Sentinel 8.5-Versionshinweise

August 2021

Sentinel 8.5 bietet Korrekturen bestimmter früherer Probleme und enthält einige neue Funktionen.

Viele der eingeführten Verbesserungen sind Umsetzungen von Vorschlägen unserer Kunden. Wir möchten uns auf diesem Wege bei Ihnen für Ihr wertvolles Feedback bedanken. Wir hoffen, Sie unterstützen uns weiterhin dabei, unsere Produkte optimal an Ihre Bedürfnisse anzupassen. Senden Sie uns Ihr Feedback als Beitrag im Sentinel-Forum, unserer Online-Community. Hier finden Sie auch Produktinformationen, Blogs und Links zu weiteren nützlichen Ressourcen. Ideen zur Verbesserung des Produkts können Sie auch in unserem Ideenportal teilen.

Die Dokumentation für dieses Produkt steht auf einer Webseite im HTML- und PDF-Format zur Verfügung. Für den Zugriff auf diese Dokumentationsseite ist keine Anmeldung erforderlich. Wenn Sie uns einen Verbesserungsvorschlag in Bezug auf die Dokumentation mitteilen möchten, klicken Sie auf das Kommentierungssymbol, das Sie auf jeder Seite der HTML-Version unserer auf der Sentinel-Dokumentationswebseite veröffentlichten Dokumentation finden. Dieses Produkt steht auf der Website der Produkt-Download-Website zum Herunterladen bereit.

Neue Funktionen

Die folgenden Abschnitte enthalten einen Überblick über die wichtigsten Funktionen, die in dieser Version bereitgestellt werden. Außerdem erfahren Sie hier, welche Probleme in dieser Version behoben wurden:

ArcSight Intelligence-Integration mit Sentinel

Mit dieser Version bietet Sentinel seinen Kunden eine Möglichkeit, die hervorragenden Analysetechnologien von ArcSight Intelligence zu integrieren. Auf diese Weise können Sentinel-Benutzer die Risikobewertung fast in Echtzeit erhalten und für ihre weitere Analyse in ihrer eigenen Korrelationsregel usw. verwenden. Dies ermöglicht es Sentinel, eine optimale Suche nach Bedrohungen auszuführen.

ArcSight Intelligence ist eine Lösung zur Analyse des Benutzer- und Entitätsverhaltens, die Data Science und erweiterte Analysen verwendet, um die wichtigsten risikobehafteten Entitäten und Verhaltensweisen in Ihrer Organisation zu identifizieren. Intelligence stellt zunächst das normale Verhalten für Ihre Organisationseinheiten fest und verwendet dann erweiterte Analysen, um anomales Verhalten von Entitäten zu identifizieren und für jede dieser Entitäten eine angemessene Risikobewertung zu liefern.

Sentinel bietet eine Möglichkeit zur Integration mit ArcSight Intelligence 6.3. Diese Integration erleichtert es Benutzern von Sentinel, ihre Daten zur Analyse an ArcSight Intelligence zu senden, und bietet außerdem die Möglichkeit, die Risikobewertungen für Entitäten von Intelligence zu erhalten. Dadurch erkennt Sentinel alle risikobehafteten Benutzer und Entitäten in der Organisation, die das gesamte System gefährden und eine potenzielle Bedrohung darstellen könnten.

MITRE ATT&CK

MITRE ATT&CK unterstützt Cybersicherheitsteams bei der Bewertung der Wirksamkeit ihrer Security Operations Center (SOC)-Prozesse und Abwehrmaßnahmen, um Verbesserungspotenziale zu identifizieren. MITRE ATT&CK ist eine weltweit zugängliche Wissensdatenbank über Taktiken und Techniken zur Gewährleistung der Cybersicherheit, die auf Beobachtungen realer Situationen basieren. Die MITRE ATT&CK-Wissensdatenbank dient als Grundlage für die Entwicklung spezifischer Bedrohungsmodelle und -methoden in privaten Unternehmen, in Behörden und in der Cybersicherheitsprodukt- und -servicegemeinschaft.

