Sentinel™

Guía de instalación y configuración

Julio de 2018

Información legal

Acerca de este libro y la biblioteca

La *Guía de instalación y configuración* ofrece una introducción a Sentinel y explica cómo instalar y configurar Sentinel.

A quién va dirigida

Esta guía está dirigida a administradores y consultores de Sentinel.

Otra información de la biblioteca

La biblioteca ofrece los siguientes recursos informativos:

Guía de administración

Proporciona información sobre administración y las tareas necesarias para gestionar una implantación de Sentinel.

Guía del usuario

Proporciona información conceptual sobre Sentinel. En este libro se ofrece también una descripción general de las interfaces del usuario y una guía paso a paso para realizar muchas tareas.

Conocer Sentinel

En esta sección se proporciona información detallada sobre Sentinel y cómo Sentinel ofrece a su organización una solución de gestión de eventos.

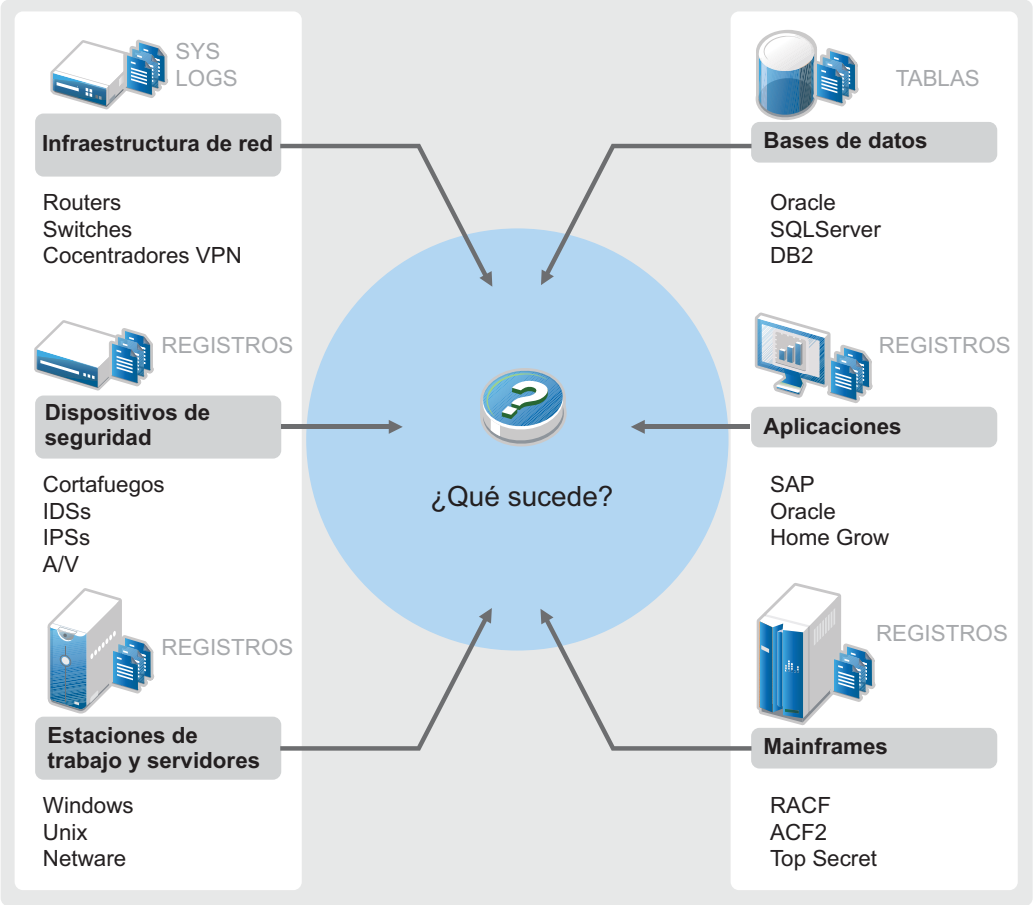
1 ¿Qué es Sentinel?

Sentinel es una solución de gestión de la información y los eventos de seguridad (SIEM), así como de supervisión de la conformidad. Sentinel supervisa automáticamente los entornos de TI más complejos y ofrece la seguridad requerida para protegerlos.

Retos de proteger un entorno de TI

La protección del entorno de TI es un desafío debido a su complejidad. Por lo general, los entornos de TI contienen muchas aplicaciones, bases de datos, mainframes, estaciones de trabajo y servidores, y todas estas entidades generan registros de eventos. Es posible que también tenga dispositivos de seguridad y dispositivos de infraestructura de red que generen registros de eventos en su entorno de TI.

Figura 1-1 *Qué ocurre en su entorno.*



Los desafíos surgen por los siguientes hechos:

- Existen muchos dispositivos en su entorno de TI.
- Los registros tienen diferentes formatos.
- Los registros se almacenan en distintas ubicaciones.
- En los archivos de registro se captura una gran cantidad de información.
- Resulta imposible determinar los activadores de eventos sin antes analizar manualmente los archivos de registro.

Para que la información de los registros sea útil, debe poder realizar las siguientes acciones:

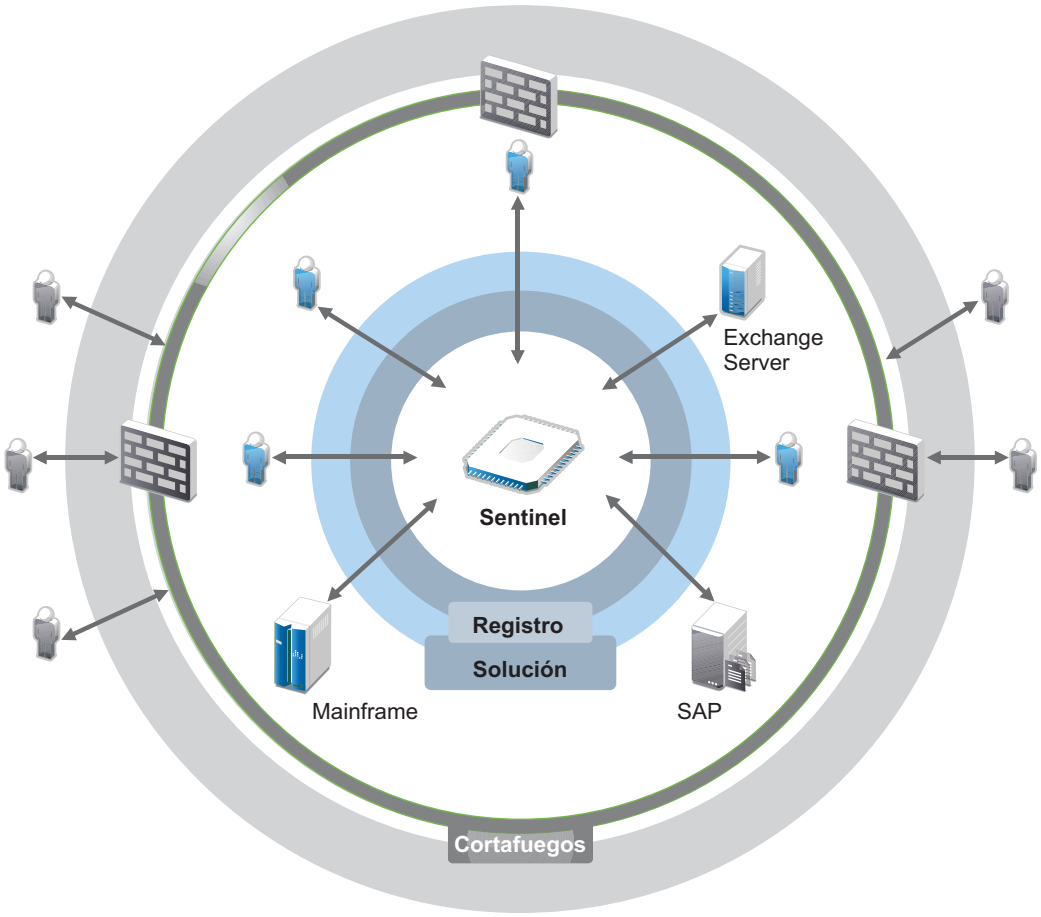
- Recopilar los datos.
- Consolidar los datos.
- Normalizar datos dispares en eventos que se puedan comparar fácilmente.
- Asignar eventos a regulaciones estándar.
- Analizar los datos.
- Comparar los eventos en múltiples sistemas para determinar si existen problemas de seguridad.
- Enviar notificaciones cuando los datos no cumplen las normas.
- Tomar medidas en las notificaciones para cumplir las directivas de empresa.
- Generar informes para demostrar el cumplimiento.

Una vez que comprenda los desafíos que conlleva proteger su entorno de TI, debe decidir cómo quiere proteger la empresa para los usuarios y frente a ellos de modo que la experiencia del usuario no se vea afectada. Sentinel ofrece la solución.

La solución que ofrece Sentinel

Sentinel actúa como el sistema nervioso central para la seguridad de la empresa. Recoge datos de toda la infraestructura: aplicaciones, bases de datos, servidores, almacenamiento y dispositivos de seguridad. Analiza y establece correlaciones entre datos, y los convierte en datos procesables, ya sea de forma manual o automática.

Figura 1-2 *La solución que ofrece Sentinel*



Con Sentinel, sabe lo que sucede en su entorno de TI en un punto dado y tiene la capacidad de conectar las acciones realizadas en los recursos con las personas que realizan dichas acciones. Esto le permite determinar el comportamiento de los usuarios y supervisar las actividades con eficacia a fin de prevenir las actividades maliciosas.

Sentinel lo consigue de la siguiente manera:

- Ofreciendo una solución única para tratar los controles de TI en múltiples estándares de seguridad.
- Abordando la distancia entre lo que debería ocurrir y lo que está ocurriendo realmente en su entorno de TI.
- Ayudándole a cumplir los estándares de seguridad.
- Ofreciendo programas de información y supervisión del cumplimiento listos para usar.

Sentinel automatiza los procesos de recopilación, análisis y generación de informes de registros con el fin de asegurar que los controles de TI sean eficaces para detectar amenazas y cumplir requisitos de auditoría. Sentinel ofrece supervisión automatizada de los eventos de seguridad, eventos de cumplimiento y controles TI. Le permite actuar de inmediato si se vulnera la seguridad o tiene lugar un evento fuera de conformidad. Sentinel también le permite recopilar información de resumen sobre su entorno, que después puede compartir con los principales participantes.

2 Cómo funciona Sentinel

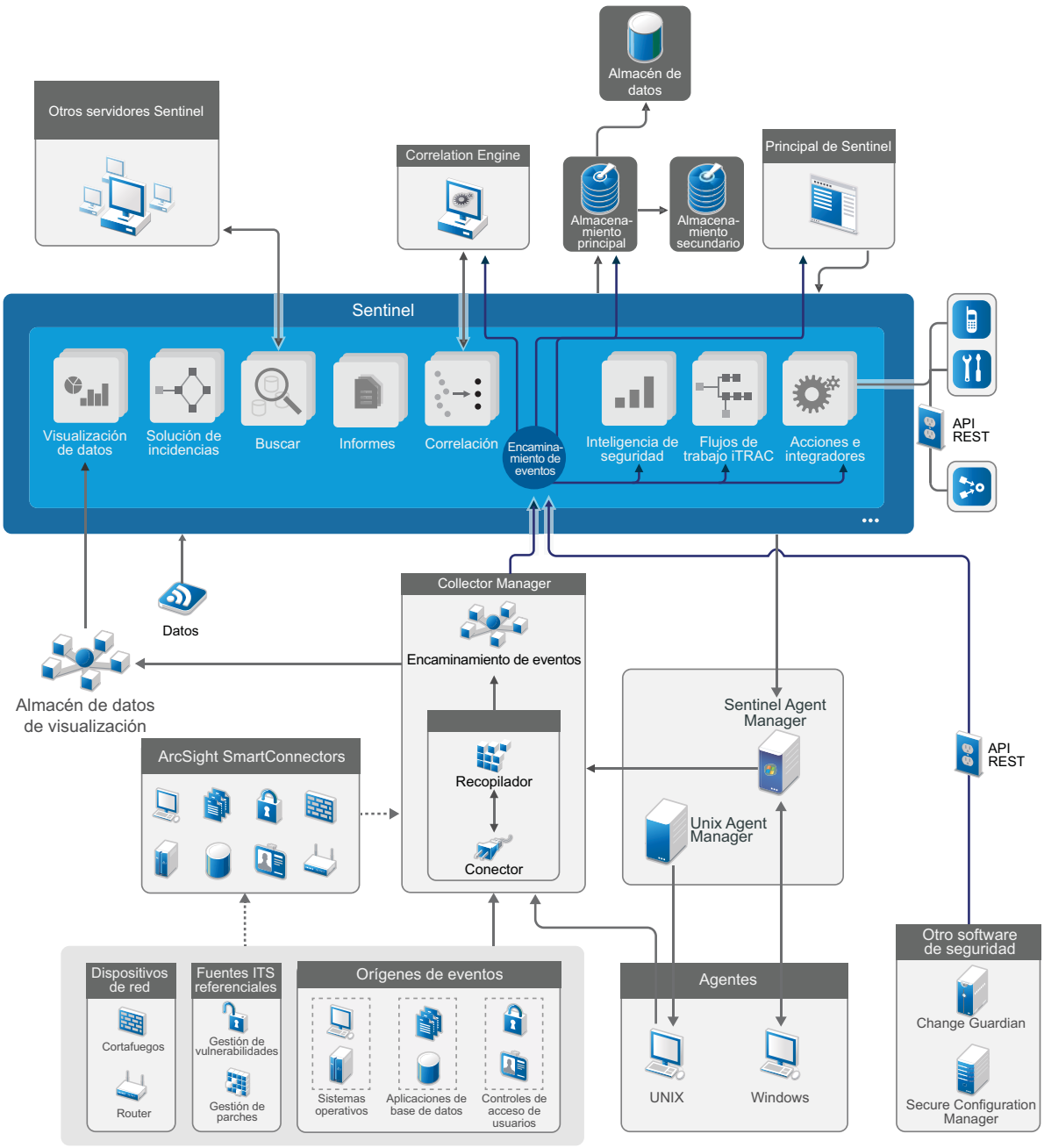
Sentinel gestiona de forma continua la información de seguridad y los eventos en todo el entorno de TI para ofrecer una solución de supervisión completa.

Sentinel hace lo siguiente:

- Reúne registros, eventos e información de seguridad de los diferentes orígenes de su entorno de TI.
- Normaliza los registros, eventos y datos de seguridad recopilados en un formato estándar de Sentinel.
- Almacena eventos en un almacenamiento de datos basado en archivos o un almacenamiento ampliable basado en Hadoop con directivas de retención de datos personalizables y flexibles.
- Recopila datos de flujo IP y ayuda a supervisar de cerca las actividades de la red.
- Proporciona la posibilidad de vincular de forma jerárquica varios sistemas Sentinel, incluido Sentinel Log Manager.
- Le permite buscar eventos en su servidor Sentinel local y en otros servidores Sentinel distribuidos por el mundo.
- Realiza un análisis estático que le permite definir una línea de base y luego lo compara con lo que está ocurriendo para determinar si hay problemas no detectados.
- Correlaciona un conjunto de eventos similares o comparables durante un período específico para determinar un patrón.
- Organiza eventos de incidentes para una gestión de la respuesta y seguimiento eficiente.
- Ofrece informes basados en eventos en tiempo real e históricos.

La siguiente ilustración muestra cómo funciona Sentinel utilizando el almacenamiento tradicional como opción de almacenamiento de datos:

Figura 2-1 *Arquitectura de Sentinel*



En las siguientes secciones se describen detalladamente los componentes de Sentinel:

- “Orígenes de eventos” en la página 21
- “Evento de Sentinel” en la página 21
- “Collector Manager” en la página 23

Orígenes de eventos

Sentinel reúne información de seguridad y eventos de diferentes orígenes de su entorno de TI. Estos orígenes se llaman orígenes de eventos. A continuación se indican los orígenes de eventos habituales en su red:

Perímetro de seguridad: Los dispositivos de seguridad —incluido el hardware y el software— utilizados para crear un perímetro de seguridad para su entorno, como cortafuegos, sistemas de detección de intrusos (IDS) y redes privadas virtuales (VPN).

Sistemas operativos: Los diferentes sistemas operativos que se ejecutan en la red.

Orígenes de TI referenciales: El software utilizado para mantener y seguir activos, revisiones, configuración y vulnerabilidad.

Aplicaciones: Las diferentes aplicaciones instaladas en la red.

Control de acceso de usuarios: Las aplicaciones o dispositivos que permiten a los usuarios acceder a los recursos de la compañía.

Para obtener más información sobre la recopilación de orígenes de eventos, consulte la sección “Collecting and Routing Event Data” (Recopilación y encaminamiento de datos de eventos) de la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Evento de Sentinel

Sentinel recibe información de los dispositivos, normaliza esta información en una estructura denominada evento, clasifica el evento y lo envía para ser procesado.

Un evento constituye una entrada de registro normalizada notificada a Sentinel desde una red o un dispositivo de aplicación, un dispositivo de seguridad de terceros o una fuente interna de Sentinel. Existen varios tipos de eventos:

- Eventos externos (eventos recibidos desde un dispositivo de seguridad), como:
  - Un ataque detectado por un sistema de detección de intrusiones (IDS)

- Un inicio de sesión correcto notificado por un sistema operativo
- Una situación definida por el cliente como el acceso de un usuario a un archivo

- Eventos internos (eventos generados por Sentinel), que incluyen:
  - Desactivación de una regla de correlación
  - Llenado de la base de datos

Sentinel añade información de categoría (taxonomía) a los eventos, de modo que resulte más fácil comparar eventos entre sistemas que informar de los eventos por separado. Los eventos se procesan mediante visualización en tiempo real, Correlation Engine, consolas y el servidor backend.

Un evento consta de más de 200 campos; los campos de evento son de diferentes tipos y tienen distintas funciones. Existen algunos campos predefinidos, como gravedad, importancia, dirección IP de destino y puerto de destino.

Existen dos conjuntos de campos configurables:

- Campos reservados: para uso interno de Sentinel, permiten ampliar la funcionalidad en el futuro.
- Campos del cliente: disponibles para que el cliente personalice sus opciones.

El origen de un campo puede ser externo o de referencia:

- El valor de un campo externo viene definido de forma explícita por el dispositivo o el recopilador correspondiente. Por ejemplo, puede definirse un campo para que sea el código de generación para la construcción que contiene el activo mencionado como la dirección IP de destino de un evento.
- El valor de un campo referencial se calcula como una función de uno o más campos utilizando el servicio de asignación. Por ejemplo, el servicio de asignación puede calcular un campo utilizando una asignación definida por el cliente mediante una dirección IP de destino desde el evento.

- “Servicio de asignación” en la página 22
- “Asignaciones de emisión continua” en la página 23
- “Detección de explotaciones” en la página 23

Servicio de asignación

El servicio de asignación propaga los datos de relevancia empresarial por todo el sistema. Estos datos pueden enriquecer los eventos con información de referencia.

Puede enriquecer los datos de eventos utilizando asignaciones para añadir información adicional, como datos del host y de identidad, a los eventos entrantes de los dispositivos de origen. Sentinel puede utilizar esta información adicional para las funciones avanzadas de generación de informes y correlación. Sentinel admite varias asignaciones integradas, así como asignaciones personalizadas definidas por el usuario.

Las asignaciones definidas en Sentinel se almacenan de dos formas diferentes:

- Las asignaciones incorporadas se almacenan en la base de datos, se actualizan de forma interna y se exportan automáticamente al servicio de asignación.
- Las asignaciones personalizadas se almacenan como archivos CSV y se pueden actualizar en el sistema de archivos o a través de la interfaz de usuario de Configuración de los datos de la asignación. Después el servicio de asignación se ocupa de cargarlos.

En ambos casos, los archivos CSV se guardan en el servidor Sentinel central, pero los cambios en las asignaciones se distribuyen a cada Collector Manager y se aplican a nivel local. Este procesamiento distribuido garantiza que la actividad de asignación no sobrecargue el servidor principal.

Asignaciones de emisión continua

El servicio de asignación emplea un modelo de actualización dinámico y reproduce las asignaciones de un punto a otro, evitando la acumulación de grandes asignaciones estáticas en la memoria dinámica. Esto es importante en un sistema de misión crítica en tiempo real como Sentinel, que requiere un traslado de datos constante, predictivo y ágil, independiente de cualquier carga transitoria en el sistema.

Detección de explotaciones

Sentinel ofrece la capacidad de contrastar las firmas de datos de eventos con los datos del escáner de vulnerabilidad. Sentinel notifica a los usuarios automáticamente y de forma inmediata cuando se intenta aprovechar un sistema vulnerable. Esto es posible gracias a las funciones siguientes:

- Datos del asesor
- Detección de intrusiones
- Exploración de vulnerabilidades
- Cortafuegos

Los datos del asesor contienen información sobre vulnerabilidades y amenazas, así como una normalización de las firmas de eventos y los módulos auxiliares (plug-in) de vulnerabilidad. Esto proporciona una referencia cruzada entre firmas de datos de eventos y datos del escáner de vulnerabilidad. Para obtener más información sobre los datos del asesor, visite “Detecting Vulnerabilities and Exploits”(Detección de vulnerabilidades y exploits) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Collector Manager

Collector Manager gestiona la recopilación de datos, supervisa los mensajes de estado del sistema y realiza un filtrado de eventos. Entre las principales funciones de Collector Manager destacan las siguientes:

- Recopilación de datos mediante conectores.
- Análisis y normalización de datos mediante recopiladores.

Recopiladores

Los recopiladores recogen información de los conectores y la normalizan. Realizan las funciones siguientes:

- Recibir datos en bruto de los conectores.
- Analizar y normalizar los datos:
  - Traducir los datos específicos del origen de eventos a los datos específicos de Sentinel.

    - Enriquecer los eventos cambiando el formato de la información que contienen por uno que Sentinel pueda leer.
    - Filtrar los eventos específicos del origen de eventos.
- Añadir relevancia empresarial a los eventos a través del servicio de asignación:
    - Asignar eventos a identidades.
    - Asignar eventos a activos.
- Encaminar eventos.
- Pasar los datos normalizados, analizados y formateados a Collector Manager.
- Enviar mensajes de estado al servidor de Sentinel.

Para obtener más información acerca de los recopiladores, consulte el sitio Web de módulos auxiliares (plug-ins) de Sentinel.

Conectores

Los conectores ofrecen conexiones desde los orígenes de eventos al sistema Sentinel.

Los conectores presentan las siguientes funciones:

- Transporte de datos de eventos en bruto desde los orígenes de eventos al recopilador.
- Filtrado específico de la conexión.
- Gestión de errores de conexión.

ArcSight SmartConnectors

Sentinel utiliza ArcSight SmartConnector para recopilar eventos de diversos tipos de orígenes de eventos no admitidos directamente por Sentinel. Los SmartConnectors recopilan eventos de los dispositivos compatibles, normalizan los eventos en el formato de eventos comunes (CEF) y los reenvían a Sentinel a través del conector de Syslog. A continuación, el conector reenvía los eventos a Universal Common Event Format Collector para su análisis.

Para obtener más información sobre la configuración de Sentinel con SmartConnectors, consulte la documentación de Universal Common Event Format Collector en el sitio Web de módulos auxiliares (plug-ins) de Sentinel.

Agent Manager

Agent Manager ofrece recopilación de datos basada en host que complementa la recopilación de datos sin agentes, de modo que le permite realizar las tareas siguientes:

- Acceder a registros que no están disponibles a través de la red.
- Operar en entornos de red con un estricto control.
- Mejorar la posición de seguridad al limitar la zona de ataque en servidores cruciales.
- Proporcionar una mayor fiabilidad en la recopilación de datos durante las interrupciones en la red..

Agent Manager le permite implementar agentes y gestionar su configuración, y además actúa como punto de recopilación de los eventos que fluyen hacia Sentinel. Para obtener más información sobre Agent Manager, consulte la documentación de Agent Manager.

Encaminamiento y almacenamiento de datos de Sentinel

Sentinel proporciona numerosas opciones de encaminamiento, almacenamiento y extracción de los datos recopilados. Por defecto, Sentinel recibe los datos de eventos analizados y los datos en bruto que envían las instancias de Collector Manager. Sentinel almacena los datos en bruto para ofrecer una cadena de evidencia segura y encamina los datos de eventos analizados de conformidad con las reglas que defina. Puede filtrar los datos de eventos analizados, enviarlos para su almacenamiento o análisis en tiempo real, y encaminarlos a sistemas externos. Sentinel hace coincidir todos los datos de eventos enviados al almacenamiento con las directivas de retención definidas por el usuario. Las directivas de retención controlan cuándo deben suprimirse los datos de eventos del sistema.

En función de la tasa de eventos por segundo (EPS) y los requisitos de implantación, se puede optar por utilizar el almacenamiento de datos tradicional basado en archivos o el almacenamiento ampliable basado en Hadoop como la opción de almacenamiento de datos. Para obtener más información, consulte “Consideraciones de almacenamiento de datos” en la página 39.

Visualizaciones de eventos

Sentinel proporciona visualizaciones de eventos que presentan datos en gráficos, tablas y mapas. Estas visualizaciones facilitan la visualización y el análisis de grandes volúmenes de eventos, incluidos los eventos de flujo IP. También puede crear sus propias visualizaciones y consolas.

Las visualizaciones de eventos están disponibles por defecto en Sentinel con almacenamiento ampliable. En una configuración de almacenamiento tradicional, las visualizaciones de eventos solo están disponibles si se ha habilitado el almacén de datos de visualización (Elasticsearch) para almacenar e indexar datos. Para obtener más información acerca de cómo habilitar Elasticsearch, consulte “Configuración del almacén de datos de visualización” en la página 43.

Correlación

Un solo evento puede parecer trivial, pero combinado con otros eventos puede indicar un problema potencial. Sentinel le ayuda a correlacionar dichos eventos utilizando las reglas que creó y desplegó en Correlation Engine, y a tomar las medidas oportunas para mitigar problemas.

La correlación añade inteligencia a la gestión de eventos de seguridad mediante la automatización del análisis de los flujos de eventos entrantes para buscar patrones de interés. Además, la correlación permite definir reglas que identifican las amenazas importantes y los patrones complejos de ataque con el fin de asignar una prioridad a los eventos e iniciar tareas eficientes de gestión y respuesta para las incidencias. Para obtener más información acerca de la correlación, consulte la sección “Correlating Event Data” (Correlación de datos de eventos) de la *Sentinel User Guide* (Guía del usuario de NetIQ Sentinel).

Para supervisar eventos de acuerdo con las reglas de correlación, debe implementar las reglas en Correlation Engine. Cuando se produce un evento que cumple los criterios de una regla, Correlation Engine genera un evento de correlación que describe el patrón. Para obtener más información, consulte “Correlation Engine” (Correlation Engine) en la *Sentinel User Guide* (Guía del usuario de NetIQ Sentinel).

Inteligencia de seguridad

La capacidad de correlación de Sentinel le permite buscar patrones de actividad conocidos, que puede analizar por cuestiones de seguridad, conformidad o cualquier otro motivo. La función de Inteligencia de seguridad busca actividad fuera de lo normal, que puede ser de tipo malicioso, pero que no coincide con ningún patrón conocido.

La característica de Inteligencia de seguridad en Sentinel se centra en el análisis estadístico de los datos de series temporales para permitir a los analistas identificar y analizar las anomalías mediante un motor estadístico automatizado o mediante la representación visual de los datos estadísticos para la interpretación manual. Para más información, consulte "Analyzing Trends in Data" (Cómo analizar tendencias en datos) en la *Sentinel User Guide (Guía del usuario de NetIQ Sentinel)*.

Solución de incidencias

Sentinel proporciona un sistema de gestión automatizada de respuestas a incidencias que le permite documentar y formalizar el proceso de seguimiento, derivación y respuesta a incidencias e infracciones de directivas. Además ofrece integración bidireccional con los sistemas de tickets de problemas. Sentinel le permite reaccionar rápidamente y solucionar incidencias de forma eficaz. Para más información, consulte "Configuring incidents" (Cómo configurar incidencias) en la *Sentinel User Guide (Guía del usuario de NetIQ Sentinel)*.

Flujos de trabajo de iTRAC

Los flujos de trabajo de iTRAC ofrecen una solución sencilla y flexible para automatizar y seguir los procesos de respuesta a incidencias de una empresa. iTRAC aprovecha el sistema de incidencias interno de Sentinel para hacer un seguimiento de los problemas de seguridad o del sistemas desde la identificación (mediante reglas de correlación o identificación manual) hasta la resolución.

Puede crea flujos de trabajo mediante pasos manuales o automatizados. Los flujos de trabajo de iTRAC admiten funciones avanzadas como la ramificación, la derivación basada en tiempo y las variables locales. La integración con guiones externos y módulos auxiliares (plug-ins) permite una interacción flexible con sistemas de terceros. La generación de informes completa permite a los administradores entender y afinar los procesos de respuesta a incidentes. Para más información, consulte "Configuring iTRAC Workflows" (Cómo configurar los flujos de trabajo iTRAC) en la *Sentinel User Guide (Guía del usuario de NetIQ Sentinel)*.

Acciones e integradores

Las acciones ejecutan algún tipo de acción de forma manual o automática, como enviar mensajes de correo electrónico. Puede activar las acciones por medio de reglas de encaminamiento, la ejecución manual de una operación de evento o incidencia y reglas de correlación. Sentinel proporciona una lista de acciones previamente configuradas. Puede usar las acciones por defecto y reconfigurarlas según sea necesario, o ben puede añadir nuevas acciones. Para obtener más información, consulte "Configuring Actions" (Configuración de acciones) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Una acción puede ejecutarse por sí misma o puede utilizar una instancia de integrador configurada desde un módulo auxiliar (plug-in) de integrador. Los módulos auxiliares (plug-in) amplían las características y la funcionalidad de las acciones de solución de Sentinel. Los integradores proporcionan la capacidad de conectarse a un sistema externo, como un servidor LDAP, SMTP o

SOAP para ejecutar una acción. Para más información, consulte “Configuring Integrators” (Configuración de integradores) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Búsqueda

Sentinel ofrece una opción para realizar búsquedas en los eventos. Con la configuración necesaria, también puede buscar eventos del sistema generados por Sentinel y ver los datos en bruto de cada evento. Para obtener más información, consulte “Searching Events” (Cómo buscar eventos) en la *Sentinel User Guide* (Guía del usuario de NetIQ Sentinel).

Además, puede buscar servidores Sentinel distribuidos en diversas ubicaciones geográficas. Para más información, consulte “Configuring Data Federation” (Cómo configurar la federación de datos) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Informes

Sentinel le permite ejecutar informes sobre los datos recopilados. Sentinel se suministra con una variedad de informes personalizables. Algunos informes son configurables, de modo que puede especificar las columnas que se mostrarán en los resultados.

Puede ejecutar, programar y enviar por correo electrónico informes en formato PDF. También puede ejecutar informes como búsquedas y después trabajar con los resultados para, por ejemplo, perfeccionar la búsqueda o realizar una acción basada en los resultados. También puede ejecutar informes en los servidores Sentinel que se distribuyen en diferentes localizaciones geográficas. Para más información, consulte “Reporting” (Informe) en la *Sentinel User Guide (Guía de usuario de NetIQ Sentinel)*.

Seguimiento de identidad

Sentinel proporciona un marco de integración para que los sistemas de gestión de identidades puedan realizar un seguimiento de las identidades de cada cuenta de usuario y de los eventos que realiza cada una de esas identidades. Sentinel proporciona información del usuario, como información de contacto, cuentas de usuario, eventos de autenticación recientes, eventos de acceso recientes, cambios en los permisos, etc. Al mostrar información acerca de los usuarios que inician una acción específica o los usuarios que se ven afectados por una acción, Sentinel mejora el tiempo de respuesta a incidencias y permite el análisis basado en el comportamiento. Para obtener más información, consulte “Leveraging Identity Information”(Cómo aprovechar la información de identidad) en la *Sentinel User Guide (Guía del usuario de NetIQ Sentinel)*.

Análisis de eventos

Sentinel proporciona un potente conjunto de herramientas que le ayudan a buscar y analizar con facilidad datos de eventos fundamentales. Sentinel optimiza el sistema para conseguir la máxima eficiencia en cualquier tipo de análisis, y proporciona métodos para realizar la transición de un tipo de análisis a otro fácilmente y sin problemas.

