を開き、SBD_DEVICE の ID を、手順 7 でコピーした ID に変更します。

9 次のコマンドを実行して、pacemaker サービスを再起動します。

rcpacemaker restart

10 クラスタが製品を管理できるように、次のコマンドを実行して自動起動スクリプトを削除します。

cd /

insserv -r sentinel

11 すべてのクラスタノードで手順 1 から 10 を繰り返します。

12 次のコマンドを実行して、環境設定ファイルの変更を同期します。

csync2 -x -v

13 次のコマンドを実行して、クラスタの保守モードを無効にします。

crm configure property maintenance-mode=false

このコマンドは、どのクラスタノードからでも実行することができます。

14 保守モードが非アクティブかどうか検証するには、次のコマンドを実行します。

crm status

クラスタリソースは起動済みと表示されるはずです。

Sentinel HA アプライアンスインストールのアップグレード

Sentinel 8.2 以降から Sentinel にアップグレードすることができます。Sentinel と SLES オペレーティングシステムの両方を、Sentinel アプライアンスマネージャまたは Zypper(アプライアンス更新チャネル) を介してアップグレードできます。

Sentinel 8.3.0.0 以降は、MongoDB ではなく PostgreSQL を使用してセキュリティインテリジェンスデータおよびアラートデータを保存するようになりました。アクティブノード上のアプライアンスをアップグレードする前に、まずデータを MongoDB から PostgreSQL に移行する必要があります。データを PostgreSQL に正常に移行した場合にのみ、アプライアンスをアップグレードできます。

- SLES 12 SP3 または SLES 12 SP4 がインストールされている必要があります。
    1. (条件による)Sentinel 8.2.0.0 で SLES 11 SP4 を使用している場合は、SLES 11 ですべてのチャネル更新を取得することが推奨されます。次に、OS を SLES 12 SP3 にアップグレードします。SLES オペレーティングシステムのアップグレードの詳細については、172 ページの 「オペレーティングシステムの SLES 12 SP3 へのアップグレード」を参照してください。Micro Focus Patch Finder Web サイトからアップグレード後のユーティリティをダウンロードして実行します。

2. (条件による)Sentinel 8.2.0.0 で SLES 12 SP3 を使用し、アップグレード後のユーティリティ sentinel_sles_iso_os_post_upgrade-release-73.tar.gz を実行している場合は、Micro Focus Patch Finder Web サイトからアップグレード後のユーティリティ sentinel_sles_iso_os_post_upgrade-release-85.tar.gz をダウンロードして実行する必要があります。
3. (条件による)Sentinel 8.2.0.0 で SLES 12 SP3 を使用し、Micro Focus Patch Finder Web サイトからアップグレード後のユーティリティ sentinel_sles_iso_os_post_upgrade-release-85.tar.gz を実行している場合は、175 ページの「アプライアンスのアップグレード」の手順に従います。

- 244 ページの 「Zypper パッチを介したアップグレード」
- 246 ページの 「Sentinel アプライアンス管理コンソールを介したアップグレード」

Zypper パッチを介したアップグレード

アップグレードの前に、Sentinel アプライアンスマネージャですべてのアプライアンスノードを登録する必要があります。詳細については、95 ページの 「アップデートの登録」を参照してください。アプライアンスを登録しないと、Sentinel で黄色の警告が表示されます。

1 クラスタの保守モードを有効にします。

```
crm configure property maintenance-mode=true
```

保守モードは、Sentinel ソフトウェアをアップデートする際、稼働中のクラスタリソースに影響を与えないようにするのに役立ちます。このコマンドは、どのクラスタノードからでも実行することができます。

2 保守モードがアクティブかどうか確認します。

```
crm status
```

クラスタリソースは非管理状態と表示されるはずです。

3 パッシブクラスタノードをアップデートします。

3a クラスタスタックを停止します。

rcpacemaker 停止

クラスタスタックを停止することで、クラスタリソースをアクセス不可のままに保ち、ノードのフェンシングを避けることができます。

3b 171 ページの 「アプライアンスをアップグレードするための前提条件」に記載されている前提条件 1 および 2 を完了します

3c Sentinel のアップデートをダウンロードします。

注 : Sentinel 8.3.1 では、アプライアンスに対して更新された rpm と新しい rpm の両方が要求されるため、zypper -v patch コマンドと zypper up コマンドが必要です。