Ab dieser Version von Sentinel können Administratoren Korrelationsregeln eine MITRE ATT&CK-ID zuordnen. MITRE ATT&CK steht für MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). Das MITRE ATT&CK-Framework ist eine gängige Branchensprache für Taktiken und Techniken zum Schutz vor Bedrohungen, die auf realen Beobachtungen basieren.

Sentinel-Administratoren können jetzt ihre eigene vordefinierte oder benutzerdefinierte Korrelationsregel direkt einer MITRE ATT&CK-ID zuordnen. Auf diese Weise erhalten sie umfangreiche Möglichkeiten der Datenanalyse und der Visualisierung der ausgelösten Regeln und der von den Kunden angewendeten MITRE-Taktikten und -Verfahren. Sentinel bietet einen Satz an Werkzeugen, die einen sofortigen Überblick über das Netzwerk und die wichtigsten zu vermeidenden Angriffe bieten.

Wenn eine Korrelationsregel ausgelöst wird, die einer MITRE ATT&CK-ID zugeordnet ist, erhalten die ausgelösten Ereignisse eine MITRE ATT&CK-ID und einen MITRE ATT&CK-Namen. Diese Ereignisse werden über ein Widget analysiert, das in einem standardmäßigen Sicherheits-Dashboard verfügbar ist. Die zehn häufigsten MITRE ATT&CK-Namen werden in diesem Dashboard für einen Zeitbereich von 1 Tag und ein Anzeigeintervall von 1 Stunde angezeigt.

JDK-Aufrüstung

Zur Vermeidung von Sicherheitsschwachstellen (CVE-2021-2161, CVE-2021-2163, CVE-2021-2341, CVE-2021-2432, CVE-2021-2369, CVE-2021-2388) und zur Nutzung der Sicherheitsfunktionen der neuen JDK-Standards wird JDK von 1.8.0_update242 auf 1.8.0_update302 aufgerüstet.

Speichern von Rohereignissen aus dem Connector

Der Sentinel Syslog-Connector ab der Version 2021.1r1 ermöglicht das Speichern der Rohereignisse, die über ArcSight SmartConnectors empfangen werden. Dies sind die unberührten, unverarbeiteten Ereignisse, die direkt vom Endgerät generiert werden. Diese Einstellung kann durch Aktivieren der Option **Preserve Raw Event** (Rohereignis beibehalten) im entsprechenden SmartConnector aktiviert werden.

TLS-Unterstützung

TLS 1.0 und TLS 1.1 werden nicht mehr unterstützt.

Betriebssystemversionen

Herkömmliche Installation: Sentinel ist jetzt auch auf der folgenden neuen Plattform zertifiziert:

- Red Hat Enterprise Linux (RHEL) 8.3

Veraltetes Betriebssystem: Folgende Betriebssysteme sind jetzt veraltet, weil RHEL und SLES keinen Support mehr für diese Betriebssysteme bieten:

- RHEL 7.6 und 7.7
- SLES 15 SP1

Softwarekorrekturen

Sentinel 8.5 enthält einige Softwarekorrekturen zur Behebung folgender Probleme:

Beim Konvertieren zu FIPS auf dem Sentinel-Server wechselt das Protokoll von TLS 1.2 zu TLS 1.1

Problem: Bei der Konvertierung zu FIPS auf dem Sentinel-Server wird das Protokoll von TLS 1.2 in TLS 1.1 geändert, was zum Beenden der Verbindung zwischen SAM und dem Sentinel-Server führt. Der Kunde muss jedoch TLS 1.2 verwenden.

Korrektur: Bei der Konvertierung zu FIPS wird die TLS-Version jetzt nicht mehr von 1.2 in 1.1 geändert.

Sentinel-REST-Aufrufe schlagen nach der Aufrüstung des Sentinel-Java-Clients fehl

Problem: Nach der Aufrüstung des Sentinel-Java-Clients von 8.1 auf 8.2 schlagen REST-Aufrufe fehl.

Korrektur: Nach der Aufrüstung des Sentinel-Java-Clients von 8.1 auf 8.2 schlagen REST-Aufrufe nun nicht mehr fehl.

Fehler beim Generieren eines neuen Berichts

Problem: Fehler beim Generieren eines neuen Berichts. Hauptursache des Problems ist üblicherweise ein manipulierter Keystore oder ein falsches Passwort.

