Notas de la versión de Sentinel 8.5

Agosto de 2021

Sentinel 8.5 soluciona varios problemas anteriores y añade también algunas funciones nuevas.

Muchas de estas mejoras se realizaron en respuesta directa a las sugerencias de nuestros clientes. A todos les agradecemos su tiempo y su valiosa aportación. Esperamos que sigan ayudándonos a garantizar que nuestros productos satisfagan todas sus necesidades. Puede publicar comentarios en el foro de Sentinel, nuestra comunidad en línea que también incluye información sobre productos, blogs y enlaces a recursos útiles. También puede compartir sus ideas para mejorar el producto en elPortal de ideas.

La documentación de este producto está disponible en formato HTML y PDF, en una página que no requiere entrar a una sesión. Si tiene sugerencias de mejoras para la documentación, haga clic en el icono de comentarios en cualquier página de la versión HTML de la documentación publicada en la documentación de Sentinel. Para descargar este producto, consulte el sitio Web de descargas de productos.

Novedades

En las siguientes secciones, se describen las principales características de esta versión, así como los problemas resueltos en ella:

Integración de ArcSight Intelligence con Sentinel

Con esta versión, Sentinel ofrece a sus clientes integración con las tecnologías de análisis de ArcSight Intelligence. Por lo tanto, los usuarios de Sentinel pueden obtener una puntuación de riesgo casi en tiempo real y utilizarla para su posterior análisis en su propia regla de correlación, etc. Esto permite a Sentinel obtener una gran experiencia de detección de amenazas.

ArcSight Intelligence es una solución de análisis de comportamiento de usuarios y entidades que utiliza ciencia de datos y análisis avanzados para identificar las principales entidades y comportamientos de riesgo que se producen en su organización. La inteligencia establece en primer lugar el comportamiento normal de las entidades de su organización y, a continuación, utiliza análisis avanzados para identificar los comportamientos anómalos de cualquier entidad y proporciona una puntuación de riesgo correspondiente a cada una de ellas.

Sentinel permite la integración con ArcSight Intelligence 6.3. Esta facilita a los usuarios de Sentinel el envío de datos a ArcSight Intelligence para su análisis y también permite recibir información sobre la puntuación de riesgo de las entidades desde Intelligence. Esto permite que Sentinel detecte cualquier usuario o entidad de mayor riesgo de la organización que pueda poner en peligro todo el sistema y que suponga una posible amenaza.

MITRE ATT&CK

MITRE ATT&CK ayuda a los equipos de ciberseguridad a evaluar la eficacia de sus procesos y medidas defensivas del Centro de operaciones de seguridad (SOC) para identificar áreas de mejora. MITRE ATT&CK es una base de conocimientos de acceso mundial sobre las tácticas y las técnicas de los adversarios de la ciberseguridad basada en observaciones del mundo real. La base de conocimientos MITRE ATT&CK permite el desarrollo de métodos y modelos de amenazas específicos en el sector privado, gubernamental y en la comunidad de productos y servicios de ciberseguridad.

A partir de esta versión de Sentinel, los administradores pueden asignar reglas de correlación con ID de MITRE ATT&CK. MITRE ATT&CK son las siglas de MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK). El marco MITRE ATT&CK es un lenguaje común de la industria sobre las tácticas y las técnicas de los actores de amenazas basado en observaciones del mundo real.

Ahora los administradores de Sentinel pueden asignar su propia regla de correlación personalizada o lista para su uso directamente con el ID de MITRE ATT&CK. Por lo tanto, facilita una gran cantidad de análisis de datos, que proporciona la capacidad de visualizar las reglas activas o las tácticas y las técnicas de MITRE que están explotando los clientes. Sentinel les proporciona un grupo específico de conjuntos de herramientas que les permite obtener al instante una vista de la red y los ataques más importantes que deben evitar.