- zypper -v patch

注 : パッチが適用された後、システムを再起動するメッセージが表示されます。次のステップである zypper up が完了するまで、再起動を無視します。

- zypper up

3d アップグレード完了後、クラスタスタックを起動します。

```
rcpacemaker start
```

4 すべてのパッシブクラスタノードに対してステップ 3 を繰り返します。

5 アクティブなクラスタノードをアップグレードします。

5a 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。

データのバックアップ方法については、『「Sentinel Administration Guide」』の「*Backing Up and Restoring Data*」を参照してください。

5b クラスタスタックを停止します。

rcpacemaker 停止

クラスタスタックを停止することで、クラスタリソースをアクセス不可のままに保ち、ノードのフェンシングを避けることができます。

5c 171 ページの 「アプライアンスをアップグレードするための前提条件」に記載されている前提条件を完了します。

5d Sentinel のアップデートをダウンロードします。

Sentinel をアップグレードするには、コマンドプロンプトから次のコマンドを実行します。

- zypper -v patch

注 : 上記のコマンドを実行すると、システムを再起動するメッセージが表示されます。246 ページのステップ 8 が完了するまで再起動を無視します。

- zypper up
- (条件による) アップグレードの前に、イベント視覚化が有効になっている場合、Sentinel 8.4.0.0 にアップグレードした後、Elasticsearch は X-Pack セキュリティプラグインで有効になっているため停止し、Elasticsearch を起動するには 188 ページの 「セキュアクラスタ通信用の Elasticsearch の設定」の手順に従います。

5e アップグレードが完了したら、次の手順を実行します。

- (条件による)Sentinel が自動的に起動されない場合は、Sentinel データベースを起動します。

  rcsentinel startdb

- クラスタスタックを開始します。

  rcpacemaker 開始

5f 次のコマンドを実行して、環境設定ファイルの変更を同期します。

```
csync2 -x -v
```

6 クラスタの保守モードを無効にします。

```
crm configure property maintenance-mode=false
```

このコマンドは、どのクラスタノードからでも実行することができます。

7 保守モードがアクティブではないことを確認します。

```
crm status
```

クラスタリソースは起動済みと表示されるはずです。

8 (任意) アップグレードが成功したかどうかを検証します。

```
rcsentinel version
```

9 手順 5d に示されているように、zypper patch メッセージに基してシステムを再起動します。

10 Sentinel にログインし、アラート、セキュリティインテリジェンスダッシュボードなどの移行されたデータが表示されるかどうかを検証します。

11 Sentinel 8.3 以降では、データは PostgreSQL にのみ格納されるようになるため、MongoDB 内のデータは冗長になります。ディスク容量を空けるには、このデータを削除してください。詳細については、187 ページの 「MongoDB からデータを削除しています」を参照してください。

Sentinel アプライアンス管理コンソールを介したアップグレード

Sentinel アプライアンス管理コンソールを使用してアップグレードするには、次の手順に従います。

1 次のコマンドをクラスタ内のアクティブノードまたはパッシブノードで実行して、保守モードを有効にします。

```
crm configure property maintenance-mode=true
```

保守モードは、Sentinel をアップデートする際、稼働中のクラスタリソースに影響を与えないようにするのに役立ちます。

2 保守モードがアクティブかどうか検証するには、次のコマンドを実行します。

```
crm status
```

クラスタリソースは非管理状態と表示されるはずです。

3 まず、すべてのパッシブクラスタノードをアップグレードします。

3a 次のコマンドを実行して、クラスタスタックを停止します。

```
rcpacemaker stop
```

クラスタスタックを停止することで、クラスタリソースをアクセス不可のままに保ち、ノードのフェンシングを避けることができます。

3b 次のコマンドを実行して、9443 ポートがアプライアンスにアクセスするためにアクティブノード上でリッスンしているかどうかを検証します。

```
netstat –na | grep 9443
```

