Sentinel™

インストールと設定ガイド

2018年7月

保証と著作権

NetIQの保証と著作権、免責事項、保証、輸出およびその他の使用制限、米国政府の規制による権利、特許ポリシー、およびFIPSコンプライアンスの詳細については、http://www.netiq.com/company/legal/を参照してください。

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

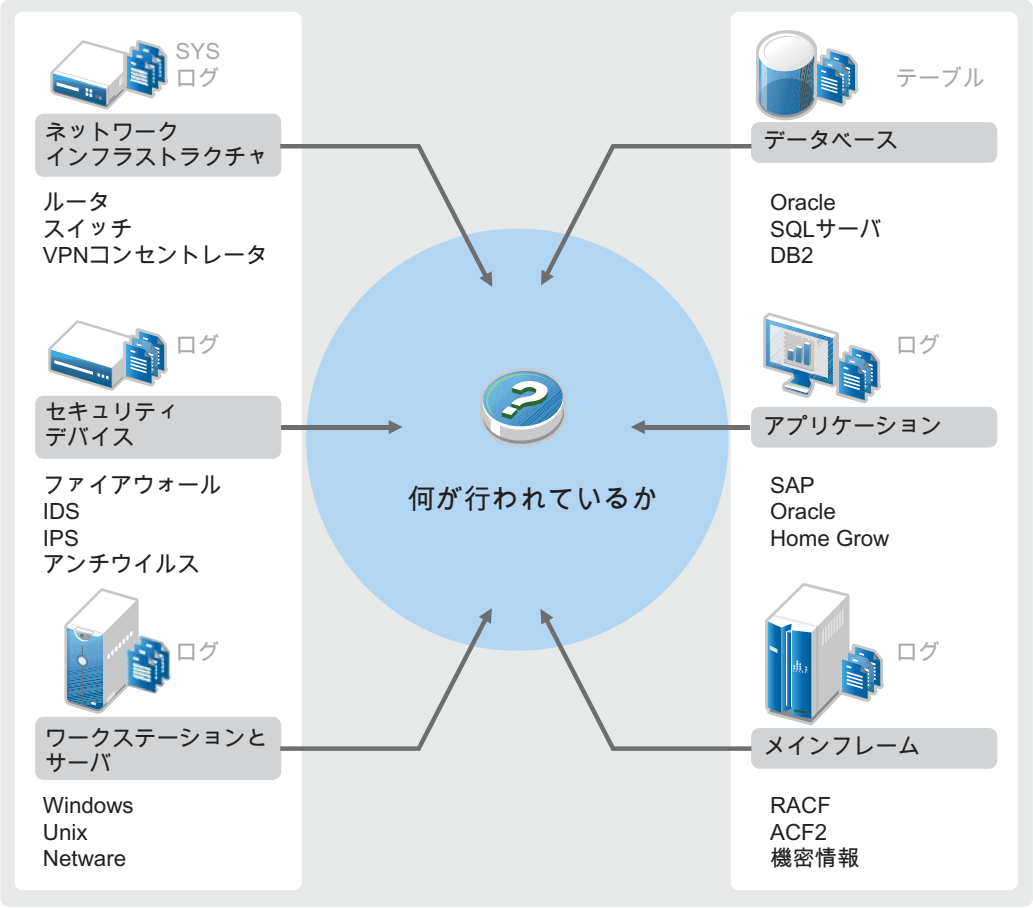
Sentinelは、セキュリティ情報およびイベント管理(SIEM)ソリューションであると同時に、コンプライアンスモニタリングソリューションでもあります。Sentinelは、最も複雑なIT環境を自動的にモニタリングし、IT環境を保護するのに必要なセキュリティを提供します。

- 15 ページの 「IT環境のセキュリティ保護の課題」
- 16 ページの 「Sentinelが提供するソリューション」

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。

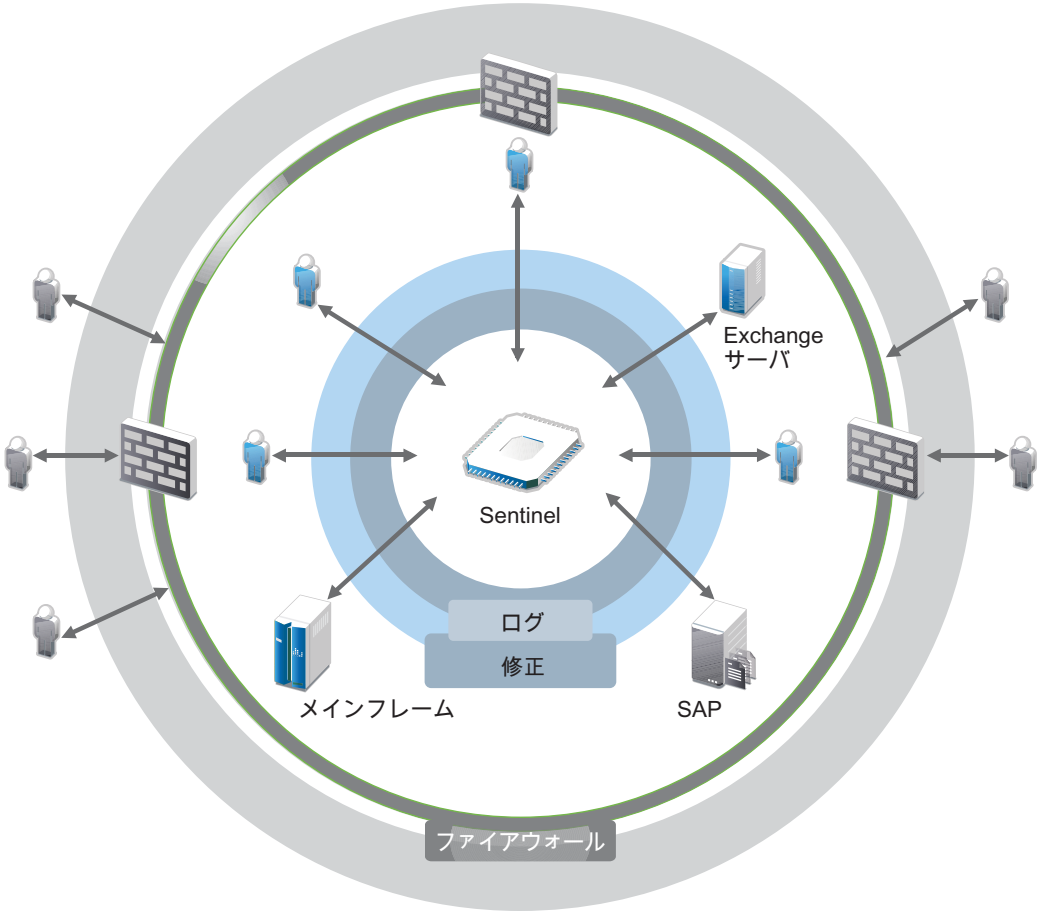
- データを収集する
- データを集約する
- 異種のデータを標準化してイベントにし、簡単に比較できるようにする
- イベントを標準規制に対応付けする
- データを分析する
- 複数のシステム間のイベントを比較し、セキュリティの問題があるかどうかを判断する
- データが基準から外れたときには通知を送信する
- ビジネスポリシーに従って通知に対する行動をとる
- コンプライアンスの証明のためにレポートを生成する

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

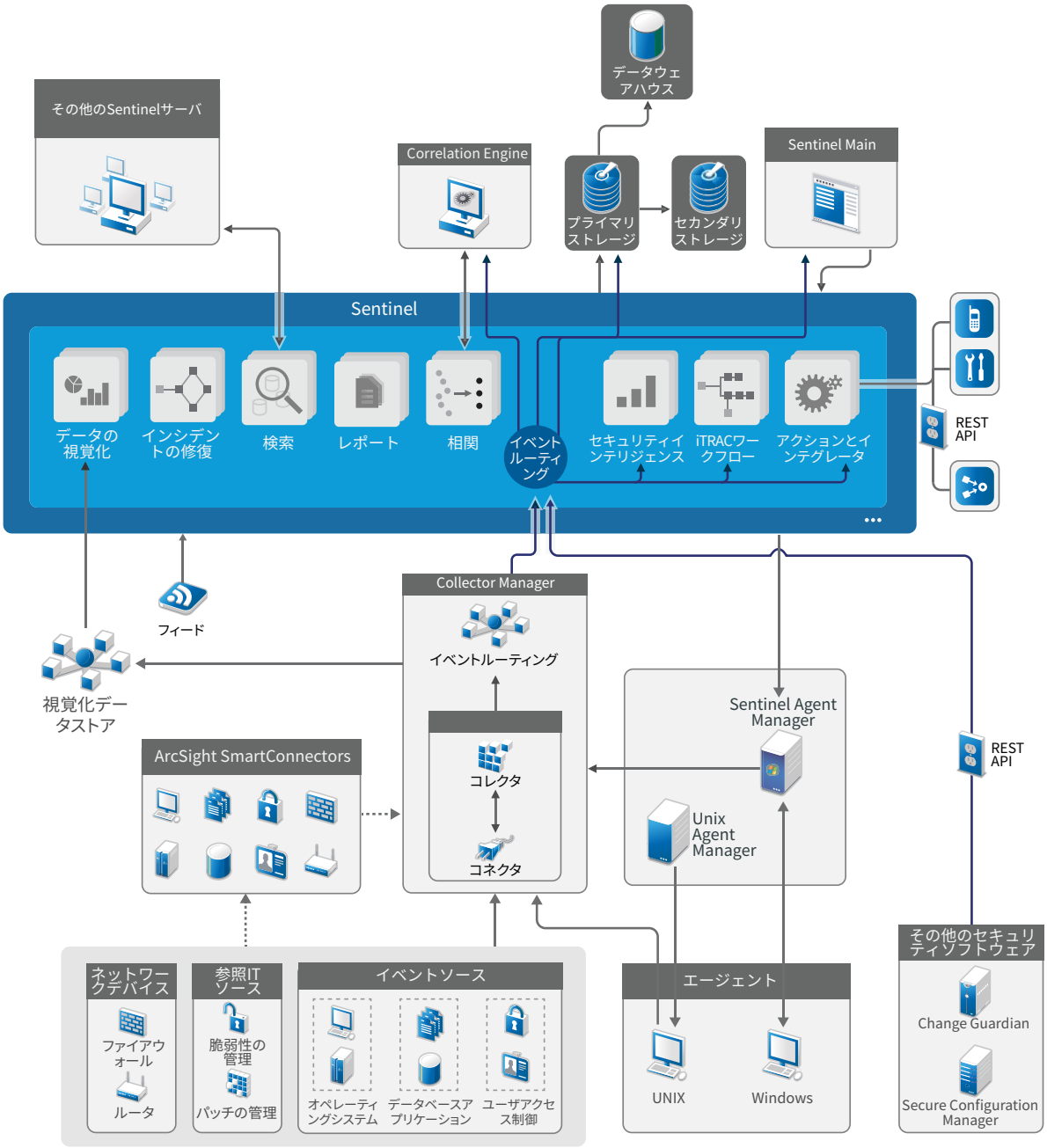
Sentinelは、IT環境全体のセキュリティ情報とイベントを継続的に管理することで、完全なモニタリングソリューションを提供します。

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またはHadoopベースのスケーラブル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。

- 21 ページの 「イベントソース」
- 22 ページの 「Sentinelイベント」
- 24 ページの 「Collector Manager」

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」
- 23 ページの 「エクスプロイト検出」

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。

エクスプロイト検出

Sentinelは、イベントデータ署名と脆弱性スキャナデータを相互参照する機能を提供します。脆弱なシステムに対してエクスプロイトが試行されると、即座にSentinelは、自動的にユーザへ通知を送信します。Sentinelは、次の機能を使用して、これを実現しています。

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

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

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(CommonEventFormat)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

AgentManager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。.

AgentManager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、Hadoopベースのスケーラブル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、41 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。

イベント視覚化は、スケーラブルストレージを使用するSentinelでデフォルトで使用できます。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、「44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。詳細については、『「SentinelUserGuide」』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、『「SentinelUserGuide」』の「*Correlation Engine*」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、『「SentinelUserGuide」』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、『「SentinelUserGuide」』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、『「SentinelUserGuide」』の「*SearchingEvents*」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。

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、147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。	35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。	39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。	41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。	73ページのパートIII「Sentinelのインストール」。
❒	Sentinelを設定します。	117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。
❒	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。	113ページの第16章「コレクタとコネクタの追加インストール」.

❒	タスク	参照先
❒	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。	73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

サービスと機能	Sentinel Enterprise	Sentinel for Log Management
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
エクスプロイト検出(Advisor)*	対応	対応
スケーラブルストレージ	対応	対応
相関	対応	非対応
◆ 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		
セキュリティインテリジェンス	対応	非対応
◆ アノマリールール ◆ リアルタイムの統計分析		

*Security Nexusを搭載したAdvisorは、アドオンのサービスです。このサービスを使用するには追加のライセンスを購入する必要があります。

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。

- 36 ページの 「評価ライセンス」
- 37 ページの 「無償ライセンス」
- 37 ページの 「エンタープライズライセンス」

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、35 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。

スケーラブルストレージの展開では、評価ライセンスの期限が切れたときにSentinelでイベントと生データが保存されなくなります。

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。

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。

- 39 ページの 「コネクタおよびコレクタのシステム要件」
- 39 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の詳細については、 Sentinel技術情報のWebサイト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、従来のストレージとスケーラブルストレージのどちらを使用するかを選択できます。お客様のSentinel展開は、選択するデータストレージのオプションによって決まります。

表 6-1 従来のストレージとスケーラブルストレージの比較

従来のストレージ	スケーラブルストレージ
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、44 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。	データはHadoopベースのスケーラブルストレージに保存され、データのインデックス作成にはスケーラブルな分散インデックス作成メカニズムが使用されます。
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。	非常に大きなEPS(1秒に100万イベントなど)までシームレスにスケールアウトします。
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。	データ収集は単一のSentinelサーバによって管理されます。したがって、データ管理とリソース管理が単一のSentinelサーバに一元化されます。
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。	データはディスク上でテナント別にラベルが付けられ、分離されます。
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。	Hadoopは汎用ハードウェアで実行されるため、データのレプリケーションや可用性はコスト効率に優れます。

- 42 ページの 「従来のストレージのプラニング」
- 45 ページの 「スケーラブルストレージのプラニング」
- 48 ページの 「Sentinelのディレクトリ構造」

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、48 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。

- 43 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」
- 44 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」
- 44 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」
- 44 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48 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。SuSEYaST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、109 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。

