Sentinel 8.5 リリースノート

2021 年 8 月

Sentinel 8.5 では、以前のいくつかの問題が解決され、新機能もいくつか追加されています。

これらの改善の多くは、お客様から直接ご提案いただいたものです。皆様の貴重なお時間とご意見に感謝いたします。弊社の製品が皆様のご期待に添えるよう、引き続きお力添えを賜りたく存じます。フィードバックは当社オンラインコミュニティ「Sentinel フォーラム」からお寄せください。こちらのコミュニティには、製品情報、ブログ、役立つリソースへのリンクなども掲載されています。製品を向上させるため、アイデアポータルでアイデアを共有することもできます。

本製品のマニュアルは、ログインが不要なページから HTML 形式および PDF 形式で入手できます。マニュアルを改善するためのご提案がございましたら、Sentinel Documentation ページに掲載されている本マニュアルの HTML 版で、各ページのコメントアイコンをクリックしてください。本製品をダウンロードするには、製品のダウンロード Web サイトをご覧ください。

新機能

以下のセクションで、このバージョンの主な特徴と機能、およびこのリリースで解決された問題の概要を示します。

- 3 ページの 「オペレーティングシステム (OS) のバージョン」
- 3 ページの 「ソフトウェアの修正」

ArcSight Intelligence と Sentinel の統合

このリリースでは、Sentinel は ArcSight Intelligence の優れた分析技術と統合する方法をお客様に提供します。この結果、Sentinel ユーザは、ほぼリアルタイムでリスクスコアを取得し、独自の相関ルールなどの詳細な分析に使用できます。これにより、Sentinel では脅威ハンティングの機能が高まります。

ArcSight Intelligence は、ユーザおよびエンティティの動作分析ソリューションで、データサイエンスと高度な分析を使用して、組織内で発生するリスクの高い上位のエンティティと振る舞いを特定します。Intelligence は、まず組織エンティティの通常の振る舞いを確立し、次に高度な分析を使用してエンティティの異常な振る舞いを特定し、各エンティティに適切なリスクスコアを提供します。

Sentinel は、ArcSight Intelligence 6.3 と統合する方法を提供します。この統合により、Sentinel のユーザはデータを ArcSight Intelligence に送信して分析することが可能となり、また Intelligence からエンティティのリスクスコアの詳細を受け取れます。これにより、Sentinel はシステム全体を危険にさらし、潜在的な脅威を生み出す可能性がある組織内のリスクの高いユーザやエンティティを検出します。

MITRE ATT&CK

MITRE ATT&CK は、サイバーセキュリティチームがセキュリティ運用センター (SOC) プロセスと改善する領域を特定するための防衛措置の有効性を評価するのに役立ちます。MITRE ATT&CK は、実世界での観察に基づいた、サイバーセキュリティ防御の戦術と技術に関するグローバルにアクセス可能なナレッジベースです。MITRE ATT&CK ナレッジベースは、民間セクタ、政府、およびサイバーセキュリティ製品やサービスコミュニティにおける特定の脅威モデルと方法論を開発する基盤として使用されています。

Sentinel のこのリリースから、管理者は相関ルールを MITRE ATT&CK ID にマップできます。MITRE ATT&CK は、MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)(敵対的な脅威における戦術とテクニック、および一般常識) の略です。MITRE ATT&CK Framework は、実世界での観察に基づく脅威における戦術と技術の業界共通言語です。

Sentinel 管理者は、独自の直ちに使用可能な、またはカスタマイズ済みの相関ルールを MITRE ATT&CK ID で直接マップできます。そのため、多くのデータ分析を簡単に行うことができ、どのようなルールが発動されているのか、どのような戦術や MITRE 技術が顧客に利用されているのかを視覚的に把握することができます。Sentinel は、自社のネットワークを把握し、回避すべき最も重大な攻撃は何かを即座に知ることができるツールセットを提供しています。