3c (条件による)9443 ポートがリッスンしていない場合は、次のコマンドを実行します。

```
systemctl restart vabase vabase-jetty vabase-datamodel
```

3d 171 ページの 「アプライアンスをアップグレードするための前提条件」に記載されている前提条件 1 および 2 を完了します

3e 次のいずれかの方法で、アプライアンスを起動します。

- Sentinel にログインします。[**[Sentinel メイン]**] > [**[アプライアンス]**] の順にクリックします。
- Web ブラウザで次の URL を指定します :https://<IP_address>:9443。

3f (条件による)Sentinel アプライアンス管理コンソールを起動できない場合 :

3f1 アクティブノードの /var/opt/novell に移動し、次のファイルを各パッシブノードの /var/opt/novell/ にコピーします。

- datamodel-service
- ganglia
- jetty
- python
- va

3f2 各パッシブノードで、jetty フォルダ内のファイルの許可を vabase-jetty に設定します。

1. /var/opt/novell/jetty に移動します。
2. 次のコマンドを実行します。

   ```
   chown -R vabase-jetty:vabase-jetty *
   ```

3f3 次のコマンドを実行して、vabase サービスを再起動します。

```
systemctl start vabase-jetty vabase-datamodel vabase
```

3f4 次のコマンドを実行して、ポート 9443 が使用可能なすべてのノードでリッスンしていることを検証します。

```
netstat -na | grep 9443
```

3g vaadmin としてログインします。

3h [**[オンラインアップデート]**] をクリックします。

3h1 (条件による) これまでにアップデートを実行していない場合は、アップデートの登録をしてください。詳細については、95 ページの 「アップデートの登録」を参照してください。

注 : 手順 5h2 の後にシステムを再起動するようメッセージが表示されますが、手順 5h3 が完了するまで無視します。

3h2 表示されている更新を Sentinel およびオペレーティングシステムにインストールするには、[**[今すぐ更新]**] > [**[OK]**] をクリックします。

3h3 **注 :** Sentinel 8.3.1 では、手順 5h2 に加えて、アプライアンスに対して更新された rpm と新しい rpm の両方が要求されるため、zypper up コマンドも必要です。

コマンドプロンプトから次のコマンドを実行して、rpm を完全にアップグレードします。

```
zypper up
```

3h4 インストールされているアップデートを適用するには、[**[再起動]**] をクリックします。

3h5 再起動後、画面の右上隅のバージョンを確認して、アップグレードが成功したかどうかを検証します。

3i アップグレード完了後、クラスタスタックを再起動します。

```
rcpacemaker start
```

4 アクティブなクラスタノードをアップグレードします。

4a 171 ページの 「アプライアンスをアップグレードするための前提条件」に記載されている前提条件を完了します。

4b アクティブなクラスタノードに対して手順 5h1 から手順 5h3 を繰り返します。

4c (条件による)Sentinel が自動的に起動されない場合は、Sentinel を起動します。

```
rcsentinel start
```

4d アップグレード完了後、クラスタスタックを再起動します。

```
rcpacemaker start
```

5 保守モードを無効にするには、クラスタ内のアクティブノードまたはパッシブノードで次のコマンドを実行します。

```
crm configure property maintenance-mode=false
```

6 保守モードが非アクティブであることを検証するには、クラスタ内のアクティブノードまたはパッシブノードで次のコマンドを実行します。

```
crm status
```

7 (条件による) アップグレードの前に、イベント視覚化が有効になっている場合、Sentinel 8.4.0.0 にアップグレードした後、Elasticsearch は X-Pack セキュリティプラグインで有効になっているため停止し、Elasticsearch を起動するには 188 ページの 「セキュアクラスタ通信用の Elasticsearch の設定」の手順に従います。

8 次に、手順 5h2 に示されているように、zypper patch メッセージに基してシステムを再起動します。

9 再起動後、画面の右上隅のバージョンを確認して、アップグレードが成功したかどうかを検証します。

10 Sentinel にログインし、アラート、セキュリティインテリジェンスダッシュボードなどの移行されたデータが表示されるかどうかを検証します。

11 Sentinel 8.3 以降では、データは PostgreSQL にのみ格納されるようになるため、MongoDB 内のデータは冗長になります。ディスク容量を空けるには、このデータを削除してください。詳細については、187 ページの 「MongoDB からデータを削除しています」を参照してください。

