Sentinel 8.5 版本說明

2021 年 8 月

Sentinel 8.5 解決數個先前的問題，同時新增一些新功能。

這些改進許多是為了直接因應來自顧客的建議。我們衷心感謝您撥冗提供寶貴的建議。也期盼您能繼續協助以確保我們的產品能滿足您所有的需求。您可以在 Sentinel 論壇中張貼意見反應，此論壇是我們的線上社群，其中也包含產品資訊、部落格，以及實用資源的連結。您可以在構想入口網站上分享有關您對改善產品的構想。

本產品的文件分別以 HTML 與 PDF 格式提供於無需登入即可存取的頁面上。若您有關於文件改進的建議，請前往 Sentinel 文件頁面，在 HTML 版本文件的任一頁面中，按一下備註圖示。若要下載此產品，請查看產品下載網站。

全新功能

以下幾節說明此版本提供的主要功能，以及此次發行所解決的問題：

Sentinel 與 ArcSight Intelligence 的整合

在此版本中，Sentinel 提供方法，讓客戶整合令人興奮的 ArcSight Intelligence 分析技術。因此，Sentinel 使用者幾乎可以即時獲得風險評分，並將其用於對專屬相關規則的進一步分析等等。這讓 Sentinel 獲得許多威脅搜捕體驗。

ArcSight Intelligence 是一種使用者和實體行為分析解決方案，可使用資料科學和進階分析來識別組織中的高風險實體和所發生的行為。Intelligence 會先建立您組織實體的正常行為，然後使用進階分析來識別任何實體的異常行為，並為每個這類實體提供適當的風險評分。

Sentinel 提供一種方法來整合 ArcSight Intelligence 6.3。這項整合可促進 Sentinel 使用者將其資料傳送至 ArcSight Intelligence 以進行分析，同時提供一種方法接收來自 Intelligence 的實體風險評分詳細資料。這讓 Sentinel 可偵測組織中任何可能危及整個系統並造成潛在威脅的高風險使用者和實體。

MITRE ATT&CK

MITRE ATT&CK 協助網路安全團隊評估其安全營運中心 (SOC) 程序和防禦措施的有效性，以識別需要改進的區域。MITRE ATT&CK 是一套可供全球存取的知識庫，其內容是根據對真實世界的網路安全攻擊者策略和技術的觀察。民營企業、政府以及網路安全產品和服務社群會運用 MITRE ATT&CK 知識庫並作為開發特定威脅模型和方法的基礎。

在這版 Sentinel 中，管理員可以將相關規則與 MITRE ATT&CK ID 進行映射。MITRE ATT&CK 代表 MITRE 攻擊策略、技術和常識 (MITRE Adversarial Tactics, Techniques, and Common Knowledge，ATT&CK)。MITRE ATT&CK Framework 是根據真實世界觀察的威脅行為者策略和技術的通用產業語言。

Sentinel 管理員現在可以直接將自己的立即可用或自定相關規則與 MITRE ATT&CK ID 進行映射。因此，在觸手可及的位置提供大量資料分析，進而讓他們可以透過視覺方式檢視引發的規則，或者其客戶正在利用的所有策略和 MITRE 技術。Sentinel 為他們提供一組特定工具集，透過這些工具集，他們可以立即檢視其網路以及他們需要防止的最重要攻擊。

如果引發與 MITRE ATT&CK ID 映射的相關規則，則引發的事件將會有 MITRE ATT&CK ID 和 MITRE ATT&CK 名稱。這些事件是透過預設安全性狀態儀表板中的小工具進行分析。在時間範圍為 1 天且顯示間隔為 1 小時的這個儀表板中，會顯示前十個 MITRE ATT&CK 名稱。

JDK 升級

為了避免安全性漏洞 (CVE-2021-2161、CVE-2021-2163、CVE-2021-2341、CVE-2021-2432、CVE-2021-2369、CVE-2021-2388)，以及利用新 JDK 標準安全性功能，已將 JDK 從 1.8.0_update242 升級為 1.8.0_update302