Si se activa una regla de correlación asignada con un ID de MITRE ATT&CK, los eventos activados tendrán un ID y un nombre de MITRE ATT&CK. Estos eventos se analizan a través de un widget disponible en una consola de estado de seguridad por defecto. Los diez nombres principales de MITRE ATT&CK aparecen en esta consola en un intervalo de tiempo de 1 día y un intervalo de visualización de 1 hora.

Actualización de JDK

Para evitar las vulnerabilidades de seguridad (CVE-2021-2161, CVE-2021-2163, CVE-2021-2341, CVE-2021-2432, CVE-2021-2369, CVE-2021-2388) y utilizar las funciones de seguridad de los nuevos estándares del JDK, este se actualiza de 1.8.0_update242 a 1.8.0_update302.

Almacenamiento de eventos en bruto desde el conector

A partir de la versión 2021.1r1, el conector Syslog de Sentinel habilitará el almacenamiento de eventos en bruto a través de los Smart Connector de ArcSight. Se trata de los eventos sin modificar ni procesar que genera directamente el dispositivo final. Para habilitar este ajuste, active la opción **Preserve Raw Event** (Conservar evento en bruto) en el Smart Connector correspondiente.

Compatibilidad con TLS

Se ha eliminado la compatibilidad con TLS 1.0 y TLS 1.1.

Versiones del sistema operativo (SO)

Instalación tradicional: Ahora Sentinel también cuenta con certificación para la siguiente plataforma nueva:

- Red Hat Enterprise Linux (RHEL) 8.3

SO obsoleto: El sistema operativo siguiente ha quedado obsoleto desde que RHEL y SLES eliminaron la compatibilidad con estos SO:

- RHEL 7.6 y 7.7
- SLES 15 SP1

Correcciones de software

Sentinel 8.5 incluye correcciones de software que solucionan los siguientes problemas:

- "La conversión a FIPS en el servidor Sentinel cambia el protocolo de TLS 1.2. a TLS 1.1" en la página 3
- "Las llamadas REST de Sentinel presentan errores después de actualizar el cliente Java de Sentinel" en la página 3
- "Error al generar un informe nuevo" en la página 4

La conversión a FIPS en el servidor Sentinel cambia el protocolo de TLS 1.2. a TLS 1.1

Problema: Al realizar la conversión a FIPS en el servidor Sentinel, el protocolo cambia de TLS 1.2 a TLS 1.1, lo que hace que termine la conexión entre SAM y el servidor Sentinel. Sin embargo, el cliente debe utilizar TLS 1.2.

Solución: Ahora, al convertir a FIPS, la versión de TLS no cambia de 1.2 a 1.1.

Las llamadas REST de Sentinel presentan errores después de actualizar el cliente Java de Sentinel

Problema: Después de actualizar el cliente Java de Sentinel de la versión 8.1 a la 8.2, las llamadas REST presentan errores.

Solución: Ahora, después de actualizar el cliente Java de Sentinel de la versión 8.1 a la 8.2, las llamadas REST no presentan errores.

Error al generar un informe nuevo

Problema: Error al generar un informe nuevo. La principal consecuencia del error puede ser que se altere el almacén de claves o que la contraseña sea incorrecta.

Solución: No se recibe ningún error al generar un informe nuevo.

Requisitos del sistema

Para obtener más información sobre los requisitos de hardware, y los sistemas operativos y los navegadores compatibles, consulte los Requisitos del sistema de Sentinel.

Información sobre licencias y compras

Para adquirir una licencia empresarial o actualizar la licencia existente, llame al número 1-800-529-3400, envíe un mensaje a info@microfocus.com o visite https://www.microfocus.com/en-us/products/netiq-sentinel/contact.

Instalación de Sentinel 8.5

Para obtener información acerca de la instalación de Sentinel 8.5, consulte la *Sentinel Installation and Configuration Guide* (Guía de instalación y configuración de Sentinel).

Nota: Todos los hosts utilizados para el servidor Sentinel y sus componentes deben configurarse en un entorno de DNS bidireccional que se pueda resolver (de nombre de host a IP y de IP a nombre de host).