La investigación de eventos en Sentinel a menudo comienza con las Vistas de eventos casi en tiempo real. Si bien se dispone de herramientas más avanzadas, Vistas de eventos muestra los flujos de eventos filtrados junto con diagramas de resumen que pueden servir para un análisis sencillo y rápido de las tendencias de los eventos y los datos de eventos, así como para la identificación de

eventos específicos. Con el tiempo, puede crear filtros mejorados para clases de datos específicas, como resultados de correlación. Puede usar Vistas de eventos como consola para ver una posición operativa y de seguridad general.

Luego puede usar la búsqueda interactiva para realizar un análisis detallado de los eventos. Esto le permite buscar fácil y rápidamente datos relacionados con una consulta específica, como la actividad de un usuario en particular o en un sistema específico. Al hacer clic en los datos del evento o usar el panel de mejora de la izquierda, podrá concentrarse rápidamente en eventos de interés específicos.

Al analizar cientos de eventos, las funciones de generación de eventos de Sentinel proporcionan un control personalizado de la disposición de los eventos y pueden mostrar un mayor volumen de datos. Sentinel facilita esta transición al permitirle transferir las búsquedas interactivas acumuladas en la interfaz de búsqueda a una plantilla de informe. Al hacerlo se crea inmediatamente un informe que muestra los mismos datos en un formato más adecuado para un mayor número de eventos.

Sentinel incluye muchas plantillas de informe para este fin. Existen dos tipos de plantillas de informe:

- Plantillas optimizadas para mostrar determinados tipos de información, como datos de autenticación o los usuarios creados.
- Plantillas generales que le permiten personalizar grupos y columnas del informe de manera interactiva.

Con el tiempo, desarrollará filtros de uso común e informes que facilitan el flujo de trabajo. Sentinel le permite almacenar esta información y distribuirla a personas de su organización. Para obtener más información, consulte la *Sentinel User Guide* (Guía del usuario de NetIQ Sentinel).

II Planificación de su instalación de Sentinel

En los capítulos siguientes se indica cómo planificar la instalación de Sentinel. Si desea instalar una configuración no contemplada en los capítulos siguientes o tiene alguna pregunta, póngase en contacto con el servicio de Asistencia técnica de .

3 Lista de verificación de implementación

Utilice la lista de verificación siguiente para planificar, instalar y configurar Sentinel.

Si realiza la actualización desde una versión anterior de Sentinel, no utilice esta lista. Para obtener información sobre la actualización, consulte la Parte V, “Actualización de Sentinel”, en la página 147.

❒	Tareas	Consulte
❒	Revise la información sobre la arquitectura del producto para conocer los componentes de Sentinel.	Parte I, “Conocer Sentinel”, en la página 13.
❒	Revise la información sobre licencias de Sentinel a fin de determinar si necesita usar la licencia de evaluación o la licencia empresarial de Sentinel.	Capítulo 4, “Información sobre licencias”, en la página 33.
❒	Evalúe su entorno para determinar la configuración de hardware. Asegúrese de que los equipos en los que instale Sentinel y sus componentes cumplan los requisitos especificados.	Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 37.
❒	Determine el tipo de implantación adecuado para su entorno en función de los eventos por segundo (EPS). Determine el número de instancias de Collector Manager y Correlation Engine que necesita instalar para mejorar el rendimiento y el equilibrio de carga.	Capítulo 6, “Consideraciones de implantación”, en la página 39.
❒	Revise las notas de la versión más recientes de Sentinel para entender la nueva funcionalidad y los problemas conocidos.	Notas de la versión de Sentinel
❒	Instale Sentinel.	Parte III, “Instalación de Sentinel”, en la página 71.
❒	Configure Sentinel.	Parte IV, “Configuración de Sentinel”, en la página 115.
❒	Sentinel incluye reglas de correlación listas para usar. Algunas reglas de correlación están configuradas por defecto para ejecutar una acción que envía un correo electrónico cuando se activa la regla. Es el caso, por ejemplo, de la acción Notificar al administrador de seguridad. Por tanto, debe configurar los ajustes del servidor de correo en el servidor Sentinel mediante el integrador SMTP y la acción Enviar correo electrónico.	Encontrará la documentación sobre el integrador SMTP y la acción Enviar correo electrónico en el sitio Web de módulos auxiliares (plug-ins) de Sentinel.
❒	Instale recopiladores y conectores adicionales en su entorno según sea necesario.	Capítulo 16, “Instalación de conectores y recopiladores adicionales”, en la página 111.
❒	Instale instancias adicionales de Collector Manager y Correlation Engine en su entorno según sea necesario.	Parte III, “Instalación de Sentinel”, en la página 71.

4 Información sobre licencias

Sentinel abarca un amplio espectro de funciones, por lo que cubre diferentes necesidades de muchos de sus clientes. Puede elegir un modelo de licencia acorde con sus necesidades.

La plataforma Sentinel ofrece estos dos modelos de licencia:

- **Sentinel Enterprise:** una solución con toda la gama de funciones que habilita todas las funciones principales de análisis visual en tiempo real y muchas funciones adicionales. Sentinel Enterprise se centra en los casos de uso de SIEM, como la detección de amenazas en tiempo real, las alertas y la corrección.
- **Sentinel for Log Management:** solución para casos de uso de gestión de registros, como las capacidades de recopilación, almacenamiento, búsqueda y notificación de datos.

  Sentinel for Log Management representa una actualización importante con respecto a las funciones incluidas en Sentinel Log Manager 1.2.2, y en algunos casos, se han modificado partes sustanciales de la arquitectura. Para planificar su actualización a Sentinel para la gestión de registros, consulte la página de preguntas frecuentes de Sentinel.

En función de las soluciones y los productos complementarios que compre, puede adquirir las claves de licencia y los derechos adecuados para habilitar la funcionalidad adecuada en Sentinel. A pesar de que las claves de licencia y los derechos rigen el acceso básico a las funciones y descargas del producto, debe consultar los términos y condiciones adicionales disponibles en el acuerdo de licencia y el acuerdo de licencia de usuario final.

En la tabla siguiente se esbozan los servicios y funciones específicos disponibles en cada una de las soluciones:

Tabla 4-1 *Servicios y funciones de Sentinel*

Servicios y funciones	Sentinel Enterprise	Sentinel for Log Management
Funciones principales	Sí	Sí
◆ Recopilación de eventos, análisis, normalización y clasificación taxonómica		
◆ Recopilación de datos no relacionados con eventos (datos de activos, datos de vulnerabilidades y datos de identidad de usuario)		
◆ Asignación contextual en línea		
◆ Almacenamiento de eventos con directivas de retención y sin rechazo		
◆ Encaminamiento de eventos al almacenamiento tradicional (interno y externo)		
◆ Visualización y búsquedas de eventos		
◆ Visualización, almacenamiento y recopilación de flujo IP		
◆ Generación de informes		
◆ Preparación de la publicación 140-2 de los estándares federales de procesamiento de la información (FIPS 140-2)		
◆ Acciones activadas manualmente		
◆ Creación y gestión manual de incidencias		
Sentinel Link	Sí	Sí
Sincronización de datos	Sí	Sí
Restauración de datos de eventos desde el archivo de reserva	Sí	Sí
Federación de datos (búsqueda distribuida)	Sí	Sí
Detección de exploits (asesor)*	Sí	Sí
Almacenamiento ampliable	Sí	Sí
Correlación	Sí	No
◆ Correlación de patrones de eventos en tiempo real		
◆ Acciones activadas por reglas de correlación		
◆ Clasificación de alertas		
◆ Visualización de alertas		
Inteligencia de seguridad	Sí	No
◆ Reglas de anomalía		
◆ Análisis estadístico en tiempo real		

*Asesor, con tecnología de Security Nexus, es un servicio adicional. Debe adquirir una licencia adicional para utilizar este servicio.

Licencias de Sentinel

En esta sección se proporciona información sobre los tipos de licencias de Sentinel.

Licencia de evaluación

La licencia de evaluación por defecto permite usar todas las funciones de Sentinel Enterprise durante un período de evaluación específico con un número ilimitado de EPS en función de la capacidad del hardware. Para obtener información sobre las funciones disponibles en Sentinel Enterprise, consulte la Tabla 4-1, “Servicios y funciones de Sentinel”, en la página 34.

La fecha de caducidad del sistema se basa en los datos más antiguos del sistema. Si restaura eventos antiguos en su sistema, Sentinel actualizará la fecha de caducidad en consonancia.

Cuando caduca la licencia de evaluación, Sentinel ejecuta una licencia gratuita básica que habilita un conjunto de funciones limitado y un número de eventos limitado de 25 EPS. Esto solo es aplicable si Sentinel está configurado con un almacenamiento tradicional.

En implantaciones de almacenamiento ampliable, Sentinel ya no almacenará eventos y datos en bruto una vez caduque la licencia de evaluación.

Después de actualizar a una licencia empresarial, Sentinel restaurará todas las funciones. Para prevenir cualquier interrupción de la funcionalidad, debe actualizar el sistema a una licencia empresarial antes de que caduque la licencia de evaluación.

Licencia gratuita

La licencia gratuita permite usar un conjunto limitado de funciones con un número de eventos limitado de 25 EPS. La licencia gratuita solo es aplicable a Sentinel con el almacenamiento tradicional.

La licencia gratuita permite recopilar y almacenar eventos. Cuando el número de eventos supere los 25, Sentinel almacenará los eventos recibidos, pero no visualizará la información de dichos eventos en los resultados de búsqueda ni en los informes. Sentinel asigna a estos eventos la etiqueta `OverEPSLimit`.

La licencia gratuita no proporciona funciones en tiempo real. Puede restaurar toda la funcionalidad actualizando la licencia a una de tipo empresarial.

Nota: La asistencia técnica y las actualizaciones de productos no están disponibles para la versión gratuita de Sentinel.

Licencias empresariales

Al adquirir Sentinel, recibe una clave de licencia a través del portal para clientes. Según la licencia que adquiera, la clave de licencia habilitará determinadas funciones, índices de recopilación de datos y orígenes de eventos. Puede haber condiciones adicionales de licencia que no aplique la clave de licencia, por lo que se recomienda leer detenidamente el acuerdo de licencia.

Para hacer cambios a la licencia, comuníquese con su gerente de cuentas.

Puede añadir la clave de licencia empresarial durante la instalación o en cualquier momento posterior. Para añadir la clave de licencia, consulte la sección “Adding a License Key” (Cómo añadir una clave de licencia) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

5 Cumplimiento de los requisitos del sistema

Una implementación de Sentinel puede variar en función de las necesidades del entorno de TI, por lo que se recomienda ponerse en contacto con los Servicios de consultoría de o con algún socio de Sentinel antes de finalizar la arquitectura de Sentinel para el entorno.

Para obtener información sobre el equipo recomendado, sistemas operativos, plataformas de dispositivos y navegadores compatibles, consulte el sitio Web de información técnica de Sentinel.

Requisitos del sistema para conectores y recopiladores

Cada conector y recopilador tiene sus propios requisitos del sistema y plataformas compatibles. Consulte la documentación del conector y del recopilador en el sitio Web de módulos auxiliares (plug-ins) de Sentinel.

Entorno virtual

Sentinel es compatible con los servidores VMware ESX. Al configurar un entorno virtual, las máquinas virtuales deben tener dos o más CPU. Para obtener resultados de rendimiento equivalentes a los resultados obtenidos en las pruebas con equipos físicos en ESX o en otro entorno virtual, el entorno virtual debe contar con la misma capacidad de memoria, CPU, espacio en disco y opciones de E/S que las recomendaciones para equipos físicos.

Para obtener información sobre los equipos físicos recomendados, consulte el sitio Web de información técnica de Sentinel.

6 Consideraciones de implantación

Sentinel tiene una arquitectura escalable que puede ampliarse para manejar la carga que necesite almacenar en él. En este capítulo se ofrece una descripción general de las consideraciones más importantes a la hora de ampliar una implantación de Sentinel. Un profesional de Asistencia técnica de o de los servicios para socios de puede ayudarle a diseñar un sistema Sentinel adecuado para su entorno de TI.

Consideraciones de almacenamiento de datos

Dependiendo de la tasa de EPS, se puede optar por utilizar el almacenamiento tradicional o el almacenamiento ampliable para almacenar e indexar los datos de Sentinel. La implantación de Sentinel dependerá de la opción de almacenamiento de datos que decida utilizar.

Tabla 6-1 *Comparación entre almacenamiento tradicional y almacenamiento ampliable*

Almacenamiento tradicional	Almacenamiento ampliable
Los datos se almacenan por defecto en el almacenamiento tradicional basado en archivos y la indexación se realiza de forma local en el servidor de Sentinel. Además del almacenamiento de datos basado en archivos, también puede optar por almacenar e indexar eventos en el almacén de datos de visualización para aprovechar las funciones de visualización de datos. Para obtener más información, consulte “Configuración del almacén de datos de visualización” en la página 43.	Los datos se almacenan en el almacenamiento ampliable basado en Hadoop y utilizan un mecanismo de indexación distribuido y ampliable para indexar los datos.
Se amplía sin problemas hasta aproximadamente 20 000 EPS. Para poder ampliar hasta valores de EPS más altos, debe añadir servidores Sentinel adicionales.	Se amplía sin problemas hasta un valor muy alto de EPS; por ejemplo, 1 millón de eventos por segundo.
La recopilación de datos se basa en una carga equilibrada entre los diferentes servidores de Sentinel. Por lo tanto, los datos se distribuyen entre los distintos servidores de Sentinel y deben gestionarse por separado.	La recopilación de datos se gestiona a través de un único servidor de Sentinel. Por lo tanto, la gestión de datos y recursos se realiza de forma centralizada en un único servidor de Sentinel.
Los datos se etiquetan en relación con los arrendatarios, pero estos no se tienen en cuenta a la hora de segregar los datos en el disco.	Los datos se etiquetan y se segregan en el disco teniendo en cuenta a los arrendatarios.
La disponibilidad y la réplica de datos deben realizarse manualmente o mediante el uso de mecanismos de almacenamiento costosos como un disco SAN.	La disponibilidad y la réplica de datos son rentables debido a que Hadoop funciona con hardware no especializado.

- “Planificación para el almacenamiento tradicional” en la página 41
- “Planificación para el almacenamiento ampliable” en la página 44
- “Estructura de directorios de Sentinel” en la página 46

Planificación para el almacenamiento tradicional

La estructura del almacenamiento de datos basado en archivos se compone de tres niveles:

Almacenamiento en línea	Almacenamiento principal, antes llamado almacenamiento local.	Optimizado para escribir y recuperar datos de forma rápida. Almacena los datos de eventos recopilados más recientemente y los datos de eventos buscados con más frecuencia.
	Almacenamiento secundario, antes llamado almacenamiento en red. (optional)	Está optimizado para reducir el uso del espacio en un almacenamiento menos costoso, que aún permite una rápida recuperación. Sentinel migra de forma automática las particiones de datos al almacenamiento secundario.
	Nota: El uso del almacenamiento secundario es opcional. Las directivas de retención de datos, las búsquedas y los informes operan en las particiones de datos de eventos independientemente de si residen en el almacenamiento principal, secundario o en ambos.	
Almacenamiento sin conexión	Almacenamiento de archivado	Cuando las particiones están cerradas, se puede hacer una copia de seguridad de la partición en cualquier servicio de almacenamiento de archivos, como Amazon Glacier. Puede volver a importar las particiones de forma temporal para llevar a cabo análisis forenses a largo plazo siempre que sea necesario.

También puede configurar Sentinel para extraer datos de eventos y resúmenes de datos de eventos a una base de datos externa mediante el uso de directivas de sincronización de datos. Para más información, consulte la sección “Configuring Data Synchronization” (Cómo configurar la sincronización de datos) de la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Al instalar Sentinel, debe montar la partición del disco para almacenamiento principal en la ubicación en la que se instalará Sentinel, por defecto, el directorio `/var/opt/novell`.

Toda la estructura del directorio `/var/opt/novell/sentinel` debe residir en una misma partición de disco para garantizar que se realicen los cálculos de utilización de disco correctos. De lo contrario, las funciones de gestión automática de datos podrían eliminar los datos de eventos de forma prematura. Para obtener más información sobre la estructura de directorios de Sentinel, consulte el “Estructura de directorios de Sentinel” en la página 46.

Una práctica óptima consiste en asegurarse de que este directorio de datos esté ubicado en una partición de disco separada de la de los archivos ejecutables, de configuración y del sistema operativo. Las ventajas de almacenar los datos variables por separado son la mayor facilidad de realizar copias de seguridad de los conjuntos de archivos, la recuperación más sencilla en caso de que se dañen los datos, y además fortalece el sistema en caso de que una partición se llene por completo. Además, mejora el rendimiento general de los sistemas donde los sistemas de archivos más pequeños son más eficientes. Para obtener más información, consulte este artículo sobre la creación de particiones de disco.

Nota: Los sistemas de archivos de ext3 tienen un límite para el almacenamiento de archivos, lo cual impide que un directorio tenga más de 32000 archivos o subdirectorios. Puede utilizar el sistema de archivos XFS si prevé tener un gran número de directivas de retención o si va a retener los datos durante períodos de tiempo más largos (un año, por ejemplo).

- “Uso de particiones en instalaciones tradicionales” en la página 42
- “Uso de particiones en instalaciones de dispositivos” en la página 42

- “Mejores prácticas para la disposición de particiones” en la página 42
- “Configuración del almacén de datos de visualización” en la página 43

Uso de particiones en instalaciones tradicionales

En las instalaciones tradicionales, puede modificar la disposición de particiones de disco del sistema operativo antes de instalar Sentinel. El administrador debe crear y montar las particiones deseadas en los directorios adecuados, en función de la estructura de directorios que se describe en la “Estructura de directorios de Sentinel” en la página 46. Al ejecutar el instalador, Sentinel se instala en los directorios creados previamente, lo que da lugar a una instalación que abarca varias particiones.

Nota:

- Puede usar la opción `--location` mientras ejecuta el instalador para especificar una ubicación de nivel superior diferente de los directorios por defecto para almacenar el archivo. El valor que asigne a la opción `--location` se antepone a las vías de los directorios. Por ejemplo, si especifica `--location=/foo`, el directorio de datos será `/foo/var/opt/novell/sentinel/data` y el directorio de configuración será `/foo/etc/opt/novell/sentinel/config`.
- No debe usar enlaces al sistema de archivos (por ejemplo, enlaces condicionales) para la opción `--location`.

Uso de particiones en instalaciones de dispositivos

Si utiliza el formato de dispositivo ISO DVD, puede configurar la partición del sistema de archivos del dispositivo durante la instalación siguiendo las instrucciones que se muestran en las pantallas de YaST. Por ejemplo, puede crear una partición separada para el punto de montaje `/var/opt/novell/sentinel` para poner todos los datos en una partición separada. Sin embargo, para otros formatos de dispositivo, puede configurar las particiones solamente después de la instalación. Puede añadir particiones y mover un directorio a la nueva partición utilizando la herramienta de configuración del sistema SuSE YaST. Para obtener más información sobre la creación de particiones después de la instalación, consulte la “Creación de particiones de almacenamiento tradicional” en la página 107.

Mejores prácticas para la disposición de particiones

Muchas organizaciones tienen sus propios esquemas documentados de prácticas óptimas de disposición de particiones para cualquier sistema instalado. La siguiente propuesta de partición tiene como fin orientar a las organizaciones sin directivas definidas y tiene en cuenta el uso específico del sistema de archivos de Sentinel. Por lo general, Sentinel cumple el Estándar de jerarquía del sistema de archivos cuando resulta viable.

Partición	Punto de montaje	Tamaño	Notas
Root	`/`	100 GB	Contiene archivos del sistema operativo y binarios/configuración de Sentinel.
Boot	`/boot`	150 MB	Partición de arranque

Partición	Punto de montaje	Tamaño	Notas
Almacenamiento principal	`/var/opt/novell/sentinel`	Calcular utilizando la Información sobre tamaño del sistema.	Esta sección incluirá los datos principales recopilados por Sentinel y otros datos variables, como archivos de registro. Esta partición puede compartirse con otros sistemas.
Almacenamiento secundario	Ubicación basada en el tipo de almacenamiento, NFS, CIFS o SAN.	Calcular utilizando la Información sobre tamaño del sistema.	Área de almacenamiento secundario, que puede montarse a nivel local tal como se indica o de forma remota.
Almacenamiento de archivado	Sistema remoto	Calcular utilizando la Información sobre tamaño del sistema.	Este almacenamiento es para datos archivados.

Configuración del almacén de datos de visualización

Sentinel proporciona visualizaciones de eventos que presentan datos en gráficos, tablas y mapas. Estas visualizaciones simplifican la visualización y el análisis de grandes volúmenes de eventos. También puede crear sus propias visualizaciones y consolas.

Sentinel hace uso de Kibana, una consola de búsqueda y análisis basada en navegador, que le ayuda a buscar y visualizar eventos. Kibana accede a los datos del almacén de datos de visualización (Elasticsearch) para presentar los eventos en las consolas. Por defecto, Sentinel incluye un nodo de Elasticsearch que almacena e indexa solo alertas. Debe habilitar la visualización de eventos para almacenar e indexar los eventos en Elasticsearch.

Al habilitar Elasticsearch para almacenar e indexar datos, Sentinel indexa solo algunos campos de eventos específicos necesarios para las visualizaciones y almacena los campos indexados en Elasticsearch. Sentinel crea un índice específico para cada día y utiliza la zona horaria UTC (de medianoche a medianoche) para calcular la fecha de índice. El nombre de índice aparece en el formato `security.events.normalized_aaaaMMdd`. Por ejemplo, el índice `security.events.normalized_20160101` contiene todos los eventos con fecha de 1 de enero de 2016.

La configuración del almacén de datos de visualización implica las siguientes acciones:

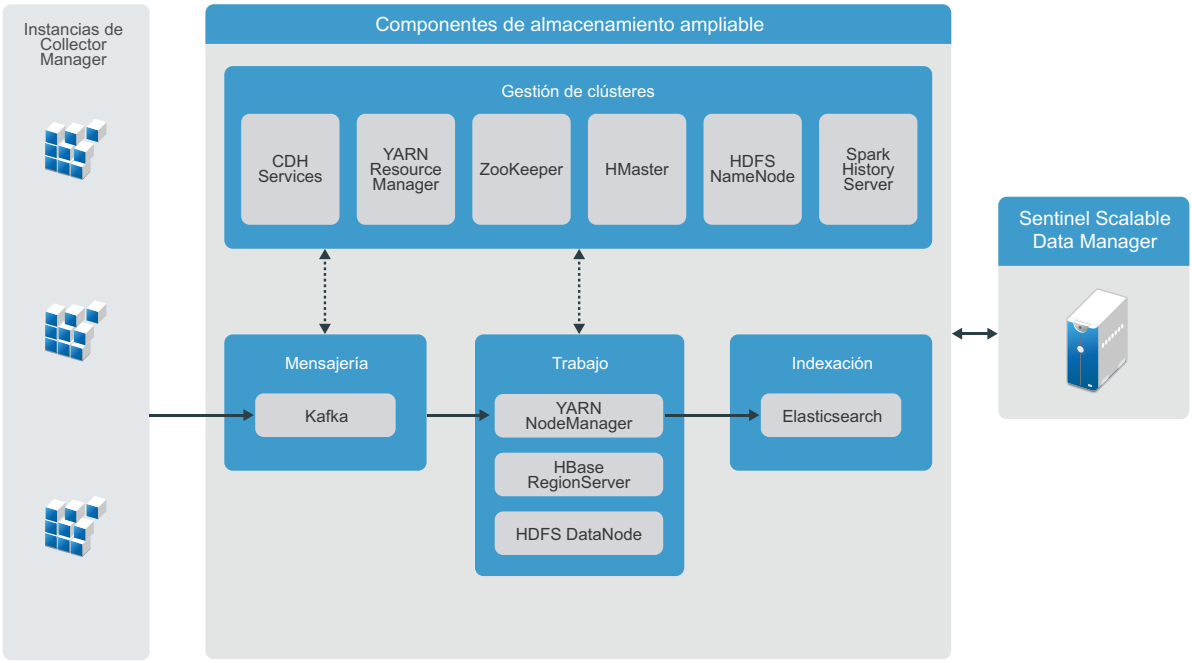
- **Instalación de nodos de Elasticsearch en modo de clúster:** Sentinel incluye por defecto un nodo de Elasticsearch. Para obtener un rendimiento y una estabilidad óptimos del servidor Sentinel, es obligatorio que instale nodos de Elasticsearch adicionales en modo de clúster. Para obtener más información, consulte Capítulo 12, “Instalación y configuración de Elasticsearch”, en la página 77.
- **Habilitar la visualización de eventos:** La visualización de eventos está inhabilitada por defecto. Para habilitar la visualización de eventos, consulte Capítulo 20, “Habilitación de la visualización de eventos”, en la página 125.
- **Ajuste del rendimiento:** Sentinel configura automáticamente determinados ajustes de Elasticsearch para obtener un rendimiento óptimo. Puede personalizar estos ajustes según sea necesario. Por ejemplo, puede modificar los campos de eventos que desee que indexe Elasticsearch. Para obtener más información, consulte “Ajuste del rendimiento para Elasticsearch” en la página 83.

Planificación para el almacenamiento ampliable

Sentinel utiliza el marco de distribución de Cloudera que incluye Apache Hadoop (CDH) para almacenar y gestionar un gran volumen de datos. Con respecto a la indexación de eventos, Sentinel utiliza el motor de indexación ampliable y distribuido Elasticsearch de Elastic.

En la siguiente ilustración se muestran los diferentes componentes utilizados en el almacenamiento ampliable:

Figura 6-1 *Arquitectura de almacenamiento ampliable*



- **Mensajería:** Sentinel utiliza Kafka de Apache como sistema de mensajería ampliable que recibe eventos normalizados y datos en bruto de las instancias de Collector Manager. Las instancias de Collector Manager envían datos en bruto y datos de eventos a los clústeres de Kafka.

  De forma predeterminada, Sentinel crea los siguientes temas de Kafka:

  - **security.events.normalized:** almacena todos los datos de eventos procesados y normalizados, incluidos los eventos generados por el sistema y los eventos internos.
  - **security.events.raw:** almacena todos los datos en bruto procedentes de las fuentes de los eventos.

  Los datos en bruto y de eventos siguen el esquema de Apach Avro. Para obtener más información, consulte la documentación de Apache Avro. Los archivos de esquema están disponibles en el directorio de `/etc/opt/novell/sentinel/scalablestore`.

- **Trabajo:** Este nodo alberga tareas de almacenamiento y procesamiento en tiempo real. Apache Spark realiza el procesamiento de datos a gran escala en tiempo real como, por ejemplo, la segregación de eventos basados en identificadores de arrendatarios, la solicitud de grandes volúmenes de datos y el almacenamiento de los mismos en el sistema de registro (SOR) y la indexación ampliable.

  Apache HBase es un almacén de datos basado en Hadoop distribuido y ampliable. Se utiliza como un SOR de datos en bruto y de eventos normalizados, segregados por identificadores de arrendatarios.

En función del identificador del arrendatario, Sentinel crea un espacio de nombres independiente para cada uno de ellos. Por ejemplo, el espacio de nombres para el arrendatario predeterminado es 1. En cada espacio de nombres, Sentinel crea las siguientes tablas y almacena los datos según la hora del evento.

- ***<ID_arrendatario>*:security.events.normalized:** almacena todos los datos de eventos procesados y normalizados, incluidos los eventos generados por el sistema y los eventos internos.
- ***<ID_arrendatario>*:security.events.raw:** almacena todos los datos en bruto procedentes de las fuentes de los eventos.

- **Gestión en clúster:** Este nodo alberga todos los patrones y los servicios de gestión de clúster. Apache ZooKeeper actúa como un servicio centralizado destinado al mantenimiento de la información de configuración, la denominación de servicios, la facilitación de la sincronización distribuida y la prestación de servicios de grupo.
- **Indexación:** Sentinel utiliza Elasticsearch como el motor de indexado distribuido y ampliable para la indexación de eventos. Es posible acceder a los datos de Elasticsearch para la búsqueda y visualización de eventos.

  Sentinel crea un índice específico para cada día y utiliza la zona horaria UTC (de medianoche a medianoche) para calcular la fecha de índice. El nombre de índice aparece en el formato `security.events.normalized_aaaaMMdd`. Por ejemplo, el índice `security.events.normalized_20160101` contiene todos los eventos con fecha de 1 de enero de 2016. Para obtener un rendimiento óptimo, Sentinel indexa solamente algunos campos de evento específicos. Puede modificar los campos de evento que desee que indexe Elasticsearch. Para obtener más información, consulte “Ajuste del rendimiento para Elasticsearch” en la página 83.

Configuración del almacenamiento ampliable

Cuando se habilita el almacenamiento ampliable, la interfaz de usuario de servidor de Sentinel se limita a algunas de las funciones de Sentinel, como la recopilación de datos, la correlación, el encaminamiento de eventos, la búsqueda y visualización de eventos y la realización de determinadas actividades administrativas. Esta versión limitada de Sentinel se conoce como Sentinel Scalable Data Manager (SSDM). Para utilizar otras funcionalidades de Sentinel como la inteligencia de seguridad, la búsqueda y generación de informes convencional, debe instalar instancias independientes de Sentinel con el almacenamiento tradicional y distribuir los datos de eventos específicos de SSDM a Sentinel mediante el uso de Sentinel Link.

En la lista siguiente se proporciona información acerca de los servicios y las funciones no disponibles en SSDM:

- Informes
- Inteligencia de seguridad
- Realización de operaciones de eventos durante la búsqueda
- Comprobación de las reglas de correlación
- Creación y gestión de incidencias
- Ejecución manual de acciones sobre eventos
- Sincronización de datos
- Flujos de trabajo de iTRAC
- Análisis forenses de los eventos que activan el evento correlacionado
- Visualización de adjuntos de los eventos de Secure Configuration Manager y Change Guardian

La habilitación del almacenamiento ampliable constituye una configuración única, la cual no se puede revertir. Si desea inhabilitar el almacenamiento ampliable y cambiar al almacenamiento tradicional, debe volver a instalar Sentinel.

La siguiente lista de verificación ofrece un alto nivel información acerca de las tareas que necesita llevar a cabo para configurar el almacenamiento ampliable:

Tabla 6-2 *Lista de verificación de la configuración del almacenamiento ampliable*

	Tareas	Consulte
❒	Revise la información de implantación para comprender la forma en que debe instalar Sentinel con almacenamiento ampliable.	"Implantación de tres niveles con almacenamiento ampliable" en la página 52
❒	Revise los requisitos previos y lleve a cabo todas las tareas requeridas.	Capítulo 13, "Instalación y configuración del almacenamiento ampliable", en la página 87.
❒	Habilite el almacenamiento ampliable. Puede habilitar el almacenamiento ampliable durante la instalación o después de esta.	Para habilitar el almacenamiento ampliable durante la instalación, lleve a cabo una instalación personalizada de Sentinel. Consulte la "Instalación personalizada del servidor Sentinel" en la página 92.
	En las instalaciones de actualización, puede habilitar el almacenamiento ampliable solo después de actualizar Sentinel.	Para habilitar el almacenamiento ampliable después de la instalación o la actualización, consulte Enabling Scalable Storage Post-Installation (Habilitación del almacenamiento ampliable después de la instalación) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).
❒	Configure los componentes de CDH y Elasticsearch con Sentinel.	Configuring Scalable Storage (Configuración del almacenamiento ampliable) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Estructura de directorios de Sentinel

Por defecto, los directorios de Sentinel se encuentran en las siguientes ubicaciones:

- Los archivos de datos se encuentran en los directorios `/var/opt/novell/sentinel/data` y `/var/opt/novell/sentinel/3rdparty`.
- Los archivos ejecutables y las bibliotecas se almacenan en el directorio `/opt/novell/sentinel`..
- Los archivos de registro se encuentran en el directorio `/var/opt/novell/log`.
- Los archivos temporales se encuentran en el directorio `/var/opt/novell/sentinel/tmp`.
- Los archivos de configuración se encuentran en el directorio `/etc/opt/novell/sentinel`.
- El archivo de ID del proceso (PID) se encuentra en el directorio `/home/novell/sentinel/server.pid`.

  Mediante el PID, los administradores pueden identificar el proceso padre del servidor Sentinel y supervisar o terminar el proceso.

Ventajas de las implantaciones distribuidas

De manera predeterminada, el servidor Sentinel incluye los siguientes componentes:

- **Collector Manager:** Collector Manager proporciona un punto de recopilación de datos flexible para Sentinel.
- **Correlation Engine:** Correlation Engine procesa eventos del flujo de eventos en tiempo real para determinar si estos deberían activar alguna de las reglas de correlación.
- **Elasticsearch:** Un componente de almacenamiento de datos opcional para almacenar e indexar los datos. Por defecto, Sentinel incluye un nodo de Elasticsearch. Si espera tasas elevadas de EPS, más de 2500, debe implantar nodos de Elasticsearch adicionales en un clúster.