41 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。

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。『「Sentinel 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。

回復

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。『「Sentinel Administration Guide」』のセクション「*Backing Up and Restoring Data*」では、Sentinel に組み込まれている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。

VIII 付録

A 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。

Default-Resource-Stickiness クラスタプロパティは非推奨

問題 : crm コマンドを使用して設定プロパティ (例 : crm configure property maintenance-mode=true) を設定または変更すると、次のメッセージが表示されます。

```
ERROR: DEBUG: Cluster properties: cib-bootstrap-options-default-resource-
stickiness: moving default-resource-stickiness under rsc_defaults as
resource-stickiness unless already defined there
WARNING: cib-bootstrap-options: unknown attribute 'default-resource-
stickiness'
```

修正 : 古いバージョンの SLE HAE が、Sentinel 製品で新しいバージョンの SLE HAE にアップグレードされた場合 (通常は SLES 12 SP3 から SLES 12 SP5 以降のバージョン)、このメッセージが表示されます。この変更による機能への影響はありません。詳細については、［SUSE KB Article］を参照してください。

HA セットアップで仮想 IP を使用して RCM/RCE を設定できない

問題 :

仮想 IP を使用して RCM/RCE を設定できません。ホストはホスト名によって到達できません。

修正 :

従来の HA

新しいセットアップと既存のセットアップの両方について、従来の HA モードで RCM/RCE を接続するには、次の手順を実行します。

1. RCM/RCE をインストール / 設定する前に、RCM/RCE ボックスの /etc/hosts ファイルに、以下のようなエントリを追加します。

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   例 : 164.99.87.27 first_active_host.dom.name first_active_host

   ---

   重要 : configure.sh を実行する前に、このエントリが /etc/hosts ファイルで指定された HA 環境で最初に正常に成功した適切なアクティブノードのホスト名と常に一致することを確認してください。

   ---

2. RCM/RCE をサーバに接続する時に、プロンプトで仮想 IP を指定します。

   重要 : 最初に成功したアクティブノードはダウンし、もう一方のノードは現在アクティブですが、/etc/hosts ファイル内の仮想 IP で最初に成功したアクティブノード名を使用します。

アプライアンス HA

新しいセットアップのためにアプライアンス HA モードで RCM/RCE を接続するには、次の手順を実行します。

- HA クラスタ内で最初に成功したアクティブノードのホスト名のみを使用します。

既存のセットアップのために RCM/RCE をアプライアンス HA モードで接続するには、次の手順を実行します。

1. RCM/RCE をインストール / 設定する前に、RCM/RCE ボックスの /etc/hosts ファイルに、以下のようなエントリを追加します。

   ```
   <virtual ip> <FQDN of first_scuccessful_activenode_host>
   <first_scuccessful_activenode_hostname>
   ```

   例 : 164.99.87.27 first_active_host.dom.name first_active_host

   ---

   重要 : configure.sh を実行する前に、このエントリが /etc/hosts ファイルで指定された HA 環境で最初に正常に成功した適切なアクティブノードのホスト名と常に一致することを確認してください。

   ---

2. RCM/RCE をサーバに接続する時に、プロンプトで仮想 IP を指定します。

   重要 : 最初に成功したアクティブノードはダウンし、もう一方のノードは現在アクティブですが、/etc/hosts ファイル内の仮想 IP で最初に成功したアクティブノード名を使用します。

DHCP 環境で、Sentinel サーバアプライアンスページの Sentinel サーバ Web UI アイコンが空白ページにリダイレクトされる

問題 : Sentinel サーバアプライアンスページの Sentinel サーバ Web UI アイコンが、DHCP 環境で空白のブロックされたページとして起動します。