Actualización a Sentinel 8.5

Puede actualizar a Sentinel 8.5 desde cualquier versión anterior de Sentinel (desde Sentinel 8.2 y versiones posteriores).

Importante: Debido a la actualización más reciente de JDK, para configurar LDAPS y SDK, el usuario debe utilizar el nombre de host en lugar de la dirección IP y este debe poder resolverse.

Importante: Hay un cambio en el procedimiento de actualización de la instalación tradicional y como dispositivo. Consulte Configuración de Elasticsearch para la comunicación segura del clúster y siga los pasos indicados. Esto solo es aplicable si va a actualizar Sentinel a las versiones más recientes desde la versión 8.3.1 y anteriores.

Importante: Puede realizar una actualización sin conexión mediante la descarga de la imagen ISO de parche sin conexión para cada dispositivo. Para obtener más información, consulte Actualizaciones sin conexión.

Advertencia: Si actualiza desde versiones anteriores a Sentinel 8.3, debe asignar manualmente el permiso **Enviar eventos y archivos adjuntos** a usuarios que no sean administradores que envíen eventos o archivos adjuntos a Sentinel. A menos que asigne este permiso, Sentinel ya no recibirá eventos y archivos adjuntos de Change Guardian ni Secure Configuration Manager.

Para realizar una instalación tradicional, consulte la sección Upgrading the Operating System (Actualización del sistema operativo) en *Sentinel Installation and Configuration Guide* (Guía de instalación y configuración de Sentinel).

Problemas conocidos

Micro Focus se esfuerza por garantizar que nuestros productos ofrezcan soluciones de calidad para sus necesidades de software empresarial. Se están investigando los siguientes problemas conocidos. Si necesita más ayuda con algún problema, póngase en contacto con el departamento de Asistencia técnica.

La actualización de Java 8 incluida en Sentinel podría afectar a los siguientes módulos auxiliares:

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

Si tiene problemas con estos módulos auxiliares (plug-ins), priorizaremos y solucionaremos los problemas de acuerdo con las directivas estándar de gestión de defectos. Para obtener más información sobre las directivas de servicio técnico, consulte el sitio Web sobre directivas de servicio técnico.

No se puede ver el gráfico de previsión de la capacidad de almacenamiento

Problema: En **Sentinel Main** (Interfaz principal de Sentinel) > **Almacenamiento** > **Actividad**, el gráfico **Previsión de la capacidad de almacenamiento** no está disponible. Esto se debe a que Zulu OpenJDK no incluye las fuentes necesarias.

Solución: Utilice los comandos siguientes para instalar las fuentes:

- yum install fontconfig
- yum install dejavu

Error al lanzar la consola de Kibana después de actualizar Sentinel

Problema: Al lanzar una consola de Kibana, se muestra el siguiente mensaje: `No default index pattern. Debe seleccionar o crear uno para continuar. (No hay ningún patrón de índice por defecto. Debe seleccionar o crear uno para continuar).`

Solución: Para definir un patrón de índice de Kibana como patrón de índice por defecto:

1. Seleccione uno de los siguientes elementos:
   - alerts.alerts
   - security.events.normalized_*
2. Haga clic en **Definir como opción por defecto**.

No se pueden copiar los enlaces de alerta de todas las alertas de una vista de alertas en Mozilla Firefox y Microsoft Edge

Problema: La opción **Seleccionar todo *<número de alertas>* Alertas** > **Copiar enlace de alerta** no funciona en Firefox ni Microsoft Edge.

Solución: Realice los siguientes pasos:

1. Seleccione manualmente todas las alertas en cada página de la vista de alertas mediante la casilla de verificación que permite seleccionar todas las alertas.
2. Haga clic en **Copiar enlace de alerta**.
3. Péguelo en la aplicación que desee.