Importante: En los entornos de producción, debe configurar una implantación distribuida porque aísla los componentes de recopilación de datos en un equipo independiente, lo que es importante para manejar aumentos repentinos de procesamiento y otras anomalías con la máxima estabilidad para el sistema.

En esta sección se describen las ventajas de las implantaciones distribuidas.

- "Ventajas de las instancias adicionales de Collector Manager" en la página 47
- "Ventajas de las instancias adicionales de Correlation Engine" en la página 48

Ventajas de las instancias adicionales de Collector Manager

El servidor Sentinel incluye Collector Manager por defecto. No obstante, para los entornos de producción, las instancias de Collector Manager proporcionan un mejor aislamiento cuando se reciben grandes volúmenes de datos. En esta situación, una instancia de Collector Manager distribuida podría verse sobrecargada, pero el servidor Sentinel seguirá respondiendo a las peticiones del usuario.

La instalación de más de una instancia de Collector Manager en una red distribuida aporta las siguientes ventajas:

- **Mejora del rendimiento del sistema:** las instancias adicionales de Collector Manager pueden analizar y procesar datos de eventos en un entorno distribuido, lo que incrementa el rendimiento del sistema.
- **Mayor seguridad de los datos y menores requisitos de ancho de banda de la red:** si las instancias de Collector Manager se encuentran ubicadas conjuntamente con los orígenes de eventos, entonces puede aplicarse el filtrado, el cifrado y la compresión de datos en el origen.
- **Almacenamiento de archivos en el caché:** las instancias adicionales de Collector Manager pueden almacenar en el caché grandes cantidades de datos mientras que el servidor está ocupado temporalmente archivando eventos o procesando un aumento del número de eventos. Esta función es una ventaja para los protocolos, como syslog, que no admiten el almacenamiento en caché de forma original.

Puede instalar instancias adicionales de Collector Manager en ubicaciones adecuadas de su red. Estas instancias remotas de Collector Manager ejecutan conectores y recopiladores y reenvían los datos obtenidos al servidor Sentinel para su almacenamiento y procesamiento. Para obtener información sobre la instalación de instancias adicionales de Collector Manager, consulte la Parte III, "Instalación de Sentinel", en la página 71.

Nota: No es posible instalar más de una instancia de Collector Manager en un solo sistema. Puede instalar más instancias de Collector Manager en sistemas remotos y conectarlos después al servidor Sentinel.

Ventajas de las instancias adicionales de Correlation Engine

Puede distribuir múltiples instancias de Correlation Engine, cada una en su propio servidor, sin necesidad de replicar configuraciones ni añadir bases de datos. En los entornos que tienen muchas reglas de correlación o un número extremadamente elevado de eventos, puede ser beneficioso instalar más de una instancia de Correlation Engine y volver a implementar algunas reglas en la nueva instancia de dicho motor. Varios instancias de Correlation Engine proporcionan la capacidad de ampliarse a medida que el sistema Sentinel incorpora orígenes de datos adicionales o aumenta el número de eventos. Para obtener información sobre la instalación de instancias adicionales de Correlation Engine, consulte la Parte III, “Instalación de Sentinel”, en la página 71 .

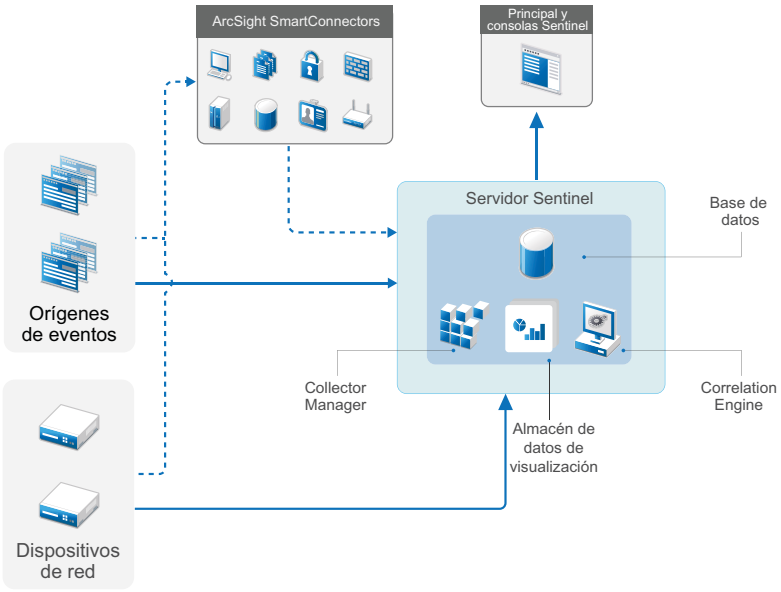
Nota: No es posible instalar más de una instancia de Correlation Engine en un solo sistema. Puede instalar instancias adicionales de Correlation Engine en sistemas remotos y luego conectarlos al servidor Sentinel.

Implantación "todo en uno"

La opción de implantación más básica es un sistema "todo en uno" que incluye todos los componentes en un solo equipo. Una implantación "todo en uno" solo es adecuada si la carga del sistema es pequeña y no es necesario supervisar los equipos Windows. En muchos entornos, las cargas fluctuantes e imprevisibles, así como los conflictos de recursos entre componentes pueden causar problemas de rendimiento.

Importante: Si utiliza entornos de producción, debe configurar una implantación distribuida porque aísla los componentes de recopilación de datos en un equipo independiente, lo que es importante para manejar aumentos repentinos de procesamiento y otras anomalías con la máxima estabilidad para el sistema.

Figura 6-2 *Implantación "todo en uno"*

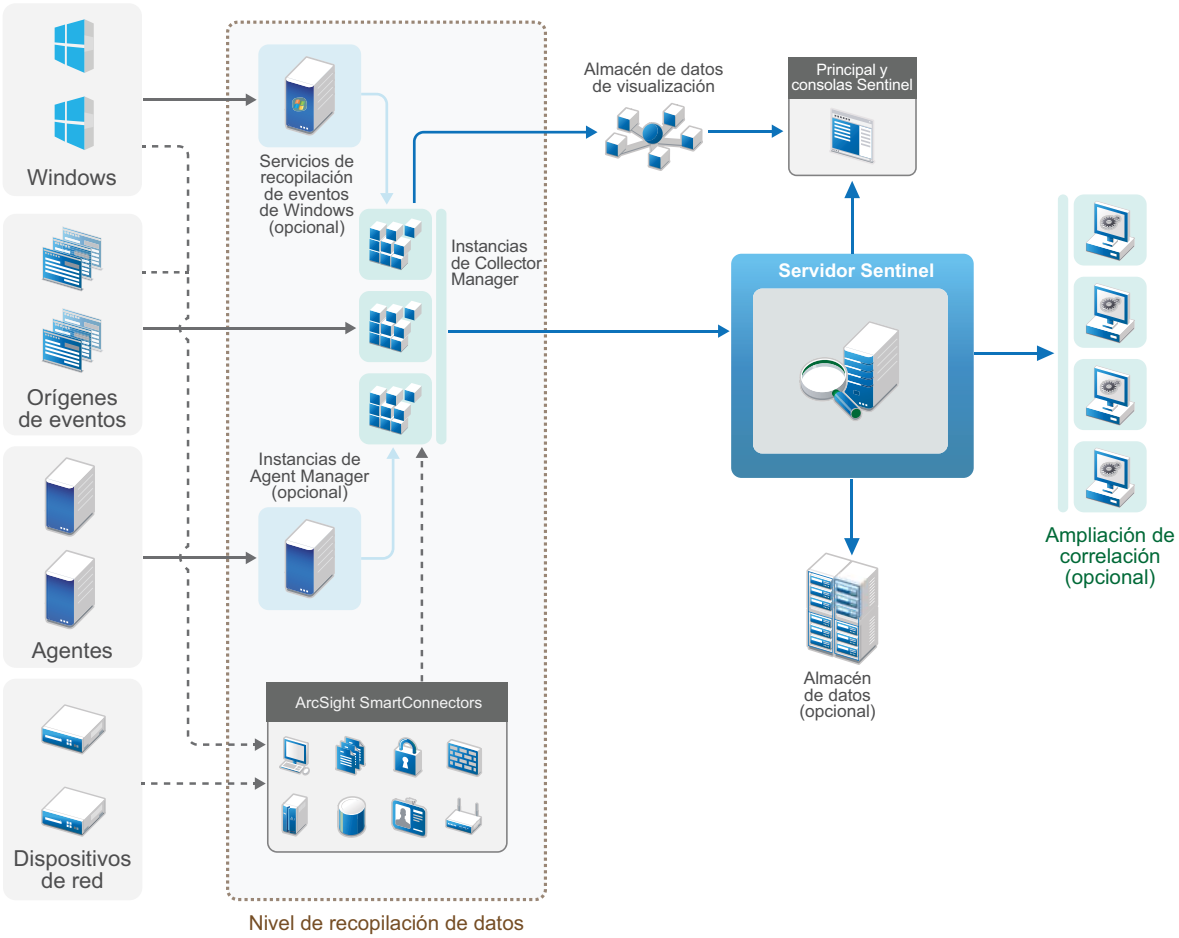


Implantación distribuida de un nivel

La implantación de un nivel añade la capacidad de supervisar equipos Windows y de manejar una carga mayor que la de la implantación "todo en uno". Puede aumentar la correlación y recopilación de datos mediante la adición de equipos de Collector Manager y Correlation Engine que liberen al servidor Sentinel central de carga de procesamiento. Además de manejar la carga de eventos y las reglas de correlación, los gestores de recopiladores remotos y los motores de correlación liberan recursos en el servidor central de Sentinel para prestar servicio a otras peticiones, como almacenamiento y búsqueda de eventos. A medida que aumente la carga del sistema, el servidor central de Sentinel formará un cuello de botella y se necesitará una implementación con más niveles para aumentar más la escala.

Opcionalmente, puede configurar Sentinel para copiar datos de eventos en un almacén de datos, que puede resultar útil para descargar informes personalizados, análisis y otras tareas de procesamiento a otro sistema.

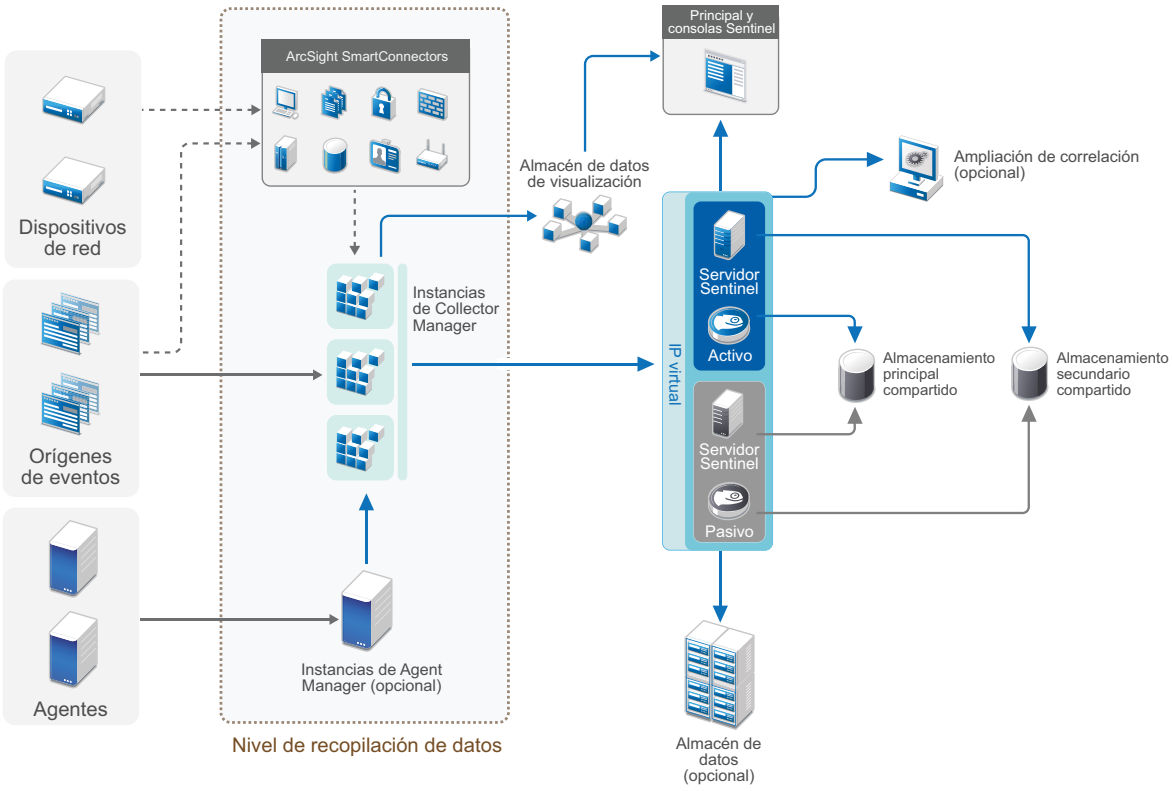
Figura 6-3 *Implantación distribuida de un nivel*



Implantación distribuida de un nivel con alta disponibilidad

La implantación distribuida de un nivel muestra cómo puede convertirse en un sistema de alta disponibilidad con redundancia de failover. Para obtener más información sobre la implementación de Sentinel con alta disponibilidad, consulte el Parte VII, “Implantación de Sentinel para alta disponibilidad”, en la página 187.

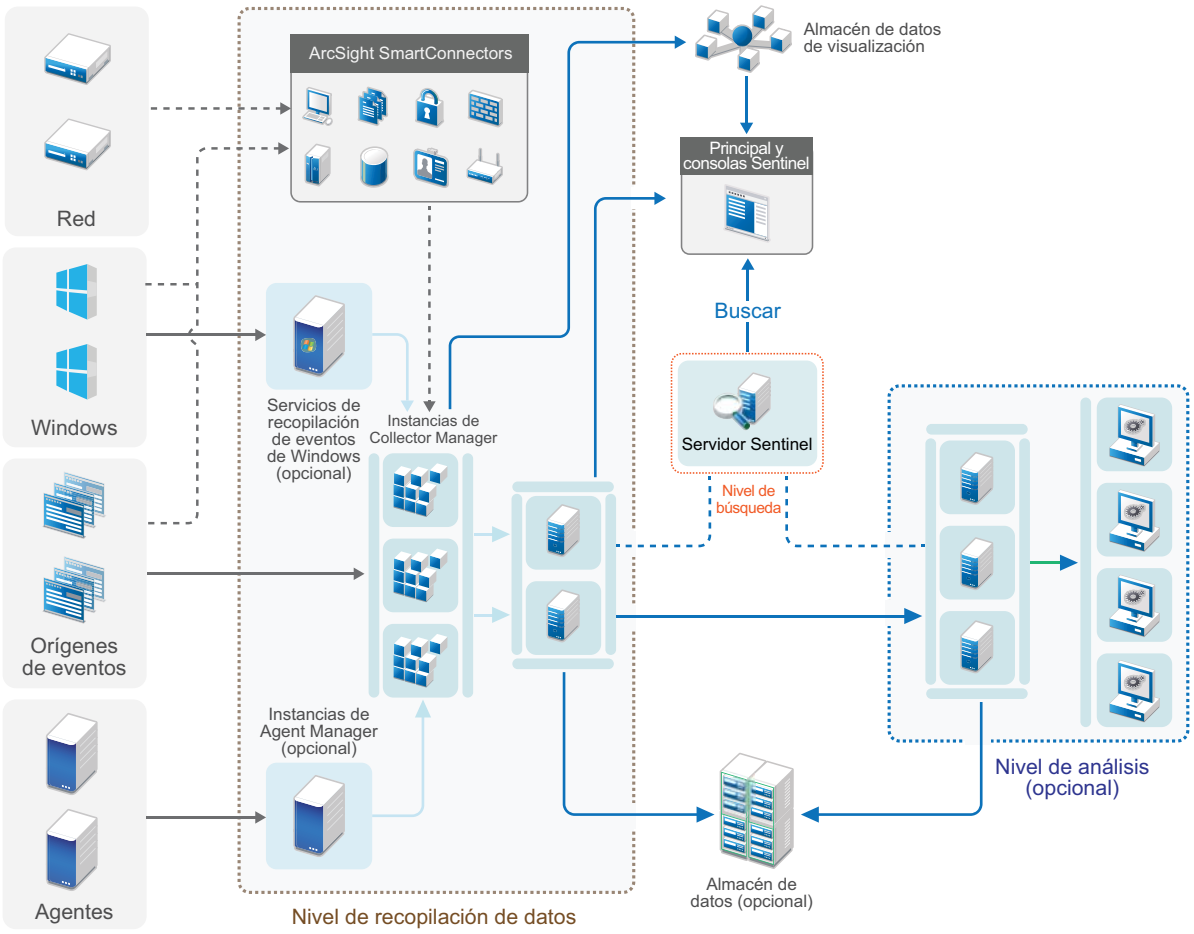
Figura 6-4 *Implantación distribuida de un nivel con alta disponibilidad*



Implantación distribuida de dos y tres niveles

Estas implantaciones permiten superar las capacidades de manejo de carga de un solo servidor Sentinel central y compartir la carga de procesamiento entre varias instancias de Sentinel al aprovechar Sentinel Link y las funciones de federación de datos de Sentinel. La recopilación de datos se realiza con equilibrio de carga entre varios servidores Sentinel, cada uno de los cuales tiene varias instancias de Collector Manager, tal como se muestra en el nivel de recopilación de datos. Si quiere llevar a cabo una correlación de eventos o inteligencia de seguridad, tiene la opción de reenviar datos al Nivel de análisis a través de Sentinel Link. El Nivel de búsqueda proporciona un único punto de acceso práctico para realizar búsquedas en todos los sistemas de todos los demás niveles por medio de la federación de datos de Sentinel. Dado que la petición de búsqueda está federada en varias instancias de Sentinel, esta implementación también tiene propiedades de equilibrio de carga de búsqueda útiles a la hora de ampliar y poder manejar una carga de búsqueda intensa.

Figura 6-5 *Implantación distribuida de dos y tres niveles*



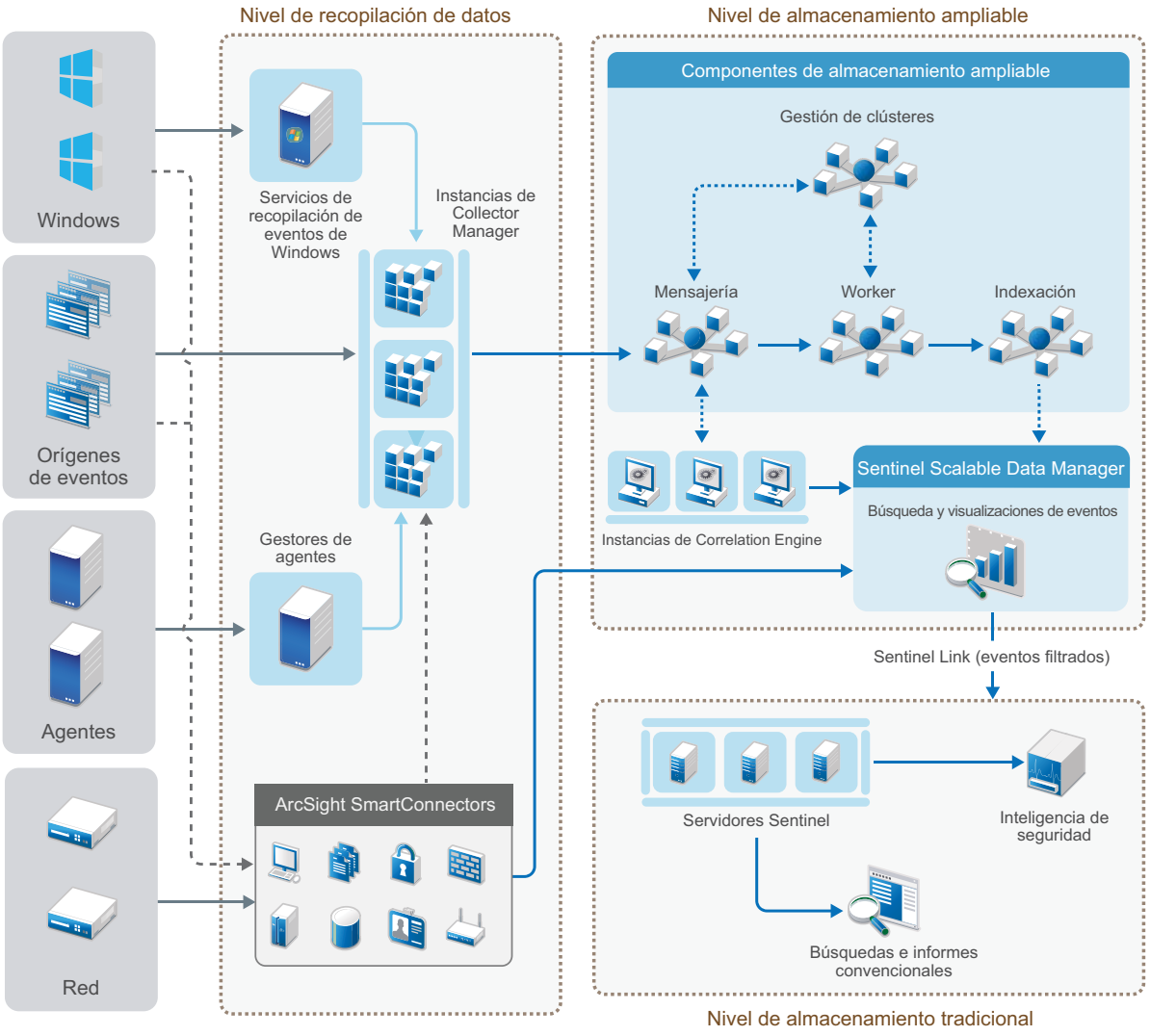
Implantación de tres niveles con almacenamiento ampliable

Para atender a las necesidades de procesamiento de datos y almacenamiento de datos de gran tamaño cuando no desea distribuir los eventos a través de varios servidores de Sentinel y duplicar los valores de configuración en varias instancias, puede configurar una implantación distribuida de tres niveles con almacenamiento ampliable. Esta implantación permite almacenar y gestionar datos de gran tamaño mediante el uso de un solo servidor de Sentinel con almacenamiento ampliable, en lugar de utilizar varios servidores de Sentinel.

Puede configurar un servidor Sentinel nuevo con almacenamiento ampliable, o bien actualizar el servidor Sentinel existente para habilitar el almacenamiento ampliable.

Dependiendo de las funciones de Sentinel que desee utilizar, puede determinar cómo desea configurar la implementación de esta solución.

Figura 6-6 *Distribución de tres niveles de almacenamiento ampliable*



Esta implantación incluye los siguientes niveles:

- **Nivel de recopilación de datos:** destinado a la recopilación de eventos de una amplia gama de orígenes de eventos. Opcionalmente, si desea conservar su configuración existente de recopilación de datos con el almacenamiento tradicional de Sentinel y aprovechar a la vez las capacidades de almacenamiento ampliable, puede reenviar los eventos que desee directamente del almacenamiento tradicional al almacenamiento ampliable utilizando el guión `data_uploader.sh`. Para obtener más información, consulte Capítulo 32, “Migración de datos al almacenamiento ampliable”, en la página 177.
- **Nivel de almacenamiento ampliable:** destinado al almacenamiento, indexación y análisis de datos de gran tamaño. En este nivel, el servidor SSDM permite gestionar la correlación y recopilación de datos y ofrece otras funciones SSDM. Para utilizar las funciones de Sentinel no disponibles en SSDM, puede configurar el nivel tradicional de almacenamiento. También puede reenviar los datos recopilados a los otros sistemas de SIEM o habilitar otras herramientas de inteligencia empresarial para consultar los datos o realizar análisis directamente en la distribución Hadoop utilizando las API ampliamente compatibles Hadoop, Kafka, chispa y Elasticsearch APIs.

- **Nivel de almacenamiento tradicional:** Para utilizar las funciones de Sentinel como inteligencia de seguridad, búsqueda convencional y generación de informes, debe instalar instancias independientes de Sentinel con almacenamiento tradicional. Puede configurar reglas de encaminamiento de eventos para reenviar los eventos que desee desde SSDM a Sentinel mediante el uso de Sentinel Link.

  También puede realizar búsquedas y generar informes utilizando cualquiera de los servidores de Sentinel en el nivel de almacenamiento tradicional. Opcionalmente, puede configurar un nivel de búsqueda independiente que proporciona un punto de acceso práctico para búsquedas y generación de informes a través de todos los servidores de Sentinel en el nivel de almacenamiento tradicional. Para buscar los eventos en el almacenamiento ampliable, utilice la opción de búsqueda en SSDM.

Para obtener más información acerca de la instalación y configuración del almacenamiento ampliable, consulte Capítulo 13, “Instalación y configuración del almacenamiento ampliable”, en la página 87.

7 Consideraciones sobre implantación para el modo FIPS 140-2

Sentinel también se puede configurar para usar los Servicios de seguridad de la red de Mozilla (NSS), que es un proveedor de cifrado validado FIPS 140-2, para sus funciones internas de cifrado y de otro tipo. El objetivo de hacer esto es garantizar que Sentinel integre 'FIPS 140-2 en su interior' y que cumpla con las directivas y los estándares federales de adquisición de los Estados Unidos.

La habilitación del modo FIPS 140-2 de Sentinel facilita la comunicación entre el servidor de Sentinel, las instancias remotas de Collector Manager y Correlation Engine de Sentinel, la interfaz principal de Sentinel, el Control Center de Sentinel y el servicio asesor de Sentinel con el fin de utilizar el cifrado validado FIPS 140-2.

Importante: El modo FIPS solo se admite en Sentinel. No se admite Sentinel si el sistema operativo está en modo FIPS.

Implementación de FIPS en Sentinel

Sentinel utiliza las bibliotecas NSS de Mozilla suministradas por el sistema operativo. Red Hat Enterprise Linux (RHEL) y SUSE Linux Enterprise Server (SLES) tienen conjuntos diferentes de paquetes NSS.

El módulo de cifrado NSS proporcionado por RHEL 6.3 y versiones posteriores está validado para FIPS 140-2. El módulo de cifrado NSS incluido en SLES 11 aún no ha sido validado oficialmente para FIPS 140-2, pero la validación del módulo SUSE para FIPS 140-2 está en curso. Una vez que esté disponible la validación, no prevé la necesidad de realizar cambios a Sentinel para integrar 'FIPS 140-2 en el interior' en la plataforma SUSE.

Para obtener más información acerca de la certificación FIPS 140-2 de RHEL, consulte https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2711 y https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1837.

Paquetes de NSS de RHEL

Sentinel requiere los siguientes paquetes NSS de 64 bits para admitir el modo FIPS 140-2:

- nspr-*
- nss-sysinit-*
- nss-util-*
- nss-softokn-freebl-*

- nss-softokn-*
- nss-*
- nss-tools-*

Si alguno de estos paquetes no está instalado, debe instalarlo antes de habilitar el modo FIPS 140-2 en Sentinel.

Paquetes NSS de SLES

Sentinel requiere los siguientes paquetes NSS de 64 bits para admitir el modo FIPS 140-2:

- libfreebl3-*
- mozilla-nspr-*
- mozilla-nss-*
- mozilla-nss-tools-*

Si alguno de estos paquetes no está instalado, debe instalarlo antes de habilitar el modo FIPS 140-2 en Sentinel.

Componentes habilitados para FIPS en Sentinel

Los siguientes componentes de Sentinel son compatibles con FIPS 140-2:

- Todos los componentes de la plataforma Sentinel se actualizan para admitir el modo FIPS 140-2.
- Los siguientes módulos auxiliares (plug-ins) de Sentinel que admiten cifrado se actualizan para admitir el modo FIPS 140-2:
  - Agent Manager Connector 2011.1r1 y versiones posteriores
  - Database (JDBC) Connector 2011.1r2 y versiones posteriores
  - File Connector 2011.1r1 y versiones posteriores (solo si el tipo de origen de evento del archivo es local o NFS)
  - LDAP Integrator 2011.1r1 y versiones posteriores
  - Sentinel Link Connector 2011.1r3 y versiones posteriores
  - Sentinel Link Integrator 2011.1r2 y versiones posteriores
  - SMTP Integrator 2011.1r1 y versiones posteriores
  - Syslog Connector 2011.1r2 y versiones posteriores
  - Windows Event (WMI) Connector 2011.1r2 y versiones posteriores
  - Check Point (LEA) Connector 2011.1r2 y versiones posteriores
  - Syslog Integrator 2011.1r1 y versiones posteriores

  Para obtener más información sobre cómo configurar estos módulos auxiliares (plug-ins) de Sentinel para ejecutarse en modo FIPS 140-2, consulte “Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2” en la página 136.

Los siguientes conectores de Sentinel que admiten cifrado opcional no se habían actualizado aún para admitir el modo FIPS 140-2 en el momento de publicar este documento. Sin embargo, puede seguir recopilando eventos con estos conectores. Para obtener información sobre cómo usar estos conectores con Sentinel en el modo FIPS 140-2, consulte la sección “Uso de conectores no habilitados para FIPS con Sentinel en el modo FIPS 140-2” en la página 142.

- Cisco SDEE Connector 2011.1r1
- File Connector 2011.1r1 - Las funciones de CIFS y SCP incluyen cifrado y no funcionarán en el modo FIPS 140-2.
- Audit Connector 2011.1r1
- SNMP Connector 2011.1r1

Los siguientes integradores de Sentinel que admiten SSL no se habían actualizado aún para admitir el modo FIPS 140-2 en la fecha de publicación de este documento. Sin embargo, puede seguir usando conexiones sin cifrar cuando se utilicen estos integradores con Sentinel en el modo FIPS 140-2.

- Remedy Integrator 2011.1r1 o versiones posteriores
- SOAP Integrator 2011.1r1 o versiones posteriores

Cualquier otro módulo auxiliar (plug-in) de Sentinel que no esté en la lista anterior no usa cifrado y no se ve afectado al habilitar el modo FIPS 140-2 en Sentinel. No es necesario realizar ningún otro paso para usarlos con Sentinel en modo FIPS 140-2.

Para obtener más información sobre los módulos auxiliares (plug-ins) de Sentinel, consulte el sitio web de módulos auxiliares de Sentinel. Si desea solicitar que uno de los módulos auxiliares (plug-ins) que aún no se han actualizado esté disponible con compatibilidad para FIPS, envíe una solicitud mediante Bugzilla.

Conexiones de datos afectadas por el modo FIPS

Si Sentinel se encuentra en el modo FIPS 140-2, no puede establecer conexiones cifradas a Microsoft SQL Server. Esta consideración afecta a los siguientes tipos de operaciones de Sentinel:

- Directivas de sincronización de datos en SQL Server
- Comunicación del servidor de Sentinel con la base de datos de Agent Manager
- Recopilación de datos de SQL Server por parte del conector de base de datos

Lista de verificación de implementación

La tabla siguiente ofrece una descripción general de las tareas necesarias para configurar Sentinel para el funcionamiento en modo FIPS 140-2.

Tareas	Para obtener más información, consulte la…
Planifique la implantación.	“Entornos de implantación” en la página 58.

Tareas	Para obtener más información, consulte la…
Determine si necesita habilitar el modo FIPS 140-2 durante la instalación de Sentinel o si desea habilitarlo en el futuro. Para habilitar Sentinel en el modo FIPS 140-2 durante la instalación, deberá seleccionar el método de instalación Personalizado o Silencioso durante el proceso de instalación.	“Instalación personalizada del servidor Sentinel” en la página 92. “Instalación silenciosa” en la página 97 Capítulo 23, “Habilitar el modo FIPS 140-2 en una instalación de Sentinel existente”, en la página 131
Configure los módulos auxiliares (plug-ins) de Sentinel para ejecutarse en modo FIPS 140-2.	“Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2” en la página 136.
Importe certificados en el Almacén de claves de FIPS de Sentinel.	“Importación de certificados en la base de datos del almacén de claves de FIPS” en la página 143

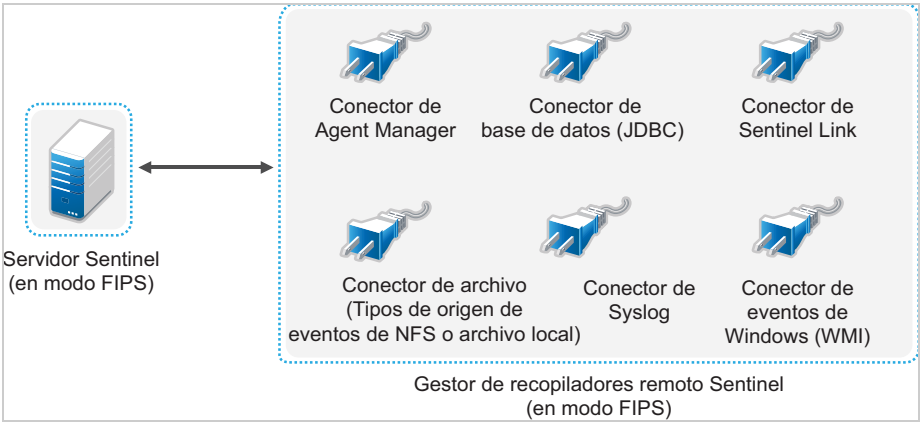
Nota: Realice copias de seguridad de los sistemas de Sentinel antes de empezar la conversión al modo FIPS. Si más adelante es necesario revertir el servidor al modo diferente de FIPS, el único método admitido consiste en restaurarlo desde una copia de seguridad. Para obtener más información sobre cómo revertir a un modo diferente de FIPS, consulte “Reversión de Sentinel al modo diferente de FIPS” en la página 143.