解決策 : 次の手順を実行します。

1. **[YaST]** メニューに移動します。
2. **［[システム］>［ネットワーク設定］>［IPv6 protocol Setting(IPv6 プロトコル設定)]］**に移動します。
3. IPv6 を無効にして保存します。
4. システムを再起動します。

正しい IP アドレス / ホスト名を指定した後、Transformation Hub (T-Hub) に接続できない

T-Hub が到達可能で、すべての T-Hub 証明書が Sentinel サーバにコピーされているにもかかわらず、Sentinel サーバが T-Hub と通信できない場合は、次の手順を実行します。

1. Sentinel サーバの /etc/opt/novell/sentinel/intelligence ディレクトリに移動します。
2. avro-schema-file-V1.json ファイルを削除します。
3. Sentinel サーバを再起動します。

   ```
   rcsentinel restart
   ```

Sentinel サーバを再起動するとスキーマファイルが再生成され、ユーザは T-Hub への接続を正常に確立できる必要があります。

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。

イメージを作成した Collector Manager instances または Correlation Engine の UUID が作成されない

Collector Manager 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 Collector Manager 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 Collector Manager 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. Collector Manager を再起動します。

   Collector Manager が自動的に UUID を生成します。

ログイン後に Internet Explorer で Sentinel Main インタフェースがブランクになる

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。

Windows Server 2012 R2 の Internet Explorer 11 で Sentinel が起動しない

Windows Server 2012 R2 を使用すると、Internet Explorer 11 のデフォルトのセキュリティ設定が原因で、Sentinel が Internet Explorer 11 で起動しません。Sentinel を起動する前に、信頼済みサイトのリストに Sentinel を手動で追加する必要があります。

Sentinel を信頼済みサイトのリストに追加する方法

1 Internet Explorer 11 を開きます。

2 ［[設定]］アイコン >［[インターネットオプション]］>［[セキュリティ]］タブ >［[信頼済みサイト]］>［[サイト]］をクリックします。

3 Sentinel ホストを信頼済みサイトのリストを追加します。

デフォルトの EPS ライセンスでは Sentinel がローカルレポートを実行できない

デフォルトの 25 EPS ライセンスがある環境でレポートを実行すると、次のエラーでレポートが失敗します : 分散検索機能のライセンスが期限切れです

Sentinel と同じ JVM でレポートを実行するには、次の手順を実行します。

1 Sentinel サーバにログインし、/etc/opt/novell/sentinel/config/obj-component.JasperReportingComponent.properties ファイルを開きます。

2 reporting.process.oktorunstandalone プロパティを見つけます。

3 (条件による) このプロパティがファイルにない場合は、追加します。

4 このプロパティを false に設定します。次に例を示します。

reporting.process.oktorunstandalone=false

5 Sentinel を再起動します。

アクティブノードを FIPS 140-2 モードに変換した後、Sentinel の高可用性で同期を手動で開始する必要がある

問題 : Sentinel HA でアクティブノードを FIPS 140-2 モードに変換すると、すべてのパッシブノードを FIPS 140-2 モードに変換するための同期が完全に実行されません。同期を手動で開始する必要があります。

解決策 : 次のようにして、すべてのパッシブノードを FIPS 140-2 モードに手動で同期します。

1 アクティブノードにルートユーザとしてログインします。

2 /etc/csync2/csync2.cfg ファイルを開きます。

3 次の行を変更します。変更前 :

```
include /etc/opt/novell/sentinel/3rdparty/nss/*;
```

変更後 :

```
include /etc/opt/novell/sentinel/3rdparty/nss;
```

4 csync2.cfg ファイルを保存します。

5 次のコマンドを実行して、手動で同期を開始します。

```
csync2 -x -v
```

いくつかの保存済み検索を編集する時のスケジュールページにイベントフィールドパネルがない

問題 : Sentinel 7.2 から新しいバージョンにアップグレードされた保存済み検索を編集する際、検索レポート CSV の出力フィールドを指定するのに使用する［**[イベントフィールド]**］パネルがスケジュールページにありません。

解決策 : Sentinel をアップグレードしたら、スケジュールページに［**[イベントフィールド]**］パネルが表示されるように、検索を再作成して再スケジュールします。