Al instalar Sentinel, Collector Manager y Correlation Engine como imagen de dispositivo OVF no se visualiza la pantalla de inicio de sesión

Problema: El instalador se detiene en la pantalla de instalación en curso y no muestra la pantalla de entrada a la sesión, aunque la instalación se haya completado.

Solución: Reinicie la máquina virtual e inicie Sentinel, Collector Manager o Correlation Engine.

El dispositivo Sentinel 8.2 en Microsoft Hyper-V Server 2016 no se inicia al reiniciar

Problema: En Hyper-V Server 2016, el dispositivo Sentinel no se inicia durante el reinicio y muestra el siguiente mensaje:

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

Este problema se produce porque el sistema operativo modifica el UUID del disco durante la instalación. Por lo tanto, no se puede encontrar el disco durante el reinicio.

Solución: Modifique manualmente el UUID del disco. Para obtener más información, consulte el artículo 7023143 de Knowledge Base.

Error al actualizar al dispositivo Sentinel 8.2 de alta disponibilidad

Problema: Al actualizar al dispositivo Sentinel 8.2 de alta disponibilidad, Sentinel muestra el siguiente mensaje de error:

```
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):
```

Solución: Antes de responder al mensaje anterior, realice lo siguiente:

1. Inicie otra sesión mediante PuTTY o un software similar en el host en el que está ejecutando la actualización.
2. Añada la siguiente entrada al archivo `/etc/csync2/csync2.cfg`:

   ```
   /etc/opt/novell/sentinel/config/configuration.properties
   ```
3. Elimine la carpeta `sentinel` de `/var/opt/novell`:

   ```
   rm -rf /var/opt/novell/sentinel
   ```
4. Regrese a la sesión con la que había iniciado la actualización e introduzca `r` para continuar con el proceso.

La instalación de las aplicaciones Collector Manager y Correlation Engine genera errores en idiomas diferentes del inglés en el modo MFA

Problema: La instalación de la aplicación Collector Manager y Correlation Engine genera errores en el modo MFA si el sistema operativo está en un idioma que no sea inglés.

Solución: Instale las aplicaciones Collector Manager y Correlation Engine en inglés. Una vez finalizada la instalación, cambie el idioma según corresponda.

Problemas de facilidad de uso en las pantallas de instalación del dispositivo

Problema: Los botones **Siguiente** y **Atrás** de las pantallas de instalación del dispositivo no aparecen o están inhabilitados en algunos casos, como los siguientes:

- Al hacer clic en **Atrás** en la pantalla Comprobación previa de Sentinel para editar o revisar la información de la pantalla de configuración de red del dispositivo de servidor de Sentinel, no aparece el botón **Siguiente** para continuar con la instalación. El botón **Configurar** solo permite editar la información especificada.
- Si ha especificado ajustes de red incorrectos, en la pantalla Comprobación previa de Sentinel, se indica que no puede continuar con la instalación debido a la información de red incorrecta. No aparece el botón **Atrás** para ir a la pantalla anterior a fin de modificar los ajustes de red.

Solución: Reinicie la instalación del dispositivo.

Collector Manager se queda sin memoria si la sincronización horaria está habilitada en open-vm-tools

Problema: Si instala y habilita de forma manual la sincronización horaria en open-vm-tools, estas herramientas sincronizan periódicamente la hora entre el dispositivo Sentinel (invitado) y el servidor VMware ESX (host). Estas sincronizaciones horarias pueden provocar que el reloj del invitado se adelante o atrase en relación con la hora del servidor ESX. Hasta que se sincronice la hora entre el dispositivo Sentinel (invitado) y el servidor ESX (host), Sentinel no procesará eventos. Como resultado, un gran número de eventos se incluirán en la cola de Collector Manager, que con el tiempo puede soltarlos una vez que se alcance el umbral. Para evitar este problema, Sentinel inhabilita la sincronización horaria por defecto en la versión de open-vm-tools disponible en Sentinel.