Entornos de implantación

En esta sección se proporciona información sobre los diferentes escenarios de implantación de Sentinel en modo FIPS 140-2.

Escenario 1: Recopilación de datos en modo FIPS 140-2 completo

En este escenario, se realiza la recopilación de datos solamente a través de conectores compatibles con el modo FIPS 140-2. Se presupone que este entorno tiene un servidor Sentinel y que los datos se recopilan a través de una instancia remota de Collector Manager. Puede tener una o varias instancias de Collector Manager.



Debe realizar el siguiente procedimiento únicamente si su entorno incluye recopilación de datos de orígenes de eventos que utilizan conectores compatibles con el modo FIPS 140-2.

1 Debe tener un servidor Sentinel en el modo FIPS 140-2.

Nota: Si su servidor Sentinel (recién instalado o actualizado) no tiene habilitado el modo FIPS, debe habilitar FIPS en el servidor Sentinel. Para obtener más información, consulte la “Habilitar el servidor Sentinel para su ejecución en modo FIPS 140-2” en la página 131.

---

2 Debe tener una instancia remota de Collector Manager de Sentinel que se ejecute en modo FIPS 140-2.

Nota: Si la instancia remota de Collector Manager (recién instalada o actualizada) no se ejecuta en el modo FIPS, debe habilitar FIPS en dicha instancia. Para obtener más información, consulte la “Habilitar el modo FIPS 140-2 en las instancias remotas de Collector Manager y Correlation Engine” en la página 132.

---

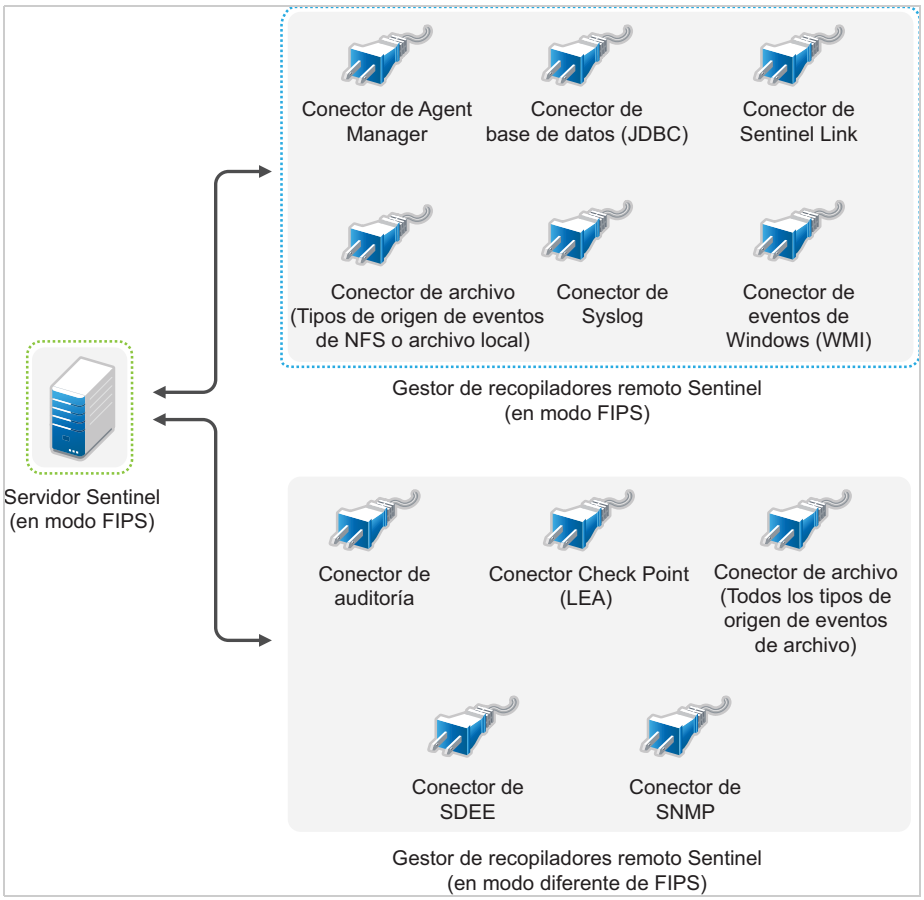
3 Asegúrese de que el servidor FIPS y las instancias remotas de Collector Manager se comuniquen entre sí.

4 Convierta las instancias remotas de Correlation Engine, si las hay, para que se ejecuten en modo FIPS. Para obtener más información, consulte el “Habilitar el modo FIPS 140-2 en las instancias remotas de Collector Manager y Correlation Engine” en la página 132.

5 Configure los módulos auxiliares (plug-ins) de Sentinel para que se ejecuten en modo FIPS 140-2. Para obtener más información, consulte la “Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2” en la página 136.

Escenario 2: Recopilación de datos en modo FIPS 140-2 parcial

En este escenario, la recopilación de datos se realiza utilizando conectores compatibles con el modo FIPS 140-2 y conectores no compatibles con el modo FIPS 140-2. Suponemos que los datos se recopilan por medio de una instancia remota de Collector Manager. Puede tener uno o varias instancias remotas de Collector Manager.



Para manejar la recopilación de datos mediante conectores compatibles y otros no compatibles con el modo FIPS 140-2, debe tener dos instancias remotas de Collector Manager: una que se ejecute en modo FIPS 140-2 para los conectores compatibles con FIPS y otra que se ejecute en modo diferente de FIPS (normal) para los conectores que no son compatibles con el modo FIPS 140-2.

Debe realizar el siguiente procedimiento si su entorno requiere la recopilación de datos de orígenes de eventos que utilicen conectores compatibles con el modo FIPS 140-2 y conectores que no son compatibles con dicho modo.

1 Debe tener un servidor Sentinel en el modo FIPS 140-2.

Nota: Si su servidor Sentinel (recién instalado o actualizado) no tiene habilitado el modo FIPS, debe habilitar FIPS en el servidor Sentinel. Para obtener más información, consulte la "Habilitar el servidor Sentinel para su ejecución en modo FIPS 140-2" en la página 131.

---

2 Asegúrese de que una instancia remota de Collector Manager se ejecute en modo FIPS 140-2 y otra instancia remota de Collector Manager siga ejecutándose en un modo diferente.

2a Si no tiene una instancia remota de Collector Manager con el modo FIPS 140-2 habilitado, debe habilitar el modo FIPS en la instancia remota de Collector Manager. Para obtener más información, consulte la "Habilitar el modo FIPS 140-2 en las instancias remotas de Collector Manager y Correlation Engine" en la página 132.

2b Actualice el certificado del servidor en la instancia remota de Collector Manager sin modo FIPS. Para obtener más información, consulte la "Actualización de certificados del servidor en instancias remotas de Collector Manager y Correlation Engine" en la página 135.

3 Asegúrese de que las dos instancias remotas de Collector Manager se comuniquen con el servidor Sentinel habilitado para FIPS 140-2.

4 Configure las instancias remotas de Correlation Engine, si las hay, para que se ejecuten en modo FIPS 140-2. Para obtener más información, consulte la “Habilitar el modo FIPS 140-2 en las instancias remotas de Collector Manager y Correlation Engine” en la página 132.

5 Configure los módulos auxiliares (plug-ins) de Sentinel para que se ejecuten en modo FIPS 140-2. Para obtener más información, consulte la “Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2” en la página 136.

5a Implemente conectores compatibles con el modo FIPS 140-2 en la instancia remota de Collector Manager que se ejecuta en modo FIPS.

5b Implemente los conectores que no son compatibles con el modo FIPS 140-2 en la instancia remota de Collector Manager que no tiene habilitado el modo FIPS.

8 Puertos utilizados

Sentinel utiliza diversos puertos para la comunicación externa con otros componentes. Para la instalación del dispositivo, los puertos se abren en el cortafuegos por defecto. No obstante, para la instalación tradicional, es necesario configurar el sistema operativo en el que va a instalar Sentinel para poder abrir los puertos en el cortafuegos.

Puertos del servidor Sentinel

El servidor Sentinel utiliza los siguientes puertos para las comunicaciones internas y externas.

Puertos locales

Sentinel utiliza los siguientes puertos para la comunicación interna con la base de datos y demás procesos internos:

Puertos	Descripción
TCP 27017	Se utiliza para la base de datos de configuración Inteligencia de seguridad.
TCP 28017	Se utiliza para la consola Web de la base de datos Inteligencia de seguridad.
TCP 32000	Se utiliza para la comunicación interna entre el proceso empaquetador (wrapper) y el proceso del servidor.
TCP 9200	Se utiliza para la comunicación con el servicio de indexado de alertas mediante REST.
TCP 9300	Se utiliza para la comunicación con el servicio de indexado de alertas mediante el protocolo nativo.

Puertos de red

Para que Sentinel funcione correctamente, asegúrese de que estén abiertos en el cortafuegos los siguientes puertos:

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 5432	Entrante	Opcional. Por defecto, este puerto solo escucha la interfaz de retrobucle.	Se utiliza para la base de datos PostgreSQL. No es necesario abrir este puerto por defecto. No obstante, debe abrir este puerto cuando elabore informes utilizando el SDK de Sentinel. Para obtener más información, consulte el SDK de módulos auxiliares (plug-in) de Sentinel.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 1099 y 2000	Entrante	Requerido	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).
TCP 1289	Entrante	Opcional	Se utiliza para las conexiones de Audit.
UDP 1514	Entrante	Opcional	Se utiliza para los mensajes de syslog.
TCP 8443	Entrante	Requerido	Se utiliza para la comunicación de HTTPS.
TCP 1443	Entrante	Opcional	Se utiliza para los mensajes de syslog con SSL cifrado.
TCP 61616	Entrante	Opcional	Se utiliza para las conexiones entrantes de instancias de Collector Manager y Correlation Engine.
TCP 10013	Entrante	Requerido	Utilizados por Solution Designer y Control Center de Sentinel.
TCP 1468	Entrante	Opcional	Se utiliza para los mensajes de syslog.
TCP 10014	Entrante	Opcional	Lo utilizan las instancias remotas de Collector Manager con el fin de conectar con el servidor a través de un proxy de SSL. Sin embargo, esto es poco común. Por defecto, las instancias remotas de Collector Manager utilizan el puerto SSL 61616 para conectar con el servidor.
TCP 443	Saliente	Opcional	Si se utiliza el Asesor, el puerto inicia una conexión con el servicio del Asesor a través de Internet en la página de actualizaciones del Asesor.
TCP 8443	Saliente	Opcional	Si se utiliza la federación de datos, el puerto inicia una conexión con otros sistemas Sentinel para llevar a cabo la búsqueda distribuida.
TCP 389 o 636	Saliente	Opcional	Si se utiliza la autenticación LDAP, el puerto inicia una conexión con el servidor LDAP.
TCP/UDP 111 y TCP/UDP 2049	Saliente	Opcional	Si está configurado el almacenamiento secundario para usar NFS.
TCP 137, 138, 139, 445	Saliente	Opcional	Si está configurado el almacenamiento secundario para usar CIFS.
TCP JDBC (dependiente de la base de datos)	Saliente	Opcional	Si se utiliza sincronización de datos, el puerto inicia una conexión con la base de datos de destino mediante JDBC. El puerto utilizado depende de la base de datos de destino.
TCP 25	Saliente	Opcional	Inicia una conexión con el servidor de correo.
TCP 1290	Saliente	Opcional	Cuando Sentinel reenvía eventos a otro sistema Sentinel, este puerto inicia una conexión de Sentinel Link a ese sistema.
UDP 162	Saliente	Opcional	Cuando Sentinel reenvía eventos al sistema que recibe mensajes de alerta de SNMP, el puerto envía un paquete al receptor.
UDP 514 o TCP 1468	Saliente	Opcional	Este puerto se utiliza cuando Sentinel reenvía eventos al sistema que recibe mensajes de Syslog. Si el puerto es UDP, envía un paquete al receptor. Si el puerto es TCP, inicia una conexión con el receptor.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 9443	Entrante	Opcional	Este puerto permite que un sistema de Sentinel reciba eventos de otro software SIEM, como Change Guardian y Secure Configuration Manager.

Puertos específicos del dispositivo del servidor Sentinel

Además de los puertos anteriores, están abiertos los siguientes puertos para el dispositivo.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 22	Entrante	Requerido	Se utiliza para el acceso mediante secure shell al dispositivo Sentinel
TCP 4984	Entrante	Requerido	También lo utiliza el dispositivo Sentinel para el servicio de actualización.
TCP 289	Entrante	Opcional	Se reenvía a 1289 para las conexiones de auditoría.
TCP 443	Entrante	Opcional	Se remite a 8443 para la comunicación HTTPS.
UDP 514	Entrante	Opcional	Se reenvía a 1514 para los mensajes de syslog.
TCP 1290	Entrante	Opcional	Puerto de Sentinel Link al que se permite conectar a través del cortafuegos de SuSE.
UDP y TCP 40000 - 41000	Entrante	Opcional	Puertos que pueden utilizarse al configurar los servidores de recopilación de datos, como syslog. Sentinel no escucha estos puertos por defecto.
TCP 443 o 80	Saliente	Requerido	Inicia una conexión al repositorio de actualización del software del dispositivo de en Internet o a un servicio de Subscription Management Tool de su red.
TCP 80	Saliente	Opcional	Inicia una conexión a Subscription Management Tool.
TCP 7630	Entrante	Requerido	Utilizado por High Availability Web Konsole (Hawk).
TCP 9443	Entrante	Requerido	Utilizado por la consola de gestión del dispositivo de Sentinel.
TCP 1098 y 2000	Entrante	Requerido	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).

Puertos de Collector Manager

Collector Manager utiliza los siguientes puertos para comunicarse con otros componentes.

Puertos de red

Para que Collector Manager de Sentinel funcione correctamente, asegúrese de que estén abiertos en el cortafuegos los siguientes puertos:

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 1289	Entrante	Opcional	Se utiliza para las conexiones de Audit.
UDP 1514	Entrante	Opcional	Se utiliza para los mensajes de syslog.
TCP 1443	Entrante	Opcional	Se utiliza para los mensajes de syslog con SSL cifrado.
TCP 1468	Entrante	Opcional	Se utiliza para los mensajes de syslog.
TCP 1099 y 2000	Entrante	Requerido	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).
TCP 61616	Saliente	Requerido	Inicia una conexión con el servidor Sentinel.
TCP 8443	Saliente	Requerido	Inicia una conexión con el puerto del servidor Web de Sentinel. Deje abierto este puerto solo durante la instalación y configuración de Collector Manager.

Puertos específicos del dispositivo de Collector Manager

Además de los puertos anteriores, los siguientes puertos están abiertos para el dispositivo de Collector Manager de Sentinel.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 22	Entrante	Requerido	Se utiliza para el acceso mediante secure shell al dispositivo Sentinel
TCP 4984	Entrante	Requerido	También lo utiliza el dispositivo Sentinel para el servicio de actualización.
TCP 289	Entrante	Opcional	Se reenvía a 1289 para las conexiones de auditoría.
UDP 514	Entrante	Opcional	Se reenvía a 1514 para los mensajes de syslog.
TCP 1290	Entrante	Opcional	Este es el puerto de Sentinel Link al que se permite conectar a través del cortafuegos de SuSE.
UDP y TCP 40000 - 41000	Entrante	Opcional	Se utiliza durante la configuración de servidores de recopilación de datos, como syslog. Sentinel no escucha estos puertos por defecto.
TCP 443	Saliente	Requerido	Inicia una conexión al repositorio de actualización del software del dispositivo de en Internet o a un servicio de Subscription Management Tool de su red.
TCP 80	Saliente	Opcional	Inicia una conexión a Subscription Management Tool.
TCP 9443	Entrante	Requerido	Utilizado por la consola de gestión del dispositivo de Sentinel.
TCP 1098 y 2000	Entrante	Requerido	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).

Puertos de Correlation Engine

Correlation Engine utiliza los siguientes puertos para comunicarse con otros componentes.

Puertos de red

Para que Correlation Engine de Sentinel funcione correctamente, asegúrese de que los siguientes puertos estén abiertos en el cortafuegos:

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 1099 y 2000	Entrante	Requerido	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).
TCP 61616	Saliente	Requerido	Inicia una conexión con el servidor Sentinel.
TCP 8443	Saliente	Requerido	Inicia una conexión con el puerto del servidor Web de Sentinel. Deje abierto este puerto solo durante la instalación y configuración de Correlation Engine.

Puertos específicos del dispositivo de Correlation Engine

Además de los puertos anteriores, los siguientes puertos están abiertos en el dispositivo de Correlation Engine de Sentinel.

Puertos	Dirección	Necesario/ Opcional	Descripción
TCP 22	Entrante	Requerido	Se utiliza para el acceso mediante secure shell al dispositivo Sentinel
TCP 4984	Entrante	Requerido	También lo utiliza el dispositivo Sentinel para el servicio de actualización.
TCP 443	Saliente	Requerido	Inicia una conexión al repositorio de actualización del software del dispositivo de en Internet o a un servicio de Subscription Management Tool de su red.
TCP 80	Saliente	Opcional	Inicia una conexión a Subscription Management Tool.
TCP 9443	Entrante	Requerido	Utilizado por la consola de gestión del dispositivo de Sentinel.
TCP 1098 y 2000	Entrante	Requerido	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).

Puertos de almacenamiento ampliable

Para que SSDM se comunique correctamente con CDH y Elasticsearch, asegúrese de que están abiertos en el firewall los puertos especificados durante la configuración del almacenamiento escalable, así como los puertos requeridos por Cloudera y los puertos enumerados en la sección Puertos del servidor Sentinel.

9 Opciones de instalación

Puede realizar una instalación tradicional de Sentinel o instalar el dispositivo. En este capítulo se proporciona información sobre las dos opciones de instalación.

Instalación tradicional

La instalación tradicional instala Sentinel en un sistema operativo existente, mediante el instalador de la aplicación. Puede instalar Sentinel de las formas siguientes:

- **Interactivo:** la instalación se lleva a cabo con datos que introduce el usuario. Durante la instalación, puede registrar las opciones de instalación (valores introducidos por el usuario o valores por defecto) en un archivo, que podrá utilizar posteriormente para una instalación en modo silencioso. Puede realizar una instalación estándar o personalizada.

Instalación estándar	Instalación personalizada
Utiliza los valores por defecto para la configuración. Sólo se requiere la intervención del usuario para introducir la contraseña.	Le indica que debe especificar valores de configuración. Puede seleccionar valores por defecto o especificar los valores necesarios.
Se instala con una clave de evaluación por defecto.	Le permite realizar la instalación con la clave de licencia de evaluación por defecto o con una clave de licencia válida.
Permite especificar la contraseña del administrador y utiliza esta contraseña como contraseña por defecto tanto para el usuario dbauser como appuser.	Permite especificar la contraseña del administrador. Para dbauser y appuser, puede especificar una contraseña nueva o usar la contraseña del administrador.
Instala los puertos por defecto para todos los componentes.	Le permite especificar puertos para diferentes componentes.
Instala Sentinel en modo diferente de FIPS.	Permite instalar Sentinel en modo FIPS 140-2.
Utiliza almacenamiento tradicional para almacenar eventos y datos en bruto.	Permite utilizar almacenamiento ampliable para almacenar eventos y datos en bruto.
Autentica los usuarios con la base de datos interna.	Proporciona la opción de establecer autenticación LDAP para Sentinel además de autenticación de la base de datos. Al configurar Sentinel para la autenticación LDAP, los usuarios pueden entrar en el servidor utilizando sus credenciales de Novell eDirectory o de Microsoft Active Directory.

  Para obtener más información sobre una instalación interactiva, consulte la “Realización de una instalación interactiva” en la página 91.

- **Silencio:** Si desea instalar varios servidores de Sentinel en su implantación, puede registrar las opciones de instalación durante la instalación estándar o personalizada en un archivo de configuración y luego usar el archivo para ejecutar una instalación silenciosa. Para obtener más información acerca de una instalación en modo silencioso, consulte la “Instalación silenciosa” en la página 97.

Instalación del dispositivo

La instalación del dispositivo instala tanto el sistema operativo SLES 12 SP3 de 64 bits como Sentinel.

El dispositivo Sentinel está disponible en los formatos siguientes:

- Una imagen de dispositivo OVF
- Una imagen de dispositivo ISO

Para obtener más información sobre la instalación de dispositivos, consulte el Capítulo 15, “Instalación del dispositivo”, en la página 101.

II Instalación de Sentinel

En esta sección se proporciona información sobre la instalación de Sentinel y componentes adicionales.

10 Descripción general de la instalación

La instalación predeterminada de Sentinel instala los siguientes componentes en el servidor del programa:

- **Procesos del servidor Sentinel y del servidor Web:** El proceso del servidor Sentinel maneja las peticiones de otros componentes de Sentinel y facilita la funcionalidad del sistema de forma transparente. El proceso del servidor Sentinel maneja las peticiones, por ejemplo de filtrado de datos, el procesamiento de consultas de búsqueda y la gestión de tareas administrativas que incluyen autenticación y autorización de usuarios.

  El servidor Web de Sentinel permite una conexión segura a la interfaz principal de Sentinel.
- **Base de datos de PostgreSQL:** Sentinel tiene una base de datos integrada que almacena la información de configuración de Sentinel, los datos de activos y vulnerabilidad, la información de identidad, el estado de incidencias y del flujo de trabajo, etc.
- **Base de datos MongoDB:** Almacena la inteligencia de seguridad y los datos de alertas.
- **Elasticsearch:** Indexa los eventos y las alertas para la búsqueda y la visualización.
- **Collector Manager:** Collector Manager proporciona un punto de recopilación de datos flexible para Sentinel. El instalador de Sentinel instala Collector Manager por defecto durante la instalación.
- **Elasticsearch:** Un componente de almacenamiento de datos opcional para almacenar e indexar los datos. Por defecto, Sentinel incluye un nodo de Elasticsearch. Si espera tasas elevadas de EPS, más de 2500, debe implantar nodos de Elasticsearch adicionales en un clúster.
- **Correlation Engine:** Correlation Engine procesa eventos del flujo de eventos en tiempo real para determinar si estos deberían activar alguna de las reglas de correlación.
- **Asesor:** El Asesor, con tecnología de Security Nexus, es un servicio de suscripción opcional que proporciona una correlación a nivel de dispositivo entre eventos en tiempo real, desde los sistemas de prevención y detección de intrusiones, y los resultados de la exploración de vulnerabilidades empresariales. Para más información sobre el asesor, visite “Detecting Vulnerabilities and Exploits” (Detección de vulnerabilidades y exploits) en la *Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.
- **Módulos auxiliares (plug-ins) de Sentinel:** Sentinel admite diversos módulos auxiliares (plug-ins) para ampliar y mejorar la funcionalidad del sistema. Algunos de estos módulos auxiliares ya están preinstalados. Puede descargar módulos auxiliares (plug-ins) adicionales y actualizaciones del sitio web de módulos auxiliares de Sentinel. Los módulos auxiliares (plug-ins) de Sentinel incluyen lo siguiente:
  - Recopiladores
  - Conectores
  - Reglas y acciones de correlación
  - Informes
  - Flujos de trabajo de iTRAC
  - Paquetes de soluciones

11 Lista de verificación de instalación

Asegúrese de haber realizado las siguientes tareas antes de iniciar la instalación:

- ❒ Verifique que el hardware y el software cumplen los requisitos del sistema enumerados en la Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 37.
- ❒ Si había una instalación previa de Sentinel, asegúrese de que no queden archivos ni ajustes del sistema de una instalación anterior. Para obtener más información, consulte la Apéndice B, “Desinstalación”, en la página 233.
- ❒ Si piensa instalar la versión con licencia, obtenga su clave de licencia del Centro de atención al cliente de .
- ❒ Asegúrese de que los puertos enumerados en el Capítulo 8, “Puertos utilizados”, en la página 63 estén abiertos en el cortafuegos.
- ❒ Para que el instalador de Sentinel funcione adecuadamente, el sistema debe poder enviar el nombre de host o una dirección IP válida. Para hacerlo, añada el nombre de host al archivo `/etc/hosts` en la línea que contiene la dirección IP y luego introduzca `hostname -f` para asegurarse de que el nombre de host se muestre correctamente.
- ❒ Sincronice el tiempo utilizando el protocolo de tiempo de red (NTP).
- ❒ Si tiene previsto implantar Sentinel con la configuración de almacenamiento ampliable, asegúrese de que ha instalado CDH y Elasticsearch. Para obtener más información sobre la implementación de Sentinel con almacenamiento ampliable, consulte “Instalación y configuración del almacenamiento ampliable” en la página 87.
- ❒ **En sistemas RHEL:** Para obtener un rendimiento óptimo, los ajustes de memoria deben definirse correctamente para la base de datos PostgreSQL. El parámetro SHMMAX debe ser mayor o igual que 1073741824.

  Para establecer el valor adecuado, añada la siguiente información al final del archivo `/etc/sysctl.conf`:

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```

- ❒ **Para instalaciones tradicionales:**

  El sistema operativo del servidor Sentinel debe incluir al menos los componentes del Servidor base del servidor SLES o del servidor RHEL 6. Sentinel requiere las versiones de 64 bits de los siguientes RPM:

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

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

❒ **En Sentinel con almacenamiento tradicional:**

Para ver las visualizaciones de eventos, ajuste la memoria virtual. Para ello, añada la propiedad `vm.max_map_count=262144` al archivo `/etc/sysctl.conf`.

12 Instalación y configuración de Elasticsearch

Debe instalar Elasticsearch en el modo de clúster para efectuar la indexación ampliable y distribuida de eventos. El clúster Elasticsearch que instale para Sentinel debe utilizarse para indexar solo datos de Sentinel.

Requisitos previos

Cumpla con el siguiente requisito previo antes de instalar Elasticsearch:

- En función de la tasa de EPS, implemente Elasticsearch en modo de clúster con el número de nodos y el número de réplicas que se recomienda en la página de Información técnica de Sentinel.
- Defina los descriptores de archivo añadiendo las siguientes propiedades en el archivo `/etc/security/limits.conf`:

  ```
  elasticsearch hard nofile 65536
  elasticsearch soft nofile 65536
  elasticsearch soft as unlimited
  ```

  Nota: Una vez completados los requisitos previos anteriores, ejecute el comando `sysctl -p` para volver a cargar los cambios realizados en los archivos.

Instalación y configuración de Elasticsearch

Debe instalar Elasticsearch y los módulos auxiliares (plug-ins) necesarios en cada nodo del clúster de Elasticsearch.

Para instalar y configurar Elasticsearch:

1. Instale la versión de JDK compatible con Elasticsearch.
2. Descargue la versión certificada de RPM de Elasticsearch. Para obtener información sobre la versión certificada de Elasticsearch y la URL de descarga, consulte la página de Información técnica de Sentinel.
3. Instale Elasticsearch:

   ```
   rpm -i elasticsearch-<version>.rpm
   ```

4. Realice las tareas mencionadas en pantalla en las instrucciones posteriores a la instalación de RPM.
5. Asegúrese de que el usuario de Elasticsearch tenga acceso a Java.
6. Configure el archivo `/etc/elasticsearch/elasticsearch.yml` mediante la actualización o adición de la siguiente información:

Propiedad y valor	Notas
cluster.name: <*Elasticsearch _cluster_name*>	El nombre del clúster que especifique debe ser el mismo para todos los nodos.
node.name: <*node_name*>	El nombre del nodo debe ser exclusivo para cada nodo.
network.host: _<*networkInterface*>:ipv4_	
discovery.zen.ping.unicast.hosts: [<nombre completo del nodo de Elasticsearch del servidor de Sentinel>,<*nombre completo del nodo1 de Elasticsearch*>, <*nombre completo del nodo2 de Elasticsearch*>, etc.]	
thread_pool.bulk.queue_size: 300	
thread_pool.search.queue_size: 10000	Una vez que el tamaño de la cola de búsqueda alcance el límite, Elasticsearch descartará cualquier solicitud de búsqueda que haya pendiente en la cola. Puede aumentar el tamaño de la cola de la búsqueda en función del siguiente cálculo:threadpool.search.queue_size = Número medio de consultas de widget por usuario por consola x número de particiones (por índice de día) x número de días (duración de la búsqueda)
index.codec: best_compression	
path.data: ["/<*es1*>", "/<*es2*>"]	Distribuya los datos en varias ubicaciones o discos independientes para reducir la latencia de E/S del disco. Configure varias vías para almacenar los datos de Elasticsearch. Por ejemplo /es1, /es2 y así sucesivamente. Para obtener un mejor rendimiento y facilidad de gestión, monte cada vía en un disco físico independiente (JBOD).

7. Actualice el tamaño de pila de Elasticsearch por defecto en el archivo `/etc/elasticsearch/jvm.options`.

El tamaño de la pila debe ser el 50% de la memoria del servidor. Por ejemplo, en un nodo de Elasticsearch de 24 GB, asigne 12 GB como tamaño de pila para un rendimiento óptimo.

8 Repita los pasos indicados anteriormente en cada nodo del clúster de Elasticsearch.

9 En el nodo de Elasticsearch del servidor de Sentinel, configue`/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml`, como se indica a continuación:

9a Asegúrese de que los valores de `cluster.name` y `discovery.zen.ping.unicast.hosts` del archivo `elasticsearch.yml` sean iguales a los del archivo `elasticsearch.yml` del nodo de Elasticsearch externo.

9b Especifique la dirección IP del host local seguida por la dirección IP del nodo de Elasticsearch local en la propiedad `network.host`, como se indica a continuación:

```
network.host: ["127.0.0.1","<dirección IP del nodo de Elasticsearch de Sentinel>"]
```

10 (Condicional) En Sentinel con almacenamiento tradicional, añada las direcciones IP de los nodos de Elasticsearch externos a la propiedad `ServerList` del archivo `/etc/opt/novell/sentinel/config/elasticsearch-index.properties`.

Por ejemplo: `ServerList=<IP1 de Elasticsearch >:<Puerto>,<IP2 de Elasticsearch >:<Puerto>`

11 Reinicie Sentinel:

```
rcsentinel restart
```

12 Reinicie todos los nodos de Elasticsearch:

```
/etc/init.d/elasticsearch start
```

13 Para obtener un rendimiento y estabilidad óptimos del servidor de Sentinel, configure el nodo de Elasticsearch en el servidor de Sentinel como un nodo específico `apto como nodo principal` para que todos los datos de visualización del evento se indexen en los nodos de Elasticsearch externos:

13a Entre en el servidor de Sentinel como el usuario novell.

13b Asegúrese de que todos los datos de alerta existentes se hayan transferido a nodos de Elasticsearch externos.

13c Abra el archivo `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` y añada la siguiente información:

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

13d Reinicie Elasticsearch:

```
rcsentinel stopSIdb
```

```
rcsentinel startSIdb
```

14 Pase a la “Protección de datos en Elasticsearch” en la página 79.

Protección de datos en Elasticsearch

Diversos clientes pueden acceder a los nodos del clúster de Elasticsearch como, por ejemplo, los siguientes:

- Sentinel: para obtener y presentar datos de eventos en la consola Visualización de eventos.

- Tareas de Spark que se ejecutan en los nodos de YARN NodeManager: para realizar una indexación masiva de los eventos recibidos desde Kafka (para SSDM).
- Collector Manager: para realizar una indexación masiva de eventos en Sentinel con almacenamiento tradicional.
- Otros clientes externos: para realizar operaciones personalizadas como, por ejemplo, análisis personalizados.

Sentinel proporciona un módulo auxiliar (plug-in) de seguridad para Elasticsearch denominado **elasticsearch-security-plugin** que lleva a cabo la autenticación y la autorización de acceso a Elasticsearch.