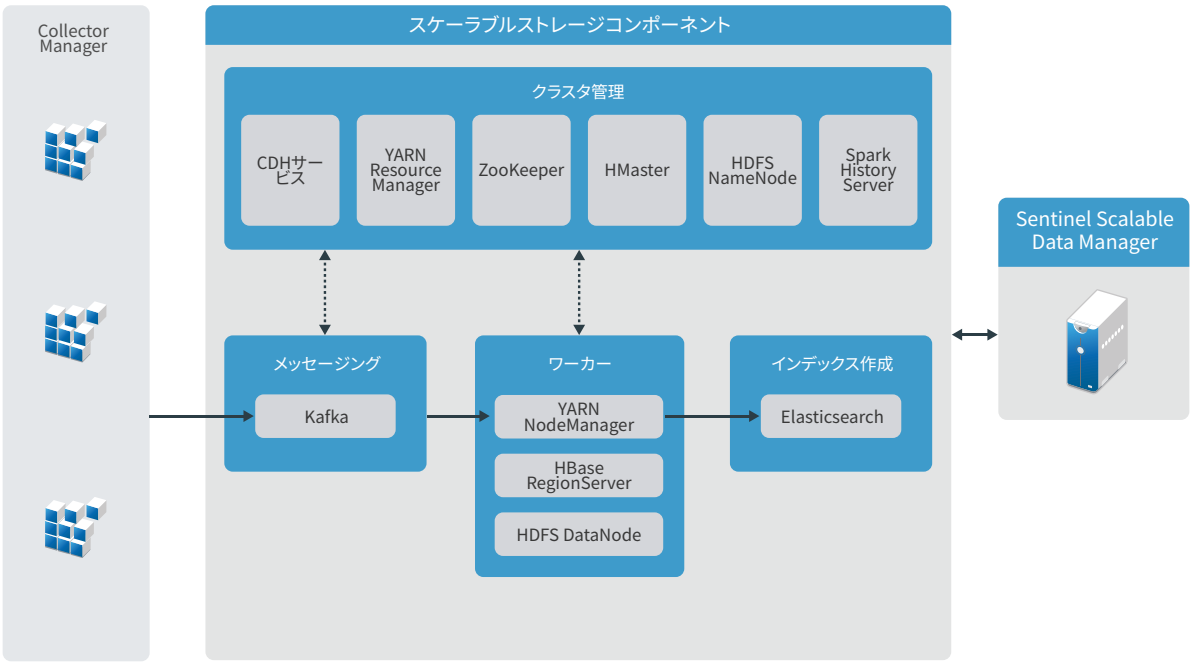
- **クラスタモードでのElasticsearchノードのインストール:** デフォルトでは、SentinelにはElasticsearchノードが1つ含まれています。Sentinelサーバの最適なパフォーマンスと安定性のためには、追加のElasticsearchノードをクラスタモードでインストールすることが必須です。詳細については、79ページの第12章「Elasticsearchのインストールと設定」を参照してください。
- **イベント視覚化の有効化:** デフォルトでは、イベント視覚化は無効です。イベント視覚化を有効にする方法については、「125ページの第20章「イベント視覚化の有効化」」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、85 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。

スケーラブルストレージのプラニング

Sentinelでは、大規模データの格納と管理にClouderaのDistribution Including Apache Hadoop (CDH)フレームワークを使用します。Sentinelでは、イベントのインデックス作成にElasticのElasticsearchと呼ばれるスケーラブルな分散インデックス作成エンジンが使用されます。

次の図では、スケーラブルストレージに使用される各種コンポーネントについて説明します。

図 6-1 スケーラブルストレージのアーキテクチャ



- **メッセージング:** Sentinelでは、Apache Kafkaを、正規化されたイベントと生データをCollector Manager instancesから受信するスケーラブルなメッセージングシステムとして利用します。Collector Manager instancesは生データとイベントデータをKafkaクラスタに送信します。

  デフォルトでは、Sentinelは次のKafkaトピックを作成します。

  - **security.events.normalized:** システム生成イベントと内部イベントを含む、処理済みの正規化されたイベントデータをすべて格納します。
  - **security.events.raw:** イベントソースからのすべての生データを格納します。

  イベントと生データはApache Avroスキーマに従います。詳細については、Apache Avroのマニュアルを参照してください。スキーマファイルは/etc/opt/novell/sentinel/scalablestoreディレクトリにあります。

- **ワーカー:** このノードは、リアルタイム処理とストレージのジョブをホストします。Apache Sparkは、テナントIDに基づくイベントの分離、大量データの要求、システムオブレコード(SOR)へのデータ保存、スケーラブルなインデックス作成など、大規模なデータ処理をリアルタイムで実行します。

  Apache HBaseは、スケーラブルな分散Hadoopベースデータストアです。正規化されたイベントおよび生データのSORとして使用され、テナントID別に分離されます。

  SentinelではテナントIDに基づき、各テナントに個別のネームスペースを作成します。たとえば、デフォルトのテナントのネームスペースは1です。Sentinelはそれぞれのネームスペースに次のテーブルを作成し、イベント時刻に基づいてデータを格納します。

  - ***<tenant_ID>*:security.events.normalized:** システム生成イベントと内部イベントを含む、処理済みの正規化されたイベントデータをすべて格納します。
  - ***<tenant_ID>*:security.events.raw:** イベントソースからのすべての生データを格納します。

- **クラスタ管理:** このノードでは、すべてのマスタとクラスタ管理サービスをホストします。Apache ZooKeeperは、環境設定情報の保守、サービスの命名、分散型同期の実行、およびグループサービスの提供を一元的に管理するサービスとして機能します。
- **インデックス作成:** Sentinelでは、イベントにインデックスを付けるためのスケーラブルで分散型のインデックス作成エンジンとしてElasticsearchを使用します。Elasticsearchからデータにアクセスし、イベントを検索して視覚化することができます。

  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。最適なパフォーマンスを得るため、Sentinelでは一部の特定のイベントフィールドにのみインデックスを作成します。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、85 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。

スケーラブルストレージの環境設定

スケーラブルストレージを有効にすると、Sentinelサーバのユーザインタフェースが縮小され、データ収集、相関、イベントルーティング、イベントの検索と視覚化、および特定の管理アクティビティの実行など、Sentinelの一部の機能だけに対応するようになります。このSentinelの縮小バージョンは、Sentinel Scalable Data Manager (SSDM)と呼ばれます。セキュリティインテリジェンス、従来の検索、レポーティングなど、その他のSentinel機能が必要な場合は、従来のストレージを使用する別個のSentinelインスタンスをインストールし、Sentinel Linkを使用して特定のイベントデータをSSDMからSentinelにルーティングする必要があります。

次のリストは、SSDMで利用できないサービスと機能に関する情報です。

- レポート
- セキュリティインテリジェンス
- 検索時のイベント操作の実行
- 相関ルールのテスト
- インシデントの作成と管理
- イベント時に手動で実行するアクション
- データの同期
- iTRACワークフロー
- 相関イベントをトリガするイベントに関するフォレンジック分析
- Secure Configuration ManagerおよびChange Guardianのイベントの添付ファイルの表示

スケーラブルストレージの有効化は1回限りの設定であり、元に戻すことはできません。スケーラブルストレージを無効にして従来のストレージに切り替えるには、Sentinelを再インストールする必要があります。

次のチェックリストでは、スケーラブルストレージを設定するために実行する必要のあるタスクの概略を示しています。

表 6-2 スケーラブルストレージの設定チェックリスト

	タスク	参照先
❒	展開の情報を確認し、スケーラブルストレージと共にどのようにSentinelを展開する必要があるかを理解します。	53 ページの 「スケーラブルストレージでの3層展開」
❒	前提条件を確認し、必要なすべてのタスクを完了します。	89ページの第13章「スケーラブルストレージのインストールと設定」。
❒	スケーラブルストレージを有効にします。 スケーラブルストレージはインストール時またはインストール後に有効にできます。 アップグレードインストールでは、Sentinelをアップグレードした後にのみ、スケーラブルストレージを有効にすることができます。	インストール時にスケーラブルストレージを有効にするには、Sentinelのカスタムインストールを実行します。詳細については、94 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。 インストール後またはアップグレード後にスケーラブルストレージを有効にするには、『 Sentinel Administration Guide』の「*Enabling Scalable Storage Post-Installation*」を参照してください。
❒	CDHコンポーネントおよびElasticsearchをSentinelと共に設定します。	『 Sentinel Administration Guide』の「*Configuring Scalable Storage*」

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。

- 49 ページの 「追加のCollector Manager instancesの利点」
- 49 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、73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、73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。

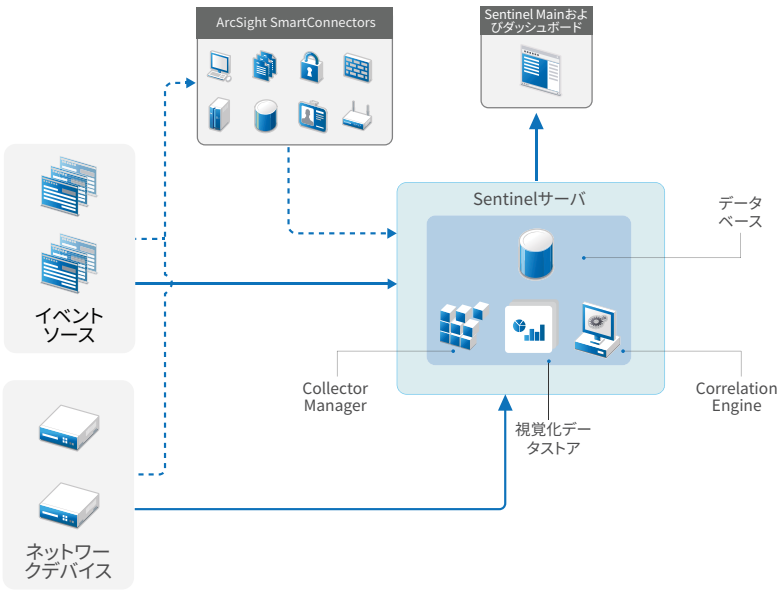
注: 1つのシステムに複数のCorrelation Engineをインストールすることはできません。リモートシステムに追加のCorrelation Engine instancesをインストールして、それらをSentinelサーバに接続することはできます。

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 6-2 オールインワン展開



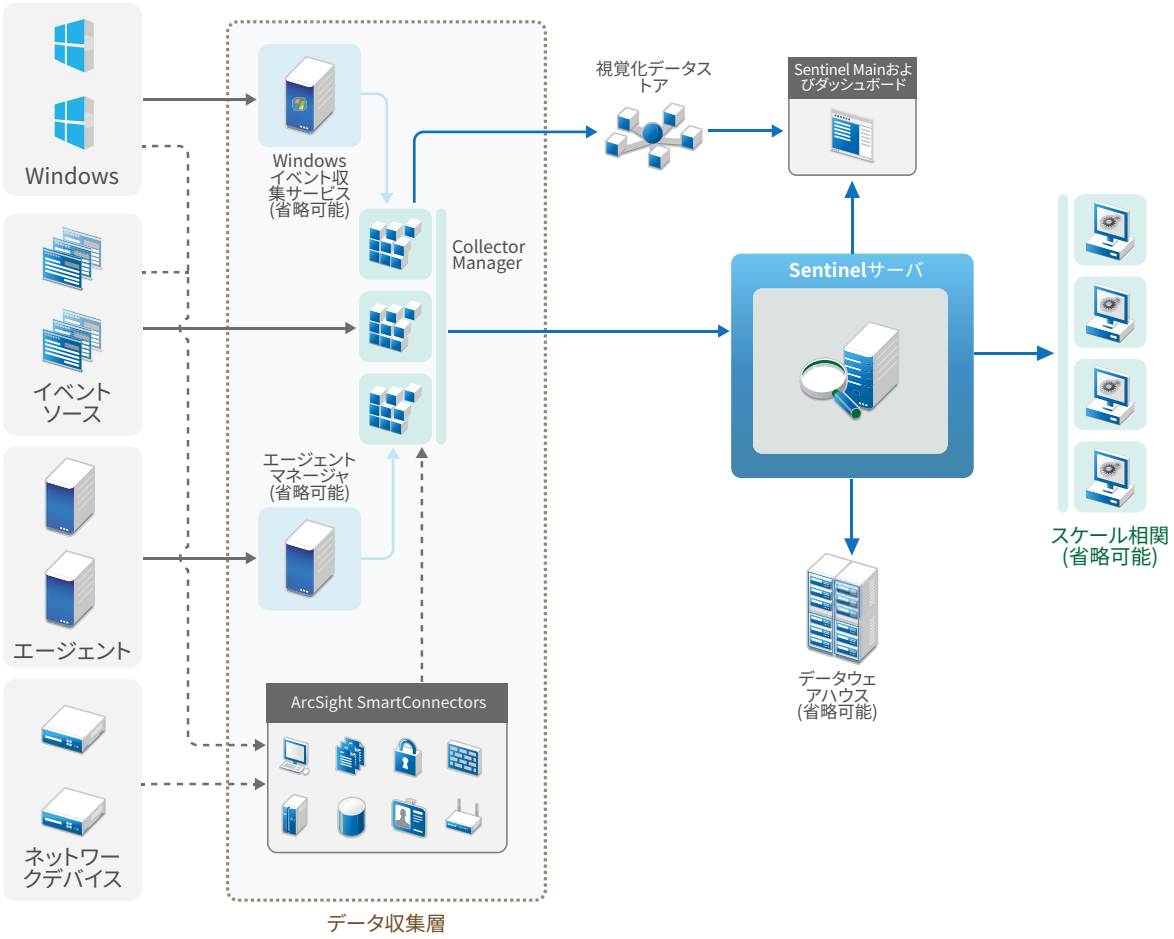
1層分散展開

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。

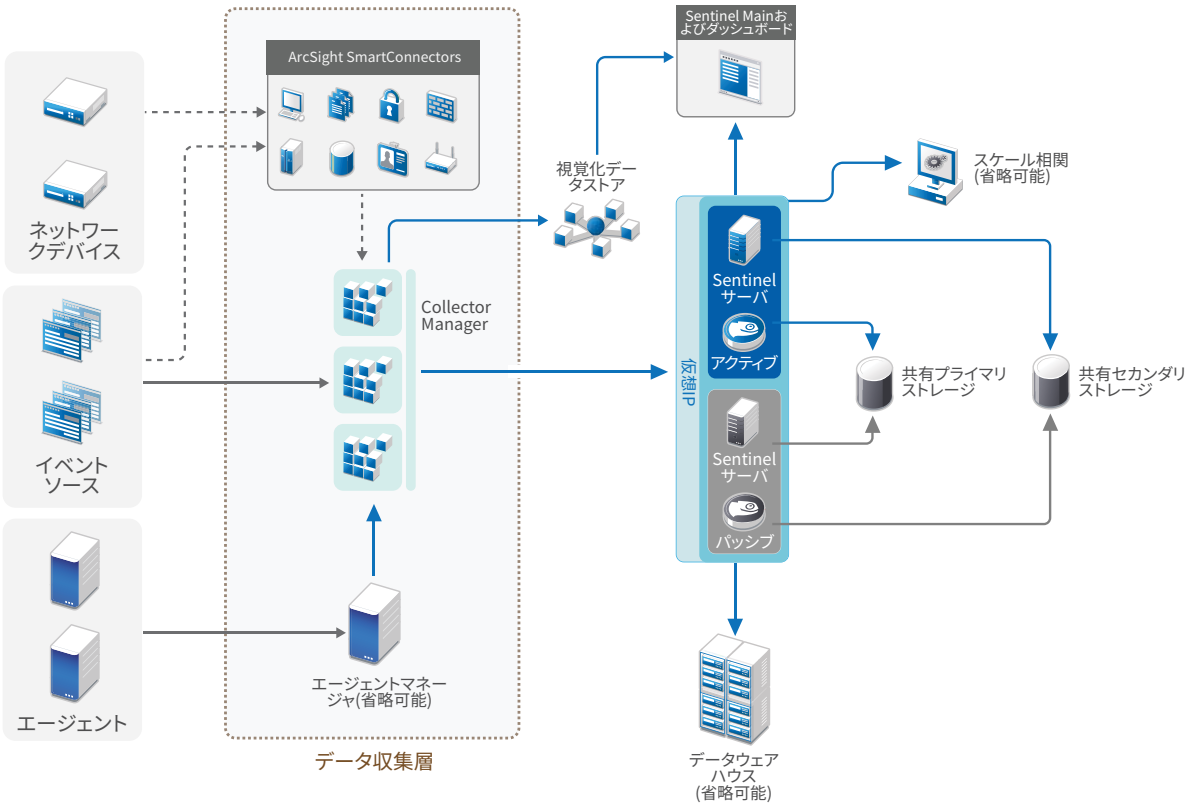
図6-3 1層分散展開



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、187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。