Korrektur: Beim Generieren eines neuen Berichts wird kein Fehler angezeigt.

Systemanforderungen

Weitere Informationen zu den Hardwareanforderungen und den unterstützten Betriebssystemen und Browsern finden Sie in Sentinel System Requirements (Systemanforderungen für Sentinel).

Lizenz- und Kaufinformationen

Um eine Unternehmenslizenz zu erwerben oder Ihre bestehende Lizenz aufzurüsten, rufen Sie 1-800-529-3400 an, senden Sie eine E-Mail an info@microfocus.com oder besuchen Sie https://www.microfocus.com/en-us/products/netiq-sentinel/contact.

Installieren von Sentinel 8.5

Informationen zur Installation von Sentinel 8.5 finden Sie im *Sentinel Installation and Configuration Guide* (Installations- und Konfigurationshandbuch für Sentinel).

HINWEIS: Alle Hosts, die für den Sentinel-Server und seine Komponenten verwendet werden, müssen in einer Umgebung eingerichtet sein, die ein DNS-Auflösen in beide Richtungen erlaubt (Hostname zu IP und IP zu Hostname).

Aufrüsten auf Sentinel 8.5

Sie können von allen früheren Versionen von Sentinel (ab Sentinel 8.2 und höher) auf Sentinel 8.5 aktualisieren.

WICHTIG: Aufgrund der neuesten JDK-Aufrüstung muss der Benutzer für die Konfiguration von LDAPS und SDK den Hostnamen anstelle der IP-Adresse verwenden und der Hostname muss auflösbar sein.

WICHTIG: Es gibt eine Änderung im Aufrüstungsverfahren für die herkömmliche Installation und die Appliance-Installation. Beachten Sie die Informationen hierzu in Settings in Elasticsearch for Secure Cluster Communication (Einstellungen in Elasticsearch für die sichere Clusterkommunikation) und führen Sie die beschriebenen Schritte aus. Dies gilt nur, wenn Sie Sentinel von 8.3.1 oder einer früheren Version auf die neueste Version aufrüsten.

WICHTIG: Sie können eine Offlineaktualisierung ausführen, indem Sie die Offline-Patch-ISO-Datei für jede Appliance herunterladen. Weitere Informationen finden Sie unter Performing Offline Updates (Ausführen von Offlineaktualisierungen).

WARNUNG: Wenn Sie von älteren Versionen als Sentinel 8.3 aufrüsten, müssen Sie die Berechtigung **Ereignisse und Anlagen senden** manuell den Nicht-Administrator-Benutzern zuweisen, die Ereignisse oder Anlagen an Sentinel senden. Wenn Sie diese Berechtigung nicht zuweisen, empfängt Sentinel keine Ereignisse und Anlagen von Change Guardian und Secure Configuration Manager mehr.

Informationen zur herkömmlichen Installation finden Sie im Abschnitt Upgrading the Operating System (Aufrüsten des Betriebssystems) im *Sentinel Installation and Configuration Guide* (Sentinel-Installations- und -Konfigurationshandbuch).

Bekannte Probleme

Micro Focus ist bestrebt, Produkte zu bieten, die hochwertige Lösungen für die Softwarebedürfnisse Ihres Unternehmens darstellen. Die nachfolgend beschriebenen bekannten Probleme werden zurzeit untersucht. Wenden Sie sich an den Technischen Support, wenn Sie weitere Hilfe zu einem Problem benötigen.

Die in Sentinel enthaltene Java 8-Aktualisierung kann die folgenden Plugins beeinträchtigen:

- Cisco SDEE Connector
- SAP (XAL)-Connector
- Remedy Integrator

Probleme mit diesen Plugins werden gemäß den Standardrichtlinien für die Mängelbehebung priorisiert und behoben. Weitere Informationen zu den Supportrichtlinien finden Sie auf der Website zu den Supportrichtlinien.

Diagramm zur Prognose der Speicherkapazität kann nicht angezeigt werden

Problem: In **Sentinel Main** > **Speicher** > **Status** ist das Diagramm **Prognose für Speicherkapazität** nicht verfügbar. Die liegt daran, dass die erforderlichen Schriftarten nicht in Zulu OpenJDK enthalten sind.