El módulo auxiliar (plug-in) utiliza un testigo SAML o una lista blanca para la validación en función del modo en que se conecten los clientes:

- Cuando un cliente envía un testigo SAML junto con la petición, el módulo auxiliar (plug-in) lo autentica en el servidor de autenticación de Sentinel. Tras una autenticación correcta, el módulo auxiliar (plug-in) permite el acceso solo a los eventos filtrados para los que el cliente tiene autorización.

  Por ejemplo, la consola (cliente) Visualización de eventos muestra solo aquellos eventos de Elasticsearch que puede ver la función de un usuario.

  Para obtener información sobre las funciones y los permisos, consulte "Creating a Role" (Creación de una función) en la *Sentinel Administration Guide* (Guía de administración de Sentinel).
- Si un cliente no puede enviar un testigo SAML, el complemento comprueba su lista blanca de clientes legítimos. Tras una validación correcta, el módulo auxiliar (plug-in) permite acceder a todos los eventos sin filtrar.
- Cuando un cliente no envía un testigo SAML válido o no tiene permiso según la lista blanca, el módulo auxiliar (plug-in) lo considera como un cliente ilegítimo y deniega el acceso al cliente.

Esta sección proporciona información sobre cómo instalar y configurar el módulo auxiliar (plug-in) de seguridad de Elasticsearch:

- "Instalación del módulo auxiliar (plug-in) de Elasticsearch" en la página 80
- "Proporcionar acceso seguro a los clientes de Elasticsearch adicionales" en la página 81
- "Actualización de la configuración del módulo auxiliar (plug-in) de Elasticsearch" en la página 83

Instalación del módulo auxiliar (plug-in) de Elasticsearch

Debe instalar el módulo auxiliar (plug-in) de seguridad de Elasticsearch en cada nodo del clúster de Elasticsearch y también en el nodo de Elasticsearch incluido en Sentinel.

Para instalar el módulo auxiliar (plug-in) de Elasticsearch (elasticsearch-security-plug-in) en el nodo de Elasticsearch incluido en Sentinel:

1. Entre en el servidor SSDM o Sentinel Main
2. Defina la vía de la variable de entorno JAVA_HOME, como se indica a continuación:

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

3. Instale el módulo auxiliar (plug-in):

   En Linux, entre como el usuario con el que se está ejecutando Elasticsearch y ejecute el siguiente comando:

```
<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
```

Cuando se le solicite para continuar con la instalación, introduzca y.

4 (Condicional) Si Elasticsearch no está escuchando en el puerto HTTP por defecto (9200), debe actualizar el número de puerto de Elasticsearch en cada entrada del archivo `<vía_instalación_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt`.

Para obtener más información, consulte "Proporcionar acceso a los clientes de Elasticsearch mediante la lista blanca" en la página 82.

5 Reinicie los servicios de indexación de Sentinel mediante el comando:

```
rcsentinel stopSIdb
rcsentinel startSIdb
```

Para instalar el módulo auxiliar (plug-in) de Elasticsearch (elasticsearch-security-plug-in) en nodos de Elasticsearch externos:

Realice los pasos siguientes en cada nodo del clúster de Elasticsearch:

1 Entre en el servidor SSDM o Sentinel Main

2 Copie el archivo `<vía_instalación_sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearch-security-plugin*.zip` en una ubicación temporal de cada nodo del clúster de Elasticsearch.

3 Instale el módulo auxiliar (plug-in):

En Linux, entre como el usuario con el que se está ejecutando Elasticsearch y ejecute el siguiente comando:

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

Cuando se le solicite para continuar con la instalación, introduzca y.

4 (Condicional) Si Elasticsearch no está escuchando en el puerto HTTP por defecto (9200), debe actualizar el número de puerto de Elasticsearch en cada entrada del archivo `<directorio_instalación_elasticsearch>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt`.

Para obtener más información, consulte "Proporcionar acceso a los clientes de Elasticsearch mediante la lista blanca" en la página 82.

5 Reinicie Elasticsearch.

Proporcionar acceso seguro a los clientes de Elasticsearch adicionales

Por defecto, los clientes de confianza, como el servidor SSDM (para la consola Visualización de eventos) y YARN NodeManagers, el servidor de Sentinel (para la consola Visualización de eventos) y RCM, tienen acceso a Elasticsearch. Si desea utilizar clientes de Elasticsearch adicionales, debe proporcionar acceso seguro a esos clientes adicionales ya sea mediante el testigo SAML o la lista blanca.

Proporcionar acceso a los clientes REST de Elasticsearch mediante el uso del testigo SAML

Si utiliza un cliente REST para tener acceso a Elasticsearch, puede incluir un testigo SAML en el encabezado de la petición, como se indica a continuación:

1. Obtenga un testigo SAML desde el servidor de autenticación de Sentinel. Para obtener más información, consulte la documentación de la API REST disponible en Sentinel.

   Haga clic en **Ayuda** > **APIs > Tutorial > API Security > Obtaining a SAML Token (Logon)**.
2. Utilice el testigo SAML en las siguientes peticiones REST: incluya el testigo SAML en el encabezado de autorización de cada petición realizada por el cliente REST. Especifique el nombre del encabezado como `Authorization` y el valor del encabezado como el <*testigo SAML*> obtenido en el paso 1.

Proporcionar acceso a los clientes de Elasticsearch mediante la lista blanca

Sentinel rellena automáticamente por defecto una lista blanca con las direcciones IP de los clientes de Elasticsearch de confianza, como el servidor SSDM (para la consola Visualización de eventos) y YARN NodeManagers, el servidor Sentinel (para el consola Visualización de eventos) y RCM. El módulo auxiliar (plug-in) de seguridad de Elasticsearch concede acceso a Elasticsearch a todos los clientes que aparecen en su lista blanca.

Para proporcionar acceso a clientes adicionales que no envían un testigo de Sentinel válido, debe añadir la dirección IP del cliente y el número de puerto HTTP del servidor de Elasticsearch a la lista blanca con el formato `dirección IP:puerto`. Debe asegurarse de que los clientes externos que añada a la lista blanca sean legítimos y de confianza para evitar el acceso no autorizado.

Para actualizar la lista blanca:

1. Entre en el servidor de Sentinel o el nodo de Elasticsearch como el usuario con el que se está ejecutando Elasticsearch.
2. Añada la entrada <IP_cliente_Elasticsearch>:<Puerto_HTTP_destino_Elasticsearch> en el archivo:
   - `<vía_instalación_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin//elasticsearch-ip-whitelist.txt` para el nodo de Elasticsearch incluido en Sentinel.
   - `<directorio_instalación_elasticsearch>/plugins/elasticsearch-security-plugin/elasticsearch-ip-whitelist.txt` para los nodos de Elasticsearch externos.

   Si hay varias entradas, añada cada una de ellas en una línea nueva y guarde el archivo.
3. Repita los pasos indicados anteriormente en cada nodo del clúster de Elasticsearch.

Actualización de la configuración del módulo auxiliar (plug-in) de Elasticsearch

En los casos en que modifique la dirección IP/nombre de host y el número de puerto de los componentes de almacenamiento ampliables o la versión de Elasticsearch y el número de puerto, debe actualizar los archivos de configuración del módulo auxiliar (plug-in) de Elasticsearch como corresponda.

Realice los pasos siguientes en cada nodo del clúster de Elasticsearch:

1. Entre en el nodo de Elasticsearch como el usuario con el que se está ejecutando Elasticsearch.
2. (Condicional) Si ha modificado las direcciones IP de YARN NodeManager, la dirección IP del servidor SSDM o de Sentinel, las direcciones IP de RCM o el número de puerto de Elasticsearch, actualice la lista blanca para garantizar que el módulo auxiliar (plug-in) de seguridad de Elasticsearch acceda a los clientes de Elasticsearch.

   Si configura SSDM o Sentinel en modo de alta disponibilidad, añada entradas para la dirección IP física de cada nodo activo y pasivo del clúster de alta disponibilidad.

   Si modifica la dirección IP física de cualquier nodo del clúster de alta disponibilidad o añade un nuevo nodo al clúster de alta disponibilidad, actualice la lista blanca con las direcciones IP físicas de los nodos modificados o recién añadidos.

   Para obtener más información, consulte “Proporcionar acceso a los clientes de Elasticsearch mediante la lista blanca” en la página 82.
3. (Condicional) Si ha modificado la dirección IP de SSDM o el servidor de Sentinel, o el número de puerto del servidor Web, actualice las propiedades `authServer.host` y `authServer.port` en los siguientes archivos y reinicie Elasticsearch:
   - `<vía_instalación_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-configuration.properties` para el nodo de Elasticsearch incluido en Sentinel.
   - `<directorio_instalación_elasticsearch>/plugins/elasticsearch-security-plugin/plugin-configuration.properties` para los nodos de Elasticsearch externos.

   Si configura SSDM o Sentinel en modo de alta disponibilidad, defina la propiedad `authServer.host` en la dirección IP virtual del clúster de alta disponibilidad.

   Si modifica la dirección IP virtual del clúster de alta disponibilidad, actualice la propiedad `authServer.host` a la dirección IP virtual modificada.
4. (Condicional) Si ha actualizado Elasticsearch a una versión más reciente, actualice la propiedad `elasticsearch.version` en los siguientes archivos y reinicie Elasticsearch:
   - `/opt/novell/sentinel/3rdparty/elasticsearch/plugins/elasticsearch-security-plugin/plugin-descriptor.properties` para el nodo de Elasticsearch incluido en Sentinel.
   - `<directorio_instalación_elasticsearch>/plugins/elasticsearch-security-plugin/plugin-descriptor.properties` para los nodos de Elasticsearch externos.

Ajuste del rendimiento para Elasticsearch

Sentinel configura automáticamente los ajustes de Elasticsearch que se describen en la tabla siguiente. Puede personalizar los ajustes de Elasticsearch según sea necesario.

Para personalizar los ajustes por defecto:

En el almacenamiento tradicional: Abra el archivo `/etc/opt/novell/sentinel/config/elasticsearch-index.properties` y actualice las propiedades que se muestran en la tabla según sea necesario.

En el almacenamiento ampliable: En la página de inicio de SSDM, haga clic en **Almacenamiento** > **Almacenamiento ampliable** > **Propiedades avanzadas** > **Elasticsearch**.

Tabla 12-1 *Propiedades de Elasticsearch*

Propiedad	Valor por defecto	Notas
elasticsearch.events.lucenefilter (opcional)		Especifique un filtro para enviar solo eventos específicos a Elasticsearch para la indexación. Por ejemplo: si especifica el valor como sev: [3-5], solo se envían los eventos con un valor de gravedad entre 3 y 5 a Elasticsearch.
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	Indica los campos de eventos que desea que indexe Elasticsearch.
es.num.shards	5	Indica el número de shards principales por índice. Puede aumentar el valor por defecto si el tamaño de shard es superior a 50 GB.
es.num.replicas	1	Indica el número de shards de réplica que debe tener cada shard principal. Se recomienda el uso de un clúster de dos nodos como mínimo, teniendo en cuenta la conmutación por error y la alta disponibilidad.

Nueva implantación del módulo auxiliar (plug-in) de Elasticsearch

Debe volver a implantar, es decir, desinstalar e instalar de nuevo el módulo auxiliar (plug-in) de seguridad de Elasticsearch en el nodo de Elasticsearch incluido en Sentinel y los nodos de Elasticsearch externos en las siguientes situaciones:

- Adición o modificación de direcciones IP de instancias remotas de Collector Manager.
- Desinstalación de instancias remotas de Collector Manager.
- Habilitación del almacenamiento ampliable tras la instalación.

Para volver a implantar el módulo auxiliar (plug-in) de Elasticsearch:

1. Entre en el servidor de Sentinel o el nodo de Elasticsearch como el usuario con el que se está ejecutando Elasticsearch.
2. Desinstale el módulo auxiliar (plug-in) mediante el siguiente comando:
   - En el nodo de Elasticsearch incluido en Sentinel: `<vía_instalación_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin remove file://localhost/<vía_instalación_sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
   - En los nodos de Elasticsearch externos: `<vía_instalación_elasticsearch> remove file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
3. Vuelva a instalar el módulo auxiliar (plug-in):
   - En el nodo de Elasticsearch incluido en Sentinel: `<vía_instalación_sentinel>/opt/novell/sentinel/3rdparty/elasticsearch/bin/elasticsearch-plugin install file://localhost/<vía_instalación_sentinel>/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
   - En los nodos de Elasticsearch externos: `<vía_instalación_elasticsearch>/bin/elasticsearch-plugin install file://localhost/etc/opt/novell/sentinel/scalablestore/elasticsearchsecurity-plugin`
4. Reinicie Elasticsearch mediante el siguiente comando:
   - En el nodo de Elasticsearch incluido en Sentinel:

     ```
     rcsentinel stopSIdb
     rcsentinel startSIdb
     ```

   - En los nodos de Elasticsearch externos:

     ```
     sudo systemctl restart elasticsearch.service
     ```

13 Instalación y configuración del almacenamiento ampliable

Complete los requisitos previos descritos en la siguiente tabla para configurar el almacenamiento ampliable como la opción de almacenamiento de datos de Sentinel:

Tabla 13-1 *Requisitos previos para habilitar el almacenamiento ampliable*

❒	Tareas	Consulte
❒	Determine el número de nodos del clúster de distribución de Hadoop y del clúster de Elasticsearch que debe configurar en función de la tasa de EPS y el número de réplicas necesarias. Determine la versión certificada de CDH y Elasticsearch.	Información técnica de Sentinel.
❒	CDH, Elasticsearch y Sentinel cuentan con su propia matriz de soporte de plataforma. Consulte la matriz de soporte de plataforma de cada uno de estos productos y determine la plataforma que desee utilizar. En Elasticsearch, se recomienda instalar RPM porque este contiene el guión init. Se instalará Elasticsearch como servicio, con la posibilidad de detenerlo e iniciarlo automáticamente durante el reinicio y las actualizaciones, de forma que no se sobrescribirán los archivos de configuración. No se admite la instalación de RPM de Elasticsearch en SLES 11. Por lo tanto, debe determinar una plataforma adecuada para Elasticsearch.	Matriz de soporte de CDH en la documentación de Cloudera. Matriz de soporte de Elasticsearch en la documentación de Elasticsearch. Matriz de soporte de Sentinel.
❒	Instale y configure CDH en el modo de clúster.	“Instalación y configuración de CDH” en la página 88.
❒	Instale y configure Elasticsearch en el modo de clúster.	“Instalación y configuración de Elasticsearch” en la página 77.
❒	Habilite el almacenamiento ampliable en Sentinel.	“Habilitación del almacenamiento ampliable” en la página 90

Instalación y configuración de CDH

En esta sección se proporciona información acerca de los valores específicos requeridos para Sentinel a la hora de instalar y configurar CDH. Para obtener más información acerca de la instalación y configuración de CHD, debe consultar la versión certificada de la documentación de Cloudera.

Sentinel es compatible con Cloudera Express, la versión gratuita de CDH. Además, Sentinel es compatible con Cloudera Enterprise, que requiere la adquisición de una licencia de Cloudera e incluye numerosas funciones que no está disponibles en la versión Cloudera Express. Si decide comenzar con Cloudera Express y, más adelante, se da cuenta de que necesita las funcionalidades disponibles en Cloudera Enterprise, puede actualizar el clúster después de adquirir la licencia de Cloudera.

- "Requisitos previos" en la página 88
- "Instalación y configuración de CDH" en la página 89

Requisitos previos

Antes de instalar CDH, debe configurar los hosts de acuerdo con los siguientes requisitos previos:

- Complete los requisitos previos que se mencionan en la documentación de Cloudera.
- Utilice el sistema de archivos ext4 o XFS para mejorar el rendimiento.
- CDH necesita determinados paquetes de sistema operativo que no se instalan de forma predeterminada. Por lo tanto, debe realizar la instalación mediante el DVD del sistema operativo correspondiente. Las instrucciones de instalación de Cloudera le guiarán acerca de los paquetes que debe instalar.
- Para los sistemas operativos de SLES, CDH requiere el paquete `python-psycopg2`. Instale el paquete `python-psycopg2`. Si desea obtener más información, consulte la documentación de openSUSE.
- Si utiliza máquinas virtuales, reserve el espacio en disco requerido en el sistema de archivos al crear nodos de máquinas virtuales. Por ejemplo, en VMware, puede utilizar un aprovisionamiento grueso.
- Asegúrese de que los nodos del clúster de Sentinel y CDH se encuentren en la misma zona horaria.
- Establezca el valor de swappiness de todos los hosts en 1 en el archivo `/etc/sysctl.conf` mediante la adición de la siguiente entrada:

  ```
  vm.swappiness=1
  ```

  Para aplicar esta configuración inmediatamente, ejecute el comando siguiente:

  ```
  sysctl -p
  ```

- La versión de JDK en CDH debe ser al menos la misma versión de JDK utilizada en Sentinel. Si la versión de JDK disponible en CDH es menor que el JDK de Sentinel, debe seguir las instrucciones para instalar el JDK manualmente, en lugar de instalar el JDK disponible en el repositorio de CDH.

  Instale JDK utilizando el archivo binario del archivo de reserva (`.tar.gz`) porque la instalación RMP de JDK causa problemas al utilizar el guión `manage_spark_jobs.sh` para enviar tareas de Spark en YARN.

  Para averiguar la versión de JDK utilizada en Sentinel, consulte las Notas de la versión de Sentinel.

Instalación y configuración de CDH

Instale la versión certificada de CDH. Para obtener información sobre la versión certificada de CDH, consulte la página de Información técnica de Sentinel. Consulte la versión certificada de la documentación de Cloudera si desea obtener instrucciones de instalación.

Mientras instala CDH, realice los siguientes pasos:

- (Condicional) Si la instalación falla durante la instalación de la base de datos PostgreSQL integrada, realice los siguientes pasos:

  ```
  mkdir -p /var/run/postgresql
  ```

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

- Si se selecciona el tipo de instalación de software en la ventana **Select Repository** (Seleccionar repositorio), asegúrese de que **Use Parcels** (Utilizar paquetes) está seleccionado y seleccione Kafka en **Additional Parcels** (Paquetes adicionales).
- Cuando añada servicios, asegúrese de que habilita los servicios siguientes:
  - Administrador de Cloudera
  - ZooKeeper
  - HDFS
  - HBase
  - YARN
  - Spark
  - Kafka

  Nota: El servidor de historial de Spark y HDFS NameNode deben instalarse en el mismo nodo para obtener una mayor fiabilidad del sistema. Para obtener información sobre la arquitectura de almacenamiento ampliable, consulte “Planificación para el almacenamiento ampliable” en la página 44.

  Al habilitar los servicios anteriores, configure el modo de alta disponibilidad para los siguientes elementos:

  - HBase HMaster
  - HDFS NameNode
  - YARN ResourceManager
- (Condicional) Si el programa de instalación no implanta la configuración del cliente debido a que falta la vía de Java, abra una nueva sesión del navegador y actualice manualmente la vía de Java como sigue:

  Haga clic en **Hosts** > **All Hosts** (Todos los hosts) > **Configuration** (Configuración) e indique la vía correcta en el campo **Java Home Directory (Directorio personal de Java)**.

Habilitación del almacenamiento ampliable

Puede habilitar el almacenamiento ampliable durante la instalación de Sentinel o después de esta. Cuando se habilita el almacenamiento ampliable durante la instalación, Sentinel permite configurar componentes de CDH con valores predeterminados. Algunas de estas configuraciones son permanentes y no se pueden cambiar. Por ejemplo, el número predeterminado de particiones para los temas de Kafka es 9 y no es posible cambiar este valor.

Si desea cambiar los valores predeterminados, debe habilitar el almacenamiento ampliable después de instalar Sentinel y, a continuación, definir las configuraciones de los componentes de CDH según sea necesario.

Para instalaciones tradicionales, puede habilitar el almacenamiento ampliable durante la instalación de Sentinel o después de la instalación de este. Para instalaciones de dispositivos, puede habilitar el almacenamiento ampliable solo después de la instalación.

En las instalaciones de actualización, puede habilitar el almacenamiento ampliable solo después de actualizar Sentinel.

Antes de continuar con la habilitación del almacenamiento ampliable, tenga a mano la lista de direcciones IP o los números de puerto y los nombres de host de los nodos de Kafka, HDFS NameNode, YARN NodeManager, ZooKeeper y Elasticsearch. Necesitará esta información cuando habilite el almacenamiento ampliable.

Para habilitar el almacenamiento ampliable durante la instalación de Sentinel, consulte “Instalación personalizada del servidor Sentinel” en la página 92.

Para habilitar el almacenamiento ampliable después de la instalación o actualización de Sentinel, consulte “Enabling Scalable Storage Post-Installation” (Habilitación del almacenamiento ampliable después de la instalación) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

14 Instalación tradicional

En este capítulo se proporciona información sobre las diversas formas de instalar Sentinel.

Realización de una instalación interactiva

En esta sección se proporciona información sobre la instalación estándar y personalizada.

Instalación estándar del servidor Sentinel

Siga los pasos indicados a continuación para llevar a cabo una instalación estándar:

1. Descargue el archivo de instalación de Sentinel del sitio Web de descargas de :
2. Especifique en la línea de comandos el siguiente comando para extraer el archivo de instalación.

   ```
   tar zxvf <install_filename>
   ```

   Reemplace <*nombre de archivo_instalación*> por el nombre real del archivo de instalación.
3. Acceda al directorio en el que ha extraído el instalador:

   ```
   cd <directory_name>
   ```

4. Especifique el siguiente comando para instalar Sentinel:

   ```
   ./install-sentinel
   ```

   O bien

   Si desea instalar Sentinel en más de un sistema, puede registrar sus opciones de instalación en un archivo. Puede utilizar este archivo para una instalación de Sentinel sin supervisión en otros sistemas. Para registrar sus opciones de instalación, especifique el siguiente comando:

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

5. Especifique el número del idioma que desea utilizar para la instalación y luego pulse Intro.

   El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.
6. Pulse la barra espaciadora para leer todo el acuerdo de licencia.
7. Introduzca `yes` o `y` para aceptar la licencia y continuar con la instalación.

   La instalación puede tardar unos segundos en cargar los paquetes de instalación y solicitar el tipo de configuración.

8 Cuando se le indique, especifique `1` para continuar con la configuración estándar.

   La instalación continúa con la clave de licencia de evaluación por defecto incluida en el instalador. En cualquier momento durante el período de evaluación o después, puede sustituir la licencia de evaluación por una clave de licencia que haya adquirido.

9 Especifique la contraseña del usuario administrador `admin`.

10 Confirme la contraseña de nuevo.

   Esta contraseña la utilizan los usuarios `admin`, `dbauser` y `appuser`.

   La instalación de Sentinel finaliza y se inicia el servidor. Puede tardarse unos segundos en iniciar todos los servicios después de la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

Para acceder a la interfaz principal de Sentinel, especifique la siguiente dirección URL en el navegador Web:

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

Donde *IP_AddressOrDNS_Sentinel_server* es la dirección IP o el nombre DNS del servidor de Sentinel y *8443* es el puerto por defecto del servidor de Sentinel.

Instalación personalizada del servidor Sentinel

Si va a instalar Sentinel con una configuración personalizada, puede personalizar la instalación de Sentinel mediante la especificación de la clave de licencia, el establecimiento de una contraseña diferente, la especificación de puertos diferentes, etc.

1 Si desea habilitar el almacenamiento ampliable, complete los requisitos previos especificados en Capítulo 13, “Instalación y configuración del almacenamiento ampliable”, en la página 87.

2 Descargue el archivo de instalación de Sentinel del sitio Web de descargas de :

3 Especifique en la línea de comandos el siguiente comando para extraer el archivo de instalación.

   ```
   tar zxvf <install_filename>
   ```

   Reemplace <*nombre de archivo_instalación*> por el nombre real del archivo de instalación.

4 Especifique el siguiente comando en la raíz del directorio extraído para instalar Sentinel:

   ```
   ./install-sentinel
   ```

   O bien

   Si desea utilizar esta configuración personalizada para instalar Sentinel en más de un sistema, puede registrar sus opciones de instalación en un archivo. Puede utilizar este archivo para una instalación de Sentinel sin supervisión en otros sistemas. Para registrar sus opciones de instalación, especifique el siguiente comando:

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

5 Especifique el número del idioma que desea utilizar para la instalación y luego pulse Intro.

   El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.

6 Pulse la barra espaciadora para leer todo el acuerdo de licencia.

7 Introduzca `yes` o `y` para aceptar el acuerdo de licencia y continuar con la instalación.

   La instalación puede tardar unos segundos en cargar los paquetes de instalación y solicitar el tipo de configuración.

8 Especifique `2` para realizar una configuración personalizada de Sentinel.

9 Introduzca `1` para usar la clave de licencia de evaluación por defecto

O bien

Introduzca `2` para especificar una clave de licencia adquirida para Sentinel.

10 Especifique la contraseña del usuario administrador `admin` y confirme de nuevo la contraseña.

11 Especifique la contraseña para el usuario de la base de datos `dbauser` y confirme de nuevo la contraseña.

La cuenta `dbauser` es la identidad utilizada por Sentinel para interactuar con la base de datos. La contraseña que introduzca aquí puede utilizarse para llevar a cabo tareas de mantenimiento de la base de datos, incluido el restablecimiento de la contraseña del administrador si se pierde o se olvida.

12 Especifique la contraseña para el usuario de la aplicación `appuser` y confirme de nuevo la contraseña.

13 Cambie las asignaciones de puertos de los servicios de Sentinel introduciendo el número deseado y luego especifique el nuevo número de puerto.

14 Después de cambiar los puertos, especifique `7` cuando haya terminado.

15 Introduzca `1` para autenticar a los usuarios utilizando únicamente la base de datos interna.

O bien

Si ha configurado un directorio LDAP en su dominio, introduzca `2` para autenticar a los usuarios mediante la autenticación de directorios LDAP.

El valor por defecto es `1`.

16 ***Si desea habilitar Sentinel en el modo FIPS 140-2***, introduzca `s`.

16a Especifique una contraseña robusta para la base de datos del almacén de claves y confirme de nuevo la contraseña.

Nota: La contraseña debe tener como mínimo siete caracteres. La contraseña debe tener al menos tres de los siguientes tipos de caracteres: dígitos, letras minúsculas en formato ASCII, letras mayúsculas en formato ASCII, caracteres no alfanuméricos en formato ASCII y caracteres que no estén en formato ASCII.

Si el primer carácter es una letra mayúscula en ASCII o si el último carácter es un dígito, estos no se cuentan.

16b Si desea insertar certificados externos en la base de datos del almacén de claves a fin de establecer confianza, pulse `s` y especifique la vía para el archivo de certificado. De lo contrario, pulse `n`

16c Lleve a cabo la configuración del modo FIPS 140-2 realizando las tareas mencionadas en el Capítulo 24, “Funcionamiento de Sentinel en el modo FIPS 140-2”, en la página 133.

17 ***Si desea habilitar el almacenamiento ampliable***, introduzca `Sí` o `s`.

Importante: Una vez habilitado el almacenamiento ampliable, no es posible revertir la configuración a menos que se vuelva a instalar Sentinel.

17a Especifique las direcciones IP o los nombres de host y números de puerto de los componentes del almacenamiento ampliable.

17b (Condicional) Si desea salir de la configuración del almacenamiento ampliable y continuar con la instalación de Sentinel, introduzca `no` o `n`.

17c Después de completar la instalación de Sentinel, realice la configuración del almacenamiento ampliable que se indica en la sección "Configuración posterior a la instalación del almacenamiento ampliable" en la página 94.

La instalación de Sentinel finaliza y se inicia el servidor. Puede tardarse unos segundos en iniciar todos los servicios después de la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

Para acceder a la interfaz principal de Sentinel, especifique la siguiente dirección URL en el navegador Web:

`https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html`

Donde <*IP_AddressOrDNS_Sentinel_server*> es la dirección IP o el nombre DNS del servidor de Sentinel y *8443* es el puerto por defecto del servidor de Sentinel.

Configuración posterior a la instalación del almacenamiento ampliable

1. Entre en el servidor SSDM.
2. Borre la caché del navegador para ver la versión de Sentinel que ha instalado.
3. Para ver eventos y alertas, añada el nodo de Elasticsearch incluido en SSDM al clúster de Elasticsearch que ha configurado para el almacenamiento ampliable:

   En el nodo de Elasticsearch local, abra el archivo `/etc/opt/novell/sentinel/3rdparty/elasticsearch/elasticsearch.yml` y añada la siguiente información:

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

   En todos los nodos de Elasticsearch externos, abra `/etc/elasticsearch/elasticsearch.yml` y realice la actualización.

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

   Nota: Asegúrese de que los valores de los parámetros del archivo `elasticsearch.yml` local y el archivo `elasticsearch.yml` de los nodos de Elasticsearch externos sean iguales, excepto `network.host` y `node.name`, ya que estos valores son exclusivos para el nodo.

4. Reinicie los servicios de indexación mediante el comando:

   ```
   rcsentinel stopSIdb
   rcsentinel startSIdb
   ```

5 Complete la configuración del almacenamiento ampliable, como se indica en las secciones siguientes:

- “Protección de datos en Elasticsearch” en la página 79
- Performance Tuning Guidelines (Directrices de ajuste del rendimiento) de la *Sentinel Administration Guide* (Guía de administración de Sentinel).
- Processing Data (Procesamiento de datos) de la *Sentinel Administration Guide* (Guía de administración de Sentinel).

Instalación de Collector Manager y Correlation Engine

Por defecto, Sentinel instala una instancia de Collector Manager y otra de Correlation Engine. Si utiliza entornos de producción, configure una implantación distribuida porque aísla los componentes de recopilación de datos en un equipo independiente, lo que es importante para manejar aumentos repentinos de procesamiento y otras anomalías con la máxima estabilidad para el sistema. Para obtener información sobre las ventajas de instalar otros componentes, consulte la “Ventajas de las implantaciones distribuidas” en la página 47.

Importante: Debe instalar las instancias adicionales de Collector Manager o Correlation Engine en sistemas independientes. Collector Manager o Correlation Engine no deben estar en el mismo sistema en el que se ha instalado el servidor Sentinel.

Lista de verificación de instalación: Asegúrese de que haya realizado las siguientes tareas antes de iniciar la instalación.

- Asegúrese de que cumple los requisitos mínimos de hardware y software. Para obtener más información, consulte la Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 37.
- Sincronice el tiempo utilizando el protocolo de tiempo de red (NTP).
- Una instancia de Collector Manager requiere conectividad de red con el puerto de bus de mensajes (61616) en el servidor Sentinel. Antes de instalar Collector Manager, asegúrese de que todos los ajustes del cortafuegos y de red puedan comunicarse a través de este puerto.

Para instalar Collector Manager y Correlation Engine, siga estos pasos:

1 Inicie la interfaz principal de Sentinel especificando la siguiente dirección URL en el navegador Web:

```
https://IP_AddressOrDNS_Sentinel_server:8443/sentinel/views/main.html
```

Donde <*IP_AddressOrDNS_Sentinel_server*> es la dirección IP o el nombre DNS del servidor de Sentinel y *8443* es el puerto por defecto del servidor de Sentinel.

Inicie sesión con el nombre de usuario y la contraseña especificados durante la instalación del servidor Sentinel.

2 En la barra de herramientas, haga clic en **Descargas**.

3 Haga clic en **Descargar instalador** en la instalación necesaria.

4 Haga clic en **Guardar archivo** para guardar el instalador en la ubicación deseada.

5 Especifique el siguiente comando para extraer el archivo de instalación.

```
tar zxvf <install_filename>
```

Reemplace <*nombre de archivo_instalación*> por el nombre de archivo de instalación.

6 Acceda al directorio en el que ha extraído el instalador.

7 Especifique el siguiente comando para instalar Collector Manager o Correlation Engine:

Para Collector Manager:

```
./install-cm
```

Para Correlation Engine:

```
./install-ce
```

o bien

Si desea instalar Collector Manager o Correlation Engine en varios sistemas, puede registrar sus opciones de instalación en un archivo. Puede utilizar este archivo para una instalación de sin supervisión en otros sistemas. Para registrar sus opciones de instalación, especifique el siguiente comando:

Para Collector Manager:

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

Para Correlation Engine:

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

8 Especifique el número del idioma que desea usar para la instalación.

El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.

9 Pulse la barra espaciadora para leer todo el acuerdo de licencia.

10 Introduzca `yes` o `y` para aceptar el acuerdo de licencia y continuar con la instalación.

La instalación puede tardar unos segundos en cargar los paquetes de instalación y solicitar el tipo de configuración.

11 Cuando se le solicite, especifique la opción adecuada para proceder con la configuración estándar o personalizada.

12 Introduzca el nombre de host del servidor de comunicaciones por defecto o la dirección IP del equipo en el que está instalado Sentinel.