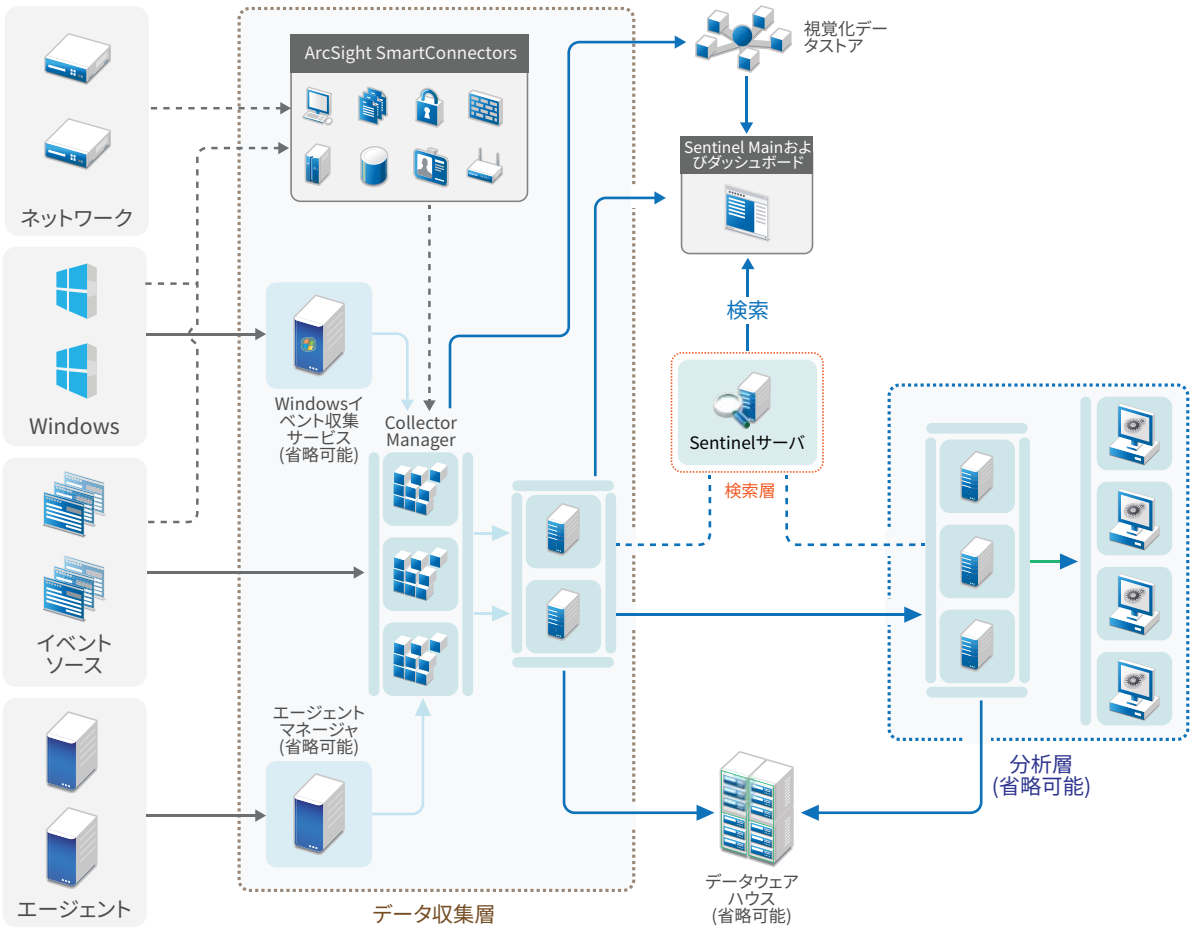
図6-4　高可用性を備えた1層分散展開



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 6-5 2層および3層分散展開



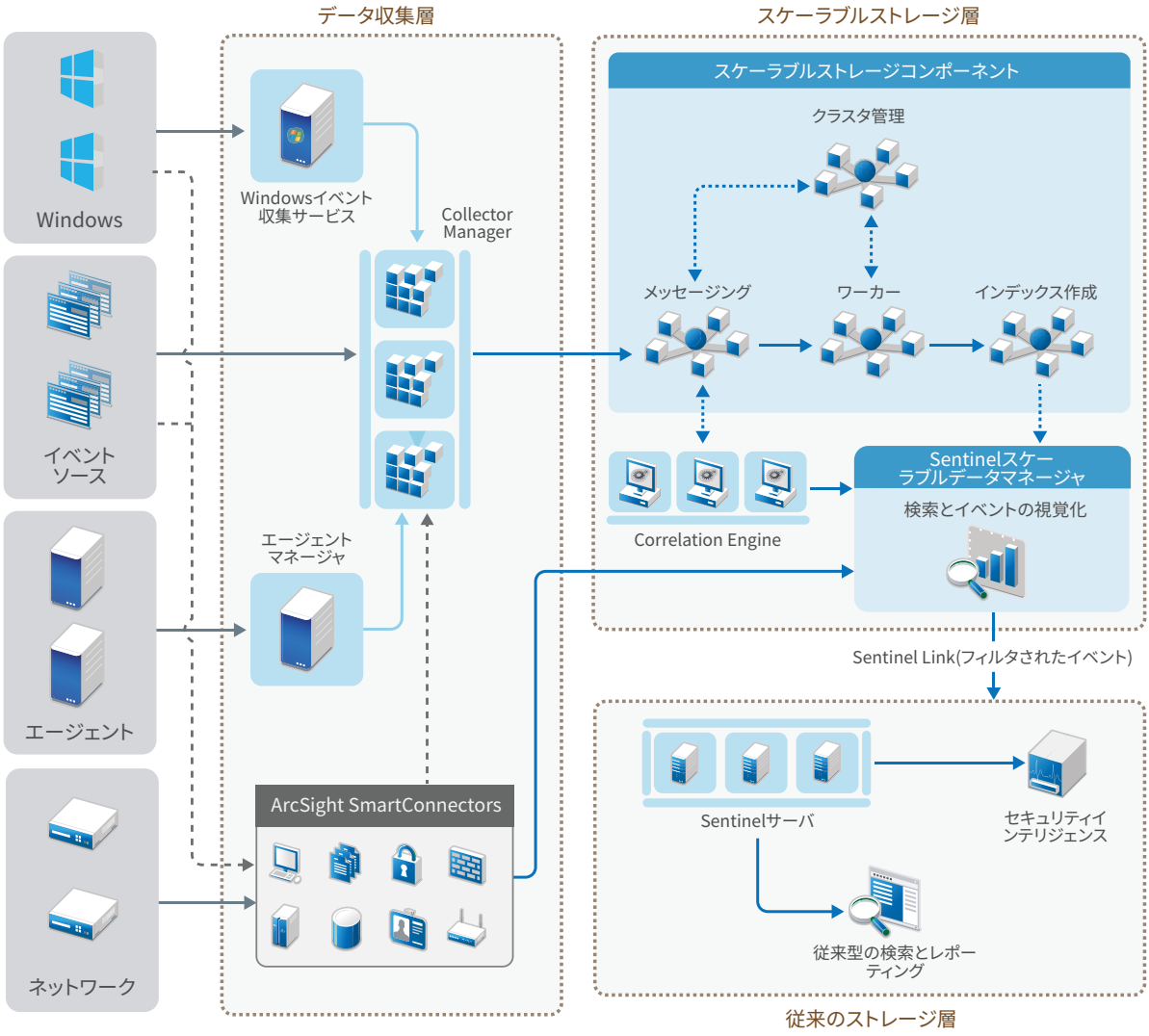
スケーラブルストレージでの3層展開

複数のSentinelサーバにイベントを分散させたり、複数のインスタンスに環境設定を重複させたりしない大規模なデータストレージとデータ処理のニーズがある場合は、スケーラブルストレージで3層分散展開を設定できます。この展開では、複数のSentinelサーバではなく、単一のSentinelサーバをスケーラブルストレージと共に使用して、大規模なデータを格納および管理できます。

スケーラブルストレージを使用するよう新しいSentinelサーバを設定することも、既存のSentinelサーバをアップグレードしてスケーラブルストレージを有効にすることもできます。

使用する必要のあるSentinel機能に応じて、Sentinel展開を設定する方法を判断できます。

図6-6 スケーラブルストレージの3層展開



この展開には、次の層が含まれます。

- **データ収集層:** さまざまなイベントソースからのイベントを収集します。従来のストレージのSentinelで既存のデータ収集のセットアップを保持しつつ、スケーラブルストレージを利用したい場合は、必要に応じて、data_uploader.shスクリプトを使用し、必要なイベントを従来のストレージからスケーラブルストレージへ直接転送できます。詳細については、177ページの第32章「スケーラブルストレージへのデータの移行」を参照してください。
- **スケーラブルストレージ層:** 大規模なデータの保存、インデックス作成、および分析を行います。この層にあるSSDMサーバでは、データの収集と相関を管理することができ、その他のSSDM機能も提供されます。SSDMで利用できないSentinel機能を使用するには、従来のストレージ層を設定することができます。収集したデータを別のSIEMシステムに転送したり、別のビジネスインテリジェンスツールからデータにクエリを実行したり、広くサポートされているHadoop、Kafka、Spark、およびElasticsearch APIを使用してHadoop配布パッケージ上で直接分析を実行したりすることもできます。

- **従来のストレージ層:** セキュリティインテリジェンス、従来の検索、およびレポーティングなどのSentinel機能を利用するには、従来のストレージを使用するSentinelの別個のインスタンスをインストールする必要があります。イベントのルーティングルールを設定すると、Sentinel Linkを使用して、目的のイベントをSentinelからSSDMに転送することができます。

  従来のストレージ層にある任意のSentinelサーバを使用すると、検索やレポーティングを実行することができます。必要に応じて、独立した検索層を設定して、従来のストレージ層にあるすべてのSentinelサーバにまたがる検索とレポーティングのために便利な単一アクセスポイントを提供することもできます。スケーラブルストレージでのイベントの検索には、SSDMの検索オプションを使用します。

スケーラブルストレージのインストールと設定の詳細については、89ページの第13章「スケーラブルストレージのインストールと設定」を参照してください。

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Collector Manager instances、SentinelリモートCorrelation Engine instances、Sentinel Mainインタフェース、Sentinel Control Center、およびSentinel Advisorサービスとの通信に、FIPS 140-2認定暗号が使用されます。

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。

RHEL6.3以降によって提供されるNSS暗号化モジュールは、FIPS140-2認定です。SLES11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FIPS140-2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、142 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。	60 ページの 「導入シナリオ」。

タスク	詳細の参照先
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。	94 ページの 「Sentinelサーバのカスタムインストール」。 99 ページの 「サイレントインストールの実行」 131ページの第23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」

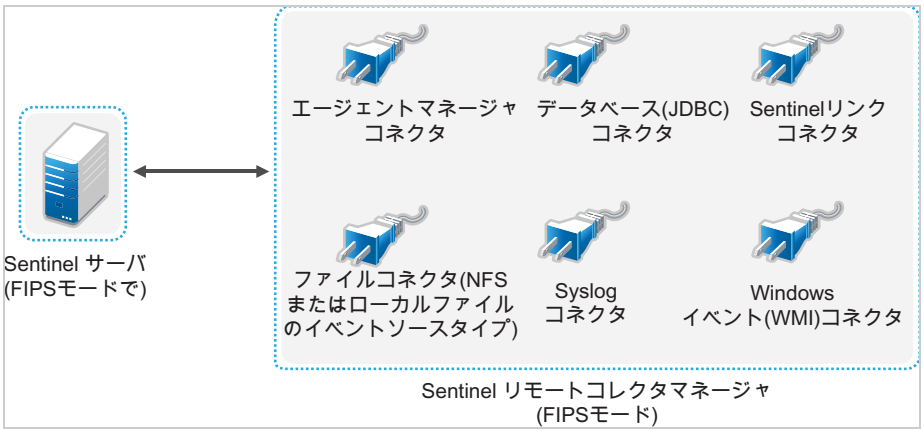
注: FIPSモードへの変換を開始する前に、Sentinelシステムをバックアップします。後でサーバを非FIPSモードに戻す必要がある場合、サポートされている方法はバックアップからの復元のみになります。非FIPSモードへ戻す方法について詳しくは、143 ページの 「Sentinelを非FIPSモードに戻す」を参照してください。

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、131 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、132 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。

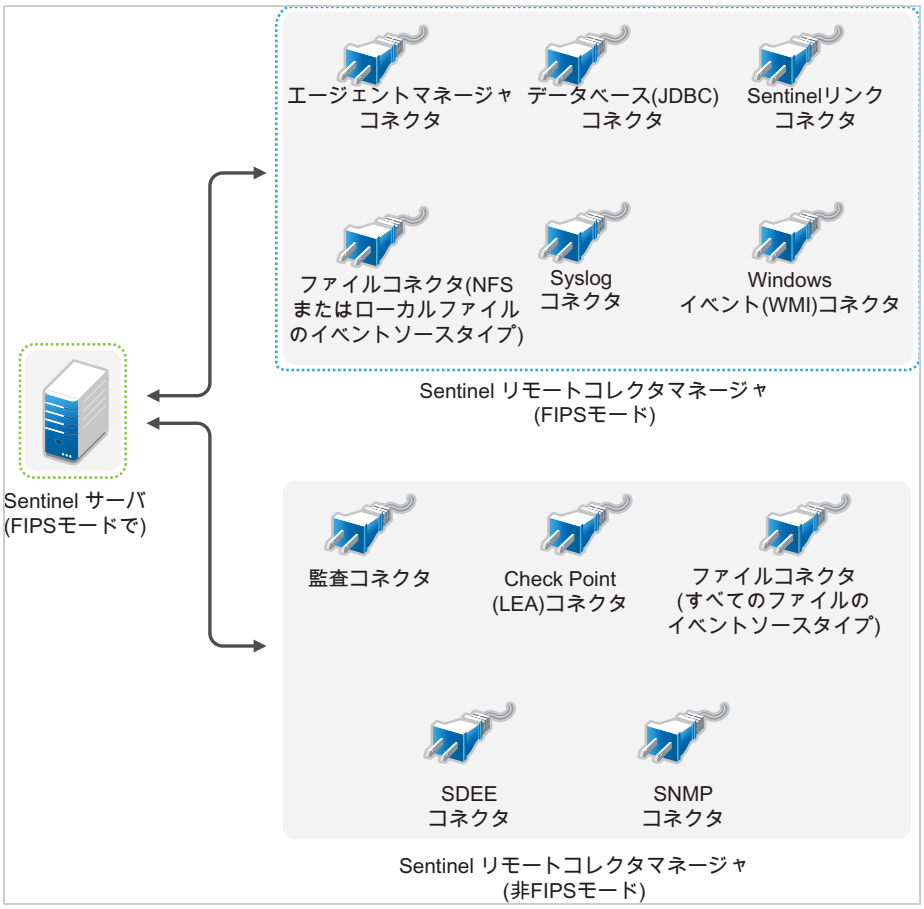
3 FIPSサーバとリモートCollector Manager instancesが相互に通信していることを確認します。

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、132 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Collector Manager instances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、131 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、132 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、132 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、「SentinelPlug-inSDK」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 443	OUTBOUND	オプション	Advisorが使用されている場合は、このポートがインターネットを経由してAdvisor Updatesページにつながるサービスへの接続を開始します。
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。
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。

ポート	方向	必須/オプション	説明
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 9443	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	INBOUND	オプション	HTTPS通信用に8443に転送されます。
UDP 514	INBOUND	オプション	Syslogメッセージ用に1514に転送されます。
TCP 1290	INBOUND	オプション	SuSE Firewallを抜けて接続することが許可されているSentinel Linkポート。
UDPおよびTCP 40000 - 41000	INBOUND	オプション	syslogなどのデータ収集サーバの設定に使用可能なポートです。Sentinelは、これらのポートをデフォルトではリスンしません。
TCP 443または80	OUTBOUND	必須	インターネット上の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。