MITRE ATT&CK ID でマップされた相関ルールがトリガされると、トリガされたイベントには MITRE ATT&CK ID と MITRE ATT&CK 名が設定されます。これらのイベントは、デフォルトのセキュリティヘルスダッシュボードで使用可能なウィジェットを介して分析されます。このダッシュボードには、1 日の時間範囲と 1 時間の表示間隔で上位 10 の MITRE ATT&CK 名が表示されます。

JDK のアップグレード

セキュリティの脆弱性を回避するため (CVE-2021-2161、CVE-2021-2163、CVE-2021-2341、CVE-2021-2432、CVE-2021-2369、CVE-2021-2388)、および新しい JDK 標準のセキュリティ機能を利用するために、JDK は 1.8.0_update242 から 1.8.0_update302 にアップグレードされます。

Connector からの生イベントの保存

バージョン 2021.1r1 以降の Sentinel Syslog コネクタは、ArcSight Smart Connector を経由して発生する生イベントを保存できます。これらは、エンドデバイスによって直接生成される、変更されていない未処理のイベントです。この設定は、対応する Smart Connector の [**[Preserve Raw Event(生イベントを保持)]**] オプションをオンにすることで有効にできます。

TLS のサポート

TLS 1.0 および TLS 1.1 のサポートは削除されました。

オペレーティングシステム (OS) のバージョン

従来型インストール : Sentinel は、次の新しいプラットフォームでも認定されています。

- Red Hat Enterprise Linux (RHEL) 8.3

非推奨の OS: 次の OS は RHEL および SLES でのサポートが廃止されたため、非推奨になります。

- RHEL 7.6 および 7.7
- SLES 15 SP1

ソフトウェアの修正

Sentinel 8.5 には、次の問題を解決するソフトウェア修正が含まれています。

- 3 ページの「Sentinel サーバで FIP に変換すると、プロトコルが TLS 1.2 から TLS 1.1 に変更されます。」
- 4 ページの 「Sentinel Java クライアントのアップグレード後に、Sentinel REST 呼び出しが失敗する」
- 4 ページの 「新しいレポートの生成時にエラーが発生する」

Sentinel サーバで FIP に変換すると、プロトコルが TLS 1.2 から TLS 1.1 に変更されます。

問題 : Sentinel サーバで FIPS に変換すると、プロトコルが TLS 1.2 から TLS 1.1 に変更され、SAM と Sentinel サーバ間の接続が終了します。ただし、お客様は TLS 1.2 を使用する必要があります。

修正 : FIPS に変換する際に、TLS バージョンが 1.2 から 1.1 に変更されなくなりました

Sentinel Java クライアントのアップグレード後に、Sentinel REST 呼び出しが失敗する

問題 : Sentinel Java Client を 8.1 から 8.2 にアップグレードした後、REST 呼び出しが失敗します。

修正 : Sentinel Java Client を 8.1 から 8.2 にアップグレードした後、REST 呼び出しが失敗しなくなりました。

新しいレポートの生成時にエラーが発生する

問題 : 新しいレポートを生成する際にエラーが発生します。エラーの主な問題は、キーストアが改ざんされている、またはパスワードが正しくないことにあります。

修正 : 新しいレポートの生成時にエラーは発生しません。

システム要件

ハードウェア要件、サポートされているオペレーティングシステム、およびブラウザの詳細については、Sentinel システム要件を参照してください。

ライセンスおよび購入情報

エンタープライズライセンスの購入、または既存のライセンスのアップグレードについては、1-800-529-3400 に電話するか、info@microfocus.com 宛てに電子メールを送信するか、https://www.microfocus.com/ja-jp/products/netiq-sentinel/contact にアクセスしてください。

Sentinel 8.5 のインストール

Sentinel 8.5 のインストールに関する詳細については、『*Sentinel インストールと設定ガイド*』を参照してください。

注 : Sentinel サーバに使用されるホストとそのコンポーネントはすべて、双方向の DNS 解決可能環境 (ホスト名から IP、IP からホスト名) でセットアップする必要があります。