13 (Condicional) Si ha elegido la configuración personalizada, especifique lo siguiente:

13a Número de puerto del canal de comunicación del servidor Sentinel.

13b Número de puerto del servidor Web de Sentinel.

14 Cuando se le solicite que acepte el certificado, ejecute el comando siguiente en el servidor de Sentinel para verificar el certificado:

Para el modo FIPS:

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

Para el modo diferente de FIPS:

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

Compare el certificado generado con el del servidor Sentinel visualizado en el Paso 12.

Nota: Si el certificado no coincide, la instalación se detiene. Vuelva a ejecutar la configuración de instalación y compruebe los certificados.

---

15 Acepte el certificado si el certificado generado coincide con el del servidor Sentinel.

16 Especifique las credenciales de cualquier usuario que desempeñe la función de administrador. Introduzca el nombre de usuario y la contraseña.

17 (Condicional) Si ha elegido la configuración personalizada, introduzca `sí` o `s` para habilitar el modo FIPS 140-2 en Sentinel y proceda con la configuración de FIPS.

18 (Condicional) Si su entorno utiliza la autenticación múltiple o segura, debe proporcionar el id de cliente de Sentinel y el secreto de cliente de Sentinel. Para obtener más información acerca de los métodos de autenticación, consulte la sección "Authentication Methods" (Métodos de autenticación) en la *Sentinel Administrator Guide* (Guía de administrador de Sentinel).

Para recuperar el secreto de cliente de Sentinel y el ID de cliente de Sentinel, vaya a la siguiente dirección URL:

`https://`*`Nombre_de_host`*`:`*`Puerto`*`/SentinelAuthServices/oauth/clients`

Dónde:

- *Nombre_de_host* es el nombre de host del servidor Sentinel.
- *Puerto* es el puerto que utiliza Sentinel (normalmente 8443).

La dirección URL especificada utiliza la sesión actual de Sentinel para recuperar el secreto de cliente de Sentinel y el ID de cliente de Sentinel.

19 (Condicional) Si ha habilitado la visualización de eventos, debe añadir Collector Manager a la lista blanca de Elasticsearch. Para obtener más información, consulte "Proporcionar acceso a los clientes de Elasticsearch mediante la lista blanca" en la página 82.

20 Continúe con la instalación según se le indique hasta finalizarla.

Instalación silenciosa

La instalación silenciosa o sin supervisión resulta útil si tiene que instalar más de un servidor Sentinel o más de una instancia de Collector Manager o Correlation Engine en su implantación. En tal caso, puede registrar los parámetros de instalación durante la instalación interactiva y luego ejecutar el archivo registrado en otros servidores.

Para llevar a cabo una instalación silenciosa, asegúrese de haber registrado los parámetros de instalación en un archivo. Para obtener información sobre cómo crear el archivo de respuesta, consulte la "Instalación estándar del servidor Sentinel" en la página 91 o la "Instalación personalizada del servidor Sentinel" en la página 92 y la "Instalación de Collector Manager y Correlation Engine" en la página 95.

Para habilitar el modo FIPS 140-2, asegúrese de que el archivo de respuesta incluya los siguientes parámetros:

- ENABLE_FIPS_MODE
- NSS_DB_PASSWORD

Para realizar una instalación en modo silencioso, siga estos pasos:

1 Descargue los archivos de instalación del sitio Web de descargas de .

2 Entre como usuario `root` al servidor donde desee instalar Sentinel, Collector Manager o Correlation Engine.

3 Especifique el siguiente comando para extraer los archivos de instalación del archivo tar:

```
tar -zxvf <install_filename>
```

Reemplace <*nombre de archivo_instalación*> por el nombre real del archivo de instalación.

4 Especifique el siguiente comando para realizar la instalación en modo silencioso:

Para el servidor Sentinel:

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

Para Collector Manager:

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

Para Correlation Engine:

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

La instalación continúa con los valores almacenados en el archivo de respuesta.

Si ya ha instalado un servidor Sentinel, puede que el inicio de todos los servicios tarde unos segundos tras la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

5 **(Condicional) Si ha elegido habilitar el modo FIPS 140-2 para el servidor Sentinel,** lleve a cabo la configuración del modo FIPS 140-2 realizando las tareas mencionadas en el Capítulo 24, “Funcionamiento de Sentinel en el modo FIPS 140-2”, en la página 133.

Instalación de Sentinel como usuario diferente de root

Si la directiva de su organización no permite ejecutar la instalación completa de Sentinel como usuario `root`, puede instalar Sentinel como usuario `diferente de root`; es decir, como el usuario `novell`. En esta instalación, algunos pasos se realizan como usuario `root` y luego se continúa la instalación de Sentinel como el usuario `novell` creado por el usuario `root`. Por último, el usuario `root` finaliza la instalación.

Si instala Sentinel como usuario `diferente de root`, deberá hacerlo como usuario novell. No se admiten las instalaciones no root que no se realicen con el usuario novell, aunque la instalación se complete correctamente.

Nota: Cuando instale Sentinel en un directorio existente que no sea el predeterminado, asegúrese de que el usuario novell tiene permisos de propiedad en el directorio. Ejecute el comando siguiente para asignar permisos de propiedad:

```
chown novell:novell <non-default installation directory>
```

---

1 Descargue los archivos de instalación del sitio Web de descargas de .

2 Especifique el siguiente comando en la línea de comandos para extraer los archivos de instalación del archivo tar:

```
tar -zxvf <install_filename>
```

Reemplace <*nombre de archivo_instalación*> por el nombre real del archivo de instalación.

3 Entre como usuario `root` al servidor donde desea instalar Sentinel as como usuario `root`.

4 Especifique el siguiente comando:

```
./bin/root_install_prepare
```

Se muestra una lista de comandos que se van a ejecutar con privilegios de usuario root. Si desea que el usuario diferente de root instale Sentinel en una ubicación diferente de la ubicación por defecto, especifique la opción --location junto con el comando. Por ejemplo:

```
./bin/root_install_prepare --location=/foo
```

El valor que utilice en la opción `--location foo` se antepone en las vías del directorio.

Además se crea un grupo `novell` y un usuario `novell`, si aún no existen.

5 Acepte la lista de comandos.

Se ejecutan los comandos visualizados.

6 Especifique el siguiente comando para cambiar al usuario diferente de root recién creado, es decir, `novell`:

```
su novell
```

7 (Condicional) Para realizar una instalación interactiva:

7a Especifique el comando adecuado dependiendo del componente que vaya a instalar:

Componente	Comando
Servidor de Sentinel	**Ubicación por defecto:** `./install-sentinel`
	Ubicación no predeterminada: `./install-sentinel --location=/foo`
Collector Manager	**Ubicación por defecto:** `./install-cm`
	Ubicación no predeterminada: `./install-cm --location=/foo`
Correlation Engine	**Ubicación por defecto:** `./install-ce`
	Ubicación no predeterminada: `./install-cm --location=/foo`

7b Continúe con el Paso 9.

8 (Condicional) Para llevar a cabo una instalación silenciosa, asegúrese de haber registrado los parámetros de instalación en un archivo. Para obtener información sobre cómo crear el archivo de respuesta, consulte la “Instalación estándar del servidor Sentinel” en la página 91 o bien la “Instalación personalizada del servidor Sentinel” en la página 92.

Para realizar una instalación silenciosa:

8a Especifique el comando adecuado dependiendo del componente que vaya a instalar:

Componente	Comando
Servidor de Sentinel	**Ubicación por defecto:** `./install-sentinel -u <archivo_respuesta>`
	Ubicación no predeterminada: `./install-sentinel --location=/foo -u <archivo_respuesta>`
Collector Manager	**Ubicación por defecto:** `./install-cm -u <archivo_respuesta>`
	Ubicación no predeterminada: `./install-cm --location=/foo -u <archivo_respuesta>`
Correlation Engine	**Ubicación por defecto:** `./install-ce -u <archivo_respuesta>`
	Ubicación no predeterminada: `./install-ce --location=/foo -u <archivo_respuesta>`

La instalación continúa con los valores almacenados en el archivo de respuesta.

8b Continúe con el Paso 12.

9 Especifique el número del idioma que desea usar para la instalación.

El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.

10 Lea el acuerdo de licencia del usuario final e introduzca `yes` o `y` para aceptar el acuerdo y continuar con la instalación.

La instalación comienza instalando todos los paquetes RPM. Esta instalación puede tardar unos segundos en finalizar.

11 Se le indicará que especifique el modo de instalación.

- Si decide continuar con la configuración estándar, continúe con el Paso 8 al Paso 10 de la "Instalación estándar del servidor Sentinel" en la página 91.
- Si decide continuar con la configuración personalizada, continúe con el Paso 8 al Paso 15 de la "Instalación personalizada del servidor Sentinel" en la página 92.

12 Entre como usuario `root` y especifique el siguiente comando para finalizar la instalación:

```
./bin/root_install_finish
```

La instalación de Sentinel finaliza y se inicia el servidor. Puede tardarse unos segundos en iniciar todos los servicios después de la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

Para acceder a la interfaz principal de Sentinel, especifique la siguiente dirección URL en el navegador Web:

`https://`*`IP_AddressOrDNS_Sentinel_server`*`:`*`8443`*`/sentinel/views/main.html`

Donde *IP_AddressOrDNS_Sentinel_server* es la dirección IP o el nombre DNS del servidor de Sentinel y *8443* es el puerto por defecto del servidor de Sentinel.

15 Instalación del dispositivo

El dispositivo Sentinel es un dispositivo de software listo para ejecutarse en función de la estructura de dispositivo común de Micro Focus. El dispositivo combina un sistema operativo SLES 12 SP3 reforzado y el servicio de actualización integrado del software de Sentinel para proporcionar una experiencia fácil y transparente al usuario, que le permite aprovechar su inversión actual. El dispositivo Sentinel proporciona una interfaz de usuario basada en la Web para configurar y supervisar el dispositivo.

La imagen del dispositivo Sentinel viene empaquetada tanto en formato ISO como OVF que pueden implantarse en los entornos virtuales. Para obtener información sobre las plataformas de virtualización compatibles, consulte el sitio Web de información técnica de .

Requisitos previos

Asegúrese de que el entorno en el que va a instalar Sentinel como dispositivo ISO cumpla los siguientes requisitos previos:

- Antes de instalar el dispositivo Sentinel, consulte las nuevas funciones y los problemas conocidos en las notas de la versión del SLES certificado.
- (Condicional) Si va a instalar un dispositivo ISO de Sentinel en un equipo físico (bare metal), descargue la imagen de disco ISO del dispositivo del sitio de asistencia técnica y cree un DVD.
- Asegúrese de que el espacio mínimo en el disco duro sea de 50 GB para que el instalador pueda realizar una propuesta de partición automática.
- Asegúrese de que el sistema disponga como mínimo de una memoria de 4 GB para la instalación. Si la memoria es inferior a 4 GB, no se completará la instalación. Si la memoria es superior a 4 GB, pero inferior al tamaño recomendado de 24 GB, la instalación muestra un mensaje que indica que hay menos memoria de la recomendada.

Instalación del dispositivo ISO de Sentinel

En esta sección se proporciona información sobre la instalación de Sentinel y de las instancias de Collector Manager y Correlation Engine utilizando la imagen del dispositivo ISO. Este formato de imagen permite generar un formato de imagen del disco completa que puede implantarse directamente en el hardware, ya sea físico (bare metal) o virtual (máquina virtual no instalada en un hipervisor) utilizando una imagen DVD de ISO de arranque.

Instalación de Sentinel

Para instalar el dispositivo ISO de Sentinel:

1. Descargue la imagen del dispositivo virtual ISO del sitio web de descargas de .
2. (Condicional) Si va a utilizar un hipervisor:

   Configure la máquina virtual mediante la imagen de dispositivo virtual ISO y actívela.

   o bien

   Grabe la imagen ISO en un DVD, configure la máquina virtual mediante el DVD y, a continuación, actívela.
3. (Condicional) Si va a instalar el dispositivo Sentinel en un equipo físico (bare metal):
   - **3a** Arranque el equipo físico de la unidad de DVD con el DVD.
   - **3b** Siga las instrucciones del asistente de instalación que se visualizan en pantalla.
   - **3c** Seleccione **Instalar servidor de sentinel <*versión*>**.
4. Seleccione el idioma que prefiera.
5. Seleccione la disposición del teclado.
6. Haga clic en **Siguiente**.
7. Lea y acepte el acuerdo de licencia del software de SUSE Enterprise Server. Haga clic en **Siguiente**
8. Lea y acepte el Acuerdo de licencia del dispositivo de servidor Sentinel. Haga clic en **Siguiente**
9. Defina las contraseñas del dispositivo Sentinel, la configuración de NTP y la zona horaria.

   Defina las credenciales del usuario `vaadmin` para entrar en la consola de gestión de dispositivos Sentinel.

   Nota: Tras la instalación, puede cambiar la configuración de NTP y la zona horaria de las siguientes formas:

   - Vaya al indicador de comandos y escriba `yast->Servicios de red->Configuración de NTP`
   - Vaya a la consola de gestión de dispositivos Sentinel y seleccione **Hora**.

   Si la hora parece no estar sincronizada inmediatamente después de la instalación, ejecute el siguiente comando para reiniciar NTP:

   ```
   rcntp restart
   ```

   ---
10. En la página Configuración de red del dispositivo de servidor Sentinel, especifique el nombre de host y el nombre de dominio. Seleccione **Dirección IP estática** o **Dirección IP DHCP**.
11. Haga clic en **Siguiente**.
12. (Condicional) Si ha seleccionado **Dirección IP estática** en el paso 10, especifique la configuración de conexión de red.
13. Haga clic en **Siguiente.**
14. Defina la contraseña de usuario de Sentinel en `admin` y, a continuación, haga clic en **Siguiente**.

    Se ha instalado el dispositivo.
15. Anote la dirección IP del dispositivo que aparece en la consola.
16. Entre a la sesión como usuario `root` en la consola para entrar en el dispositivo.

Introduzca el nombre de usuario como `root` e introduzca la contraseña que ha definido en Paso 9.

17 Pase a la “Configuración del dispositivo posterior a la instalación” en la página 106.

Instalación de las instancias de Collector Manager y Correlation Engine

El procedimiento para instalar Collector Manager o Correlation Engine es similar al procedimiento de instalación de Sentinel, excepto que es necesario descargar el archivo del dispositivo ISO adecuado desde el sitio Web de descargas.

1 Realice los pasos 1 a 13 de la “Instalación de Sentinel” en la página 102.

   La instalación comprueba si hay memoria y espacio disponible en el disco. Si la memoria disponible es inferior a 1 GB, la instalación no le permitirá continuar y el botón **Siguiente** aparece atenuado.

2 Especifique la siguiente configuración para Collector Manager o Correlation Engine:

   - **Nombre de host o dirección IP del servidor Sentinel:** especifique el nombre de host o la dirección IP de servidor Sentinel al que debe conectarse Collector Manager o Correlation Engine.
   - **Puerto del canal de comunicación de Sentinel:** especifique el número de puerto del canal de comunicación del servidor Sentinel. El número de puerto por defecto es `61616`.
   - **Puerto del servidor Web de Sentinel:** Especifique el puerto del servidor Web de Sentinel. El puerto por defecto es 8443.
   - **Nombre de usuario con la función de administrador:** Especifique el nombre de cualquier usuario que desempeñe la función de administrador.
   - **Contraseña de usuario con la función de administrador:** introduzca la contraseña del nombre de usuario especificado en el campo anterior.

3 (Condicional) Si su entorno utiliza la autenticación múltiple o segura, debe proporcionar el id de cliente de Sentinel y el secreto de cliente de Sentinel. Para obtener más información acerca de los métodos de autenticación, consulte la sección “Authentication Methods” (Métodos de autenticación) en la *Sentinel Administrator Guide* (Guía de administrador de Sentinel).

   Para recuperar el secreto de cliente de Sentinel y el ID de cliente de Sentinel, vaya a la siguiente dirección URL:

   `https://Nombre_de_host:Puerto/SentinelAuthServices/oauth/clients`

   Dónde:

   - *Nombre_de_host* es el nombre de host del servidor Sentinel.
   - *Puerto* es el puerto que utiliza Sentinel (normalmente 8443).

   La dirección URL especificada utiliza la sesión actual de Sentinel para recuperar el secreto de cliente de Sentinel y el ID de cliente de Sentinel.

4 Haga clic en **Siguiente**.

5 Acepte el certificado cuando se le indique.

6 Anote la dirección IP del dispositivo que aparece en la consola.

   La consola muestra un mensaje para indicar que el dispositivo es el Collector Manager o Correlation Engine de Sentinel, en función de lo que eligió instalar, junto con la dirección IP. También muestra la dirección IP de la interfaz del usuario del servidor Sentinel.

7 Realice el Paso 16 al Paso 17 de la “Instalación de Sentinel” en la página 102.

Instalación del dispositivo OVF de Sentinel

En esta sección se proporciona información sobre la instalación de Sentinel, Collector Manager y Correlation Engine como una imagen de dispositivo OVF.

OVF es un formato de máquina virtual estándar admitido por la mayoría de hipervisores, ya sea directamente o mediante una conversión sencilla. Sentinel admite el dispositivo OVF con dos hipervisores certificados, pero también se puede utilizar con otros hipervisores.

- "Instalación de Sentinel" en la página 104
- "Instalación de las instancias de Collector Manager y Correlation Engine" en la página 105

Instalación de Sentinel

Para instalar el dispositivo OVF de Sentinel:

1. Descargue la imagen del dispositivo virtual OVF del sitio de descargas de .
2. En la consola de gestión del hipervisor, importe el archivo de imagen OVF como nueva máquina virtual. Deje que el hipervisor convierta la imagen de OVF al formato nativo si se le indica.
3. Revise los recursos de hardware virtual asignados a su máquina virtual para asegurarse de que cumplan los requisitos de Sentinel.
4. Encienda la máquina virtual.
5. Seleccione el idioma que prefiera.
6. Seleccione la disposición del teclado.
7. Haga clic en **Siguiente**.
8. Lea y acepte el acuerdo de licencia del software de SUSE Enterprise Server. Haga clic en **Siguiente**.
9. Lea y acepte el Acuerdo de licencia del dispositivo de servidor Sentinel. Haga clic en **Siguiente**.
10. Defina las contraseñas del dispositivo Sentinel, la configuración de NTP y la zona horaria.

    Defina las credenciales del usuario `vaadmin` para entrar en la consola de gestión de dispositivos Sentinel.

    Nota: Tras la instalación, puede cambiar la configuración de NTP y la zona horaria de las siguientes formas:

    - Vaya al indicador de comandos y escriba `yast->Servicios de red->Configuración de NTP`
    - Vaya a la consola de gestión de dispositivos Sentinel y seleccione **Hora**.

    Si la hora parece no estar sincronizada inmediatamente después de la instalación, ejecute el siguiente comando para reiniciar NTP:

    ```
    rcntp restart
    ```

    ---
11. En la página Configuración de red del dispositivo de servidor Sentinel, especifique el nombre de host y el nombre de dominio. Seleccione **Dirección IP estática** o **Dirección IP DHCP**.
12. Haga clic en **Siguiente**.
13. (Condicional) Si ha seleccionado **Dirección IP estática** en el paso 11, especifique la configuración de conexión de red.
14. Haga clic en **Siguiente**.

15 Defina la contraseña del administrador de Sentinel y luego haga clic en **Siguiente**.

   Puede tardarse unos minutos en iniciar todos los servicios después de la instalación porque el sistema realiza una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

16 Anote la dirección IP del dispositivo que aparece en la consola. Utilice la misma dirección IP para acceder a la interfaz principal de Sentinel.

Instalación de las instancias de Collector Manager y Correlation Engine

Para instalar una instancia de Collector Manager o Correlation Engine en un servidor VMware ESX como imagen de dispositivo OVF:

1 Realice los pasos 1 a 14 de la "Instalación de Sentinel" en la página 104.

   La instalación comprueba si hay memoria y espacio disponible en el disco. Si la memoria disponible es inferior a 1 GB, la instalación no le permitirá continuar y el botón **Siguiente** aparece atenuado.

2 Especifique el nombre de host/la dirección IP del servidor Sentinel al que debe conectarse Collector Manager.

3 Especifique el número de puerto del servidor de comunicaciones. El puerto por defecto es el `61616`.

4 Especifique las credenciales de cualquier usuario que desempeñe la función de administrador. Introduzca el nombre de usuario y la contraseña.

5 (Condicional) Si su entorno utiliza la autenticación múltiple o segura, debe proporcionar el id de cliente de Sentinel y el secreto de cliente de Sentinel. Para obtener más información acerca de los métodos de autenticación, consulte la sección "Authentication Methods" (Métodos de autenticación) en la *Sentinel Administrator Guide* (Guía de administrador de Sentinel).

   Para recuperar el secreto de cliente de Sentinel y el ID de cliente de Sentinel, vaya a la siguiente dirección URL:

   `https://`*`Nombre_de_host`*`:`*`Puerto`*`/SentinelAuthServices/oauth/clients`

   Dónde:

   - *Nombre_de_host* es el nombre de host del servidor Sentinel.
   - *Puerto* es el puerto que utiliza Sentinel (normalmente 8443).

   La dirección URL especificada utiliza la sesión actual de Sentinel para recuperar el secreto de cliente de Sentinel y el ID de cliente de Sentinel.

6 Haga clic en **Siguiente.**

7 Acepte el certificado.

8 Haga clic en **Siguiente** para completar la instalación.

   Cuando haya finalizado la instalación, el instalador mostrará un mensaje que indica que el dispositivo es el Collector Manager o Correlation Engine de Sentinel, en función de lo que haya elegido instalar, además de la dirección IP. Además, muestra la dirección IP de la interfaz del usuario del servidor Sentinel.

Configuración del dispositivo posterior a la instalación

Después de instalar Sentinel, es necesario realizar una configuración adicional para que el dispositivo funcione correctamente.

Registro para recibir actualizaciones

Debe registrar el dispositivo Sentinel con el canal de actualización de dispositivos para recibir las actualizaciones más recientes del sistema operativo y Sentinel. Para registrar el dispositivo, primero debe obtener el código de registro de dispositivo o la clave de activación del dispositivo en el Centro de atención al cliente de .

Registrarse mediante la consola de gestión de dispositivos Sentinel

Si utiliza SLES 12 SP3, puede registrarse para recibir actualizaciones mediante la consola de gestión de dispositivos Sentinel.

1. Lance el dispositivo Sentinel mediante cualquiera de las siguientes acciones:
   - Entre en Sentinel. Haga clic en **Sentinel Main** > **Dispositivo**.
   - Especifique la siguiente dirección URL en el navegador Web: `https://<dirección_IP>:9443`.
2. Entre a la sesión como usuario `vaadmin` o `root`.
3. Haga clic en **Actualización en línea** > **Regístrese ahora**.
4. En el campo **Correo electrónico**, especifique el ID de correo electrónico en el que desea recibir actualizaciones.
5. En el campo **Clave de activación**, escriba el código de registro.
6. Haga clic en **Registrarse** para completar el registro.

Registro mediante comandos

Si utiliza SLES 11 SP4 o SLES 12 SP3, puede realizar el registro mediante comandos.

Para registrarse a fin de recibir actualizaciones

1. Entre al servidor de Sentinel como usuario `root`.
2. Especifique los siguientes comandos:
   - Para registrar el servidor, especifique: `suse_register -a regcode-sentinel="<código_registro>" -a email="<ID_correo_electrónico>"`
   - Para registrar Collector Manager, especifique: `suse_register -a regcode-sentinel-collector="<código_registro>" -a email="<ID_correo_electrónico>"`

- Para registrar Correlation Engine, especifique: `suse_register -a regcode-sentinel-correlation ="<código_registro>" -a email="<ID_correo_electrónico>"`
- Para registrar Sentinel en el modo de alta disponibilidad, especifique: `suse_register -a regcode-sentinel-ha ="<código_registro>" -a email="<ID_correo electrónico>"`

Con respecto al parámetro de correo electrónico, especifique el ID de correo electrónico en el que desea recibir actualizaciones.

Creación de particiones de almacenamiento tradicional

La información de esta sección solo es aplicable si desea utilizar el almacenamiento tradicional como la opción de almacenamiento de datos.

Una buena práctica consiste en asegurarse de que se crean particiones separadas para almacenar datos de Sentinel en una partición diferente de la de los archivos ejecutables, de configuración y del sistema operativo. Las ventajas de almacenar los datos variables por separado son la mayor facilidad de realizar copias de seguridad de los conjuntos de archivos, la recuperación más sencilla en caso de que se dañen los datos, y además fortalece el sistema en caso de que una partición se llene por completo. Para obtener información sobre cómo planificar sus particiones, consulte la "Planificación para el almacenamiento tradicional" en la página 41. Puede añadir particiones en el dispositivo y mover un directorio a la nueva partición mediante la herramienta YaST.

Utilice el siguiente procedimiento para crear una partición nueva y mover archivos de datos de su directorio a la partición recién creada:

1. Acceda a Sentinel como usuario `root`.
2. Ejecute el siguiente comando para detener Sentinel en el dispositivo:

   ```
   /etc/init.d/sentinel stop
   ```
3. Especifique el siguiente comando para cambiar al usuario `novell`:

   ```
   su -novell
   ```
4. Mueva el contenido del directorio en `/var/opt/novell/sentinel/` a una ubicación temporal.
5. Cambie al usuario `root`.
6. Introduzca el siguiente comando para acceder a Control Center de YaST2:

   ```
   yast
   ```
7. Seleccione **System > Partitioner** (Sistema > Creador de particiones).
8. Lea la advertencia y seleccione **Yes** (Sí) para añadir la nueva partición no utilizada.

   Para obtener información sobre la creación de particiones, consulte Using the YaST Partitioner (Uso del particionador de YaST) en la *documentación de SLES 11*.
9. Monte la nueva partición en `/var/opt/novell/sentinel`.
10. Especifique el siguiente comando para cambiar al usuario `novell`:

    ```
    su -novell
    ```
11. Mueva el contenido del directorio de datos de la ubicación temporal (donde se guardó en el Paso 4) de nuevo a `/var/opt/novell/sentinel/` en la nueva partición.
12. Ejecute el siguiente comando para reiniciar el dispositivo Sentinel:

    ```
    /etc/init.d/sentinel start
    ```

Configuración del almacenamiento ampliable

Para habilitar y configurar el almacenamiento ampliable como la opción de almacenamiento de datos, consulte “Configuring Scalable Storage” (Configuración de almacenamiento ampliable) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Configuración del dispositivo con SMT

En entornos protegidos en los que el dispositivo debe ejecutarse sin acceso directo a Internet, puede configurar el dispositivo con la herramienta SMT (Subscription Management Tool), que le permite actualizar el dispositivo a la versión más reciente de Sentinel a medida que se vayan lanzando. SMT es un sistema de servidor proxy integrado en el Centro de servicios al cliente que proporciona funciones clave de dicho centro.

- “Requisitos previos” en la página 108
- “Configuración del dispositivo” en la página 109
- “Actualización del dispositivo” en la página 109

Requisitos previos

Antes de configurar el dispositivo con SMT, asegúrese de que cumple los requisitos previos siguientes:

- Obtenga las credenciales del Centro de servicios al cliente para obtener actualizaciones de Sentinel. Para obtener más información sobre la forma de obtener credenciales, póngase en contacto con el servicio de asistencia técnica.
- Asegúrese de que SLES 11 SP3 esté instalado con los siguientes paquetes en el equipo donde desea instalar la herramienta SMT:
  - 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

- Instale SMT y configure el servidor de SMT. Para obtener más información, consulte las siguientes secciones de la documentación de SMT:
  - Instalación de SMT
  - Configuración del servidor de SMT
  - Duplicación de los repositorios de instalación y actualizaciones con SMT
- Instale la utilidad `wget` en el equipo del dispositivo.