ポート	方向	必須/オプション	説明
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。

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。
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。

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。

ポート	方向	必須/オプション	説明
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。
TCP1098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。

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。
TCP1098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。

スケーラブルストレージポート

SSDMがCDHおよびElasticsearchと正常に通信するには、Clouderaで必要とされているポート、および「Sentinelサーバのポート」セクションに記載されているポートに加えて、スケーラブルストレージの設定時に指定したポートがファイアウォール上で開いている必要があります。

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。
生データとイベントの格納には、従来のストレージを使用します。	スケーラブルストレージでは、生データとイベントを格納できます。
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、93 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、99 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 12 SP3 64ビット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、103ページの第15章「アプライアンスインストール」を参照してください。

Sentinelのインストール

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

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などはそこに格納されます。
- **MongoDBデータベース:** セキュリティインテリジェンスとアラートのデータを格納します。
- **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。
- **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。
- **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。
- **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。
- **アドバイザ:** Security Nexusを搭載したアドバイザは、オプションのデータサブスクリプションサービスです。侵入検出と防止システムから、および企業脆弱性スキャン結果から、リアルタイムイベント間のデバイスレベルの相関関係を提供します。アドバイザの詳細については、『「Sentinel Administration Guide」』の「*Detecting Vulnerabilities and Exploits*」を参照してください。
- **Sentinelのプラグイン:** Sentinelは、システムの機能を拡張および強化するさまざまなプラグインをサポートしています。これらのプラグインの一部はプリインストールされています。追加のプラグインおよびアップデートは、Sentinel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、39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、231 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、CustomerCareCenterからライセンスキーを取得してください。
- ❒ 65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。
- ❒ スケーラブルストレージ設定でSentinelを展開する予定の場合は、CDHとElasticsearchをインストールしておく必要があります。スケーラブルストレージでのSentinelの展開の詳細については、89 ページの 「スケーラブルストレージのインストールと設定」を参照してください。
- ❒ **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 6サーバのBase Serverコンポーネントが含まれている必要があります。Sentinelでは、次のRPMの64ビットバージョンが必要です。

  - bash
  - bc
  - coreutils
  - gettext
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof

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

❒ **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、/etc/sysctl.confファイルにプロパティvm.max_map_count=262144を追加して仮想メモリを設定します。

12 Elasticsearchのインストールと設定

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

Elasticsearchをインストールする前に、次の前提条件を満たします。

- 現在のEPSレートに基づき、「Sentinelの技術情報」ページ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。
- /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。

Elasticsearchのインストールと設定

Elasticsearchと必要なプラグインをElasticsearchクラスタの各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 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、『Technical Information for Sentinel』ページを参照してください。
3. Elasticsearchをインストールします。

   rpm -i elasticsearch-<*version*>.rpm
4. 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。

5 ElasticsearchユーザがJavaにアクセスできることを確認します。

6 次の情報を更新または追加して、/etc/elasticsearch/elasticsearch.ymlファイルを設定します。

プロパティと値	備考
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_	
discovery.zen.ping.unicast.hosts: [<Sentinelサーバの ElasticsearchノードのFQDN>,<*Elasticsearch node1のFQDN*>, <*Elasticsearch node2のFQDN*>,以下同様]	
thread_pool.bulk.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	
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。

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クラスタの各ノードで上記の手順をすべて繰り返します。

9 SentinelサーバのElasticsearchノードで、/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.ymlを次のように設定します。

9a elasticsearch.yml ファイル内のcluster.name値とdiscovery.zen.ping.unicast.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。

9b network.hostプロパティに、localhost IPアドレスに続けてローカルElasticsearchノードのIPアドレスを次のように指定します。

network.host: ["127.0.0.1","<*SentinelのElasticsearchノードのIPアドレス*>"]

10 (状況によって実行)従来のストレージを使用するSentinelの場合、/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*>

11 Sentinelを再起動します。

rcsentinel restart

12 各Elasticsearchノードを再起動します。

/etc/init.d/elasticsearch start

13 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。

13a Sentinelサーバにnovellユーザとしてログインします。

13b 既存のすべてのアラートデータが外部Elasticsearchノードに移動したことを確認します。

13c /etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.ymlファイルを開き、次の情報を追加します。

```
node.master: true
node.data: false
node.ingest: false
search.remote.connect: false
```

13d Elasticsearchを再起動します。

rcsentinel stopSIdb

rcsentinel startSIdb

14 81 ページの 「Elasticsearchにおけるデータのセキュリティ保護」に従って手順を進めます。

Elasticsearchにおけるデータのセキュリティ保護

Elasticsearchクラスタノードには、次のようにさまざまなクライアントがアクセスできます。

- Sentinel: イベントデータをフェッチしてイベント視覚化ダッシュボードに表示します。
- YARN NodeManagerノードで実行されるSparkジョブ: Kafkaから受信したイベントの一括インデックス作成を行います。(SSDM用)
- Collector Manager: 従来のストレージを使用するSentinelでイベントの一括インデックス作成を行います。
- その他の外部クライアント: カスタム分析などのカスタム操作を実行します。

Sentinelには、Elasticsearchへのアクセスを認証して許可する**elasticsearch-security-plugin**という名前のElasticsearch用セキュリティプラグインが備わっています。

このプラグインは、以下のようにクライアントの接続方法に応じた検証を行うため、SAMLトークンとホワイトリストのいずれかを使用します。

- クライアントが要求と一緒にSAMLトークンを送信する場合、このプラグインはSentinel認証サーバに照合してトークンを認証します。認証に成功すると、プラグインは、クライアントが権限を持つフィルタ済みのイベントに対するアクセスのみを許可します。

  たとえば、イベント視覚化ダッシュボード(クライアント)には、ユーザ役割で表示が許可されているElasticsearchのイベントのみが表示されます。

  役割と許可については、『*Sentinel Administration Guide*』の「「Creating a Role」」を参照してください。
- クライアントがSAMLトークンを送信できない場合、このプラグインは正当なクライアントを記載したホワイトリストをチェックします。検証に成功すると、プラグインは、フィルタ処理せずにすべてのイベントへのアクセスを許可します。
- クライアントが有効なSAMLトークンを送信しない、またはホワイトリストで許可されていない場合、プラグインはこれを正当なクライアントではないと見なし、クライアントにアクセスを与えません。

このセクションでは、Elasticsearchセキュリティプラグインのインストールと設定に関する情報を示します。

- 82 ページの 「Elasticsearchセキュリティプラグインのインストール」
- 83 ページの 「追加のElasticsearchクライアントへのセキュリティ保護されたアクセスの提供」
- 85 ページの 「Elasticsearchプラグイン設定の更新」

Elasticsearchセキュリティプラグインのインストール

Elasticsearchセキュリティプラグインは、Elasticsearchクラスタの各ノードと、Sentinelに含まれるElasticsearchノードにもインストールする必要があります。

Sentinelに含まれるElasticsearchノードにelasticsearch-security-plug-inをインストールする方法:

1. Sentinel MainまたはSSDMサーバにログインします。
2. 次のように、JAVA_HOME環境変数のパスを設定します。

   ```
   export JAVA_HOME=/<Sentinel_installation_path>/opt/novell/sentinel/jdk/
   ```

3. プラグインをインストールします。

   Linuxの場合は、Elasticsearchを実行しているユーザとしてログインし、次のコマンドを実行します。

   ```
   <sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/
   elasticsearch-plugin install file://localhost/<Sentinel_installation_path>/
   etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip --
   verbose
   ```

   インストールを続行するプロンプトが表示されたら、yと入力します。

4 (状況によって実行) ElasticsearchがデフォルトのHTTPポート(9200)でリスンしていない場合、<Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txtファイルの各エントリでElasticsearchポート番号を更新する必要があります。

   詳細については、84 ページの 「ホワイトリストを使用して、Elasticsearchクライアントにアクセスを提供」を参照してください。

5 次のコマンドを使用して、Sentinelでインデックス作成サービスを再開します。

```
rcsentinel stopSIdb
rcsentinel startSIdb
```

外部Elasticsearchノードにelasticsearch-security-plug-inをインストールする方法:

Elasticsearchクラスタ内の各ノードで次の手順を実行します。

1 Sentinel MainまたはSSDMサーバにログインします。

2 <Sentinel_installation_path>/etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zipファイルを、Elasticsearchクラスタの各ノードで一時的な場所にコピーします。

3 プラグインをインストールします。

   Linuxの場合は、Elasticsearchを実行しているユーザとしてログインし、次のコマンドを実行します。

```
<elasticsearch_install_directory>/bin/elasticsearch-plugin install file://
localhost/<full path of elasticsearch-security-plugin*.zip file> --verbose
```

   インストールを続行するプロンプトが表示されたら、yと入力します。

4 (状況によって実行)ElasticsearchがデフォルトHTTPポート(9200)でリスンしていない場合、<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txtファイルの各エントリでElasticsearchポート番号を更新する必要があります。

   詳細については、84 ページの 「ホワイトリストを使用して、Elasticsearchクライアントにアクセスを提供」を参照してください。

5 Elasticsearchを再起動します。

追加のElasticsearchクライアントへのセキュリティ保護されたアクセスの提供

デフォルトでは、SSDMサーバ(イベント視覚化ダッシュボード用)、YARN NodeManagers、Sentinelサーバ(イベント視覚化ダッシュボード用)、およびRCMなどの信頼できるクライアントがElasticsearchにアクセスできます。その他のElasticsearchクライアントを使用する場合は、SAMLトークンまたはホワイトリストのいずれかを使用して、それらの追加クライアントにセキュリティ保護されたアクセスを提供する必要があります。

SAMLトークンを使用して、ElasticsearchRESTクライアントにアクセスを提供

ElasticsearchにアクセスするためにRESTクライアントを使用している場合、次のように要求ヘッダにSAMLトークンを含めることができます。

1 Sentinel認証サーバからSAMLトークンを取得します。詳細については、Sentinelで使用可能なREST APIのマニュアルを参照してください。

［**ヘルプ**］>［**API**］>［**チュートリアル**］>［**APIセキュリティ**］>［**SAMLトークンの取得(ログオン)**］をクリックします。

2 後続のREST要求でSAMLトークンを使用します。RESTクライアントによる各要求の認証ヘッダにSAMLトークンを含めます。ヘッダ名を［認証］に、ヘッダ値をステップ1で取得した<*SAMLトークン*>に指定します。

ホワイトリストを使用して、Elasticsearchクライアントにアクセスを提供

デフォルトで、信頼されているElasticsearchクライアントのIPアドレスはSentinelによって自動的にホワイトリストに入力されます。たとえば、SSDMサーバ(イベント視覚化ダッシュボード用)、YARN NodeManagers、Sentinelサーバ(イベント視覚化ダッシュボード用)、およびRCMなどです。Elasticsearchセキュリティプラグインは、ホワイトリストに記載されているすべてのクライアントにElasticsearchへのアクセス権を付与します。

有効なSentinelトークンを送信しないその他のクライアントにアクセスを提供するには、クライアントのIPアドレスと、ElasticsearchサーバのHTTPポート番号をIPアドレス:ポートの形式でホワイトリストに追加する必要があります。不正アクセスを防止するため、ホワイトリストに追加する外部クライアントが正当で信頼に値することを確認しなければなりません。

ホワイトリストを更新する方法:

1 Elasticsearchを実行しているユーザとしてSentinelサーバまたはElasticsearchノードにログインします。

2 次のファイルに<Elasticsearch_Client_IP>:<Target_Elasticsearch_HTTP_Port>エントリを追加します。

- Sentinelに含まれるElasticsearchノードの場合、<Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin//elasticsearch-ip-whitelist.txt。
- 外部Elasticsearchノードの場合、<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt。

複数のエントリがある場合、各エントリを新しい行に追加し、ファイルを保存します。

3 Elasticsearchクラスタのノードごとに前述のステップを繰り返します。

Elasticsearchプラグイン設定の更新

スケーラブルストレージコンポーネントのIPアドレス/ホスト名とポート番号またはElasticsearchバージョンとポート番号を変更する場合、Elasticsearchプラグイン設定ファイルもそれに応じて更新しなければなりません。

Elasticsearchクラスタの各ノードで次の手順を実行します。

1. Elasticsearchを実行しているユーザとしてElasticsearchノードにログインします。
2. (状況によって実行)YARN NodeManagerのIPアドレス、SSDMまたはSentinelサーバのIPアドレス、RCMのIPアドレス、またはElasticsearchポート番号を変更した場合、それに応じてホワイトリストも更新し、Elasticsearchセキュリティプラグインが Elasticsearchクライアントにアクセス権を付与できるようにします。

   HAモードでSSDMまたはSentinelを設定している場合、HAクラスタのアクティブノードとパッシブノードごとの物理IPアドレスエントリを追加します。

   HAクラスタの任意のノードの物理IPアドレスを変更したり、HAクラスタに新しいノードを追加したりした場合、ホワイトリストを更新して、変更したノードまたは新たに追加したノードの物理IPアドレスを反映します。

   詳細については、84 ページの 「ホワイトリストを使用して、Elasticsearchクライアントにアクセスを提供」を参照してください。
3. (状況によって実行)SSDMのIPアドレス、SentinelサーバのIPアドレス、またはWebサーバのポート番号を変更した場合、次のファイルのauthServer.hostおよびauthServer.portのプロパティを更新して、Elasticsearchを再開します。
   - Sentinelに含まれるElasticsearchノードの場合、<Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-configuration.properties。
   - 外部Elasticsearchノードの場合、<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/plugin-configuration.properties。

   HAモードでSSDMまたはSentinelを設定している場合、authServer.hostプロパティをHAクラスタの仮想IPアドレスに設定します。

   HAクラスタの仮想IPアドレスを変更する場合は、authServer.hostプロパティを変更後の仮想IPアドレスに更新します。
4. (状況によって実行)Elasticsearchを新しいバージョンにアップグレードした場合は、次のファイルのelasticsearch.versionプロパティを更新してElasticsearchを再開します。
   - Sentinelに含まれるElasticsearchノードの場合、/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-descriptor.properties。
   - 外部Elasticsearchノードの場合、<elasticsearch_install_directory>/plugins/elasticsearch-security-plugin/plugin-descriptor.properties。

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: /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。

スケーラブルストレージの場合: SSDMホームページで、［**ストレージ**］>［**スケーラブルストレージ**］>［**詳細プロパティ**］>［**Elasticsearch**］をクリックします。

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。
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	5	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。

Elasticsearchセキュリティプラグインの再展開

以下のシナリオでは、Sentinelに含まれるElasticsearchノードおよび外部ElasticsearchノードにElasticsearchセキュリティプラグインを再展開、つまりアンインストールしてから再インストールする必要があります。

- リモートCollector ManagerのIPアドレスを追加または変更した場合。

- リモートCollector Managerインスタンスをアンインストールした場合。
- インストール後にスケーラブルストレージを有効化した場合。

Elasticsearchセキュリティプラグインを再展開する方法:

1. Elasticsearchを実行しているユーザとしてSentinelサーバまたはElasticsearchノードにログインします。
2. 次のコマンドを使用してプラグインをアンインストールします。
   - Sentinelに含まれるElasticsearchの場合: <Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin remove file://localhost/<sentinel_installation_path>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin
   - 外部Elasticsearchの場合: <elasticsearch_install_directory> remove file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin
3. プラグインを再インストールします。
   - Sentinelに含まれるElasticsearchの場合: <Sentinel_installation_path>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin install file://localhost/<sentinel_installation_path>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin
   - 外部Elasticsearchの場合: <elasticsearch_install_directory>/bin/elasticsearch-plugin install file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin
4. 次のコマンドを使用してElasticsearchを再開します。
   - Sentinelに含まれるElasticsearchノードの場合:

     ```
     rcsentinel stopSIdb
     rcsentinel startSIdb
     ```

   - 外部Elasticsearchノードの場合:

     sudo systemctl restart elasticsearch.service

13 スケーラブルストレージのインストールと設定

Sentinelのデータストレージオプションとしてスケーラブルストレージを設定するには、次の表に示す前提条件を満たします。

表 13-1 スケーラブルストレージを有効にする前提条件

❒	タスク	参照先
❒	EPSレートおよび必要なレプリカ数に基づいて、設定が必要なHadoop分散クラスタおよびElasticsearchクラスタノードの数を決定します。 CDHおよびElasticsearchの認定バージョンを決定します。	Technical Information for Sentinel。
❒	CDH、Elasticsearch、およびSentinelには独自のプラットフォームのサポートマトリックスがあります。これらの製品の各プラットフォームのサポートマトリックスを確認し、使用するプラットフォームを決定します。 Elasticsearchの場合、RPMにはinitスクリプトが含まれているため、RPMインストールをお勧めします。これによってElasticsearchはサービスとしてインストールされて再起動時とアップグレード時に自動的に停止および開始するようになり、設定ファイルが上書きされなくなります。 Elasticsearch RPMのインストールはSLES 11ではサポートされていません。このため、Elasticsearchに適したプラットフォームを決定してください。	ClouderaマニュアルのCDHサポートマトリックス。 ElasticsearchマニュアルのElasticsearchサポートマトリックス。 Sentinelサポートマトリックス。
❒	クラスタモードでCDHをインストールし、設定します。	90 ページの 「CDHのインストールと設定」。
❒	クラスタモードでElasticsearchをインストールし、設定します。	79 ページの 「Elasticsearchのインストールと設定」。
❒	Sentinelでスケーラブルストレージを有効にします。	92 ページの 「スケーラブルストレージの有効化」

CDHのインストールと設定

このセクションでは、CDHのインストールおよび設定時にSentinelに必要な特定の設定について説明します。CDHのインストールと設定の詳細については、Clouderaの認定バージョンのマニュアルを参照してください。

SentinelはCDHの無料版であるCloudera Expressで動作します。SentinelはCloudera Enterpriseとも連携します。これにはClouderaからのライセンス購入が必要ですが、Cloudera Expressエディションでは使用できないさまざまな機能が含まれています。ClouderaExpressで開始すると決定し、後でCloudera Enterpriseの機能が必要であると判明した場合は、Clouderaからライセンスを購入した後でクラスタをアップグレードすることができます。

前提条件

CDHをインストールする前に、次の前提条件に従ってホストを設定する必要があります。

- Clouderaのマニュアルで説明されている前提条件を満たします。
- パフォーマンス向上のため、ext4またはXFSファイルシステムを使用します。
- CDHではデフォルトでインストールされないオペレーティングシステムパッケージがいくつか必要です。そのため、それぞれのオペレーティングシステムのDVDをマウントする必要があります。インストールするパッケージについては、Clouderaのインストール手順で示します。
- CDHでは、SLESオペレーティングシステムにpython-psycopg2パッケージが必要です。python-psycopg2パッケージをインストールします。詳細については、openSUSEのマニュアルを参照してください。
- 仮想マシンを使用する場合は、仮想マシンのノードを作成するときに、必要なディスク容量をファイルシステムに確保します。たとえば、VMwareでシックプロビジョニングを使用できます。
- SentinelとCDHクラスタノードのタイムゾーンが同じであることを確認します。
- /etc/sysctl.confファイルで、次のエントリを追加してすべてのホストのswappinessを1に設定します。

  ```
  vm.swappiness=1
  ```

  この設定をすぐに適用するには、次のコマンドを実行します。

  ```
  sysctl -p
  ```

- CDHのJDKバージョンは、最低限、Sentinelで使用されているものと同じJDKバージョンである必要があります。CDHで使用できるJDKバージョンがSentinel JDKのバージョンより低い場合、CDHリポジトリで使用可能なJDKをインストールするのではなく、次の手順に従ってJDKを手動でインストールする必要があります。

  manage_spark_jobs.shスクリプトを使用してSparkジョブをYARNで送信するとJDK RPMのインストールでエラーが発生するため、アーカイブバイナリファイル(.tar.gz)を使用してJDKをインストールしてください。

  Sentinelで使用されているJDKバージョンを判別するには、Sentinelリリースノートを参照してください。

CDHのインストールと設定

CDHの認定バージョンをインストールします。CDHの認定バージョンの詳細は、『Technical Information for Sentinel』ページを参照してください。インストールの手順については、Clouderaのマニュアルで認定バージョンを参照してください。

CDHのインストール中に、次を実行します。

- (条件による)内蔵PostgreSQLデータベースのインストール中にインストールエラーが発生する場合、次の手順を実行します。

  mkdir -p /var/run/postgresql

  sudo chown cloudera-scm:cloudera-scm /var/run/postgresql

- ［**Select Repository(リポジトリ選択)**］ ウィンドウでソフトウェアインストールの種類を選択するときに、［**Use Parcels(パーセルを使用)**］が選択されていることを確認し、［**Additonal Parcels(追加パーセル)**］でKafkaを選択します。
- サービスを追加する場合は、次のサービスを必ず有効にします。
  - Cloudera Manager
  - ZooKeeper
  - HDFS
  - HBase
  - YARN
  - Spark
  - Kafka

  注: Spark履歴サーバとHDFS NameNodeはシステム信頼性の面から、同じノードにインストールする必要があります。スケーラブルストレージアーキテクチャの詳細については、45 ページの「スケーラブルストレージのプラニング」を参照してください。

  上記のサービスを有効にする場合、次の高可用性を設定します。
  - HBaseのHMaster
  - HDFSのNameNode
  - YARNのResourceManager
- (条件による)Javaパスがないためにインストーラでクライアントの環境設定が展開されない場合、新しいブラウザセッションを開き、次のように手動でJavaパスを更新します。

  ［**Hosts(ホスト)**］>［**All Hosts(すべてのホスト)**］>［**Configuration(環境設定)**］をクリックし、［**Java Home Directory(Javaホームディレクトリ)**］フィールドで正しいパスを指定します。

スケーラブルストレージの有効化

スケーラブルストレージは、Sentinelのインストール時またはインストール後に有効にできます。インストール時にスケーラブルストレージを有効にすると、SentinelはCDHコンポーネントをデフォルト値で設定します。これらの設定の一部は永続的であり、変更できません。たとえば、Kafkaトピックのデフォルトのパーティション数は9であり、この値は変更できません。

デフォルト値を変更する場合は、Sentinelをインストールした後にスケーラブルストレージを有効にし、その後、必要に応じてCDHコンポーネントの環境設定を行う必要があります。

従来型インストールでは、スケーラブルストレージはSentinelのインストール時またはインストール後のどちらでも有効にできます。アプライアンスインストールの場合、スケーラブルストレージはインストール後にのみ有効にすることができます。

アップグレードインストールでは、Sentinelをアップグレードした後にのみ、スケーラブルストレージを有効にすることができます。

スケーラブルストレージの有効化に移る前に、Kafka、HDFS NameNode、YARN NodeManager、ZooKeeper、およびElasticsearchのノードのIPアドレス、ホスト名、ポート番号のリストを控えておきます。この情報はスケーラブルストレージを有効にするときに必要です。

Sentinelのインストール時にスケーラブルストレージを有効にするには、94 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。

Sentinelのインストールまたはアップグレードの後にスケーラブルストレージを有効にするには、『「 Sentinel Administration Guide」』の「*Enabling Scalable Storage Post-Installation*」を参照してください。

14 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 スケーラブルストレージを有効にするには、89ページの第13章「スケーラブルストレージのインストールと設定」で指定されている前提条件を満たす必要があります。

2 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。

3 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。

4 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>
```

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 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。

9 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。

10 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。

11 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。

12 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。

13 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。

14 ポートを変更してから「7」を指定し、完了します。

15 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。

16 ***Sentinel をFIPS 140-2 モードで有効にする場合は、***「y」を入力します。

16a 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。

16b 外部証明書をキーストアデータベースに挿入してトラストを確立する場合は、「y」を押して証明書ファイルのパスを指定します。そうしない場合は、「n」を押します。

16c 133ページの第24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。

17 ***スケーラブルストレージを有効にする場合は、***「yes」または「y」を入力してスケーラブルストレージを有効にします。

重要: スケーラブルストレージは、有効にすると、Sentinelを再インストールしない限り設定を元に戻すことはできません。

17a スケーラブルストレージコンポーネントのIPアドレスまたはホスト名、およびポート番号を指定します。

17b (条件による)スケーラブルストレージの環境設定を終了し、Sentinelのインストールを続行する場合は、「no」または「n」を入力します。

17c Sentinelのインストール後、セクション「96 ページの 「スケーラブルストレージのインストール後の設定」」で取り上げられているスケーラブルストレージ設定を行います。

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。

スケーラブルストレージのインストール後の設定

1. SSDMサーバにログインします。
2. インストールしたSentinelバージョンを表示するため、ブラウザのキャッシュをクリアします。
3. イベントとアラートを表示するには、SSDMに含まれるElasticsearchノードを、スケーラブルストレージ用にセットアップしたElasticsearchクラスタに追加します。

   ローカルのElasticsearchノードで/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.ymlファイルを開き、次の情報を追加します。

   - cluster.name: <*Elasticsearch _cluster_name*>
   - node.name: <*node_name*>
   - discovery.zen.ping.unicast.hosts: ["<*FQDN of elasticsearch node1*>", "<*FQDN of elasticsearch node2*>", "以下同様"]

   すべての外部Elasticsearchノードで/etc/elasticsearch/elasticsearch.ymlを開き、次のように更新します。

   discovery.zen.ping.unicast.hosts: ["<*FQDN of elasticsearch node1*>", "<*FQDN of elasticsearch node2*>", "以下同様"]

   注: ローカルのelasticsearch.ymlファイルと外部Elasticsearchノードのelasticsearch.ymlファイルのパラメータ値が、network.hostとnode.name以外は同じであることを確認します。これらの値は、ノードごとに固有であるためです。

4. 次のコマンドを使用して、インデックス作成サービスを再開します。

   ```
   rcsentinel stopSIdb
   rcsentinel startSIdb
   ```

5. 次のセクションに示されているスケーラブルストレージ設定を行います。
   - 81 ページの 「Elasticsearchにおけるデータのセキュリティ保護」

- 『*Sentinel Administration Guide*』の「Performance Tuning Guidelines」
- 『*Sentinel Administration Guide*』の「Processing Data」

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、48 ページの 「分散展開の利点」を参照してください。

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、39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。

Collector ManagerとCorrelation Engine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. 次のコマンドを指定して、Collector ManagerまたはCorrelation Engineをインストールします。

   Collector Managerの場合:

   `./install-cm`

Correlation Engineの場合:

```
./install-ce
```

または

複数のシステムにコレクタマネジャまたはCorrelation Engine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。

Collector Managerの場合:

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

Correlation Engineの場合:

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

8 インストールに使用する言語の番号を指定します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

9 スペースキーを押して使用許諾契約を確認します。

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

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。

11 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。

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

13 (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。

13a Sentinelサーバ通信チャネルのポート番号。

13b Sentinel Webサーバのポート番号。

14 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:

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

非FIPSモードの場合:

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

証明書の出力をステップ 12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。

---

15 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。

16 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。

17 (条件による)カスタム環境設定を選択する場合は、「yes」または「y」と入力し、SentinelでFIPS 140-2モードを有効にして、FIPS環境設定を続行します。

18 (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、『*SentinelAdministratorGuide*』の「「AuthenticationMethods」」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。

19 (状況によって実行)イベント視覚化を有効にした場合は、Collector ManagerをElasticsearchホワイトリストに追加する必要があります。詳細については、84 ページの 「ホワイトリストを使用して、Elasticsearchクライアントにアクセスを提供」を参照してください。

20 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、Collector ManagerまたはCorrelation Engine instancesをインストールして展開する必要がある場合は、サイレントインストール(無人インストール)が便利です。そのような場合には、インタラクティブインストール中にインストールパラメータを記録し、記録したファイルをその他のサーバで実行します。

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、93 ページの 「Sentinelサーバの標準インストール」または94 ページの 「Sentinelサーバのカスタムインストール」および97 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。

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、以下のステップを行います。

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 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 次のコマンドを指定して、サイレントモードでインストールを実行します。

Sentinelサーバの場合:

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

Collector Managerの場合:

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

Correlation Engineの場合:

```
./install-ce -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) SentinelサーバのFIPS 140-2モードを有効にする場合は、** 133ページの第24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。

非rootユーザとしてSentinelをインストール

組織のポリシーにより、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。

注: デフォルト以外の既存のディレクトリにSentinelをインストールする場合は、そのディレクトリに対する所有権をnovellユーザが所持していることを確認してください。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>
```

---

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 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

7 (条件による)インタラクティブインストールを実行するには:

7a 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

7b ステップ 9に進みます。

8 (条件による)サイレントインストールを実行する場合、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、93 ページの「Sentinelサーバの標準インストール」または94 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。

サイレント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 -u <*response_file*>
	デフォルト以外の場所: ./install-sentinel --location=/foo -u <*response_file*>
Collector Manager	**デフォルトの場所:** ./install-cm -u <*response_file*>
	デフォルト以外の場所: ./install-cm --location=/foo -u <*response_file*>
Correlation Engine	**デフォルトの場所:** ./install-ce -u <*response_file*>
	デフォルト以外の場所: ./install-ce --location=/foo -u <*response_file*>

インストールは、レスポンスファイルに格納された値を使用して進行します。

8b ステップ 12に進みます。

9 インストールに使用する言語の番号を指定します。

エンドユーザの使用許諾契約が、選択した言語で表示されます。

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

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

11 インストールのモードを指定するように求められます。

- 標準環境設定で続行する場合は、93 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、94 ページの 「Sentinelサーバのカスタムインストール」のステップ 8からステップ 15に従って手順を進めます。

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

```
./bin/root_install_finish
```

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

Sentinel 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。

15 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SLES12SP3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。サポートされる仮想化プラットフォームについて詳しくは、 Sentinelの技術情報Webサイトを参照してください。

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。

- 104 ページの 「Sentinelのインストール」
- 105 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。

17 108 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。

1 104 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、『*SentinelAdministratorGuide*』の「「AuthenticationMethods」」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アドレスも表示されます。

7 104 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。

- 106 ページの 「Sentinelのインストール」
- 107 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:

1 106 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、『*SentinelAdministratorGuide*』の「「AuthenticationMethods」」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。

- 108 ページの 「アップデートの登録」
- 109 ページの 「従来のストレージのパーティションの作成」
- 110 ページの 「スケーラブルストレージの設定」
- 110 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。

Sentinelアプライアンス管理コンソールによる登録

SLES 12 SP3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更新するよう登録できます。

1 次のいずれかの方法では、Sentinelアプライアンスを起動します。

- Sentinelログインし、［**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

SLES 11 SP4またはSLES 12 SP3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。

更新用に登録する方法

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、42 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

スケーラブルストレージの設定

データストレージオプションとしてスケーラブルストレージを有効にして設定するには、『「Sentinel Administration Guide」』の「*Configuring Scalable Storage*」を参照してください。

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。

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

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SLES11SP3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-7.0-Updates sle-11-x86_64

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

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

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、159 ページの 「Sentinelのアップグレード」を参照してください。

16 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。

- 113 ページの 「コレクタのインストール」
- 113 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。

17 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>
  ```