Sentinel 8.5 へのアップグレード

Sentinel の以前のバージョン (Sentinel 8.2 以降) から、Sentinel 8.5 にアップグレードできます。

重要 : 最新の JDK アップグレードにより、LDAPS および SDK を設定するために、ユーザは IP アドレスの代わりにホスト名を使用する必要があります。また、解決可能である必要があります。

重要 : 従来のインストールとアプライアンスのインストールのアップグレード手順に変更があります。「Settings in Elasticsearch for Secure Cluster Communication（セキュアなクラスタ通信のための Elasticsearch の設定）」を参照し、手順に従ってください。これは、Sentinel を 8.3.1 以前から最新バージョンにアップグレードする場合にのみ適用されます。

重要 : 各アプライアンスのオフラインパッチ ISO をダウンロードして、オフラインアップデートを実行できます。詳細については、「Performing Offline Updates(オフラインアップデートの実行」を参照してください。

警告 : 以前のバージョンからは Sentinel 8.3 にアップグレードする場合、イベントまたは添付ファイルを Sentinel に送信する管理者以外のユーザに、**[イベントおよび添付ファイルの送信]** 許可を手動で割り当てる必要があります。この許可を割り当てない限り、Sentinel は Change Guardian および Secure Configuration Manager からイベントおよび添付ファイルを受信しなくなります。

従来のインストールについては、『*Sentinel インストールと設定ガイド*』の「Upgrading the Operating System(オペレーティングシステムのアップグレード)」セクションを参照してください。

既知の問題

Micro Focus は、弊社の製品が企業のソフトウェアニーズを満たす高品質のソリューションを提供できるように、常に努力しています。次の既知の問題は、現在調査中です。いずれかの問題についてさらに支援が必要な場合は、テクニカルサポートに連絡してください。

Sentinel に含まれている Java 8 のアップデートは、次のプラグインに影響を与える可能性があります。

- Cisco SDEE コネクタ
- SAP (XAL) コネクタ
- Remedy Integrator

これらのプラグインの問題について、標準の欠陥処理ポリシーに従って問題の優先度を定め、修正します。サポートポリシーの詳細については、「サポートポリシー」を参照してください。

ストレージ容量予測チャートを表示できません

問題 : **[Sentinel メイン]**> **[ストレージ]**> **[ヘルス]** では、**[ストレージ容量予測]** チャートが使用できません。これは、Zulu OpenJDK に必要なフォントが含まれていないためです。

解決策 : 次のコマンドを使用して、フォントをインストールします。

- yum install fontconfig
- yum install dejavu

Sentinel のアップグレード後に Kibana ダッシュボードを起動するとエラーが発生します

問題 : Kibana ダッシュボードを起動すると、次のメッセージが表示されます。デフォルトのインデックスパターンはありません。続行するには、選択するか、作成する必要があります。

解決策 : Kibana インデックスパターンをデフォルトのインデックスパターンとして設定するには :

1. 次のいずれかを選択します。
   - alerts.alerts
   - security.events.normalized_*
2. [デフォルトにする] をクリックします。

Mozilla Firefox および Microsoft Edge ではアラートビュー内のすべてのアラートのアラートリンクをコピーできません

問題 : [[すべて選択 *<number of alerts(アラート数)>* アラート]] > [[アラートリンクのコピー]] オプションは Firefox および Edge では機能しません。

解決策 : 次の手順を実行します。

1. すべてのアラートを選択できるチェックボックスを使用して、アラートビューの各ページにあるすべてのアラートを手動で選択します。
2. [[アラートリンクのコピー]] をクリックします。
3. ご希望のアプリケーションに貼り付けます。