從連接器儲存原始事件

2021.1r1 版的 Sentinel Syslog 連接器，將會啟用儲存來自 ArcSight Smart Connector 的原始事件。這些是由終端裝置直接產生的未觸及且未處理事件。勾選相應 Smart Connector 中的 **「保留原始事件」**選項，即可啟用此設定。

TLS 支援

已移除 TLS 1.0 和 TLS 1.1 的支援。

作業系統 (OS) 版本

傳統安裝：Sentinel 現在也在以下新平台上獲得認證：

- Red Hat Enterprise Linux (RHEL) 8.3

已淘汰的作業系統：以下作業系統已被淘汰，因為 RHEL 和 SLES 已移除對這些作業系統的支援：

- RHEL 7.6 和 7.7
- SLES 15 SP1

軟體修復

Sentinel 8.5 包含可解決下列問題的軟體修復：

- 「在 Sentinel Server 上轉換為 FIP，會將協定從 TLS 1.2 變更為 TLS 1.1」(第 3 頁)
- 「升級 Sentinel Java Client 之後，Sentinel REST 呼叫將會失敗」(第 3 頁)
- 「產生新報告時發生錯誤」(第 3 頁)

在 Sentinel Server 上轉換為 FIP，會將協定從 TLS 1.2 變更為 TLS 1.1

問題：在 Sentinel 伺服器上轉換 FIP 時，協定會從 TLS 1.2 變更為 TLS 1.1 且這會導致 SAM 和 Sentinel 伺服器之間的連接終止。不過，客戶必須使用 TLS 1.2

修復：現在，轉換為 FIPS 時，不會將 TLS 版本從 1.2 變更為 1.1

升級 Sentinel Java Client 之後，Sentinel REST 呼叫將會失敗

問題：將 Sentinel Java Client 從 8.1 升級至 8.2 之後，REST 呼叫將會失敗。

修復：現在，將 Sentinel Java Client 從 8.1 升級至 8.2 之後，REST 呼叫將不會失敗。

產生新報告時發生錯誤

問題：產生新報告時發生錯誤。錯誤的主要問題可能是 KeyStore 遭竄改或密碼不正確。

修復：產生新報告時未發生錯誤。

系統要求

如需關於硬體要求、支援的作業系統和瀏覽器的詳細資訊，請參閱 Sentinel 系統要求。

授權和購買資訊

若要購買企業授權或升級現有授權，請致電 1-800-529-3400、將電子郵件傳送至 info@microfocus.com，或造訪 https://www.microfocus.com/en-us/products/netiq-sentinel/contact。

安裝 Sentinel 8.5

如需安裝 Sentinel 8.5 的詳細資訊，請參閱 *《Sentinel 安裝與組態指南》*。

附註：您必須在雙向 DNS 可解析環境 (主機名稱到 IP 和 IP 到主機名稱) 中設定所有用於 Sentinel 伺服器的主機和其元件。

升級至 Sentinel 8.5

您可以從任何舊版 Sentinel (從 Sentinel 8.2 和更新版本) 升級至 Sentinel 8.5。

重要：因為執行最新 JDK 升級，所以設定 LDAPS 和 SDK 時，使用者需要使用主機名稱，而非 IP 位址，同時必須為可進行解析。

重要：傳統和裝置安裝的升級程序已變更。請參閱 Elasticsearch 中適用於安全叢集通訊的設定，並遵循步驟操作。只有在您將 Sentinel 從 8.3.1 和之前版本升級至最新版本時，這才適用。

重要：您可以下載每個裝置的離線修補程式 ISO 來執行離線更新。如需詳細資訊，請參閱執行離線更新。

警告：如果您從 Sentinel 8.3 之前的版本升級，則必須手動將 **「傳送事件和附件」**許可指定給負責將事件或附件傳送至 Sentinel 的非管理員使用者。若您未指定此許可權，Sentinel 即無法接收來自 Change Guardian 和 Secure Configuration Manager 的事件和附件。

對於傳統安裝，請參閱 *《Sentinel 安裝和設定指南》*中的升級作業系統小節。

已知問題

Micro Focus 致力於確保我們的產品提供最優質的解決方案，以符合貴企業的軟體需求。以下是現在正在研究的已知問題。若您有任何問題需要進一步的協助，請聯絡技術支援。