Behelfslösung: Installieren Sie die Schriftarten mit den folgenden Befehlen:

- yum install fontconfig
- yum install dejavu

Fehler beim Starten eines Kibana-Dashboards nach der Aufrüstung von Sentinel

Problem: Beim Starten eines Kibana-Dashboards wird die folgende Meldung angezeigt: `No default index pattern. You must select or create one to continue. (Kein standardmäßiges Indexmuster. Zum Fortfahren müssen Sie eines auswählen oder erstellen.)`

Behelfslösung: So legen Sie ein Kibana-Indexmuster als standardmäßiges Indexmuster fest:

1. Wählen Sie eines der folgenden aus:
   - alerts.alerts
   - security.events.normalized_*
2. Klicken Sie auf **Als Standard festlegen**.

Warnmeldungslinks für alle Warnmeldungen können in der Warnmeldungsansicht in Mozilla Firefox oder Microsoft Edge nicht kopiert werden

Problem: Die Option **Alle *<Anzahl der Warnmeldungen>* Warnmeldungen auswählen** > **Warnmeldungslink kopieren** funktioniert in Firefox und Edge nicht.

Behelfslösung: Führen Sie die folgenden Schritte aus:

1. Wählen Sie auf jeder Seite der Warnmeldungsansicht mithilfe des Kontrollkästchens zur Auswahl aller Warnmeldungen manuell alle Warnmeldungen aus.
2. Klicken Sie auf **Warnmeldungslink kopieren**.
3. Fügen Sie den Link in der gewünschten Anwendung ein.

Bei der Installation von Sentinel, Collector Manager und Correlation Engine als OVF-Appliance-Image wird der Anmeldebildschirm nicht angezeigt

Problem: Das Installationsprogramm zeigt weiterhin den Bildschirm zum Installationsfortschritt und nicht den Anmeldebildschirm an, obwohl die Installation abgeschlossen ist.

Behelfslösung: Booten Sie die virtuelle Maschine neu und starten Sie Sentinel, Collector Manager oder Correlation Engine.

Sentinel 8.2 Appliance in Microsoft Hyper-V Server 2016 wird beim Reboot nicht gestartet

Problem: In Hyper-V Server 2016 wird Sentinel Appliance beim Reboot nicht gestartet und die folgende Meldung wird angezeigt:

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

Dieses Problem wird dadurch verursacht, dass das Betriebssystem während der Installation die Datenträger-UUID ändert. Beim Reboot wird der Datenträger daher nicht gefunden.

Behelfslösung: Bearbeiten Sie manuell die Datenträger-UUID. Weitere Informationen hierzu finden Sie in der Knowledge Base in Artikel 7023143.

Fehler beim Aufrüsten auf die Hochverfügbarkeitsversion von Sentinel 8.2 Appliance

Problem: Wenn Sie auf die Hochverfügbarkeitsversion von Sentinel 8.2 Appliance aufrüsten, zeigt Sentinel den folgenden Fehler an:

```
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):
```

Behelfslösung: Führen Sie die folgenden Schritte aus, bevor Sie auf die Eingabeaufforderung antworten:

1. Starten Sie mit PuTTY oder einer ähnlichen Software eine weitere Sitzung zum Host, auf dem Sie die Aufrüstung ausführen.
2. Fügen Sie den folgenden Eintrag in der Datei `/etc/csync2/csync2.cfg` hinzu:

   ```
   /etc/opt/novell/sentinel/config/configuration.properties
   ```
3. Entfernen Sie den Ordner `sentinel` aus `/var/opt/novell`:

   ```
   rm -rf /var/opt/novell/sentinel
   ```
4. Kehren Sie zur Sitzung zurück, in der Sie die Aufrüstung initiiert haben, und geben Sie `r` ein, um mit der Aufrüstung fortzufahren.

Fehler bei der Installation im MFA-Modus von Collector Manager und Correlation Engine Appliance in anderen Sprachen als Englisch

Problem: Bei der Installation der Collector Manager- und Correlation Engine-Appliance im MFA-Modus tritt ein Fehler auf, wenn die Betriebssystemsprache nicht Englisch ist.

Behelfslösung: Installieren Sie Collector Manager und Correlation Engine Appliance auf Englisch. Bei Bedarf können Sie die Sprach nach Abschluss der Installation ändern.