Configuración del dispositivo

Realice los pasos siguientes para configurar el dispositivo con SMT:

1. Habilite los repositorios del dispositivo ejecutando los comandos siguientes en el servidor de SMT:

   ```
   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. Configure el dispositivo con SMT llevando a cabo los pasos descritos en la sección “Configuring Clients to Use SMT” (Configuración de clientes para la utilización de SMT) en la documentación de SMT.

Actualización del dispositivo

Para obtener información sobre cómo actualizar el dispositivo, consulte la “Actualización de Sentinel” en la página 159.

16 Instalación de conectores y recopiladores adicionales

Por defecto, todos los recopiladores y conectores distribuidos están instalados en Sentinel. Si desea instalar un nuevo recopilador o conector publicado después del lanzamiento de Sentinel, utilice la información de las siguientes secciones.

Instalación de un recopilador

Siga los pasos indicados a continuación para instalar un recopilador:

1. Descargue el recopilador deseado del sitio Web de módulos auxiliares (plug-ins) de Sentinel.
2. Desde **Principal de Sentinel**, haga clic en el menú desplegable **admin** y luego haga clic en **Aplicaciones**.
3. Haga clic en **Lanzar Control Center** para lanzar Control Center de Sentinel.
4. En la barra de herramientas, haga clic en **Gestión de orígenes de eventos** > **Vista activa** y luego haga clic en **Herramientas** > **Importar módulo auxiliar (plug-in)**.
5. Busque y seleccione el archivo de recopilador que descargó en el Paso 1, y luego haga clic en **Siguiente**.
6. Siga las indicaciones restantes y luego haga clic en **Finalizar**.

Para configurar el recopilador, consulte la documentación específica del recopilador en el sitio Web de módulos auxiliares (plug-ins) de Sentinel.

Instalación de un conector

Siga los pasos indicados a continuación para instalar un conector:

1. Descargue el conector deseado del sitio Web de módulos auxiliares (plug-ins) de Sentinel.
2. En **Principal de Sentinel**, haga clic en el menú desplegable **admin** y luego haga clic en **Aplicaciones**.
3. Haga clic en **Lanzar Control Center** para lanzar Control Center de Sentinel.
4. En la barra de herramientas, seleccione **Gestión de orígenes de eventos** > **Vista activa** y luego haga clic en **Herramientas** > **Importar módulo auxiliar (plug-in)**.
5. Busque y seleccione el archivo de conector que descargó en el Paso 1, y luego haga clic en **Siguiente**.
6. Siga las indicaciones restantes y luego haga clic en **Finalizar**.

Para configurar el conector, consulte la documentación específica del conector en el sitio Web de módulos auxiliares (plug-ins) de Sentinel.

17 Verificación de la instalación

Puede determinar si la instalación se realizó correctamente mediante los siguientes pasos:

- Verificación de la versión de Sentinel:

  ```
  /etc/init.d/sentinel version
  ```

- Compruebe si los servicios de Sentinel están activos y funcionan en modo FIPS o diferente de FIPS:

  ```
  /etc/init.d/sentinel status
  ```

- Verifique si los servicios Web funcionan y están activos:

  ```
  netstat -an |grep 'LISTEN' |grep <HTTPS_port_number>
  ```

  El número de puerto por defecto es 8443.

- Lance Sentinel:

  1. Inicie un navegador Web compatible.
  2. Especifique la dirección URL de Sentinel:

     ```
     https://IP_AddressOrDNS_Sentinel_server:8443
     ```

     Donde *IP_AddressOrDNS_Sentinel_server* es la dirección IP o el nombre DNS del servidor de Sentinel y *8443* es el puerto por defecto del servidor de Sentinel.
  3. Entre a una sesión con el nombre y la contraseña del administrador especificados durante la instalación. El nombre de usuario por defecto es admin.

IV Configuración de Sentinel

En esta sección se proporciona información sobre la configuración de Sentinel y sobre los módulos auxiliares (plug-ins) genéricos de Sentinel.

18 Configuración de la hora

La hora de un evento es crucial para su procesamiento en Sentinel. Es importante para la generación de informes y para fines de auditoría, además de para el procesamiento en tiempo real. En esta sección se proporciona información para comprender el tiempo en Sentinel, cómo configurar la hora y cómo manejar las zonas horarias.

Comprender el tiempo en Sentinel

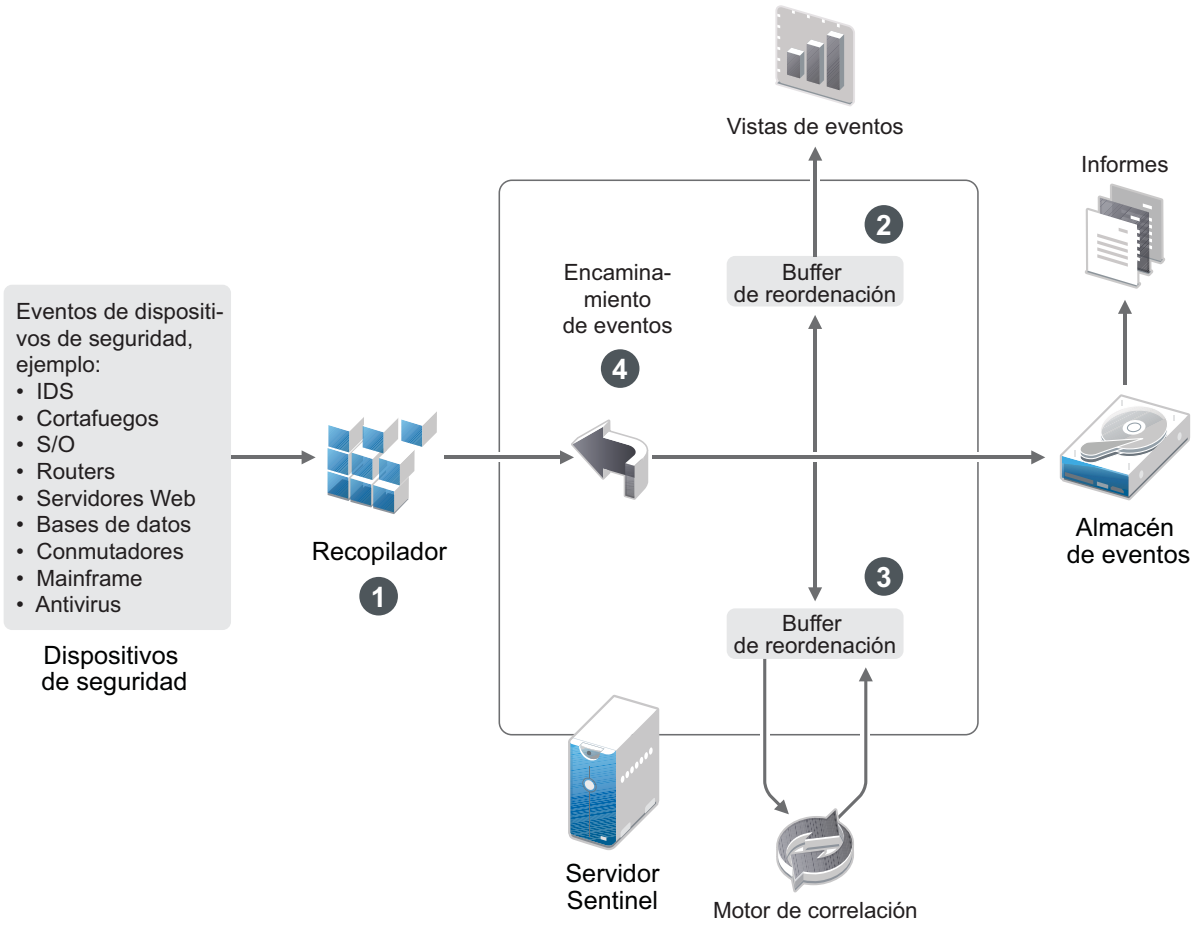
Sentinel es un sistema distribuido compuesto por varios procesos distribuidos a través de la red. Además, puede haber algún retraso introducido por el origen de evento. Para adaptarlo, los procesos de Sentinel reordenan los eventos en un flujo ordenado por tiempo antes de procesarlos.

Cada evento tiene tres campos de tiempo:

- **Hora del evento:** este tiempo u hora del evento lo utilizan todos los motores analíticos, las búsquedas, los informes, etc.
- **Hora de proceso de Sentinel:** la hora a la que Sentinel recopiló los datos del dispositivo, que se obtiene de la hora del sistema de Collector Manager.
- **Hora del evento del observador:** se trata de la marca horaria que el dispositivo pone en los datos. Los datos podrían no incluir siempre una marca horaria fiable y puede ser bastante diferente de la hora de proceso de Sentinel. Por ejemplo, cuando el dispositivo proporciona los datos por lotes.

La siguiente ilustración explica cómo Sentinel realiza esta acción en una configuración de almacenamiento tradicional:

Figura 18-1 *Hora de Sentinel*



1. Por defecto, la hora del evento se define en la hora de proceso de Sentinel. Lo ideal, sin embargo, es que la hora del evento coincida con la hora del evento del observador, si está disponible y es de confianza. Lo mejor es configurar la recopilación de datos en **Hora del origen de eventos predeterminado** si está disponible la hora del dispositivo, es exacta y es analizada correctamente por el recopilador. El recopilador define la hora del evento para que coincida con la hora del evento del observador.
2. Los eventos que tienen una hora de evento dentro de un intervalo de 5 minutos con respecto a la hora del servidor (anterior o posterior) se procesan normalmente en Vistas de eventos. Los eventos que tienen una hora del evento más de 5 minutos posterior no se muestran en las Vistas de eventos, pero se ingresan en el almacén de eventos. Los eventos que tienen una hora del evento más de 5 minutos posterior y menos de 24 horas anterior siguen mostrándose en los diagramas, pero no se muestran en los datos de eventos de dicho diagrama. Es necesaria una operación en profundidad para recuperar esos eventos del almacén de eventos.
3. Los eventos se clasifican en intervalos de 30 segundos para que Correlation Engine pueda profesarlos en orden cronológico. En el caso de que la hora del evento sea más de 30 segundos anterior a la hora del servidor, Correlation Engine no procesará los eventos.
4. Si la hora del evento es más de 5 minutos anterior a la hora del sistema de Collector Manager, Sentinel encamina directamente los eventos al almacén de eventos, omitiendo los sistemas en tiempo real como Correlation Engine e Inteligencia de seguridad.

Configuración de la hora en Sentinel

Correlation Engine procesa flujos de eventos ordenados por tiempo y detecta patrones dentro de los eventos, además de patrones temporales en el flujo. Sin embargo, el dispositivo que generó el evento podría no incluir la hora en sus mensajes de registro.

Para configurar la hora para que funcione correctamente con Sentinel, tiene dos opciones:

- Configure NTP en Collector Manager y deseleccione **Hora del origen de eventos predeterminado** en el origen de eventos del Gestor de orígenes de eventos. Sentinel utiliza Collector Manager como origen de la hora de los eventos.
- Seleccione **Hora del origen de eventos predeterminado** en el origen de evento del Gestor de orígenes de eventos. Sentinel utiliza la hora del mensaje de registro como la hora correcta.

Para cambiar este ajuste en el origen de evento:

1. Entre en Gestión de orígenes de eventos.

   Para obtener más información, consulte “Accessing Event Source Management” (Cómo acceder a Gestión de orígenes de eventos) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).
2. Haga clic con el botón derecho del ratón en el origen de evento cuya hora desea cambiar y luego seleccione **Editar**.
3. Seleccione o deseleccione **Origen de eventos predeterminado** en la parte de abajo de la pestaña **General**.
4. Haga clic en **Aceptar** para guardar el cambio.

Configuración del límite de tiempo de demora para los eventos

Cuando Sentinel recibe eventos de los orígenes de eventos, puede producirse un retraso entre el tiempo en que se generó el evento y el tiempo que tarda Sentinel en procesarlo. Sentinel almacena los eventos con grandes demoras en particiones separadas. Si muchos eventos sufren una demora por un período de tiempo prolongado, podría indicar que un origen de eventos está configurado incorrectamente. Esto podría perjudicar el rendimiento de Sentinel cuando trate de manejar estos eventos demorados. Puesto que la demora de los eventos puede ser consecuencia de una mala configuración y, en ese caso, quizá no sea aconsejable almacenarlos, Sentinel le permite configurar un tiempo de demora aceptable para los eventos entrantes. El router de eventos abandona los eventos que exceden el límite de demora. Especifique el límite de demora en la siguiente propiedad del archivo`configuration.properties`:

```
esecurity.router.event.delayaccepttthreshold = <time in milliseconds>
```

También puede registrar periódicamente una lista en el archivo de registro del servidor Sentinel que muestre los orígenes de eventos de los que se reciben eventos demorados más allá de un umbral específico. Para registrar esta información, especifique el umbral en la siguiente propiedad del archivo `configuration.properties`:

```
sentinel.indexedlog.eventdelay.reportthreshold= <time in milliseconds>
```

Cómo manejar las zonas horarias

El manejo de las zonas horarias puede llegar a ser muy complejo en un entorno distribuido. Por ejemplo, podría tener un origen de evento en una zona horaria, Collector Manager en otra zona, el servidor Sentinel posterior en otra y el cliente podría visualizar los datos en otra zona horaria. Si además se añade el componente del horario de verano y los numerosos orígenes de eventos que no informan de la zona horaria en la que están definidos (por ejemplo, los orígenes de syslog), son numerosos los problemas a tener en cuenta. Sentinel es flexible para que pueda representar adecuadamente la hora a la que los eventos ocurren realmente, y comparar esos eventos con eventos de otros orígenes de la misma zona horaria o zonas horarias diferentes.

En general, tres escenarios diferentes representan la forma en que los orígenes de eventos informan de las marcas horarias:

- El origen de evento informa de la hora en UTC. Por ejemplo, todos los eventos del Registro de eventos de Windows siempre se informan en UTC.
- El origen de evento se informa en la hora local, pero siempre incluye la zona horaria en la marca horaria. Por ejemplo, cualquier origen de evento que siga el formato RFC3339 para la estructuración de marcas horarias incluye la zona horaria como diferencia horaria; otros orígenes informan IDs de zona horaria en formato largo, como América/Nueva York, o en formato corto como EST, lo cual puede presentar problemas debido a conflictos y resoluciones inadecuadas.
- El origen de evento informa de la hora local, pero no indica la zona horaria. Desgraciadamente, el formato syslog tan común sigue este modelo.

Para el primer escenario, siempre es posible calcular la hora UTC absoluta a la que se produjo un evento (suponiendo que se está utilizando un protocolo de sincronización horaria), de manera que se puede comparar fácilmente la hora del evento con cualquier otro origen de evento en el mundo. Sin embargo, no es posible determinar automáticamente la hora local a la que ocurrió el evento. Por este motivo, Sentinel permite a los clientes definir manualmente la zona horaria de un origen de evento editando el nodo Origen de evento en el Gestor de orígenes de eventos y especificando la zona horaria adecuada. Esta información no afecta al cálculo de la hora del evento del dispositivo (DeviceEventTime) o la hora del evento (EventTime), pero se coloca en el campo de zona horaria de observador (ObserverTZ), y se utiliza para calcular varios campos de zona horaria del observador (ObserverTZ), como hora de la zona horaria del observador (ObserverTZHour). Estos campos siempre se expresan en la hora local.

En el segundo escenario, si se utilizan las IDs de zona horaria de formato largo o diferencias horarias, es posible convertir al formato UTC para obtener la hora UTC canónica absoluta (guardada en DeviceEventTime), pero también se pueden calcular los campos ObserverTZ de hora local. Si se utiliza la ID de zona horaria de formato corto, existe la posibilidad de que surjan conflictos.

El tercer escenario requiere que el administrador defina manualmente la zona horaria del origen del evento para todos los orígenes afectados de manera que Sentinel pueda calcular correctamente la hora UTC. Si la zona horaria no se especifica correctamente editando el nodo de Origen de eventos en el Gestor de orígenes de eventos, entonces puede que DeviceEventTime (y probablemente EventTime) sea incorrecto; además, el campo ObserverTZ y sus campos asociados podrían ser incorrectos.

En general, el recopilador de un tipo determinado de origen de evento (por ejemplo, Microsoft Windows) sabe cómo un origen de evento presenta las marcas horarias y se ajusta en la forma adecuada. Siempre es una buena directiva definir manualmente la zona horaria para todos los nodos de orígenes de eventos en el gestor de orígenes de eventos, a menos que el origen del evento informe la hora local y siempre incluya la zona horaria en su marca horaria.

El procesamiento de la presentación de la marca horaria en el origen del evento tiene lugar en el recopilador y en Collector Manager. Los campos DeviceEventTime y EventTime se almacenan como UTC, y los campos de ObserverTZ se almacenan como cadenas definidas en la hora local del origen de evento. Esta información se envía desde Collector Manager al servidor Sentinel y se guarda en el almacén de eventos. La zona horaria en la que se encuentran Collector Manager y el servidor Sentinel no debería afectar a este proceso ni a los datos almacenados. Sin embargo, cuando un cliente visualiza el evento en un navegador Web, la hora UTC del evento se convierte a la hora local en función del navegador Web, de manera que todos los eventos se presentan a los clientes en la zona horaria local. Si los usuarios desean ver la hora local del origen, pueden examinar los campos ObserverTZ para obtener más detalles.

19 Protección de datos en Elasticsearch

Sentinel utiliza Kibana, una consola de análisis y búsqueda basada en navegador, que ayuda a visualizar eventos y alertas en consolas. Sentinel almacena e indexa alertas en Elasticsearch. Puede configurar Sentinel para almacenar e indexar también eventos de Elasticsearch a fin de aprovechar las funciones visualización de eventos. Las consolas de Sentinel acceden a los datos de Elasticsearch para presentar eventos y alertas en consolas. Para garantizar que en las consolas solo se muestren los datos que puede ver la función de un usuario y evitar el acceso no autorizado a los datos de Elasticsearch, debe instalar el módulo auxiliar (plug-in) de seguridad de Elasticsearch. Para obtener más información, consulte “Protección de datos en Elasticsearch” en la página 79.

20 Habilitación de la visualización de eventos

En una configuración de almacenamiento ampliable, hay disponibles por defecto visualizaciones de eventos. En una configuración de almacenamiento tradicional, las visualizaciones de eventos solo están disponibles si se ha habilitado el almacén de datos de visualización (Elasticsearch) para almacenar e indexar datos.

Requisitos previos

Para la indexación ampliable y distribuida de eventos en entornos de producción, debe configurar nodos de Elasticsearch adicionales en modo de clúster. Para instalar y configurar Elasticsearch en modo de clúster, consulte “Instalación y configuración de Elasticsearch” en la página 77.

Habilitación de la visualización de eventos

Para habilitar la visualización de eventos:

1. Entre en el servidor de Sentinel como el usuario novell.
2. Abra el archivo `/etc/opt/novell/sentinel/config/configuration.properties`.
3. Defina `eventvisualization.traditionalstorage.enabled` en `true` (verdadero).
4. Actualice la interfaz de usuario tras unos minutos para ver las visualizaciones de eventos.

   Ahora debería ver todas las consolas habilitadas en la interfaz de usuario de **Mi Sentinel**. Lance cualquier consola como, por ejemplo, Búsqueda de amenazas y haga clic en **Buscar**. En la consola, se muestran todos los eventos generados en la última hora.
5. (Opcional) En las consolas de visualización de eventos, solo se muestran los eventos procesados después de habilitar la visualización de eventos. Para ver los eventos existentes presentes en el almacenamiento basado en archivos, debe migrar los datos del almacenamiento basado en archivos a Elasticsearch. Para obtener más información, consulte Capítulo 33, “Migración de datos a Elasticsearch”, en la página 183.

Nota: Al habilitar o inhabilitar la visualización de eventos, se genera una excepción mientras se reinician los servicios de indexación de Sentinel. Se espera que reciba esta excepción, por lo que puede omitirla.

---

21 Modificación de la configuración después de la instalación

Después de instalar Sentinel, si desea introducir una clave de licencia válida, cambiar la contraseña o modificar cualquiera de los puertos asignados, puede ejecutar el guión `configure.sh` para modificarlos. El guión se encuentra en la carpeta `/opt/novell/sentinel/setup`.

1. Apague Sentinel utilizando el siguiente comando:

   ```
   rcsentinel stop
   ```

2. Especifique el siguiente comando en la línea de comandos para ejecutar el guión `configure.sh`:

   ```
   ./configure.sh
   ```

3. Especifique `1` para llevar a cabo una configuración estándar o bien `2` para realizar una configuración personalizada de Sentinel.
4. Pulse la barra espaciadora para leer todo el acuerdo de licencia.
5. Introduzca `yes` o `y` para aceptar el acuerdo de licencia y continuar con la instalación.

   La instalación puede tardar varios segundos en cargar los paquetes de instalación.
6. Introduzca `1` para usar la clave de licencia de evaluación por defecto

   O bien

   Introduzca `2` para especificar una clave de licencia adquirida para Sentinel.
7. Decida si desea conservar la contraseña existente para el usuario administrador `admin`.
   - Si desea conservar la contraseña existente, introduzca `1` y luego continúe con el Paso 8.
   - Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 8.

     El usuario `admin` es la identidad que se utiliza para realizar tareas administrativas a través de la interfaz principal de Sentinel, tales como la creación de otras cuentas de usuario.
8. Decida si desea conservar la contraseña existente para el usuario de la base de datos `dbauser`.
   - Si desea conservar la contraseña existente, introduzca `1` y luego continúe con el Paso 9.
   - Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 9.

   La cuenta `dbauser` es la identidad que utiliza Sentinel para interactuar con la base de datos. La contraseña que introduzca aquí puede utilizarse para llevar a cabo tareas de mantenimiento de la base de datos, incluido el restablecimiento de la contraseña del administrador si se pierde o se olvida.
9. Decida si desea conservar la contraseña existente para el usuario de la aplicación `appuser`.
   - Si desea conservar la contraseña existente, introduzca `1` y luego continúe con el Paso 10.
   - Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 10.

     La cuenta `appuser` es una identidad interna, que utiliza el proceso java de Sentinel para establecer conexión e interactuar con la base de datos. La contraseña que introduce aquí sirve para realizar tareas en la base de datos.

10 Cambie las asignaciones de puertos de los servicios de Sentinel introduciendo el número deseado y luego especifique el nuevo número de puerto.

11 Después de cambiar los puertos, especifique 7 cuando haya terminado.

12 Introduzca 1 para autenticar a los usuarios utilizando únicamente la base de datos interna.

O bien

Si ha configurado un directorio LDAP en su dominio, introduzca 2 para autenticar a los usuarios mediante la autenticación de directorios LDAP.

El valor por defecto es 1.

22 Configuración de módulos auxiliares (plug-ins) genéricos

Sentinel viene preinstalado con los módulos auxiliares (plug-ins) por defecto disponibles en el momento del lanzamiento de la versión de Sentinel.

En este capítulo se proporciona información sobre cómo configurar los módulos auxiliares (plug-ins) genéricos.

Visualización de módulos auxiliares (plug-ins) preinstalados

Puede ver la lista de módulos auxiliares (plug-ins) preinstalados en Sentinel. También puede ver las versiones de los módulos auxiliares (plug-ins) y otros metadatos, que le ayudan a determinar si tiene la versión más reciente de un módulo auxiliar.

Para ver los módulos auxiliares (plug-ins) que tiene instalados en su servidor Sentinel:

1. Entre como administrador en la interfaz principal de Sentinel en la dirección `https://<IP address>:8443`, donde 8443 es el puerto por defecto del servidor de Sentinel.
2. Haga clic en **Módulos auxiliares (plug-ins)** > **Catálogo**.

Configuración de la recopilación de datos

Para obtener más información sobre cómo configurar Sentinel para la recopilación de datos, consulte la sección “Collecting and Routing Event Data” (Recopilación y encaminamiento de datos de eventos) de la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Configuración de paquetes de soluciones

Sentinel se suministra con un variado contenido predefinido que resulta útil y que puede usar de inmediato para satisfacer muchas de las necesidades de análisis. Gran parte de este contenido viene de los paquetes Sentinel Core Solution Pack y del paquete de soluciones para la serie ISO 27000. Para obtener más información, consulte “Using Solution Packs” (Uso de paquetes de soluciones) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1).

Los paquetes de soluciones permiten clasificar y agrupar el contenido en controles o conjuntos de directivas que se consideran como una unidad. Los controles de los paquetes de soluciones vienen preinstalados para proporcionarle este contenido predefinido, pero tiene que implementarlos formalmente o probarlos mediante la interfaz principal de Sentinel.

Si se desea contar con un cierto grado de rigor para ayudar a mostrar que la implementación de Sentinel funciona según el diseño, puede usar el proceso de certificación formal incorporado a los Paquetes de soluciones. Este proceso de certificación implementa y prueba los controles del Paquete de soluciones de la misma forma que se implementarían y probarían los controles de cualquier otro paquete de soluciones. Dentro de este proceso, el implementador y el responsable de la prueba certificarán que han finalizado su trabajo; estas certificaciones luego formarán parte de un seguimiento de auditoría que se puede examinar a fin de demostrar que cualquier control dado se implementó adecuadamente.

Puede realizar este proceso de certificación mediante Solution Manager. Para obtener más información sobre cómo implementar y probar los controles, consulte “Installing and Managing Solution Packs” (Instalación y gestión de paquetes de soluciones) de la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Configuración de acciones e integradores

Para obtener información acerca de la configuración de módulos auxiliares (plug-ins) predefinidos, consulte la documentación específica al respecto disponible en el sitio Web de módulos auxiliares (plug-ins) de Sentinel.

23 Habilitar el modo FIPS 140-2 en una instalación de Sentinel existente

En este capítulo se proporciona información sobre cómo habilitar el modo FIPS 140-2 en una instalación de Sentinel existente.

Nota: En estas instrucciones se presupone que Sentinel está instalado en el directorio `/opt/novell/sentinel`. Los comandos deben ejecutarse como usuario `novell`.

Habilitar el servidor Sentinel para su ejecución en modo FIPS 140-2

Para habilitar el servidor Sentinel para ejecutarse en modo FIPS 140-2:

1. Entre en el servidor Sentinel.
2. Cambie al usuario `novell` (`su novell`).
3. Busque el directorio bin de Sentinel.
4. Ejecute el guión `convert_to_fips.sh` y siga las instrucciones en pantalla.
5. (Condicional) Si su entorno utiliza la autenticación múltiple o segura, deberá ejecutar el guión `create_mfa_fips_keys.sh` y seguir las instrucciones en pantalla.

   Nota: Mientras se ejecuta el guión, se requiere la contraseña para la base de datos de nss.
6. (Condicional) Si su entorno utiliza la autenticación múltiple o segura, debe proporcionar el id de cliente de Sentinel y el secreto de cliente de Sentinel. Para obtener más información acerca de los métodos de autenticación, consulte la sección "Authentication Methods" (Métodos de autenticación) en la *Sentinel Administrator Guide* (Guía de administrador de Sentinel).

   Para recuperar el secreto de cliente de Sentinel y el ID de cliente de Sentinel, vaya a la siguiente dirección URL:

   `https://Nombre_de_host:Puerto/SentinelAuthServices/oauth/clients`

   Dónde:

   - *Nombre_de_host* es el nombre de host del servidor Sentinel.
   - *Puerto* es el puerto que utiliza Sentinel (normalmente 8443).

   La dirección URL especificada utiliza la sesión actual de Sentinel para recuperar el secreto de cliente de Sentinel y el ID de cliente de Sentinel.
7. Reinicie el servidor Sentinel.
8. Lleve a cabo la configuración del modo FIPS 140-2 realizando las tareas mencionadas en el Capítulo 24, "Funcionamiento de Sentinel en el modo FIPS 140-2", en la página 133.

Habilitar el modo FIPS 140-2 en las instancias remotas de Collector Manager y Correlation Engine

Debe habilitar el modo FIPS 140-2 en las instancias remotas de Collector Manager y Correlation Engine si desea usar las comunicaciones aptas para FIPS con el servidor Sentinel que se ejecuta en modo FIPS 140-2.

Para habilitar una instancia remota de Collector Manager o Correlation Engine para ejecutarse en modo FIPS 140-2:

1. Acceda al sistema remoto de Collector Manager o Correlation Engine.
2. Cambie al usuario `novell` (`su novell`).
3. Busque el directorio bin. La ubicación por defecto es `/opt/novell/sentinel/bin`.
4. Ejecute el guión `convert_to_fips.sh` y siga las instrucciones en pantalla.
5. Reinicie el Collector Manager o Correlation Engine.
6. Lleve a cabo la configuración del modo FIPS 140-2 realizando las tareas mencionadas en el Capítulo 24, “Funcionamiento de Sentinel en el modo FIPS 140-2”, en la página 133.

24 Funcionamiento de Sentinel en el modo FIPS 140-2

En este capítulo se proporciona información sobre la configuración y el funcionamiento de Sentinel en modo FIPS 140-2.

Configuración del servicio Asesor en modo FIPS 140-2

El servicio Asesor utiliza una conexión HTTPS segura para descargar su contenido desde el servidor del Asesor. El certificado utilizado por el servidor para la comunicación segura debe añadirse a la base de datos del almacén de claves de FIPS de Sentinel.

Para verificar el registro correcto en la base de datos de Gestión de recursos:

1. Descargue el certificado desde el servidor del Asesor y guarde el archivo como `advisor.cer`.
2. Importe el certificado del servidor del Asesor al almacén de claves de FIPS de Sentinel.

   Para obtener más información sobre la importación del certificado, consulte “Importación de certificados en la base de datos del almacén de claves de FIPS” en la página 143.

Configuración de búsqueda distribuida en modo FIPS 140-2

En esta sección se proporciona información sobre cómo configurar búsquedas distribuidas en el modo FIPS 140-2.

Escenario 1: tanto los servidores Sentinel de origen como de destino están en modo FIPS 140-2

Para permitir búsquedas distribuidas en varios servidores Sentinel que se ejecutan en modo FIPS 140-2, es necesario añadir los certificados utilizados para las comunicaciones seguras al almacén de claves FIPS.

1. Entre en el equipo de origen de búsqueda distribuida.
2. Busque el directorio del certificado:

   ```
   cd <sentinel_install_directory>/config
   ```

3. Copie el certificado de origen (`sentinel.cer`) a una ubicación temporal en el equipo de destino.
4. Importe el certificado de origen al almacén de claves de FIPS de Sentinel de destino.

   Para obtener más información sobre la importación del certificado, consulte “Importación de certificados en la base de datos del almacén de claves de FIPS” en la página 143.
5. Entre en el equipo de destino de búsqueda distribuida.
6. Busque el directorio del certificado:

   ```
   cd /etc/opt/novell/sentinel/config
   ```

7. Copie el certificado de destino (`sentinel.cer`) a una ubicación temporal del equipo de origen.
8. Importe el certificado del sistema de destino en el almacén de claves de FIPS de Sentinel.
9. Reinicie los servicios Sentinel tanto en el equipo de origen como en el de destino.

Escenario 2: el servidor Sentinel de origen no está en modo FIPS y el servidor Sentinel de destino está en modo FIPS 140-2.

Debe convertir el almacén de claves del servidor Web del equipo de origen al formato del certificado y luego exportar el certificado al equipo de destino.

1. Entre en el equipo de origen de búsqueda distribuida.
2. Cree el almacén de claves del servidor Web en el formato del certificado (`.cer`):

   ```
   <sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -
   keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
   password -file <certificate_name.cer>
   ```

3. Copie el certificado del origen de la búsqueda distribuida (`Sentinel.cer`) a una ubicación temporal del equipo de destino de búsqueda distribuida.
4. Entre en el equipo de destino de búsqueda distribuida.
5. Importe el certificado de origen al almacén de claves de FIPS de Sentinel de destino.

   Para obtener más información sobre la importación del certificado, consulte “Importación de certificados en la base de datos del almacén de claves de FIPS” en la página 143.
6. Reinicie los servicios de Sentinel en el equipo de destino.

Escenario 3: el servidor Sentinel de origen está en el modo FIPS y el servidor Sentinel de destino está en modo diferente de FIPS.

1. Entre en el equipo de destino de búsqueda distribuida.
2. Cree el almacén de claves del servidor Web en formato del certificado (.cer):

   ```
   <sentinel_install_directory>/jdk/jre/bin/keytool -export -alias webserver -
   keystore <sentinel_install_directory>/config/.webserverkeystore.jks -storepass
   password -file <certificate_name.cer>
   ```

3. Copie el certificado a una ubicación temporal del equipo de origen de búsqueda distribuida.
4. Importe el certificado de destino al almacén de claves de FIPS de Sentinel de origen.

Para obtener más información sobre la importación del certificado, consulte “Importación de certificados en la base de datos del almacén de claves de FIPS” en la página 143.

5 Reinicie los servicios de Sentinel en el equipo de origen.

Configuración de autenticación de LDAP en el modo FIPS 140-2

Para configurar la autenticación de LDAP para los servidores Sentinel que se ejecutan en modo FIPS 140-2:

1 Obtenga el certificado del servidor LDAP del administrador de LDAP, o bien utilice un comando. Por ejemplo,