Sentinel 所包含的 Java 8 更新可能會影響下列外掛程式 :

- Cisco SDEE Connector
- SAP (XAL) Connector
- 因應措施整合器

針對任何外掛程式的相關問題，我們將根據標準的缺陷處理規則排列優先程度並修正問題。如需有關支援規則的詳細資訊，請參閱支援規則。

- 「無法檢視儲存容量預測表」 (第 5 頁)
- 「在升級 Sentinel 之後啟動 Kibana 儀表板時發生錯誤」 (第 5 頁)
- 「無法在 Mozilla Firefox 和 Microsoft Edge 的警告檢視中複製所有警告的警告連結」 (第 6 頁)

無法檢視儲存容量預測表

問題： 在 「Sentinel Main」 > 「儲存」 > 「狀態」中，「儲存容量預測」表無法使用。這是因為 Zulu OpenJDK 未包含必要的字型。

解決方式：使用下列指令安裝字型：

- yum install fontconfig
- yum install dejavu

在升級 Sentinel 之後啟動 Kibana 儀表板時發生錯誤

問題： 啟動 Kibana 儀表板時會顯示下列訊息：沒有預設索引模式。您必須選取或建立該模式才能繼續作業。

解決方式：若要將 Kibana 索引模式設定為預設索引模式：

1. 選取下列任一項：
   - alerts.alerts
   - security.events.normalized_*
2. 按一下**設定為預設值**。

無法在 Mozilla Firefox 和 Microsoft Edge 的警告檢視中複製所有警告的警告連結

問題：「**全選 < *警告數目* > 個警告**」 >「**複製警告連結**」選項在 Firefox 和 Edge 中無法運作。

解決方式：請執行以下步驟：

1. 使用可讓您選取所有警告的核取方塊，手動選取每個警告檢視頁面上的所有警告。
2. 按一下「**複製警告連結**」。
3. 將其貼到所需的應用程式中。

以 OVF 應用裝置映像形式安裝 Sentinel、Collector Manager 及 Correlation Engine 時，將無法顯示登入畫面

問題： 安裝程式停滯於「安裝進行中」畫面，且即使安裝已完成，也不會顯示登入畫面。

解決方式：將虛擬機器重新開機，並啟動 Sentinel、Collector Manager 或 Correlation Engine。

在您重新開機時 Microsoft Hyper-V Server 2016 中的 Sentinel 8.2 應用裝置不會啟動

問題： 在您重新開機時 Hyper-V Server 2016 中的 Sentinel 8.2 應用裝置不會啟動，並顯示下列訊息：

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

此問題的起因是作業系統會在安裝時修改磁碟 UUID。因此在重新開機時找不到磁碟。

解決方式：手動修改磁碟 UUID。如需更多資訊，請參閱知識庫文章 7023143。

升級至 Sentinel 8.2 HA 應用裝置時發生錯誤

問題： 當您要升級至 Sentinel 8.2 HA 應用裝置時，Sentinel 顯示下列錯誤：

```
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):
```

解決方式：在回應上述提示之前，請執行下列動作：

1. 使用 PuTTY 或類似軟體開啟另一個工作階段至執行升級的主機。
2. 在 /etc/csync2/csync2.cfg 檔案中加入下列項目：

/etc/opt/novell/sentinel/config/configuration.properties

3 從 /var/opt/novell 移除 sentinel 資料夾：

rm -rf /var/opt/novell/sentinel

4 返回您啟始升級所在的工作階段並輸入 r 以繼續進行升級。

在 MFA 模式下，以英語以外的語言安裝 Collector Manager 和 Correlation Engine 工具會失敗

問題：在 MFA 模式下，如果以英語以外的操作系統語言安裝 Collector Manager 和 Correlation Engine 工具會失敗。

解決方式：以英語安裝 Collector Manager 和 Correlation Engine 工具安裝完成後，請視需要變更語言。

應用裝置安裝畫面中的可用性問題

問題： 應用裝置安裝畫面未顯示**下一步**和**上一步**按鈕，或在某些情況下停用，例如：

- 當您從 Sentinel 檢查前畫面按一下**上一步**，以編輯或檢閱 Sentinel 伺服器應用裝置網路設定畫面中的資訊時，系統未顯示**下一步**按鈕以繼續進行安裝作業。**設定**按鈕可讓您僅編輯特定資訊。
- 如果您指定了錯誤的網路設定，Sentinel 檢查前畫面將指示由於網路資訊不正確，無法繼續進行安裝。系統未顯示可前往下一個畫面的**「上一步」**按鈕，以供修改網路設定。