Sentinel、コレクタマネージャ、および相関エンジンを OVF アプライアンスイメージとしてインストールすると、ログイン画面が表示されません

問題 : インストーラは、インストールの進行中画面で停止し、インストールが完了してもログイン画面を表示しません。

解決策 : 仮想マシンを再起動して、Sentinel、コレクタマネージャ、または相関エンジンを起動します。

再起動した場合、Microsoft Hyper-V Server 2016 の Sentinel 8.2 アプライアンスが起動しません

問題 : Hyper-V Server 2016 で Sentinel アプライアンスを再起動しても起動せず、次のメッセージが表示されます。

```
A start job is running for dev-disk-by\..
```

この問題は、オペレーティングシステムがインストール中にディスク UUID を変更するために発生します。そのため、再起動時にディスクを見つけることができません。

解決策 : ディスク UUID を手動で変更してください。詳細については、「Knowledge Base Article 7023143」を参照してください。

Sentinel 8.2 HA アプライアンスにアップグレードする際のエラー

問題 : Sentinel 8.2 HA アプライアンスにアップグレードするときに、Sentinel で次のエラーが表示されます。

```
Installation of novell-SentinelSI-db-8.2.0.0-<version> failed:
with --nodeps --force) Error: Subprocess failed. Error: RPM failed: Command exited
with status 1.
Abort, retry, ignore? [a/r/i] (a):
```

解決策 : 上記のプロンプトに応答する前に、次の手順を実行します。

1. PuTTY などのソフトウェアを使用して、アップグレードを実行しているホストで別のセッションを開始します。
2. /etc/csync2/csync2.cfg ファイルに次のエントリを追加します。

   /etc/opt/novell/sentinel/config/configuration.properties
3. /var/opt/novell から sentinel フォルダを削除します。

   rm -rf /var/opt/novell/sentinel
4. アップグレードを開始したセッションに戻り、r を入力してアップグレードを続行します。

英語以外の言語では、MFA モードの場合に Collector Manager と Correlation Engine アプライアンスのインストールが失敗する

問題 : オペレーティングシステムの言語が英語以外の場合、MFA モードでは、コレクタマネージャと相関エンジンアプライアンスのインストールが失敗します。

解決策 : Collector Manager と Correlation Engine アプライアンスを英語でインストールします。インストールの完了後、必要に応じて言語を変更します。

アプライアンスのインストール画面でのユーザビリティに関する問題

問題 : 次のような状況において、アプライアンスのインストール画面で［**[次へ]**］ボタンと［**[戻る]**］ボタンが表示されない、または無効になります。

- Sentinel 事前確認画面で［**[戻る]**］をクリックして Sentinel サーバのアプライアンスのネットワーク設定画面の情報を編集または確認するときに、インストールを続行するための［**[次へ]**］ボタンが表示されません。［**[設定]**］ボタンを使用すると、指定された情報のみを編集できます。
- 間違ったネットワーク設定を指定すると、Sentinel 事前確認画面に、ネットワーク情報が正しくないためインストールを続行できないことが示されます。その際、ネットワーク設定を変更するために前の画面に戻る［**[戻る]**］ボタンがありません。

解決策 : アプライアンスのインストールを再開します。

Open-vm-tools で時刻同期が有効になっていると、コレクタマネージャがメモリ不足になる

問題 : open-vm-tools で手動で時刻同期をインストールして有効にすると、Sentinel アプライアンス (ゲスト) と VMware ESX サーバ (ホスト) 間の時間が定期的に同期されます。この時刻同期によって、ゲストクロックを ESX サーバ時刻の後ろまたは前に移動させることができます。Sentinel アプライアンス (ゲスト) と ESX サーバ (ホスト) の間で時刻が同期されるまで、Sentinel でイベントが処理されません。その結果、多数のイベントが Collector Manager でキューに登録されます。イベント

数がしきい値に達すると、イベントが最終的に削除される可能性があります。この問題を回避するために、Sentinel はデフォルトで、Sentinel で使用可能な open-vm-tools バージョンの時刻同期を無効にします。