Probleme mit der Bedienbarkeit in den Appliance-Installationsbildschirmen

Problem: Die Schaltflächen **Weiter** und **Zurück** werden in bestimmten Fällen in den Appliance-Installationsbildschirmen nicht angezeigt oder sind deaktiviert. Beispiele:

- Wenn Sie im Sentinel-Vorprüfungsbildschirm auf **Zurück** klicken, um die Informationen auf dem Bildschirm für die Netzwerkeinstellungen von Sentinel Server Appliance zu bearbeiten oder zu überprüfen, wird keine Schaltfläche **Weiter** zum Fortsetzen der Installation angezeigt. Über die Schaltfläche **Konfigurieren** können Sie nur die angegebenen Informationen bearbeiten.
- Wenn Sie falsche Netzwerkeinstellungen angegeben haben, wird auf dem Sentinel-Vorprüfungsbildschirm angezeigt, dass Sie aufgrund von falschen Netzwerkinformationen nicht mit der Installation fortfahren können. Es ist keine Schaltfläche **Zurück** vorhanden, über die zum Bearbeiten der Netzwerkeinstellungen zum vorigen Bildschirm zurückgekehrt werden kann.

Behelfslösung: Starten Sie die Appliance-Installation neu.

Collector Manager hat nicht genügend Arbeitsspeicher, wenn die Zeitsynchronisierung in open-vm-tools aktiviert ist

Problem: Wenn Sie die Zeitsynchronisierung manuell installieren und in open-vm-tools aktivieren, wird die Zeit zwischen Sentinel Appliance (Gast) und dem VMware ESX-Server (Host) regelmäßig synchronisiert. Diese Zeitsynchronisierungen können dazu führen, dass die Gastuhrzeit vor oder nach der Uhrheit des ESX-Servers liegt. Sentinel verarbeitet keine Ereignisse, solange die Uhrzeit zwischen Sentinel Appliance (Gast) und dem ESX-Server (Host) nicht synchronisiert ist. Das führt dazu, dass eine große Menge Ereignisse in Collector Manager in der Warteschlange sitzen und bei Erreichen des Grenzwerts möglicherweise Ereignisse gelöscht werden. Um dieses Problem zu verhindern, deaktiviert Sentinel die Zeitsynchronisierung standardmäßig in der open-vm-tools-Version, die in Sentinel verfügbar ist.

Behelfslösung: Deaktivieren Sie die Zeitsynchronisierung. Weitere Informationen zur Deaktivierung der Zeitsynchronisierung finden Sie unter Disabling Time Synchronization (Deaktivieren der Zeitsynchronisierung).

Bei aktiviertem FIPS-140-2-Modus verlangt Agent Manager die SQL-Authentifizierung

Problem: Wenn der FIPS-140-2-Modus in Sentinel aktiviert ist, führt die Windows-Authentifizierung mit Agent Manager dazu, dass die Synchronisierung mit der Agent Manager-Datenbank fehlschlägt.

Behelfslösung: Verwenden Sie die SQL-Authentifizierung für Agent Manager.

Sentinel-Hochverfügbarkeitsinstallation im Nicht-FIPS-140-2-Modus gibt einen Fehler zurück

Problem: Die Sentinel-Hochverfügbarkeitsinstallation im Nicht-FIPS-140-2-Modus wird erfolgreich abgeschlossen, es wird jedoch zweimal der folgende Fehler angezeigt:

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

Behelfslösung: Der Fehler wird erwartet und kann problemlos ignoriert werden. Die Sentinel-Hochverfügbarkeitskonfiguration funktioniert problemlos im Nicht-FIPS-140-2-Modus, obwohl das Installationsprogramm den Fehler zurückgibt.

Keytool-Befehl zeigt Warnmeldung an

Problem: Bei Verwendung des Keytool-Befehls wird die folgende Warnmeldung angezeigt:

```
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".
```

Behelfslösung: Die Warnmeldung wird erwartet und kann problemlos ignoriert werden. Trotz Anzeige der Warnmeldung arbeitet der Keytool-Befehl wie erwartet.