デフォルト起動回数検索で展開済みのルールのイベントを検索しても相関イベントが返されない

問題 : ルールの相関要約ページの［**[アクティビティ統計情報]**］パネルの［**[起動回数]**］の隣にあるアイコンをクリックすることにより、ルールが展開または有効化された後に生成されたすべての相関イベントを検索しても相関イベントが返されません。

解決策 : イベント検索ページの［ **[開始]**］フィールドの値を、フィールドに取り込まれた時間よりも早い時間に変更してから、再び［ **[検索]**］をクリックします。

ベースラインの再生成中、セキュリティインテリジェンスダッシュボードに無効なベースライン期間が表示される

問題 : セキュリティインテリジェンスベースラインの再生成中に、ベースラインの開始日と終了日が誤って「1/1/1970」と表示されます。

解決策 : ベースラインの再生成が完了すると、正しい日付にアップデートされます。

単一のパーティションに多数のイベントが存在すると検索の実行中に Sentinel サーバがシャットダウンする

問題 : 単一のパーティションで索引付けされたイベントが多数ある場合、検索の実行中に Sentinel サーバがシャットダウンします。

解決策 : 1 日に少なくとも 2 つのパーティションが開かれるように保持ポリシーを作成します。1 つ以上のパーティションが開かれるようにすることで、パーティションで索引付けされたイベント数を減らすことができます。

［estzhour］フィールドに基づいてイベントをフィルタリングする保持ポリシーを作成して、特定の時間帯を追跡します。つまり、estzhour:[0 TO 11] をフィルタとして使用して 1 つの保持ポリシーを作成し、estzhour:[12 TO 23] をフィルタとして使用して別の保持ポリシーを作成できます。

詳細については『「Sentinel Administration Guide」』の「*Configuring Data Retention Policies*」を参照してください。

report_dev_setup.sh スクリプトを使用して、アップグレードインストールした Sentinel アプライアンスでファイアウォール例外の Sentinel ポートを構成するとエラーが発生する

問題 : report_dev_setup.sh スクリプトを使用して、ファイアウォール例外の Sentinel ポートを構成すると、Sentinel でエラーが発生します。

解決策 : 次の手順を実行して、ファイアウォール例外の Sentinel ポートを構成してください。

1. /etc/sysconfig/SuSEfirewall2 ファイルを開きます。
2. 次の行を変更します。変更前 :

```
FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
40000:41000 1290 1099 2000 1024 1590"
```

変更後 :

```
FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
40000:41000 1290 1099 2000 1024 1590 5432"
```

3 Sentinel を再起動します。

B 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。

Sentinel をアンインストールするためのチェックリスト

以下のチェックリストを使用して、Sentinel をアンインストールします。

- ❒ Sentinel サーバをアンインストールする。
- ❒ Collector ManagerおよびCorrelation Engine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。

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。

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。

```
<sentinel_installation_path>/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。

Collector Manager および Correlation Engine のアンインストール

次の手順に従って、Collector Manager および Correlation Engine をアンインストールします :

1 root として Collector Manager および Correlation Engine のコンピュータにログインします。

注 : root ユーザとしてインストールを実行した場合、root 以外のユーザとしてリモート Collector Manager またはリモート Correlation Engine をアンインストールすることはできません。ただし、root 以外のユーザとしてインストールを行った場合は、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、Collector Manager または Correlation Engine 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、Collector Manager または Correlation Engine 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、Collector Manager と Correlation Engine のアイコンは、Sentinel メインインタフェースに非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、Sentinel メインインタフェースの Collector Manager と Correlation Engine を手動で削除します :

Collector Manager:

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 Collector Manager を右クリックして、［ **[削除]**］をクリックします。

Correlation Engine:

1. 管理者として **[Sentinel Main]** インタフェースに移動します。
2. ［ **[相関関係]**］を展開してから、削除する Correlation Engine 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。

Sentinel のアンインストール後のタスク

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 をアンインストールした後も、特定のシステム設定が残ります。Sentinel のアンインストール中にエラーが発生した場合は特に、Sentinel の新しいインストールを実行する前に設定を削除する必要があります。

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。