解決方式：重新啟動應用裝置安裝程式。

如果在 Open-vm-tools 中啟用時間同步，則 Collector Manager 會耗盡記憶體

問題： 如果您在 open-vm-tool 中手動安裝並啟用時間同步，在 Sentinel 應用裝置 (客體) 和 VMware ESX 伺服器 (主機) 之間會週期性地同步時間。這些時間同步可能會造成客體的時鐘較 ESX 伺服器的時間慢或快。在 Sentinel 應用裝置 (客體) 和 VMware ESX 伺服器 (主機) 之間的時間同步之前，Sentinel 不會處理事件。因此，大量事件在 Collector Manager 中佇列，最終達到臨界值時可能會捨棄事件。為了避免此問題，依預設在 Sentinel 中可用的 open-vm-tool 版本中 Sentinel 會停用時間同步。

解決方式：停用時間同步。如需關於停用時間同步的詳細資訊，請參閱停用時間同步。

啟用 FIPS 140-2 模式時，代辦管理員需要 SQL 驗證

問題：當在 Sentinel 中啟用 FIPS 140-2 模式時，使用 Agent Manager 的 Windows 驗證會造成與 Agent Manager 資料庫同步失敗。

解決方式：使用 Agent Manager 的 SQL 驗證。

Sentinel 高可用性安裝在非 FIPS 140-2 模式中顯示錯誤

問題：已成功使用 FIPS 140-2 模式完成安裝 Sentinel 高可用性，但出現下列錯誤兩次：

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

解決方式：此為預期的錯誤，您可以安全地忽略它。雖然安裝程式顯示錯誤，但是 Sentinel High Availability 組態在非 FIPS 140-2 模式中仍可順利運作。

Keytool 指令會顯示警告

問題： 使用 Keytool 指令時，將顯示下列警告：

```
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".
```

解決方式：此為預期的警告，您可以安全地忽略它。雖然會顯示此警告，但 Keytool 指令仍可如預期般運作。

Sentinel 在 FIPS 模式下不會處理威脅情報摘要

問題： 在 FIPS 模式中，Sentinel 在處理來自 URL 的現成可用威脅情報摘要時會顯示下列錯誤：接收到嚴重警示 : protocol_version。此問題的發生原因是立即可用的威脅摘要現在僅支援無法以 FIPS 模式運作的 TLS 1.2。

解決方式：請執行下列作業：

1. 按一下 **「Sentinel Main」** > **「整合」** > **「威脅情報來源」**。
2. 編輯每個 URL，將通訊協定從 http 變更為 https。

在多因素驗證模式中，從 Sentinel 主視圖登出將無法登出儀表板，反之亦然

問題： 在多因素驗證模式中，您在登出 **Sentinel Main** 後並不會登出 Sentinel 儀表板，反之亦然。這是由於進階驗證架構的問題所致。

解決方式：在進階驗證架構提供修正程式之前，請重新整理畫面以檢視登入畫面。

升級至 Sentinel 8.3.1 之後，未顯示 Kibana 自定儀表板

問題：當您從 Sentinel 8.3 或更早版本升級至 Sentinel 8.3.1 時，未顯示 Kibana 自定儀表板。

解決方式：升級 Sentinel 之後，請確保重新建立自定儀表板。

當您啟動 Kibana 時，顯示衝突錯誤訊息

問題：安裝或升級 Sentinel 之後，以及您第一次啟動 Kibana 時，會顯示衝突錯誤訊息。

解決方式：忽略衝突錯誤訊息，因為不會影響功能。

當您重新啟動 OS Redhat 8.1 和 8.2 時，不會自動啟動 Sentinel

問題：在 OS Redhat 8.1 和 8.2 上安裝 Sentinel 之後，未在重新啟動後自動啟動 Sentinel (Server、RCM 或 RCE)。