Solución: Inhabilite la sincronización horaria. Para obtener más información sobre cómo inhabilitar la sincronización horaria, consulte la sección Inhabilitación de la sincronización horaria.

Agent Manager requiere la autenticación de SQL cuando está habilitado el modo FIPS 140-2

Problema: Si tiene el modo FIPS 140-2 habilitado en Sentinel, la autenticación de Windows para Agent Manager impide la sincronización con la base de datos de Agent Manager.

Solución: Utilice la autenticación de SQL para Agent Manager.

La instalación de alta disponibilidad de Sentinel en un modo que no sea FIPS 140-2 muestra un error

Problema: La instalación de alta disponibilidad de Sentinel en un modo diferente de FIPS 140-2 se realiza correctamente, pero muestra el error siguiente dos veces:

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

Solución: Se trata de un error previsto y puede ignorarlo de forma segura. A pesar de que el instalador muestra un error, la configuración de alta disponibilidad de Sentinel funciona correctamente en el modo diferente de FIPS 140-2.

El comando Keytool muestra una advertencia

Problema: Cuando se utiliza el comando Keytool, se muestra la siguiente advertencia:

```
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".
```

Solución: Se trata de una advertencia prevista, por lo que puede ignorarla de forma segura. A pesar de la advertencia, el comando Keytool funciona según lo esperado.

Sentinel no procesa las fuentes de inteligencia de amenazas en el modo FIPS

Problema: En el modo FIPS, al procesar fuentes de inteligencia de amenazas listas para usar desde las direcciones URL, Sentinel muestra el siguiente error: `Received fatal alert: protocol_version`. Este problema se produce porque las fuentes de amenazas listas para usar ahora solo son compatibles con TLS 1.2, que no funciona en el modo FIPS.

Solución: Haga lo siguiente:

1. Haga clic en **Sentinel Main** (Interfaz principal de Sentinel) > **Integración** > **Orígenes de inteligencia de amenazas**.
2. Edite cada dirección URL para cambiar el protocolo de `http` a `https`.

Al cerrar la sesión principal de Sentinel no se cierra la sesión de las consolas y viceversa cuando está activo el modo de autenticación de varios factores

Problema: En el modo de autenticación multifactor, si sale de **Sentinel Main** (Interfaz principal de Sentinel), no saldrá de la sesión de las consolas de Sentinel y viceversa. Esto se debe a un problema en Advanced Authentication Framework.

Solución: Hasta que haya una solución disponible en Advanced Authentication Framework, actualice la pantalla para ver la pantalla de entrada.

La consola personalizada de Kibana no se muestra después de actualizar a Sentinel 8.3.1

Problema: La consola personalizada de Kibana no se muestra al actualizar de Sentinel 8.3 o versiones anteriores a Sentinel 8.3.1.

Solución: Asegúrese de volver a crear la consola personalizada después de actualizar Sentinel.

Cuando se lanza Kibana, se muestra un mensaje de error de conflicto

Problema: Después de instalar o actualizar Sentinel y lanzar Kibana por primera vez, se muestra el mensaje de error de conflicto.

Solución: Ignore el mensaje de error de conflicto, ya que no afecta a la funcionalidad.

Al reiniciar Redhat 8.1 y 8.2, Sentinel no se inicia automáticamente

Problema: Después de instalar Sentinel en Redhat 8.1 y 8.2, Sentinel (el servidor, RCM o RCE) no se inicia automáticamente tras el reinicio.

Solución: Cambie el valor de SELINUX a **SELINUX=disabled** en el archivo `/etc/selinux/config`.

Al abrir la consola de gestión de dispositivos de Sentinel, se muestra un mensaje de error

Problema: Después de actualizar a Sentinel 8.3, al intentar abrir la consola de gestión de dispositivos de Sentinel de los servidores de Correlation Engine (CE) o Collector Manager (CM) de alta disponibilidad (HA), se muestra el mensaje de error `Error 404 - Not found` (Error 404: no encontrado).