解決策 : 時刻同期を無効にします。時刻同期の無効化の詳細については、「時刻同期の無効化」を参照してください。

FIPS 140-2 モードが有効になっていると、Agent Manager が SQL 認証を必要とする

問題 : Sentinel で FIPS 140-2 モードが有効になっていると、エージェントマネージャに Windows 認証を使用したときに、エージェントマネージャデータベースとの同期が失敗します。

解決策 : Agent Manager の SQL 認証を使用してください。

非 FIPS 140-2 モードで Sentinel 高可用性インストールを実行すると、エラーが表示される

問題 : 非 FIPS 140-2 モードで Sentinel 高可用性インストールを実行すると、正常に完了しますが、次のエラーが 2 回表示されます。

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```

解決策 : このエラーは予期されるものであり、無視してかまいません。インストーラはエラーを表示しますが、Sentinel 高可用性環境設定は非 FIPS 140-2 モードで正常に動作します。

Keytool コマンドで警告が表示されます

問題 : Keytool コマンドの使用中に、次の警告が表示されます。

```
The JKS keystore uses a proprietary format. It is recommended to migrate to
PKCS12which is an
industry standard format using "keytool -importkeystore -srckeystore
 /<sentinel_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -destkeystore
 /<sentinel_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -deststoretype pkcs12".
```

解決策 : この警告は予期されるものであり、無視してかまいません。警告は表示されますが、Keytool コマンドは正常に機能しています。

Sentinel が FIPS モードで脅威インテリジェンスフィードを処理しません

問題 : FIPS モードで、導入後直ちに使用可能な脅威インテリジェンスのフィードを URL から処理しているときに、Sentinel に次のエラーが表示されます。Received fatal alert: protocol_version。この問題の原因は、導入後直ちに使用可能な脅威フィードで TLS 1.2 のみがサポートされるようになったのに対して、これが FIPS モードでは動作しないことにあります。

解決策 : 以下を実行します。

1. [**[Sentinel メイン]**] > [**[統合]**] > [**[脅威インテリジェンスのソース]**] の順にクリックします。
2. 各 URL を編集して、プロトコルを http から https に変更します。

Sentinel メインからログアウトしても、多要素認証モードではダッシュボードからログアウトされず、その逆も同様です

問題 : 多要素認証モードでは、**[Sentinel メイン]** からログアウトしても、Sentinel ダッシュボードからログアウトされず、その逆も同様になります。これは、高度な認証フレームワークの問題が原因で発生します。

解決策 : Advanced Authentication Framework で修復プログラムが提供されるまでは、画面を更新してログイン画面を表示します。

Sentinel 8.3.1 へのアップグレード後に Kibana カスタムダッシュボードが表示されない

問題 : Sentinel 8.3 以前から Sentinel 8.3.1 にアップグレードすると、Kibana カスタムダッシュボードが表示されません。

解決策 : Sentinel をアップグレードした後で、カスタムダッシュボードを再作成してください。

Kibana を起動すると、衝突エラーメッセージが表示される

問題 : Sentinel をインストールまたはアップグレードした後、Kibana を初めて起動すると、衝突エラーメッセージが表示されます。

解決策 : 機能に影響がないため、衝突エラーメッセージは無視してください。

OS Redhat 8.1 および 8.2 を再起動すると、Sentinel が自動的に起動しない

問題 : Sentinel を OS Redhat 8.1 および 8.2 にインストールした後、再起動後に、Sentinel (サーバ、RCM、または RCE) が自動的に起動しません。

解決策 : /etc/selinux/config ファイルで SELINUX 値を **SELINUX=disabled** に変更します。

Sentinel アプライアンス管理コンソールを開く際にエラーメッセージが表示される

問題 : Sentinel 8.3 にアップグレードした後、HA (高可用性) サーバの CE (相関エンジン) または CM (コレクタマネージャ) の Sentinel アプライアンス管理コンソールを開こうとすると、エラーメッセージ「404 エラー - 見つかりません」が表示されます。