解決方式：在檔案 /etc/selinux/config 中，將 SELINUX 值變更為 **SELINUX=disabled**。

開啟 Sentinel 裝置管理主控台時顯示錯誤訊息

問題：升級至 Sentinel 8.3 之後，當您嘗試開啟 HA (高可用性) 伺服器之 CE (Correlation Engine) 或 CM (Collector Manager) 的 Sentinel 裝置管理主控台時顯示錯誤 404 - 找不到錯誤訊息。

解決方式：如需詳細資訊，請參閱 Micro Focus 知識庫文件。

具有隱藏視覺化管理許可的使用者，仍然可以在 Kibana 頁面中看到管理索引標籤

問題：升級至 Sentinel 8.4 之後，具有隱藏視覺化管理許可的使用者仍然可以在 Kibana 頁面上看到「管理」索引標籤，但無法存取 「管理」索引標籤的功能。

管理員變更警示使用者角色時，未在 Kibana 頁面中更新立即變更

問題：雖然管理員已更新查看警示的許可，但是現有使用者還是無法立即在 Kibana 頁面上看到任何警示。

解決方式：更新使用者許可時，您需要登出並重新登入。

以租用戶使用者身分啟動視覺化儀表板時顯示錯誤訊息

問題：非預設租用戶使用者啟動視覺化儀表板時，顯示 **「禁止」**錯誤訊息。只要非預設租用戶使用者啟動儀表板時，就會顯示此錯誤訊息，而此租用戶使用者對 **「管理」**選項具有 **「僅檢視」**許可，而且沒有使用者在該租用戶下具有 **「管理」**選項的 **「編輯」**許可。

解決方式：忽略錯誤訊息，因為不會影響功能。

在 RHEL 中，啟用 CRL 時，RCM 和 RCE 未連接至伺服器

問題：在 RHEL 中，啟用 CRL 時，遠端 Collector Manager (RCM) 和遠端 Correlation Engine (RCE) 無法連接至伺服器。

解決方式：將機器上的 **cURL 版本**升級至 7.60 或以上版本。

啟用事件視覺化、FIPS 和 CRL 時，RCM 未將事件轉遞至 Sentinel Server

問題：在重新安裝分散式設定時，於啟用事件視覺化、FIPS 和 CRL 服務之後，遠端 Collector Manager (RCM) 未將事件轉遞至 Sentinel Server。

解決方式：如果啟用事件視覺化和 FIPS 或是啟用事件視覺化和 CRL，則 RCM 會將事件轉遞至 Sentinel Server。

將作業系統從任何舊版本升級至最新版本之後，事件報告將會失敗並發生例外

問題：當您將作業系統從舊版本升級至最新版本時，事件報告失敗，並發生例外。

第一次嘗試重新編製索引時記錄例外

問題：第一次執行重新編製索引操作時，將會記錄例外。

在 Sentinel 8.5 RCM/RCE 裝置版次中執行 convert_to_fips.sh 時發生錯誤

問題：系統管理員在 Sentinel 8.5 RCM/RCE 裝置版次中執行 convert_to_fips.sh 時，在連續迴圈中提供使用者的正確身分證明之後，顯示下列錯誤訊息：

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

解決方式：請執行以下步驟：

1. 結束程序檔執行。
2. 前往 <Sentinel RCM/RCE installation>/etc/opt/novell/sentinel/config/configuration.properties
3. 將 rest.endpoint.port 的值設定為相應的網頁伺服器連接埠。

   例如，rest.endpoint.port=8443
4. 重新執行 convert_to_fips.sh

聯絡 Micro Focus

如果遇到具體的產品問題，請在 https://www.microfocus.com/support-and-services/ 上聯絡 Micro Focus 支援人員。

可透過多種來源取得其他技術資訊或建議：

- 產品文件、知識庫文章和視訊： https://www.microfocus.com/support-and-services/
- Micro Focus 社群網頁： https://www.microfocus.com/communities/

法律聲明