  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。

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。

18 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

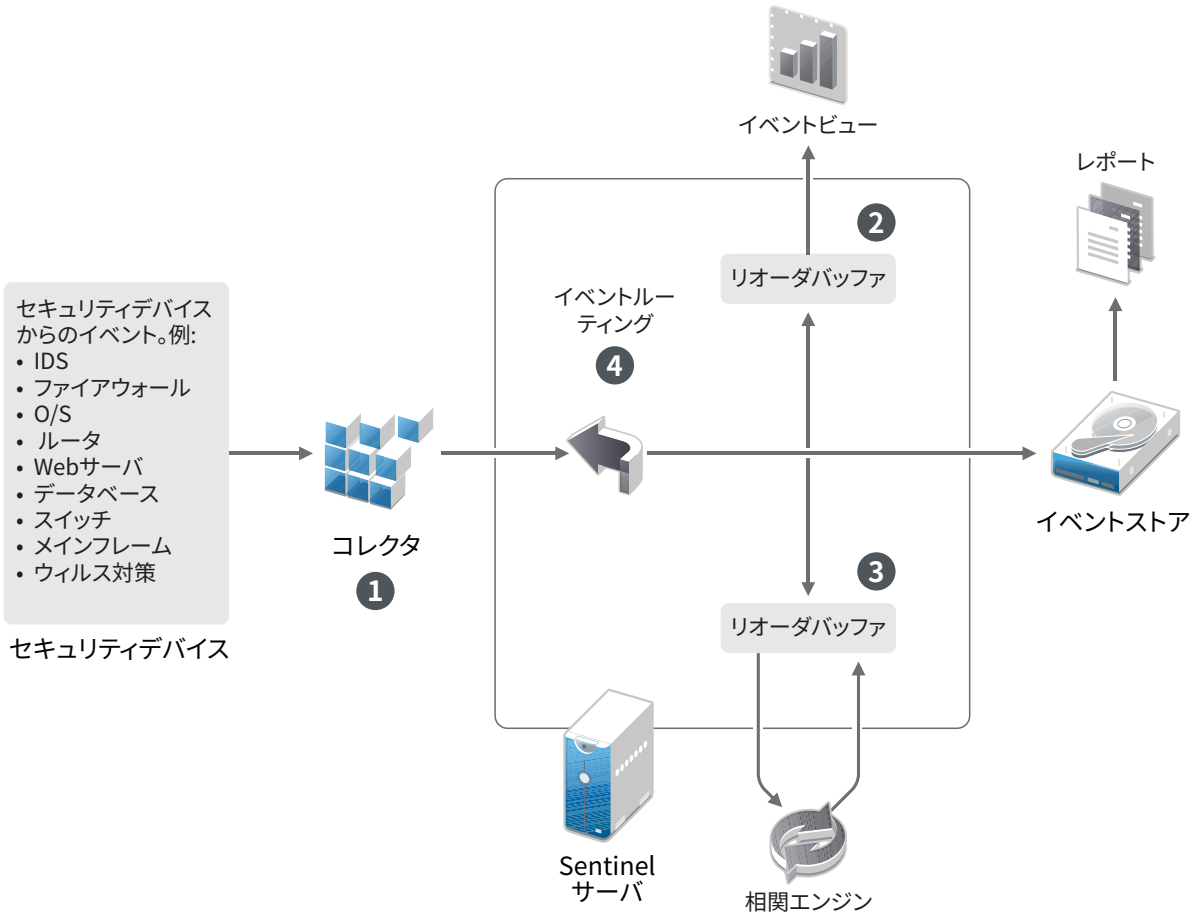
Sentinelは、ネットワーク全体に分散するいくつものプロセスで構成される分散システムです。また、イベントソースによって多少の遅延が発生する可能性があります。これに対応するために、Sentinelプロセスは、イベントを処理する前に、イベントを時間順に並び替えます。

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 18-1 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。

19 Elasticsearchにおけるデータのセキュリティ保護

Sentinelではブラウザベースの分析と検索のダッシュボードであるKibanaを使用していて、ダッシュボードでイベントとアラートを視覚化できます。Sentinelは、アラートの保存とインデックス作成をElasticsearchで行います。またイベント視覚化機能を利用するために、Elasticsearchでイベントの保存とインデックス作成を行うようSentinelを設定することもできます。Sentinelのダッシュボードは Elasticsearchのデータにアクセスして、ダッシュボードにイベントやアラートを表示します。ダッシュボードに表示されるデータを、ユーザの役割で表示することが許可されているものだけに限定し、Elasticsearchで承認されていないデータアクセスを防止するには、Elasticsearchセキュリティプラグインをインストールする必要があります。詳細については、81 ページの 「Elasticsearchにおけるデータのセキュリティ保護」を参照してください。

20 イベント視覚化の有効化

スケーラブルストレージのセットアップでは、デフォルトでイベント視覚化機能が利用できます。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。

必要条件

運用環境でイベントのスケーラブルで分散型のインデックスを作成するには、追加のElasticsearchノードをクラスタモードで設定する必要があります。Elasticsearchをクラスタモードでインストールする方法については、「79 ページの 「Elasticsearchのインストールと設定」」を参照してください。

イベント視覚化の有効化

イベント視覚化を有効にする方法:

1. Sentinelサーバにnovellユーザとしてログインします。
2. /etc/opt/novell/sentinel/config/configuration.propertiesファイルを開きます。
3. eventvisualization.traditionalstorage.enabledをtrueに設定します。
4. 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。
5. (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、183ページの第33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。

---

21 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。

22 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。

23 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(su novell)に切り替えます。
3. Sentinelのbinディレクトリを参照します。
4. convert_to_fips.shスクリプトを実行して、画面の指示に従います。
5. (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する場合は、create_mfa_fips_keys.shスクリプトを実行し、画面の指示に従って操作してください。

   注: スクリプトの実行中に、nssデータベースのパスワードが必要になります。

6. (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、『*SentinelAdministratorGuide*』の「「AuthenticationMethods」」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。

7 Sentinelサーバを再起動します。

8 133ページの第24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。

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(su novell)に切り替えます。

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

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

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

6 133ページの第24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。

24 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。

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

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

リソース管理データベースに正常に登録されたことを検証するには:

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

   証明書のインポートについて詳しくは、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。

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(su novell)に切り替えます。
3. binディレクトリを参照します。デフォルトの場所は/opt/novell/sentinel/binです。
4. updateServerCert.shスクリプトを実行して、画面の指示に従います。

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. AgentManager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、『*WindowsEvent(WMI)ConnectorGuide*』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コレクタマネージャを再起動するようプロンプトが表示されたら、「yes」または「y」と入力します。

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、73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。

- 143 ページの 「Sentinelサーバを非FIPSモードに戻す」
- 144 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-fips20130124191111359034887.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-fips20130124191111359034887.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(su novell)に切り替えます。
3. binディレクトリを参照します。デフォルトの場所は/opt/novell/sentinel/binです。
4. revert_to_nonfips.shスクリプトを実行して、画面の指示に従います。
5. リモートCollector ManagerまたはリモートCorrelation Engineを再起動します。

25 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。

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。

26 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 26-1 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技術情報Webサイト
❒	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。	151ページの第27章「前提条件」

27 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 8.1には、Jettyの更新済みバージョンが含まれています。Jettyの更新済みバージョンには、ファイル構造に対する変更が含まれています。

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。7.4.4より前のSentinelバージョンからアップグレードする場合は、設定していたイベント関連付けデータの保持期間が、アップグレード後14日間に上書きされます。これを回避するには、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。

アップグレード前のSSDMの環境設定

アップグレードプロセスでは、Sparkアプリケーションに関連するファイルが更新されます。更新されたファイルを使用するには、Sparkジョブを再開し、Kafkaトピック上のすべてのSparkチェックポイントをリセットする必要があります。Kafkaトピックチェックポイントのリセットによるデータ損失を防ぐためには、SSDMをアップグレードする前に、Collector ManagerからKafkaへのデータ転送を一時停止する必要があります。データ転送の一時停止中は、データ転送が再開されるまでの間、データはCollector Managerに格納されます。転送が一時停止される前までに、Kafkaに転送されたデータの処理をSparkアプリケーションが完了した場合は、データを失うことなく安全にチェックポイントをリセットできます。

Collector ManagerからKafkaへのイベントの転送を一時停止するには:

1. Sentinel Mainで、［**ストレージ**］>［**スケーラブルストレージ**］>［**高度な環境設定**］>［**Kafka**］の順にクリックします。
2. 次のプロパティを追加し、それをtrueに設定します。

   pause.events.tokafka
3. ［**保存**］をクリックします。

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。

28 従来のSentinelインストールのアップグレード

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。

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. インストールファイルを抽出したディレクトリに移動します。
7. 次のコマンドを指定して、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. インストールスクリプトで、古いバージョンの製品が存在していることが検出され、製品をアップグレードするかどうかを指定するよう求められます。アップグレードを続行するには、「y」を押します。

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

11 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。

12 クライアントコンピュータ上のJava Web Startキャッシュを消去してから、最新バージョンのSentinelアプリケーションを使用します。

javaws -clearcacheコマンドを使用するか、Java Control Centerを使用して、Java Web Startキャッシュを消去できます。詳細については、http://www.java.com/en/download/help/plugin_cache.xmlを参照してください。

13 (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。

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 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、156 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。

15 (条件による) Kerberos認証を使用している場合、Java Runtime EnvironmentでAES256を有効にします。javaフォルダがアップグレード中にデフォルトファイルに置き換わるためです。Java Runtime EnvironmentでAES256を有効にするには、次の手順を実行します。

15a 次の場所からJava Cryptography Extension (JCE) 8をダウンロードします: http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

15b 2つの*.jarファイルを取り出して/opt/novell/sentinel/jdk/jre/lib/securityディレクトリにコピーします。

15c (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。

15d Sentinelを再起動します。

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。

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

su novell

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 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。

アップグレードですべての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 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。

14 クライアントコンピュータ上のJava Web Startキャッシュを消去してから、最新バージョンのSentinelアプリケーションを使用します。

javaws -clearcacheコマンドを使用するか、Java Control Centerを使用して、Java Web Startキャッシュを消去できます。詳細については、http://www.java.com/en/download/help/plugin_cache.xmlを参照してください。

15 (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。

15a novellユーザに切り替えます。

```
su novell
```

15b binフォルダを参照します。

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

15c 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
```

16 (条件による) Kerberos認証を使用している場合、Java Runtime EnvironmentでAES256を有効にします。javaフォルダがアップグレード中にデフォルトファイルに置き換わるためです。Java Runtime EnvironmentでAES256を有効にするには、次の手順を実行します。

16a 次の場所からJava Cryptography Extension (JCE) 8をダウンロードします: http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

16b 2つの*.jarファイルを取り出して/opt/novell/sentinel/jdk/jre/lib/securityディレクトリにコピーします。

16c (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。

16d Sentinelを再起動します。

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。

注: 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をアップグレードしておく必要があります。

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 (条件による) Mozilla Network Security Services (NSS) 3.29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。

7 (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

7a 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

7b 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。

8 次についてこの手順を繰り返します。

- Collector Manager instances
- Correlation Engine instances
- NetFlow Collector Manager instances

9 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。

29 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。SLESオペレーティングシステムをアップグレードしないでSentinelをアップグレードするか、SentinelとSLESオペレーティングシステムの両方をアップグレードできます。Sentinel 8.2アプライアンスにはSLES12SP3が組み込まれているため、SLES11のアップデートチャネルは非推奨になりました。SUSEによるSLES11の一般サポートが終了した時点でこのアップデートチャネルは削除されます。そのため、今後も継続してオペレーティングシステムの更新を受信するには、SLES12SP3オペレーティングシステムを含む、Sentinel 8.2アプライアンスにアップグレードする必要があります。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をアップグレードしておく必要があります。

- 159 ページの 「Sentinelのアップグレード」
- 162 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

- 159 ページの 「アプライアンス更新チャネルによるSentinelのアップグレード」
- 161 ページの 「SMTによるSentinelのアップグレード」

アプライアンス更新チャネルによるSentinelのアップグレード

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。

アプライアンス更新チャネルを使用してアプライアンスをアップグレードする方法:

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. アプライアンスコンソールにrootユーザでログインします。
4. 次のコマンドを実行します。

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

5 (条件による)OpenSSHパッケージ依存の問題を解決する必要があるというメッセージがインストーラに表示される場合は、適切なオプションを入力してOpenSSHパッケージをダウングレードします。

6 (条件による)ncgOverlayアーキテクチャの変更を示すメッセージがインストーラに表示される場合は、適切なオプションを入力してアーキテクチャの変更を受諾します。

7 (条件による)一部のアプライアンスパッケージ依存の問題を解決する必要があるというメッセージがインストーラに表示される場合は、適切なオプションを入力して従属するパッケージをアンインストールします。

8 「Y」と入力して続行します。

9 使用許諾契約書の条項を確認し、「yes」と入力します。

10 Sentinel アプライアンスを再起動します。

11 (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
```

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 クライアントコンピュータ上のJava Web Startキャッシュを消去してから、最新バージョンのSentinelアプリケーションを使用します。

javaws -clearcacheコマンドを使用するか、Java Control Centerを使用して、Java Web Startキャッシュを消去できます。詳細については、http://www.java.com/en/download/help/plugin_cache.xmlを参照してください。

14 (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。

14a novellユーザに切り替えます。

```
su novell
```

14b binフォルダを参照します。

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

14c 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
```

15 (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 11までを実行します。

16 (条件による) Kerberos認証を使用している場合、Java Runtime EnvironmentでAES256を有効にします。javaフォルダがアップグレード中にデフォルトファイルに置き換わるためです。Java Runtime EnvironmentでAES256を有効にするには、次の手順を実行します。

16a 次の場所からJava Cryptography Extension (JCE) 8をダウンロードします: http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

16b 2つの*.jarファイルを取り出して/opt/novell/sentinel/jdk/jre/lib/securityディレクトリにコピーします。

16c Sentinelを再起動します。

17 (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。

18 (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方法については、「162 ページの 「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。

19 Sentinelを再起動します。

SMTによるSentinelのアップグレード

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

1 アプライアンスがSMTで設定されていることを確認します。

詳細については、110 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 アプライアンスを再起動します。

```
rcsentinel restart
```

11 (条件による) Sentinelをカスタムポートにインストールした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
```

12 (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 11までを実行します。

13 (条件による) Kerberos認証を使用している場合、Java Runtime EnvironmentでAES256を有効にします。javaフォルダがアップグレード中にデフォルトファイルに置き換わるためです。Java Runtime EnvironmentでAES256を有効にするには、次の手順を実行します。

13a 次の場所からJava Cryptography Extension (JCE) 8をダウンロードします: http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

13b 2つの*.jarファイルを取り出して/opt/novell/sentinel/jdk/jre/lib/securityディレクトリにコピーします。

13c Sentinelを再起動します。

14 (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。

15 (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方法については、「162 ページの 「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。

16 Sentinelを再起動します。

オペレーティングシステムのアップグレード

Sentinelのアップグレード後に、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。オペレーティングシステムをアップグレードした後は、新しいSentinelアプライアンスマネージャの機能を活用するようアプライアンスを構成する必要があります。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と管理を行える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。既存のWebYast機能に代わるものです。

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をアップグレードします。詳細については、「159 ページの 「Sentinelのアップグレード」」を参照してください。

2 Sentinelサービスを停止します。

```
rcsentinel stop
```

3 (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
```

4 (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。

5 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。

6 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。

7 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
```