解決策 : 詳細については、Micro Focus Knowledge Base(Micro Focus ナレッジベース) ドキュメントを参照してください。

視覚化の管理許可を非表示にしているユーザでも、Kibana ページの [管理] タブが表示できる

問題 : Sentinel 8.4 にアップグレードした後も、視覚化の管理許可を非表示にしたユーザは、Kibana ページの [管理] タブを表示できますが、[管理] タブの機能にはアクセスできません。

管理者がアラートのユーザ役割を変更した場合、Kibana ページで即時変更が更新されない

問題 : 既存のユーザは、アラートを表示するために管理者によって権限が更新されていますが、Kibana ページでアラートを即時に表示することはできません。

解決策 : ユーザ許可が更新された場合は、ログアウトして再度ログインする必要があります。

テナントユーザとして視覚化ダッシュボードを起動すると、エラーメッセージが表示される

問題 : デフォルト以外のテナントユーザが視覚化ダッシュボードを起動すると、「**[禁止]**」というエラーメッセージが表示されます。このエラーメッセージは、ダッシュボードがデフォルト以外のテナントユーザによって起動され、[**[管理]**] オプションの **[表示専用]** 許可を持ち、そのテナントの下に [**[管理]**] オプションの **[編集]** 許可を持つユーザがいな場合は常に表示されます。

解決策 : 機能に影響がないため、エラーメッセージは無視してください。

RHEL で CRL が有効になっていると RCM と RCE がサーバに接続しない

問題 : RHEL で CRL が有効になっていると、リモートコレクタマネージャ (RCM) およびリモート相関エンジン (RCE) がサーバに接続できません。

解決策 : マシン上の **[cURL バージョン]** を 7.60 以上にアップグレードします。

イベント視覚化、FIPS、および CRL が有効な場合、RCM がイベントを Sentinel サーバに転送しない

問題 : 分散セットアップの新しいインストールでは、イベント視覚化サービス、FIPS サービス、および CRL サービスを有効にした後、リモートコレクタマネージャ (RCM) はイベントを Sentinel サーバに転送しません。

解決策 : イベント視覚化と FIPS、またはイベント視覚化と CRL が有効になっている場合、RCM はイベントを Sentinel サーバに転送します。

OS を古いバージョンから最新バージョンにアップグレードした後、インシデントレポートが例外で失敗する

問題 : オペレーティングシステムを古いバージョンから最新バージョンにアップグレードする場合、インシデントレポートは例外を除き失敗します。

初めてインデックスを再作成しようとすると例外がログに記録される

問題 : インデックスの再作成操作が初めて実行されると、例外がログに記録されます。

Sentinel 8.5 RCM/RCE アプライアンスビルドで convert_to_fips.sh を実行中にエラーが発生する

問題 : システム管理者が Sentinel 8.5 RCM/RCE アプライアンスビルドで convert_to_fips.sh を実行する際に、継続的なループでユーザの正しい資格情報を入力した後、次のエラーメッセージが表示されます。

```
ERROR: Failed to connect to <Sentinel server IP>:
Failed to retrieve token for communication channel.
```

解決策 : 次の手順を実行します。

1. スクリプトの実行を終了します。
2. <Sentinel RCM/RCE installation>/etc/opt/novell/sentinel/config/configuration.properties に移動します。
3. rest.endpoint.port の値を対応する Web サーバポートに設定します。

   たとえば、rest.endpoint.port=8443
4. convert_to_fips.sh を再実行します。

Micro Focus への連絡方法

特定の製品の問題については https://www.microfocus.com/support-and-services/ にある、Micro Focus サポートに連絡してください。

追加のテクニカル情報またはアドバイスについては、次の複数のソースを参照してください。

- 製品ドキュメント、ナレッジベース記事およびビデオ : https://www.microfocus.com/support-and-services/
- Micro Focus コミュニティページ : https://www.microfocus.com/communities/

保証と著作権