Sentinel verarbeitet Bedrohungsintelligenz-Feeds nicht im FIPS-Modus

Problem: Im FIPS-Modus zeigt Sentinel beim Verarbeiten standardmäßig verfügbarer Bedrohungsintelligenz-Feeds von URLs den folgenden Fehler an: `Received fatal alert: protocol_version`. Dieses Problem wird dadurch verursacht, dass die standardmäßig verfügbaren Bedrohungs-Feeds nun nur TLS 1.2 unterstützen, diese Version aber im FIPS-Modus nicht funktioniert.

Behelfslösung: Führen Sie Folgendes aus:

1. Klicken Sie auf **Sentinel Main** > **Integration** > **Bedrohungsintelligenzquellen**.
2. Bearbeiten Sie jede URL, indem Sie das Protokoll von `http` in `https` ändern.

Beim Abmelden von Sentinel Main erfolgt im Modus der Multifaktor-Authentifizierung keine Abmeldung von den Dashboards und umgekehrt

Problem: Wenn Sie sich im Modus der Multifaktor-Authentifizierung von **Sentinel Main** abmelden, werden Sie nicht von den Sentinel-Dashboards abgemeldet (und umgekehrt). Dies wird durch ein Problem im Advanced Authentication-Framework verursacht.

Behelfslösung: Solange noch keine Korrektur des Advanced Authentication-Frameworks verfügbar ist, aktualisieren Sie den Bildschirm, damit der Anmeldebildschirm angezeigt wird.

Das benutzerdefinierte Kibana-Dashboard wird nach der Aufrüstung auf Sentinel 8.3.1 nicht angezeigt

Problem: Das benutzerdefinierte Kibana-Dashboard wird nicht angezeigt, wenn Sie von Sentinel 8.3 oder früher auf Sentinel 8.3.1 aufrüsten.

Behelfslösung: Erstellen Sie das benutzerdefinierte Dashboard nach der Aufrüstung von Sentinel neu.

Beim Starten von Kibana wird die Konfliktfehlermeldung angezeigt

Problem: Nach der Installation oder Aufrüstung von Sentinel und beim ersten Start von Kibana wird die Konfliktfehlermeldung angezeigt.

Behelfslösung: Ignorieren Sie die Konfliktfehlermeldung. Sie hat keine Auswirkungen auf die Funktionalität.

Beim Neubooten des Betriebssystems Red Hat 8.1 und 8.2 wird Sentinel nicht automatisch gestartet

Problem: Nach der Installation von Sentinel auf dem Betriebssystem Red Hat 8.1 oder 8.2 wird Sentinel (Server, RCM oder RCE) nach dem Neubooten nicht automatisch gestartet.

Behelfslösung: Ändern Sie den SELINUX-Wert in **SELINUX=disabled** in der Datei `/etc/selinux/config`.

Beim Öffnen von Sentinel Appliance Management Console wird eine Fehlermeldung angezeigt

Problem: Wenn Sie nach der Aufrüstung auf Sentinel 8.3 versuchen, Sentinel Appliance Management Console der CE (Correlation Engine) oder des CM (Collector Manager) von HA-Servern (Hochverfügbarkeitsservern) zu öffnen, wird die Fehlermeldung `Error 404 – Not found` (Fehler 404 – Nicht gefunden) angezeigt.

Behelfslösung: Weitere Informationen finden Sie im Micro Focus-Knowledgebase-Dokument.

Benutzer mit der Einstellung „Hide Management Permission of Visualization“ (Verwaltungsberechtigung für Grafik ausblenden) können weiterhin die Registerkarte „Verwaltung“ auf der Kibana-Seite sehen

Problem: Nach der Aufrüstung auf Sentinel 8.4 können Benutzer mit der Einstellung „Hide Management Permission of Visualization“ (Verwaltungsberechtigung der Grafik ausblenden) weiterhin die Registerkarte „Verwaltung“ auf der Kibana-Seite sehen, aber nicht auf die Funktionen der Registerkarte „Verwaltung“ zugreifen.

Wenn der Administrator die Benutzerrolle von Warnmeldungen ändert, werden die sofortigen Änderungen nicht auf der Kibana-Seite aktualisiert

Problem: Vorhandene Benutzer können nicht sofort Warnmeldungen auf der Kibana-Seite anzeigen, obwohl die Berechtigung vom Administrator aktualisiert wurde, um die Warnmeldungen anzuzeigen.