8 (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。

- 216 ページの 「iSCSI Targetの環境設定」
- 217 ページの 「iSCSIイニシエータの環境設定」
- 218 ページの 「HAクラスタの設定」

9 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。

9a ファイルを次のようにuntarします。

tar -xvf <*アップグレード後ユーティリティのインストーラファイル名*>.tar.gz

9b 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 <*アップグレード後ユーティリティのインストーラファイル名*>

9c 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。

9d 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。

10 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、「108ページの「アップデートの登録」」を参照してください。

30 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。

Elasticsearchにおけるデータのセキュリティ保護

SentinelではブラウザベースのKibanaを使用していて、ダッシュボードでイベントとアラートを視覚化できます。Sentinelは、アラートの保存とインデックス作成をElasticsearchで行います。またイベント視覚化機能を利用するために、Elasticsearchでイベントの保存とインデックス作成を行うようSentinelを設定することもできます。Sentinelのダッシュボードは Elasticsearchのデータにアクセスして、ダッシュボードにイベントやアラートを表示します。ダッシュボードに表示されるデータを、ユーザの役割で表示することが許可されているものだけに限定し、Elasticsearchで承認されていないデータアクセスを防止するには、Elasticsearchセキュリティプラグインをインストールする必要があります。詳細については、81 ページの 「Elasticsearchにおけるデータのセキュリティ保護」を参照してください。

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、44 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。

注: Sentinel 8.2にアップグレードした後、Kibanaを利用している一部のSentinelダッシュボードがロードされません。ElasticsearchとKibanaのバージョンがSentinel 8.2でアップグレードされ、既存のKibanaのインデックスファイルがElasticsearchおよびKibanaのアップグレードされ

たバージョンと互換性がないために、この問題が発生します。この問題を修復するには、Kibanaの既存のインデックスファイルを手動で削除し、新しいKibanaインデックスファイルを再作成する必要があります。詳細については、Knowledge Base Article 7022736を参照してください。

IPフローデータ収集の設定

SentinelではArcSight SmartConnectorを使用するようになりました。これは、NetFlowデータに加えて、IPフローデータを収集して、企業のネットワークを監視するのに役立ちます。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Collector Managerインスタンスを使用してIPフローデータを収集します。NetFlowデータを収集するためにNetFlow Collector Managerインスタンスが不要になります。
- 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。

Sentinelのアップグレード後、NetFlow機能の使用を継続するか、IPフローデータ収集を設定するか、そのどちらかを選択できます。しかし、IPフローデータ収集と視覚化機能が利用できるようになったことに伴い、NetFlowビューを含む、以前に利用可能であったNetFlow機能は非推奨になりました。将来、これは、ユーザエクスペリエンスを向上させるために削除される予定です。

IPフローデータ収集を有効にすると、次のようになります:

- IPフローデータはイベントとして収集されるため、EPSカウントと見なされます。
- IPフローを有効にする前に収集されたNetFlowデータは失われます。非推奨のNetFlowシステムの最大保持日数は3日です。IPフローイベントは必要な期間、保持できます。
- IPフローを有効にする前に収集されたNetFlowデータをIPフロー機能に移行することはできません。
- Sentinelを再インストールする場合を除き、設定を元に戻すことはできません。
- Sentinel Mainからログアウトされるので、もう一度ログインする必要があります。

IPフローデータ収集を設定する方法:

1. 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。

2. ［**Sentinel Main**］>［**収集**］>［**IPフロー**］で、［**IPフローデータの収集**］を選択して［**有効**］をクリックします。

注: IPフローイベントはCollector Managerに送信されるようになったため、NetFlow Collector Managerインスタンスを使用する必要はなくなりました。そのため、既存のNetFlow Collector Managerインスタンスはすべてアンインストールできます。詳細については、232 ページの「NetFlow Collector Managerのアンインストール」を参照してください。

アップグレード後のSentinelスケーラブルデータマネージャの環境設定

Elasticsearchセキュリティプラグインのインストール

Sentinelには、外部Elasticsearchノードに加えて、データ視覚化用にデフォルトでローカルElasticsearchノードが含まれるようになりました。このために、ローカルElasticsearch用にElasticsearchプラグインをインストールする必要があります。詳細については、82 ページの「Elasticsearchセキュリティプラグインのインストール」を参照してください。

Sentinelで使用されるElasticsearchとKibanaがアップグレードされるため、既存のElasticsearchノードにあるすべてのElasticsearchセキュリティプラグインを再展開する必要があります。Elasticsearchセキュリティプラグインを再展開する方法の詳細については、「86 ページの 「Elasticsearchセキュリティプラグインの再展開」」を参照してください。

YARN上でのSparkアプリケーションの更新

Sentinelのアップグレード中には、Sparkアプリケーションのいくつかのファイルも更新されます。次の手順を実行することにより、これらの更新されたファイルと共にSparkアプリケーションを再送信する必要があります。

1. SSDMサーバにnovellユーザとしてログインし、HDFS NameNodeがインストールされているSpark履歴サーバにファイルをコピーします。

   cd /etc/opt/novell/sentinel/scalablestore

   scp SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties log4j.properties manage_spark_jobs.sh root@<*hdfs_node*>:<*destination_directory*>

   ここで、<*destination_directory*>は、コピーしたファイルを配置する任意のディレクトリです。また、hdfsユーザがこのディレクトリに対して完全な許可を持っていることも確認します。

2. <*hdfs_node*>サーバにルートユーザとしてログインし、コピーしたファイルの所有権をhdfsユーザに変更します。

   cd <*destination_directory*>

   chown hdfs SparkApp-*.jar avroevent-*.avsc avrorawdata-*.avsc spark.properties log4j.properties manage_spark_jobs.sh

   manage_spark_jobs.shスクリプトに実行可能許可を割り当てます。

3. Sparkジョブによるすべてのデータ処理が完了したことを確認します。

   YARN ResourceManager Webユーザインタフェースに移動し、それぞれのSentinel Sparkアプリケーションを表示します。 Spark Streamingアプリケーションデータは、Kafkaのすべてのデータが処理されると入力レートがゼロになります。

4. 次のコマンドを実行して、データ処理を停止します。

./manage_spark_jobs.sh stop

5 データ処理チェックポイントを消去します。

```
sudo -u hdfs hadoop fs -rm -R -skipTrash  /spark/checkpoint
```

ここで、/spark/checkpointはチェックポイントディレクトリです。

6 次のスクリプトを実行して、Sparkジョブを再送信します。

./manage_spark_jobs.sh start

上記のコマンドは、送信プロセスを完了するまでしばらく時間がかかります。

7 (オプション)送信したSparkジョブのステータスを検証するには、次のコマンドを実行します。

./manage_spark_jobs.sh status

8 Sparkによるイベントの処理を開始するために、Kafkaへのイベント転送を再開します。

8a Sentinel Mainで、［**ストレージ**］>［**スケーラブルストレージ**］>［**高度な環境設定**］>［**Kafka**］の順にクリックします。

8b 次のプロパティをfalseに設定します。

pause.events.tokafka

8c ［**保存**］をクリックします。

Sentinelの機能の有効化

SSDM 8.0.*x*.*x*からアップグレードした場合は、Sentinel 8.1以降で追加された一部のSentinel機能が、デフォルトでは使用可能になっていないことがあります。これらの機能は、/etc/opt/novell/sentinel/config/ui-configuration.propertiesファイル内で手動で有効にする必要があります。

1 Sentinelサーバにnovellユーザとしてログインします。

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

3 以下のプロパティをfalseに変更します。

```
alerts.hideUI
solutionDesigner.launcher.hideUI
correlation.hideUI
scc.configurations.solutionPacks.hideUI
people.hideUI
permission.knowledgeBase.hideUI
scc.menuBarItem.toolsMenu.hideUI
scc.toolBarItem.peopleBrowser.hideUI
integration.hideUI
```

4 Sentinelブラウザを更新します。

Sentinelスケーラブルデータマネージャのダッシュボードと視覚化の更新

SSDMのアップグレード後にダッシュボードと視覚化を更新し、ダッシュボードと視覚化の最新バージョンに含まれている機能強化を適用する必要があります。

デフォルトでは、SSDMをアップグレードしてもダッシュボードと視覚化は更新されません。しかし、アップグレード後にこれらを手動で更新できます。ダッシュボードおよび視覚化は、既存のダッシュボードと視覚化を削除して、load_kibana_data.shスクリプトを実行すると更新できます。このスクリプトは最新のダッシュボードと視覚化をインストールします。

重要: ダッシュボードと視覚化の機能に対してカスタマイズを加えていたかもしれませんが、それらはダッシュボードと視覚化を更新すると失われます。

ダッシュボードと視覚化を更新する方法は次のとおりです。

1. SSDM Webインタフェースにログインし、［Event Visualization (イベント視覚化)］に進みます。
2. ［Event Visualization (イベント視覚化)］で、［**設定**］>［**Objects (オブジェクト)** ］>［**ダッシュボード**］の順に進みます。
3. 更新するダッシュボードを選択して、［**削除**］をクリックします。
4. ［**Visualizations (視覚化)**］をクリックします。更新する視覚化を選択して、［**削除**］をクリックします。
5. SSDM Webインタフェースからログアウトします。
6. SSDMサーバにnovellユーザでログインします。
7. /opt/novell/sentinel/binディレクトリに移動します。
8. 次のコマンドを使用してload_kibana_data.shを実行します。

   ./load_kibana_data.sh http://<ip address>:<port>> <alerts/events/misc>

   次に例を示します。

   ./load_kibana_data.sh http://127.0.0.1:9200 alerts

   ./load_kibana_data.sh http://127.0.0.1:9200 events
9. SSDM Webインタフェースにログインし、［Event Visualization (イベント視覚化)］に進み、更新されたダッシュボードと視覚化を表示します。

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、「108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。

多要素認証モードでのSentinelの再認証

SentinelサーバをMFAモードでアップグレードする場合、既存のNetFlow Collector Managerインスタンスは Sentinelサーバに対して自動的に再認証しません。SentinelサーバにNetFlow Collector Managerインスタンスを手動で再認証するには、次の手順を実行する必要があります。

SentinelをMFAモードで再認証する方法:

1. NetFlow Collector Managerのコンピュータにログインします。
2. /opt/novell/sentinel/setupに移動します。
3. configure.shスクリプトを実行します。

   Sentinelサーバにログインするよう求めるメッセージが表示されます。
4. LDAPユーザ名とパスワードを指定します。
5. 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。

   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://Sentinel_FQDN:port/SentinelAuthServices/oauth/clients

   各要素の内容は次のとおりです。

   - Sentinel_FQDNはSentinelサーバの完全修飾ドメイン名(FQDN)です。

     abc.netiq.comなどです。

     abcはSentinelサーバホスト名で、netiq.comはドメイン名です。
   - 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。

31 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。

32 スケーラブルストレージへのデータの移行

従来のストレージを使用するSentinelサーバは、1台の場合と複数台の場合があります。データマイグレーションプロセスの実行内容は、Sentinel展開を設定および管理する方法に応じて異なります。

表 32-1 *Sentinel展開のデータマイグレーションプロセス*

Sentinel展開	マイグレーションプロセス
1台のSentinelサーバがあり、既存のSentinelサーバを、スケーラブルストレージを使用するようにアップグレードすることを計画しています。	Sentinelサーバをアップグレードし、スケーラブルストレージを有効にした後、従来のストレージからスケーラブルストレージにイベントデータと生データを移行します。 詳細については、185ページの第34章「データの移行」を参照してください。
従来のストレージを使用する1台のSentinelサーバがある場合に、スケーラブルストレージ用にもう1台のSentinelサーバを設定して、Sentinelのすべての機能を使用できるようにすることを考えています。	バックアップと復元ユーティリティを使用し、従来のストレージを使用するSentinelからスケーラブルストレージを使用するSentinelにデータを移行します。 バックアップと復元ユーティリティの使用方法の詳細については、『「Sentinel Administration Guide」』の「*Backing Up and Restoring Data*」を参照してください。

Sentinel展開	マイグレーションプロセス
複数のSentinelサーバがある多層のセットアップを使用しており、新しいSentinelサーバを設定するか既存のサーバの1台を使用してスケーラブルストレージを利用することを計画しています。イベントデータと生データだけでなく、環境設定データも移行する必要があります。	多層のセットアップでは、従来のSentinelサーバのうちデータが一番多いサーバを識別し、バックアップと復元ユーティリティを使用してそのデータを移行します。 残りのSentinelサーバからデータをバックアップする必要がある場合は、このセクションで後述するさまざまなアプローチを使用して、それらのサーバから環境設定データ、イベントデータ、および生データを移行する必要があります。また、環境設定の一部は、手動で再作成する必要があります。 バックアップと復元ユーティリティを使用して複数のサーバからデータを移行しようとすると、復元の際にユーティリティが既存のデータを上書きしてしまうため、この方法は利用できません。たとえば、サーバAからデータを復元した後、サーバBからデータを復元しようとすると、このユーティリティはすでにサーバAから復元したデータを上書きしてしまいます。 したがって、関連するデータ移行プロセスについて理解するには、以下のセクションの指示に(以下の順序で)従ってください。 ◆ 移行できるデータ ◆ 環境設定データの移行 ◆ データの移行 ◆ アラートおよびNetFlowデータの移行 ◆ Sentinelクライアントの更新 ◆ ESMの環境設定のインポート

移行できるデータ

イベントデータ、生データ、および一部の環境設定データを移行することができます。移行できない、環境設定の残りの部分は、手動で再作成する必要があります。

表 32-2 移行できる環境設定と再作成する必要がある環境設定

移行できる環境設定	再作成する必要がある環境設定
◆ 相関ルール ◆ アクション ◆ マップ ◆ フィルタ ◆ 脅威フィード ◆ ESMの環境設定 ◆ アラート(ナレッジベースのデータを除く) ◆ NetFlow	◆ テナント、役割、ユーザ、およびLDAPの環境設定 ◆ イベントおよびアラートのルーティングルール ◆ データおよびアラートの保持ポリシー ◆ ダッシュボード ◆ リアルタイムビュー ◆ 識別情報 ◆ フィードの環境設定 ◆ アクションとインテグレータのプラグインの環境設定 ◆ セキュリティの環境設定

環境設定データの移行

イベントデータを移行する前に、まず環境設定データをSentinelのターゲットサーバに移行する必要があります。一部の環境設定は、Solution Designerや、イベントソースの管理(ESM)にあるエクスポートとインポートのオプションを使用してバックアップすることができます。バックアップまたはエクスポートすることができない、環境設定データの残りの部分は、手動で再作成する必要があります。

- 179 ページの 「ソースサーバ上のデータのバックアップ」
- 180 ページの 「ターゲットサーバ上のデータの復元」

ソースサーバ上のデータのバックアップ

Sentinelでさまざまなオプションを使用して、必要なデータをバックアップする必要があります。

- 180 ページの 「ソリューションパックの使用」
- 180 ページの 「ESMでのエクスポート環境設定オプションの使用」

ソリューションパックの使用

ソースサーバ上の以下の環境設定は、Solution Designerを使用してバックアップします。

表 32-3　環境設定データ

	データ	備考
❒	相関ルール	Correlation Engineごとに別個のコントロールを作成して、特定のCorrelation Engine instancesに個別にルールを移行できます。
❒	アクション	バックアップできるのはJavaScriptアクションのみで、ダイナミックリストやインシデント作成などのレガシアクションはバックアップできません。
❒	イベント強化	Sentinelでは、イベントフィールドに関連付けられたマップもバックアップされます。したがって、イベント強化データを復元した後、関連付けられたマップを再作成する必要はありません。
❒	フィルタ	すべてのカスタムフィルタをバックアップします。
❒	フィード	ソリューションパックはフィードプラグインのみをバックアップし、プラグインの環境設定はバックアップしません。