Solución: Para obtener más información, consulte el documento de la Knowledge Base de Micro Focus.

Los usuarios con permisos de visualización para ocultar la gestión todavía pueden ver la pestaña Gestión en la página de Kibana

Problema: Después de actualizar a Sentinel 8.4, los usuarios con el permiso de visualización para ocultar la gestión aún pueden ver la pestaña Gestión en la página de Kibana, pero no pueden acceder a sus funciones.

Cuando el administrador cambia la función de usuario de las alertas, los cambios no se actualizan al instante en la página de Kibana

Problema: Los usuarios existentes no pueden ver al instante ninguna alerta en la página de Kibana, aunque el administrador haya actualizado los permisos de visualización de alertas.

Solución: Cuando se actualice el permiso de usuario, deberá salir de la sesión y volver a entrar.

Cuando se lanza la consola de visualización como usuario arrendatario, se muestra un mensaje de error

Problema: Cuando un usuario diferente del arrendatario por defecto lanza la consola de visualización, se muestra el mensaje de error **Prohibido**. Este mensaje de error se muestra siempre que el usuario diferente del arrendatario por defecto que tiene permiso **solo de visualización** para la opción **Gestión** lanza la consola y no hay ningún usuario con permiso de **edición** para la opción **Gestión** en ese arrendatario.

Solución: Ignore el mensaje de error, ya que no afecta a la funcionalidad.

En RHEL, RCM y RCE, no se conectan con el servidor cuando CRL está habilitado

Problema: Las instancias remotas de Collector Manager (RCM) y Correlation Engine (RCE) no pueden conectarse con el servidor cuando CRL está habilitado en RHEL.

Solución: Actualice la **versión de cURL** en la máquina a la versión 7.60 o superior.

RCM no reenvía los eventos al servidor Sentinel cuando la visualización de eventos, FIPS y CRL están habilitados

Problema: En la nueva instalación de la configuración distribuida, después de habilitar los servicios de visualización de eventos, FIPS y CRL, la instancia remota de Collector Manager (RCM) no reenvía los eventos al servidor Sentinel.

Solución: Si la visualización de eventos y FIPS o CRL se han habilitado, RCM reenvía los eventos al servidor Sentinel.

Los informes de incidencias presentan excepciones después de actualizar el SO desde cualquier versión anterior a la más reciente

Problema: Al actualizar el sistema operativo desde una versión anterior a la más reciente, el informe de incidencias presenta excepciones.

Se registra una excepción al intentar reindexar por primera vez

Problema: Se registra una excepción cuando la operación de reindexación se ejecuta por primera vez.

Error al ejecutar `convert_to_fips.sh` en la compilación de dispositivo RCM/RCE de Sentinel 8.5

Problema: Cuando el administrador del sistema ejecuta `convert_to_fips.sh` en la compilación de dispositivo de RCM/RCE de Sentinel 8.5, después de proporcionar las credenciales correctas de los usuarios en un bucle continuo, aparece el siguiente mensaje de error:

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

Solución: Realice los siguientes pasos:

1. Salga de la ejecución del guión.

2. Vaya a `<instalación de RCM/RCE de Sentinel>/etc/opt/novell/sentinel/config/configuration.properties`.
3. Defina el valor de `rest.endpoint.port` en el puerto correspondiente del servidor Web.

   Por ejemplo, `rest.endpoint.port=8443`.
4. Vuelva a ejecutar `convert_to_fips.sh`.

Contactar con Micro Focus

Para obtener información sobre problemas de productos específicos, póngase en contacto con el servicio de asistencia técnica en https://www.microfocus.com/support-and-services/.

Puede obtener información o asesoramiento técnicos de diversas fuentes:

- Documentación del producto, artículos de Knowledge Base y vídeos: https://www.microfocus.com/support-and-services/
- Las páginas de la Comunidad de Micro Focus: https://www.microfocus.com/communities/

Información legal