Behelfslösung: Wenn die Benutzerberechtigung aktualisiert wird, müssen Sie sich abmelden und erneut anmelden.

Beim Starten des Grafik-Dashboards als Mandantenbenutzer wird eine Fehlermeldung angezeigt

Problem: Wenn ein nicht standardmäßiger Mandantenbenutzer das Grafik-Dashboard startet, wird die Fehlermeldung **Verboten** angezeigt. Diese Fehlermeldung wird immer dann angezeigt, wenn das Dashboard von einem nicht standardmäßigen Mandantenbenutzer gestartet wird, der über die Berechtigung **Nur Anzeigen** für die Option **Verwaltung** verfügt, und wenn unter diesem Mandanten kein Benutzer mit der Berechtigung **Bearbeiten** für die Option **Verwaltung** vorhanden ist.

Behelfslösung: Ignorieren Sie die Fehlermeldung. Sie hat keine Auswirkungen auf die Funktionalität.

In RHEL stellen RCM und RCE keine Verbindung zum Server her, wenn die Zertifikatswiderrufsliste aktiviert ist

Problem: Remote Collector Manager (RCM) und Remote Correlation Engine (RCE) können keine Verbindung zum Server herstellen, wenn die Zertifikatswiderrufsliste in RHEL aktiviert ist.

Behelfslösung: Rüsten Sie die **cURL-Version** auf dem Computer auf 7.60 oder höher auf.

RCM leitet die Ereignisse nicht an den Sentinel-Server weiter, wenn die Ereignisgrafik, FIPS und die Zertifikatswiderrufsliste aktiviert sind

Problem: Bei der neuen Installation der verteilten Einrichtung leitet Remote Collector Manager (RCM) nach der Aktivierung der Ereignisgrafik-, FIPS- und Zertifikatswiderrufslisten-Services die Ereignisse nicht an den Sentinel-Server weiter.

Behelfslösung: Wenn entweder die Ereignisgrafik und FIPS oder die Ereignisgrafik und die Zertifikatswiderrufsliste aktiviert sind, leitet RCM die Ereignisse an den Sentinel-Server weiter.

Nach der Aufrüstung des Betriebssystems von einer älteren auf die neueste Version schlagen Vorfallberichte mit Ausnahmen fehl

Problem: Wenn Sie das Betriebssystem von einer älteren Version auf die neueste Version aufrüsten, schlagen Vorfallberichte mit Ausnahmen fehl.

Beim ersten Versuch der Neuindizierung wird eine Ausnahme protokolliert

Problem: Eine Ausnahme wird protokolliert, wenn der Neuindizierungsvorgang zum ersten Mal ausgeführt wird.

Fehler beim Ausführen von `convert_to_fips.sh` im Sentinel 8.5 RCM/RCE-Appliance-Build

Problem: Wenn der Systemadministrator `convert_to_fips.sh` im Sentinel 8.5 RCM/RCE-Appliance-Build ausführt, wird nach der Angabe des richtigen Berechtigungsnachweises der Benutzer in einer kontinuierlichen Schleife die folgende Fehlermeldung angezeigt:

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

Behelfslösung: Führen Sie die folgenden Schritte aus:

1. Beenden Sie die Skriptausführung.
2. Wechseln Sie zu `<Sentinel RCM/RCE-Installation>/etc/opt/novell/sentinel/config/configuration.properties`
3. Legen Sie den Wert von `rest.endpoint.port` auf den entsprechenden Webserverport fest.

   Beispiel: `rest.endpoint.port=8443`
4. Führen Sie `convert_to_fips.sh` erneut aus

Kontakt mit Micro Focus

Bei konkreten Problemen mit einem Produkt wenden Sie sich an den Micro Focus-Support unter https://www.microfocus.com/support-and-services/.

Weitere technische Informationen oder Tipps erhalten Sie in verschiedenen Quellen:

- Produktdokumentation, Knowledge Base-Artikel und Videos: https://www.microfocus.com/support-and-services/
- Seiten der Micro Focus-Community: https://www.microfocus.com/communities/

Rechtliche Hinweise