Solution Designerでのデータのバックアップの詳細については、『「Sentinel Administration Guide」』の「*Creating Solution Packs*」を参照してください。

ESMでのエクスポート環境設定オプションの使用

データ収集の環境設定をバックアップするには、ESMのエクスポート環境設定オプションを使用します。詳細については、『「Sentinel Administration Guide」』の「*Exporting Configurations*」を参照してください。

ターゲットサーバ上のデータの復元

- 180 ページの 「ソリューションパックからの環境設定データのインストール」
- 181 ページの 「環境設定の手動による再作成」

ソリューションパックからの環境設定データのインストール

ソースサーバでバックアップした環境設定データは、Solution Designerを使用してインポートします。詳細については、『「Sentinel Administration Guide」』の「*Installing Content from Solution Packs*」を参照してください。

フィルタ、アクション、および相関ルールなどのオブジェクトで重複している名前はすべて名前変更してください。デフォルトでは、すべてのフィルタは、ターゲットサーバ上にインポートした時点でパブリックになります。フィルタごとに許可を手動で再割り当てしてください。

環境設定の手動による再作成

ソリューションパックからインポートした環境設定データ以外のすべて環境設定データは、手動で再作成する必要があります。手動で再作成する必要のある環境設定の詳細については、179 ページの 表 32-2 「移行できる環境設定と再作成する必要がある環境設定」を参照してください。

イベントデータと生データの移行

イベントデータと生データを移行する方法については、「データの移行」を参照してください。

アラートおよびNetFlowデータの移行

バックアップと復元ユーティリティを使用すると、アラートおよびNetFlowデータをソースサーバからターゲットサーバに移行できます。アラートについては、このユーティリティにより、アラートをトリガしたイベントが復元されます。ただし、関連付けられた相関ルールと知識ベースの情報は復元されません。

次のコマンドを使用して、アラートおよびNetFlowデータのバックアップと復元を実行します。

```
For backing up:
./backup_util.sh -i

For restore:
./backup_util.sh -m restore -f <backup_file_path>
```

アラートおよびNetFlowデータについては、既存のデータを上書きするか、または既存のデータに追加するオプションがあります。必要なオプションを選択してください。

上記のコマンドでは、セキュリティインテリジェンスのデータがバックアップおよび復元されますが、SSDMではセキュリティインテリジェンスを利用できないため、そのデータは使用できません。

バックアップと復元ユーティリティの使用方法の詳細については、『「 Sentinel Administration Guide」』の「*Backing Up and Restoring Data*」を参照してください。

Sentinelクライアントの更新

すべての既存のCollector Manager instances、Correlation Engine instances、およびNetFlow Collector Manager instancesの環境設定を更新して、ターゲットSentinelサーバとの通信を開始するように設定する必要があります。詳細については、『「 Sentinel Administration Guide」』の「*Updating Sentinel Clients*」を参照してください。

注: イベントデータはソースサーバからすでに移行しましたが、今回のデータ移行プロセスの処理中または処理後に到着したイベントデータをすべて移行するために、もう一度データ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。詳細については、185ページの第34章「データの移行」を参照してください。

ESMの環境設定のインポート

ESMユーザインタフェースの環境設定インポートオプションを使用して、ソースサーバで使用していたデータ収集の設定をインポートします。詳細については、『「SentinelAdministrationGuide」』の「*Importing Configurations*」を参照してください。

33 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、「185ページの第34章「データの移行」」を参照してください。

34 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、125 ページの「イベント視覚化の有効化」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てLinux。
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。

35 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。

36 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 SP3
  - 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 11 SP4またはSLES 12 SP1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、39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、39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。

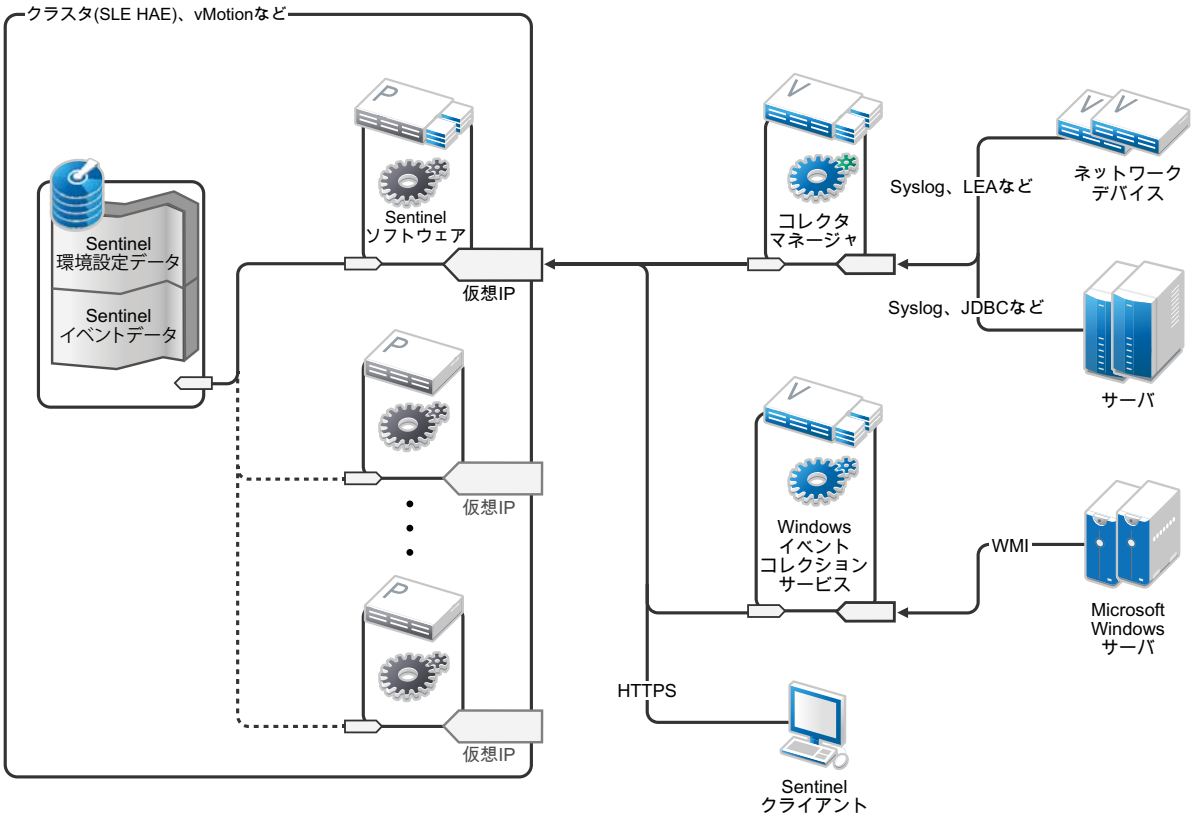
  iSCSIの場合は、ハードウェアがサポートする最大のメッセージ転送単位(MTU)を使用してください。MTUを大きくすることで、ストレージのパフォーマンスが向上します。ストレージのレイテンシと帯域幅が推奨値より遅いと、Sentinelで問題が生じる可能性があります。

- ❒ 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。

37 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、39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、39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、65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、104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iSCSITargetを構成した、SLES11SP4またはSLES12SP1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。

- 196 ページの 「iSCSI Targetの環境設定」
- 198 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 11 SP4を使用している場合は、［**ネットワークサービス**］>［**iSCSI Target (iSCSIターゲット)**］を選択します。
- 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 11 SP4の場合: iscsitarget RPM
- SLES 12 SP1以降の場合: iscsiliotarget RPM

9 (条件による) SLES 12 SP1以降を使用する場合は、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。

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 (条件による) SLES 11 SP4を使用している場合は、次の手順を実行します。

16a 他のオプションをデフォルトのままにし、［**OK**］をクリックして［**次へ**］をクリックします。

16b (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。

17 (条件による) SLES 12 SP1以降を使用している場合は、次の手順を実行します。

17a 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。

17b **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。

17c (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。

18 ［**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。

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

8 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 ［**DiscoveredTargets(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) 196 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 ［**ConnectedTargets(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

- 200 ページの 「従来のHAインストール」
- 201 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。
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。
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. 以下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/* /tmp/new
   ```

   ```
   umount /tmp/new/
   ```

6. 以下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/
   ```

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

後続のノードインストール

- 202 ページの 「従来のHAインストール」
- 202 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/*
```

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。

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. SLEHAE資料に従って、コアとなるSLEHAE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の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、「207 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 ［**完了**］をクリックして設定を完了します。

22 YaSTを終了します。

23 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。

2 所定の場所でのリソースの実行およびリソースの移動がリソースマネージャで許可されるようにするには、グローバルクラスタオプションdefault-resource-stickinessを「1」に設定します。

crm configure property default-resource-stickiness=1

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。

38 Sentinel HAをSSDMとして環境設定する

この章では、Sentinel HAセットアップをSSDMとして設定する方法について説明します。これらの手順は従来のインストールとアプライアンスインストールの両方に該当します。

Sentinel HAセットアップをSSDMとして環境設定する方法:

1. Sentinelのスケーラブルストレージをインストールして環境設定します。詳細については、89ページの第13章「スケーラブルストレージのインストールと設定」を参照してください。
2. アクティブノード上でスケーラブルストレージを有効にします。詳細については、『「Sentinel Administration Guide」』の「*Enabling Scalable Storage Post-Installation*」を参照してください。
3. アクティブノード上で次のコマンドを実行します。

   csync2 -x -v

   これにより、SSDM環境設定がすべてのパッシブノードと同期されます。
4. (条件による)手順3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。
   - **4a** 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。
   - **4b** すべてのサーバ上で次のコマンドを実行し、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 -clr /
   - **4c** 次のコマンドを実行して、信頼されたサーバとリモートサーバの間の差異をすべて検出し、同期対象としてマークを付けます。

     csync2 -TUXI
   - **4d** 次のコマンドを実行して、競合があった場合に現在のサーバを強制的に優先するようデータベースをリセットします。

     csync2 -fr /
   - **4e** その他のすべてのサーバへの同期を開始するには、次のコマンドを実行します。

     csync2 -xr /
   - **4f** すべてのファイルが同期されていることを検証するには、次のコマンドを実行します。

     csync2 -T

     このコマンドでは、同期が成功した場合はファイルを何も一覧表示しません。

39 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インストールのアップグレード

このセクションでは、従来のSentinelインストールをアップグレードする方法、および従来のSentinelインストールでオペレーティングシステムをアップグレードする方法について説明します。

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。

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。

rcopenais 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。

rcopenais start

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。

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。

rcopenais 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 アップグレード完了後、クラスタスタックを起動します。

rcopenais start

4g 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

4h 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

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、SentinelHAクラスタ内で、SLES11からSLES12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。

- 215 ページの 「オペレーティングシステムのアップグレード」
- 216 ページの 「iSCSI Targetの環境設定」
- 217 ページの 「iSCSIイニシエータの環境設定」
- 218 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。

```
rcopenais 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。

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SLES12SP3にアップグレードされていることを確認します。

iSCSI Targetの環境設定

iSCSIターゲットを設定するには、次のとおり実行します。

1 共有ストレージ上で、iSCSI LIOパッケージがインストールされているかどうかをチェックします。まだインストールされていない場合は、YaST2ソフトウェア管理に移動し、iSCSI LIOパッケージをインストールします(iscciliotarget RPM)。

2 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。

2a 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
```

2b 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。

3 ［**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。

4 ［**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。

5 ［**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。

6 ［**追加**］をクリックして、新しいLUNを追加します。

7 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。

8 6と7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。

9 6と7の手順を繰り返して、今回はLUN 2を追加し、/sbdを選択します。

10 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。

11 **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2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。

12 (条件による)手順4で認証を有効にした場合は、手順4で指定した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。

13 ［**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。

14 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) 216 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 ［**ConnectedTargets(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

Zypperパッチを使用して、Sentinel HAアプライアンスインストールをアップグレードできます。

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。

- 219 ページの 「Zypperを使用したSentinel HAアプライアンスのアップグレード」

Zypperを使用したSentinel HAアプライアンスのアップグレード

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、108 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。

rcopenais 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 Sentinel HAアプライアンスの更新をダウンロードします。

zypper -v patch

3c (条件による)OpenSSHパッケージ依存の問題を解決する必要があるというメッセージがインストーラに表示される場合は、適切なオプションを入力してOpenSSHパッケージをダウングレードします。

3d (条件による)ncgOverlayアーキテクチャの変更を示すメッセージがインストーラに表示される場合は、適切なオプションを入力してアーキテクチャの変更を受諾します。

3e (条件による)一部のアプライアンスパッケージ依存の問題を解決する必要があるというメッセージがインストーラに表示される場合は、適切なオプションを入力して従属するパッケージをアンインストールします。

3f アップグレード完了後、クラスタスタックを起動します。

```
rcopenais 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、『「SentinelAdministrationGuide」』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。

```
rcopenais 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。

5c Sentinel HAアプライアンスの更新をダウンロードします。

```
zypper -v patch
```

5d (条件による)OpenSSHパッケージ依存の問題を解決する必要があるというメッセージがインストーラに表示される場合は、適切なオプションを入力してOpenSSHパッケージをダウングレードします。

5e (条件による)ncgOverlayアーキテクチャの変更を示すメッセージがインストーラに表示される場合は、適切なオプションを入力してアーキテクチャの変更を受諾します。

5f (条件による)一部のアプライアンスパッケージ依存の問題を解決する必要があるというメッセージがインストーラに表示される場合は、適切なオプションを入力して従属するパッケージをアンインストールします。

5g アップグレード完了後、クラスタスタックを起動します。

```
rcopenais start
```

5h 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)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
```

9 (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方法については、「162 ページの 「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。

40 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。

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

Sentinelスケーラブルデータマネージャに変換した後、Sentinel Mainインタフェースに空白のページが表示される

問題: SSDMを有効にした後、Sentinel Mainインタフェースにログインすると、ブラウザに空白のページが表示されます。

解決策: ブラウザを閉じ、Sentinel Mainインタフェースに再ログインします。この問題は、SSDMを有効にした後、Sentinel Mainインタフェースに初めてログインしたときに、1回限り発生します。

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。

アンインストールの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 Main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 (条件による)イベント視覚化を有効にした場合は、Elasticsearchセキュリティプラグインを再展開する必要があります。詳細については、86 ページの 「Elasticsearchセキュリティプラグインの再展開」を参照してください。

6 次の追加の手順を行って、Sentinel Main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。

NetFlow Collector Managerのアンインストール

NetFlow Collector Managerをアンインストールするには、以下の手順に従います。

1 NetFlow Collector Managerのコンピュータにログインします。

注: NetFlow Collector Managerのインストールに使用したのと同じユーザ許可でログインする必要があります。

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、完全にアンインストールします。

アンインストール後の作業

Sentinelサーバをアンインストールしても、Sentinel管理者ユーザはオペレーティングシステムから削除されません。このユーザを手動で削除する必要があります。

Sentinelのアンインストール後も、特定のシステム設定が残ります。これらの設定は、Sentinelのクリーンインストールを実行する前に削除する必要があります。特に、Sentinelのアンインストール時にエラーが発生した場合にその必要があります。

Sentinelのシステム設定を手動でクリーンアップするには:

1 rootとしてログインします。

2 すべてのSentinelプロセスを停止します。

3 /opt/novell/sentinelまたはSentinelソフトウェアがインストールされていた場所の内容を削除します。

4 Sentinel管理者オペレーティングシステムユーザ(デフォルトではnovell)としてログインしているユーザがいないことを確認してから、ユーザ、ホームディレクトリ、およびグループを削除します。

```
userdel -r novell

groupdel novell
```

5 オペレーティングシステムを再起動します。