```
openssl s_client -connect <LDAP server IP>:636
```

y después copie el texto recibido (entre las líneas BEGIN y END, excluyendo ambas) a un archivo.

2 Importe el certificado del servidor LDAP al almacén de claves de FIPS de Sentinel.

Para obtener más información sobre la importación del certificado, consulte “Importación de certificados en la base de datos del almacén de claves de FIPS” en la página 143.

3 Diríjase a la interfaz **Sentinel principal** como usuario con la función de administrador y continúe con la configuración de autenticación LDAP.

Para obtener más información, consulte “LDAP Authentication Against a Single LDAP Server Or Domain” (Autenticación LDAP en un único dominio o servidor LDAP) en la *Sentinel Administration Guide* (Guía de administración de Sentinel).

Nota: También puede configurar la autenticación LDAP para un servidor Sentinel que se ejecute en modo FIPS 140-2 ejecutando el guión `ldap_auth_config.sh` en el directorio `/opt/novell/sentinel/setup`.

Actualización de certificados del servidor en instancias remotas de Collector Manager y Correlation Engine

Para configurar instancias remotas de Collector Manager y Correlation Engine existentes de manera que se comuniquen con un servidor Sentinel que se ejecuta en modo FIPS 140-2, puede bien convertir el sistema remoto en modo FIPS 140-2 o bien actualizar el certificado del servidor Sentinel para el sistema remoto y dejar Collector Manager o Correlation Engine en el modo diferente de FIPS. Las instancias remotas de Collector Manager en modo FIPS podrían no funcionar con orígenes de eventos que no sean compatibles con FIPS o que requieran uno de los conectores de Sentinel que aún no se hayan habilitado para FIPS.

Si no tiene previsto habilitar el modo FIPS 140-2 en las instancias remotas de Collector Manager o Correlation Engine, debe copiar el certificado del servidor Sentinel más actualizado al sistema remoto, de manera que Collector Manager o Correlation Engine puedan comunicarse con el servidor Sentinel.

Para actualizar el certificado del servidor Sentinel en instancias remotas de Collector Manager o Correlation Engine:

1 Entre en el equipo remoto de Collector Manager o Correlation Engine

2 Cambie al usuario `novell` (`su novell`).

3 Busque el directorio bin. La ubicación por defecto es `/opt/novell/sentinel/bin`.

4 Ejecute el guión `updateServerCert.sh`y siga las instrucciones en pantalla.

Configuración de módulos auxiliares (plug-ins) de Sentinel para la ejecución en modo FIPS 140-2

En esta sección se proporciona información sobre la configuración de varios módulos auxiliares (plug-in) de Sentinel en modo FIPS 140-2.

Nota: Estas instrucciones se proporcionan siempre que se haya instalado Sentinel en el directorio `/opt/novell/sentinel`. Ejecute todos los comandos como usuario `novell`.

Conector de Agent Manager

Siga el procedimiento a continuación solamente si ha seleccionado la opción **Cifrado (HTTPS)** al configurar los ajustes de red del Servidor de orígenes de eventos de Agent Manager.

Para configurar el conector de Agent Manager para su ejecución en modo FIPS 140-2:

1 Añada o edite el servidor de orígenes de eventos de Agent Manager. Siga por las pantallas de configuración hasta que se muestre la ventana de Seguridad. Para obtener más información, consulte la *Agent Manager Connector Guide* (Guía de conectores de Agent Manager).

2 Seleccione una de las opciones del campo *Tipo de autenticación del cliente*. El tipo de autenticación del cliente determina qué grado de control ejerce el servidor de orígenes de eventos de SSL Agent Manager al verificar la identidad de los orígenes de eventos de Agent Manager que están tratando de enviar datos.

- **Abrir:** Permite todas las conexiones SSL procedentes de agentes de Agent Manager. No realiza ninguna validación o autenticación del certificado del cliente.
- **Estricto:** Confirma que el certificado sea del tipo X.509 válido y comprueba además que el certificado del cliente sea de confianza para el servidor de orígenes de eventos. Los nuevos orígenes se deberán añadir de forma explícita a Sentinel (esto evita que orígenes ficticios envíen datos no autorizados).

Para la opción **Estricto**, debe importar el certificado de cada cliente de Agent Manager nuevo al almacén de claves de FIPS de Sentinel. Cuando Sentinel se ejecuta en modo FIPS 140-2, no es posible importar el certificado de cliente utilizando la interfaz de Gestión de orígenes de eventos (ESM).

Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 143.

Nota: En el modo FIPS 140-2, el servidor de orígenes de eventos de Agent Manager utiliza el par de claves del servidor Sentinel; no se requiere importar el par de claves del servidor.

---

3 Si está habilitada la autenticación del servidor en los agentes, estos deben configurarse además para confiar en el servidor Sentinel o en el certificado del Collector Manager remoto, dependiendo de donde esté implementado el conector.

Ubicación del certificado del servidor Sentinel: `/etc/opt/novell/sentinel/config/sentinel.cer`

Ubicación del certificado de Collector Manager remoto: `/etc/opt/novell/sentinel/config/rcm.cer`

Nota: Al utilizar certificados personalizados con firma digital de una autoridad certificadora (CA), el agente de Agent Manager debe confiar en el archivo de certificado correspondiente.

Conector de base de datos (JDBC)

Siga el procedimiento a continuación solamente si ha seleccionado la opción *SSL* al configurar la conexión de base de datos.

Para configurar el conector de la base de datos para su ejecución en el modo FIPS 140-2:

1 Antes de configurar el conector, descargue el certificado del servidor de la base de datos y guárdelo como archivo `database.cert` en el directorio`/etc/opt/novell/sentinel/config` del servidor Sentinel.

Para obtener más información, consulte la documentación respectiva de la base de datos.

2 Importe el certificado al almacén de claves de FIPS de Sentinel.

Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 143.

3 Continúe con la configuración del conector.

Conector de Sentinel Link

Siga el procedimiento a continuación solamente si ha seleccionado la opción **Cifrado (HTTPS)** al configurar los ajustes de red del servidor de orígenes de eventos de Sentinel Link.

Para configurar el conector de Sentinel Link para su ejecución en modo FIPS 140-2:

1 Añada o edite el servidor de orígenes de eventos de Sentinel Link. Siga por las pantallas de configuración hasta que se muestre la ventana de Seguridad. Para obtener más información, consulte la *Sentinel Link Connector Guide* (Guía de conectores de Sentinel Link).

2 Seleccione una de las opciones del campo *Tipo de autenticación del cliente*. El tipo de autenticación del cliente determina qué grado de control ejerce el servidor de orígenes de eventos de SSL Sentinel Link al verificar la identidad de los orígenes de eventos de Sentinel Link (integradores de Sentinel Link) que están tratando de enviar datos.

- **Abrir:** Permite las conexiones SSL procedentes de los clientes (integradores de Sentinel Link). No lleva a cabo ninguna validación ni autenticación de certificados de integrador.
- **Estricto:** Comprueba que el certificado del integrador sea del tipo X.509 válido y además comprueba que el certificado del integrador sea de confianza para el servidor de orígenes de eventos. Para obtener más información, consulte la documentación respectiva de la base de datos.

  Para la opción **Estricto**:

  - Si el integrador de Sentinel Link está en modo FIPS 140-2, debe copiar el archivo `/etc/opt/novell/sentinel/config/sentinel.cer` del equipo Sentinel remitente al equipo Sentinel destinatario. Importe este certificado al almacén de claves de FIPS del Sentinel destinatario.

    Nota: Al usar certificados personalizados con firma digital de una autoridad certificadora (CA), debe importar el archivo de certificado personalizado adecuado.

  - Si el integrador de Sentinel Link no está en modo FIPS, debe importar el certificado del integrados al almacén de claves de FIPS de Sentinel destinatario.

    Nota: Si el remitente es Sentinel Log Manager (en modo diferentes de FIPS) y el destinatario es Sentinel en modo FIPS 140-2, el certificado de servidor que se debe importar en el remitente es el archivo `/etc/opt/novell/sentinel/config/sentinel.cer` del equipo Sentinel destinatario.

  Cuando Sentinel se ejecuta en modo FIPS 140-2, no es posible importar el certificado de cliente utilizando la interfaz de Gestión de orígenes de eventos (ESM). Para obtener más información sobre la importación del certificado, consulte “Importación de certificados en la base de datos del almacén de claves de FIPS” en la página 143.

Nota: En el modo FIPS 140-2, el servidor de orígenes de eventos de Sentinel Link utiliza el par de claves del servidor Sentinel. No se requiere importar el par de claves del servidor.

Conector syslog

Siga el procedimiento a continuación solamente si ha seleccionado el protocolo **SSL** al configurar los ajustes de red del servidor de orígenes de eventos de Syslog.

Para configurar el conector Syslog para su ejecución en el modo FIPS 140-2:

1 Añada o edite el servidor de orígenes de eventos de Syslog. Continúe por las pantallas de configuración hasta que se muestre la ventana Conectividad. Para obtener más información, consulte la *Syslog Connector Guide* (Guía de conectores de Syslog).

2 Haga clic en **Ajustes**.

3 Seleccione una de las opciones del campo *Tipo de autenticación del cliente*. El tipo de autenticación del cliente determina qué grado de control ejerce el servidor de orígenes de eventos SSL de Syslog al verificar la identidad de los orígenes de eventos de Syslog que están tratando de enviar datos.

- **Abrir:** Permite las conexiones SSL procedentes de los clientes (orígenes de eventos). No realiza ninguna validación ni autenticación de certificados del cliente.

- **Estricto:** Confirma que el certificado sea del tipo X.509 válido y comprueba además que el certificado del cliente sea de confianza para el servidor de orígenes de eventos. Será necesario añadir nuevos orígenes de forma explícita a Sentinel (esto impide que orígenes ficticios envíen datos a Sentinel).

  Para la opción **Estricto**, debe importar el certificado del cliente syslog al almacén de claves de FIPS de Sentinel.

  Cuando Sentinel se ejecuta en modo FIPS 140-2, no es posible importar el certificado de cliente utilizando la interfaz de Gestión de orígenes de eventos (ESM).

  Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 143.

Nota: En el modo FIPS 140-2, el servidor de orígenes de eventos de Syslog utiliza el par de claves del servidor Sentinel. No se requiere importar el par de claves del servidor.

---

4 Si está habilitada la autenticación del servidor en el cliente syslog, el cliente debe confiar en el certificado del servidor Sentinel o en el certificado de Collector Manager remoto, dependiendo de donde esté implementado el conector.

El archivo de certificado del servidor Sentinel se encuentra en `/etc/opt/novell/sentinel/config/sentinel.cer`.

El archivo de certificado del gestor de recopiladores remoto se encuentra en `/etc/opt/novell/sentinel/config/rcm.cer`.

Nota: Al utilizar certificados personalizados con firma digital de una autoridad certificadora (CA), el cliente debe confiar en el archivo de certificado adecuado.

Conector de eventos Windows (WMI)

Para configurar el conector de eventos de Windows (WMI) para su ejecución en modo FIPS 140-2:

1 Añada o edite el conector de eventos de Windows. Siga por las pantallas de configuración hasta que se muestre la ventana de Seguridad. Para obtener más información, consulte la *Windows Event (WMI) Connector Guide* (Guía de conectores de eventos de Windows (WMI)).

2 Haga clic en **Ajustes**.

3 Seleccione una de las opciones del campo *Tipo de autenticación del cliente*. El tipo de autenticación del cliente determina qué grado de control ejerce el conector de eventos de Windows al verificar la identidad de los servicios de recopilación de eventos de Windows (WECS) del cliente que están tratando de enviar datos.

- **Abrir:** permite todas las conexiones SSL procedentes de WECS del cliente. No realiza ninguna validación ni autenticación de certificados del cliente.
- **Estricto:** Comprueba que el certificado sea del tipo X.509 válido y comprueba además que el certificado de WECS del cliente esté firmado por una CA. Los nuevos orígenes deberán añadirse de forma explícita (esto impide que orígenes ficticios envíen datos a Sentinel).

  Para la opción **Estricto**, debe importar el certificado de WECS del cliente al almacén de claves de FIPS de Sentinel. Cuando Sentinel se ejecuta en modo FIPS 140-2, no es posible importar el certificado de cliente utilizando la interfaz de Gestión de orígenes de eventos (ESM).

  Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 143.

Nota: En el modo FIPS 140-2, el servidor de orígenes de eventos de Windows utiliza el par de claves del servidor Sentinel. No se requiere importar el par de claves del servidor.

4 Si está habilitada la autenticación del servidor en el cliente Windows, el cliente debe confiar en el certificado del servidor Sentinel o en el certificado de Collector Manager remoto, dependiendo de donde esté implementado el conector.

El archivo de certificado del servidor Sentinel se encuentra en `/etc/opt/novell/sentinel/config/sentinel.cer`.

El archivo de certificado de Collector Manager remoto se encuentra en `/etc/opt/novell/sentinel/config/rcm.cer`.

Nota: Al utilizar certificados personalizados con firma digital de una autoridad certificadora (CA), el cliente debe confiar en el archivo de certificado adecuado.

5 Si desea sincronizar automáticamente los orígenes de eventos o completar la lista de orígenes de eventos mediante una conexión a un Active Directory, debe importar el certificado del servidor Active Directory al almacén de claves de FIPS de Sentinel.

Para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 143.

Integrador de Sentinel Link

Siga el procedimiento a continuación solamente si ha seleccionado la opción **Cifrado (HTTPS)** al configurar los ajustes de red del integrador de Sentinel Link.

Para configurar el integrador de Sentinel Link para su ejecución en el modo FIPS 140-2:

1 Cuando el integrador de Sentinel Link se encuentre en el modo FIPS 140-2, es obligatoria la autenticación del servidor?. Antes de configurar la instancia del integrador, importe el certificado del servidor de Sentinel Link al almacén de claves de FIPS de Sentinel:

- **Si el conector de Sentinel Link está en el modo FIPS 140-2**:

  Si el conector se implementa en el servidor Sentinel, debe copiar el archivo`/etc/opt/novell/sentinel/config/sentinel.cer` desde el equipo Sentinel destinatario al equipo Sentinel remitente.

  Si el conector se implementa en una instancia remota de Collector Manager, debe copiar el archivo `/etc/opt/novell/sentinel/config/rcm.cer` desde el equipo de Collector Manager remoto destinatario al equipo Sentinel destinatario.

  Importe este certificado al almacén de claves de FIPS de Sentinel.

  Nota: Al utilizar certificados personalizados con firma digital de una autoridad certificadora (CA), debe importar el archivo de certificado personalizado adecuado.

- Si el conector de Sentinel Link no está en modo FIPS:

  Importe el certificado del servidor de Sentinel Link personalizado al almacén de claves de FIPS de Sentinel remitente.

  Nota: Cuando el integrador de Sentinel Link está en el modo FIPS 140-2 y el conector de Sentinel Link está en modo diferente de FIPS, utilice el par de claves de servidor personalizado en el conector. No instale el par de claves del servidor interno.

para obtener más información sobre la importación del certificado, consulte "Importación de certificados en la base de datos del almacén de claves de FIPS" en la página 143.

2 Continúe con la configuración de la instancia del integrador.

Nota: En el modo FIPS 140-2, el integrador de Sentinel Link utiliza el par de claves del servidor Sentinel. No se requiere importar el par de claves del integrador.

Integrador de LDAP

Para configurar el integrador de LDAP para que se ejecute en modo FIPS 140-2:

1 Antes de configurar la instancia del integrador, descargue el certificado del servidor LDAP y guárdelo como archivo `ldap.cert` en el directorio `/etc/opt/novell/sentinel/config` del servidor Sentinel.

Por ejemplo, utilice:

```
openssl s_client -connect <LDAP server IP>:636
```

y después copie el texto enviado (entre las líneas BEGIN y END, excluyéndolas) a un archivo.

2 Importe el certificado al almacén de claves de FIPS de Sentinel.

Para obtener más información sobre la importación del certificado, consulte “Importación de certificados en la base de datos del almacén de claves de FIPS” en la página 143.

3 Continúe con la configuración de la instancia del integrador.

Integrador de SMTP

El integrador de SMTP admite FIPS 140-2 a partir de la versión 2011.1r2 y versiones posteriores. No se requieren cambios de configuración.

Integrador de Syslog

Siga el procedimiento que se muestra a continuación solamente si ha seleccionado la opción Cifrado (SSL) al configurar los ajustes de red del integrador de Syslog.

Para configurar el integrador de Syslog para que se ejecute en modo FIPS 140-2:

1 Cuando el integrador de Syslog se encuentre en el modo FIPS 140-2, es obligatoria la autenticación del servidor. Antes de configurar la instancia del integrador, importe el certificado del servidor de Syslog al almacén de claves de FIPS de Sentinel:

- **Si el conector de Syslog está en el modo FIPS 140-2:** Si el conector se implementa en el servidor de Sentinel, debe copiar el archivo`/etc/opt/novell/sentinel/config/sentinel.cer` desde el servidor de Sentinel destinatario al servidor de Sentinel remitente.

  Si el conector se implementa en una instancia remota de Collector Manager, debe copiar el archivo `/etc/opt/novell/sentinel/config/rcm.cer` desde el equipo de Collector Manager remoto destinatario al equipo Sentinel destinatario.

  Importe este certificado al almacén de claves de FIPS de Sentinel.

  Nota: Al utilizar certificados personalizados con firma digital de una autoridad certificadora (CA), debe importar el archivo de certificado personalizado adecuado.

- **Si el conector de Syslog no está en modo FIPS:** Debe importar el certificado del servidor de Syslog personalizado al almacén de claves de FIPS de Sentinel remitente.

Nota: Cuando el integrador de Syslog está en el modo FIPS 140-2 y el conector de Syslog está en modo diferente de FIPS, utilice el par de claves de servidor personalizado en el conector. No instale el par de claves del servidor interno.

Para importar certificados a la base de datos del almacén de claves de FIPS:

1. Copie el archivo de certificado a cualquier ubicación temporal del servidor Sentinel o de Collector Manager remoto.
2. Diríjase al directorio `/opt/novell/sentinel/bin`.
3. Ejecute el siguiente comando para importar el certificado a la base de datos del almacén de claves de FIPS y luego siga las instrucciones en pantalla:

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```

4. Introduzca `sí` o `s` cuando se le indique reiniciar el servidor Sentinel o Collector Manager remoto.

2 Continúe con la configuración de la instancia del integrador.

Nota: en el modo FIPS 140-2, el integrador de Syslog utiliza el par de claves del servidor de Sentinel. No es necesario importar el par de claves del integrador.

Uso de conectores no habilitados para FIPS con Sentinel en el modo FIPS 140-2

En esta sección se proporciona información sobre cómo usar conectores no habilitados para FIPS con un servidor Sentinel en el modo FIPS 140-2. Se recomienda este planteamiento si tiene orígenes que no son compatibles con FIPS o si desea recopilar eventos de los conectores no compatibles con FIPS en su entorno.

Para usar conectores que no están en modo FIPS con Sentinel en el modo FIPS 140-2:

1 Instale una instancia de Collector Manager en el modo diferente de FIPS para conectar con el servidor Sentinel en el modo FIPS 140-2.

Para obtener más información, consulte la Parte III, “Instalación de Sentinel”, en la página 71.

2 Implemente los conectores sin FIPS específicamente en la instancia remota de Collector Manager que no está en modo FIPS.

Nota: Estos son algunos de los problemas conocidos que surgen cuando conectores que no admiten FIPS como el conector de auditoría y el conector de archivos se implementan en una instancia remota de Collector Manager que no admite FIPS conectado a un servidor Sentinel en el modo FIPS 140-2. Para obtener más información sobre estos problemas conocidos, consulte Sentinel Release Notes (Notas de la versión de Sentinel).

Importación de certificados en la base de datos del almacén de claves de FIPS

Debe insertar los certificados en la base de datos del almacén de claves de FIPS para establecer comunicaciones seguras (SSL) desde los componentes propietarios de dichos certificados a Sentinel. No se pueden cargar certificados mediante la interfaz de usuario de Sentinel cuando está habilitado el modo FIPS 140-2. Debe importar manualmente el certificado a la base de datos del almacén de claves de FIPS.

Para los orígenes de eventos que utilizan conectores implementados en una instancia remota de Collector Manager, debe importar los certificados a la base de datos del almacén de claves de FIPS de la instancia remota de Collector Manager en lugar de al servidor central de Sentinel.

Para importar certificados a la base de datos del almacén de claves de FIPS:

1. Copie el archivo de certificado a cualquier ubicación temporal del servidor Sentinel o de Collector Manager remoto.
2. Busque el directorio bin de Sentinel. La ubicación por defecto es `/opt/novell/sentinel/bin`.
3. Ejecute el siguiente comando para importar el certificado a la base de datos del almacén de claves de FIPS y luego siga las instrucciones en pantalla.

   ```
   ./convert_to_fips.sh -i <certificate file path>
   ```

4. Introduzca `sí` o `s` cuando se le indique reiniciar el servidor Sentinel o Collector Manager remoto.

Reversión de Sentinel al modo diferente de FIPS

En esta sección se proporciona información sobre cómo revertir Sentinel y sus componentes al modo diferente de FIPS.

- “Reversión del servidor Sentinel al modo diferente de FIPS” en la página 143
- “Reversión de las instancias remotas de Collector Manager o Correlation Engine al modo diferente de FIPS” en la página 144

Reversión del servidor Sentinel al modo diferente de FIPS

Puede revertir un servidor Sentinel que se ejecuta en modo FIPS 140-2 al modo diferente de FIPS solamente si ha realizado una copia de seguridad del servidor Sentinel antes de convertirlo para ejecutarse en modo FIPS 140-2.

Nota: Cuando revierte un servidor Sentinel al modo diferente de FIPS, perderá los eventos, datos de incidencia y cambios de configuración que haya realizado al servidor Sentinel después de convertirlo para ejecutarse en modo diferente de FIPS 140-2. El sistema Sentinel se restaurará al último punto de restauración en el modo diferente de FIPS. Debe realizar una copia de seguridad del sistema actual antes de revertirlo al modo diferente a FIPS para su uso en el futuro.

Para revertir el servidor Sentinel al modo diferente de FIPS:

1. Entre al servidor de Sentinel como usuario `root`.
2. Cambie al usuario `novell`.
3. Busque el directorio bin de Sentinel. La ubicación por defecto es `/opt/novell/sentinel/bin`.

4 Ejecute el siguiente comando para revertir el servidor Sentinel al modo diferente de FIPS y siga las instrucciones en pantalla:

```
./backup_util.sh -f <backup_file_name.tar.gz> -m 'restore'
```

Por ejemplo, si `non-fips2013012419111359034887.tar.gz` es el archivo de copia de seguridad, ejecute el siguiente comando:

```
./backup_util.sh -f non-fips2013012419111359034887.tar.gz -m 'restore'
```

5 Reinicie el servidor Sentinel.

Reversión de las instancias remotas de Collector Manager o Correlation Engine al modo diferente de FIPS

Puede revertir las instancias remotas de Collector Manager o Correlation Engine al modo diferente de FIPS.

Para revertir las instancias remotas de Collector Manager o Correlation Engine al modo diferente de FIPS:

1 Entre en el sistema remoto de Collector Manager o Correlation Engine.

2 Cambie al usuario `novell` (`su novell`).

3 Busque el directorio bin. La ubicación por defecto es `/opt/novell/sentinel/bin`.

4 Ejecute el guión `revert_to_nonfips.sh` y siga las instrucciones en pantalla.

5 Reinicie las instancias remotas de Collector Manager o Correlation Engine.

25 Adición de una portada de consentimiento

Sentinel le permite mostrar una portada de consentimiento antes de la entrada. Puede especificar el contenido de la portada según sus necesidades. Después de añadir la portada de consentimiento, deberá aceptar los términos incluidos en ella cada vez que entre en Sentinel.

Para añadir una portada de consentimiento:

1. Entre en el servidor de Sentinel como el usuario `novell`.
2. Desplácese a `/<vía_instalación_sentinel>/var/opt/novell/sentinel/3rdparty/jetty/webapps/ROOT/siemdownloads`.
3. Añada un archivo de texto con el nombre, `USER_AGREEMENT.txt`.
4. Introduzca el texto del Acuerdo de usuario.
5. Guarde el archivo.
6. Lance Sentinel para ver la portada de consentimiento.

Ahora Sentinel muestra la portada de consentimiento en la pantalla de entrada.

Nota: Debe realizar de forma manual una copia de seguridad del archivo `USER_AGREEMENT.txt` antes de actualizar Sentinel.

V Actualización de Sentinel

En esta sección se proporciona información sobre la actualización de Sentinel y otros componentes.

26 Lista de verificación de implementación

Antes de actualizar Sentinel, revise la siguiente lista de verificación para garantizar una actualización satisfactoria:

Tabla 26-1 *Lista de verificación de implementación*

❒	Tareas	Consulte
❒	Asegúrese de que los equipos en los que instale Sentinel y sus componentes cumplan los requisitos especificados.	Sitio Web de información técnica de Sentinel
❒	Revise las notas de la versión del sistema operativo compatible para conocer los problemas conocidos.	Notas de la versión de SUSE
❒	Revise las notas de la versión de Sentinel para ver la nueva funcionalidad y conocer los problemas conocidos.	Notas de la versión de Sentinel
❒	Efectúe las tareas que se indica en Requisitos previos.	Capítulo 27, “Requisitos previos”, en la página 151

27 Requisitos previos

Cómo guardar la información de configuración personalizada

Almacenamiento de la configuración de archivo server.conf

Si ha definido valores de parámetro de configuración personalizados en el archivo `server.conf`, guarde dichos valores en archivos separados antes de proceder con la actualización.

Para guardar la información de configuración personalizada:

1. Entre en el servidor Sentinel como usuario `novell` y vaya al directorio `/etc/opt/novell/sentinel/config/`.
2. Cree un archivo de configuración llamado `server-custom.conf` y añada sus parámetros de configuración personalizada en este archivo.

Sentinel aplica la configuración personalizada guardada a estos archivos de configuración durante la actualización.

Almacenamiento de la configuración de archivo jetty ssl

Sentinel 8.1 incluye una versión actualizada de Jetty. La versión actualizada de Jetty incluye cambios en su estructura de archivos.

Si ha modificado el archivo `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl.xml` en versiones anteriores de Sentinel, por ejemplo, excluyendo cualquier cifrado, guarde los cambios realizados en un archivo independiente antes de la actualización de Sentinel.

Una vez completada la actualización de Sentinel, copie esos cambios al archivo `/etc/opt/novell/sentinel/3rdparty/jetty/jetty-ssl-context.xml` y reinicie Sentinel.

Ampliación del periodo de retención para datos de asociaciones de eventos

A partir de Sentinel 7.4.4, el período de retención por defecto para los datos de las asociaciones de eventos es de 14 días. Si va a actualizar desde una versión de Sentinel anterior a la 7.4.4, el período de retención que había establecido para datos de asociaciones de eventos se suprimirá a los 14 días después de la actualización. Para evitar esta situación, puede definir el período de retención para el valor deseado mediante la adición de una propiedad del archivo `configuration.properties`. Para

obtener más información, consulte la sección “Configuring the Retention Period for the Event Associations Data” (Configuración el período de retención para los datos de las asociaciones de eventos) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Configuración de SSDM previa a la actualización

El proceso de actualización actualizará archivos relacionados con las aplicaciones Spark. Para utilizar los archivos actualizados, debe reiniciar la tarea de Spark y restablecer todos los puntos de comprobación chispa sobre temas de Kafka. Para evitar la pérdida de datos debido al restablecimiento del punto de comprobación del tema de Kafka, debe pausar el reenvío de datos de las instancias de Collector Manager a Kafka antes de actualizar SSDM. Mientras esté en pausa el reenvío de datos, estos se almacenarán en el Collector Manager hasta que se reanude dicho reenvío. Una vez que la aplicación Spark realiza el procesamiento de datos que se remitieron a Kafka antes de pausar el reenvío, el punto de comprobación se puede restablecer con seguridad sin pérdida de datos.

Para poner en pausa el reenvío de eventos desde Collector Manager a Kafka:

1. En Sentinel principal, haga clic en **Storage** (Almacenamiento) > **Scalable Storage** (Almacenamiento ampliable) > **Advanced Configuration** (Configuración avanzada) > **Kafka** (Kafka).
2. Añada la siguiente propiedad y ajústela en verdadero:

   `pause.events.tokafka`
3. Haga clic en **Guardar**.

Integración de Change Guardian

Sentinel es compatible con Change Guardian 4.2 y versiones posteriores. Para recibir eventos de Change Guardian, antes debe actualizar el servidor de Change Guardian, Agentes y el Editor de directivas a la versión 4.2 o una posterior para asegurarse de que Sentinel sigue recibiendo eventos de Change Guardian tras la actualización.

28 Actualización de la instalación tradicional de Sentinel

Actualización de Sentinel

Siga los pasos indicados a continuación para actualizar el servidor Sentinel:

1. Realice una copia de seguridad de su configuración y luego cree una exportación de ESM.

   Para obtener más información sobre la copia de seguridad de datos, consulte la sección “Backing Up and Restoring Data” (Copia de seguridad y restauración de datos) en la *Sentinel Administration Guide (Guía de administración de NetIQ Sentinel 7.1)*.
2. (Condicional) Si ha personalizado los ajustes de configuración en los archivos `server.xml`, `collector_mgr.xml` o `correlation_engine.xml`, asegúrese de que ha creado los archivos de propiedades adecuados con el nombre de obj-component id para estar seguro de que las personalizaciones se mantendrán después de la actualización. Para obtener más información, consulte “Maintaining Custom Settings in XML Files” (Cómo mantener los ajustes personalizados en los archivos XML) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).
3. Descargue el programa de instalación más reciente desde el sitio Web de descargas.
4. Entre como usuario `root` en el servidor en el que desea actualizar Sentinel.
5. Especifique el siguiente comando para extraer los archivos de instalación del archivo tar:

   ```
   tar xfz <install_filename>
   ```

   Reemplace <*nombre de archivo_instalación*> por el nombre real del archivo de instalación.
6. Vaya al directorio donde extrajo el archivo de instalación.
7. Especifique el siguiente comando para actualizar Sentinel:

   ```
   ./install-sentinel
   ```
8. Para continuar con el idioma deseado, seleccione el número especificado junto al idioma.

   El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.
9. Lea el acuerdo de licencia del usuario final e introduzca`sí` o `s` para aceptar la licencia y continuar con la instalación.
10. El guión de instalación detecta que ya existe una versión del producto más antigua y le indica que debe especificar si desea actualizar el producto. Para continuar con la actualización, pulse s.

    La instalación comienza instalando todos los paquetes RPM. Esta instalación puede tardar unos segundos en finalizar.

11 Borre la memoria caché del navegador web para ver la versión más reciente de Sentinel.

12 Borre la caché de Java Web Start en los equipos cliente para utilizar la versión más reciente de las aplicaciones Sentinel.

La caché de Java Web Start se puede borrar con el comando `javaws -clearcache` o desde Control Center de Java. Para obtener más información, vaya al sitio http://www.java.com/es/download/help/plugin_cache.xml.

13 (Condicional) Si se ha actualizado la base de datos PostgreSQL a una versión importante (por ejemplo, de 8.0 a 9.0 o de 9.0 a 9.1), elimine los archivos PostgreSQL antiguos de la base de datos PostgreSQL. Para obtener información sobre si se ha actualizado la base de datos PostgreSQL, consulte las notas de la versión de Sentinel.

13a Cambie al usuario novell.

```
su novell
```

13b Busque en la carpeta `bin`:

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

13c Elimine todos los archivos postgreSQL anteriores mediante el siguiente comando:

```
./delete_old_cluster.sh
```

14 Para actualizar los sistemas de Collector Manager y Correlation Engine, consulte la “Actualización de Collector Manager o Correlation Engine” en la página 156.

15 (Condicional) Si utiliza la autenticación Kerberos, habilite AES256 en Java Runtime Environment, ya que la carpeta `java` se reemplaza con archivos por defecto durante la actualización. Para habilitar AES256 en Java Runtime Environment, complete los siguientes pasos:

15a Descargue Java Cryptography Extension (JCE) 8 en la siguiente ubicación: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

15b Extraiga los dos archivos `*.jar` y cópielos en el directorio `/opt/novell/sentinel/jdk/jre/lib/security`.

15c (Condicional) Si ejecuta Sentinel en un entorno de alta disponibilidad, repita estos pasos en todos los nodos del clúster.

15d Reinicie Sentinel.

Actualización de Sentinel como usuario diferente de root

Si la directiva de su organización no le permite ejecutar la actualización completa de Sentinel como usuario `root`, puede realizar la actualización de Sentinel como un usuario diferente. En esta actualización, algunos pasos se realizan como usuario `root` y luego se continúa la actualización de Sentinel como otro usuario diferente creado por el usuario `root`.

1 Realice una copia de seguridad de su configuración y luego cree una exportación de ESM.

Para obtener más información sobre la copia de seguridad de los datos, consulte “Backing Up and Restoring Data” (Copia de seguridad y restauración de datos) en *Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.

2 (Condicional) Si ha personalizado los ajustes de configuración en los archivos `server.xml`, `collector_mgr.xml` o `correlation_engine.xml`, asegúrese de que ha creado los archivos de propiedades adecuados con el nombre de obj-component id para estar seguro de que las

personalizaciones se mantendrán después de la actualización. Para obtener más información, consulte “Backing Up and Restoring Data (Copia de seguridad y restauración de datos)” en la *Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.

3. Descargue los archivos de instalación del sitio Web de descargas de .
4. Especifique el siguiente comando en la línea de comandos para extraer los archivos de instalación del archivo tar:

   ```
   tar -zxvf <install_filename>
   ```

   Reemplace <*nombre de archivo_instalación*> por el nombre real del archivo de instalación.
5. Entre como usuario `root` en el servidor en el que desea actualizar Sentinel.
6. Extraiga el RPM `squashfs` de los archivos de instalación de Sentinel.
7. Instale el `squashfs` en el servidor Sentinel.

   ```
   rpm -Uvh <install_filename>
   ```
8. Especifique el siguiente comendo para cambiar al nuevo usuario de `novell` diferente de root recién creado: `novell`:

   ```
   su novell
   ```
9. (Condicional) Para realizar una actualización interactiva:

   9a Especifique el siguiente comando:

   ```
   ./install-sentinel
   ```

   Para actualizar Sentinel en una ubicación no predeterminada, especifique la opción --location junto con el comando. Por ejemplo:.

   ```
   ./install-sentinel --location=/foo
   ```

   9b Continúe con el Paso 11.
10. (Condicional) Para realizar una actualización silenciosa, especifique el siguiente comando:

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

    La instalación continúa con los valores almacenados en el archivo de respuesta. La actualización de Sentinel ha finalizado.
11. Especifique el número del idioma que desea usar para la actualización.

    El acuerdo de licencia de usuario final se muestra en el idioma seleccionado.
12. Lea el acuerdo de licencia del usuario final e introduzca `sí` o `s` para aceptar el acuerdo y continuar con la actualización.

    La actualización comienza instalando todos los paquetes RPM. Esta instalación puede tardar unos segundos en finalizar.
13. Borre la memoria caché del navegador web para ver la versión más reciente de Sentinel.
14. Borre la caché de Java Web Start en los equipos cliente para utilizar la versión más reciente de las aplicaciones Sentinel.

    La caché de Java Web Start se puede borrar con el comando `javaws -clearcache` o desde Control Center de Java. Para obtener más información, vaya al sitio http://www.java.com/es/download/help/plugin_cache.xml.

15 (Condicional) Si se ha actualizado la base de datos PostgreSQL a una versión importante (por ejemplo, de 8.0 a 9.0 o de 9.0 a 9.1), elimine los archivos PostgreSQL antiguos de la base de datos PostgreSQL. Para obtener información sobre si se ha actualizado la base de datos PostgreSQL, consulte las notas de la versión de Sentinel.

15a Cambie al usuario novell.

```
su novell
```

15b Busque en la carpeta `bin`:

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

15c Elimine todos los archivos postgreSQL antiguos mediante el siguiente comando:

```
./delete_old_cluster.sh
```

16 (Condicional) Si utiliza la autenticación Kerberos, habilite AES256 en Java Runtime Environment, ya que la carpeta `java` se reemplaza con archivos por defecto durante la actualización. Para habilitar AES256 en Java Runtime Environment, complete los siguientes pasos:

16a Descargue Java Cryptography Extension (JCE) 8 en la siguiente ubicación: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

16b Extraiga los dos archivos `*.jar` y cópielos en el directorio `/opt/novell/sentinel/jdk/jre/lib/security`.

16c (Condicional) Si ejecuta Sentinel en un entorno de alta disponibilidad, repita estos pasos en todos los nodos del clúster.

16d Reinicie Sentinel.

Actualización de Collector Manager o Correlation Engine

Siga los pasos indicados a continuación para actualizar Collector manager o Correlation Engine:

1 Realice una copia de seguridad de su configuración y cree una exportación de ESM.

Para obtener más información, consulte “Backing Up and Restoring Data (Copia de seguridad y restauración de datos)” en la *Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.

2 Diríjase a la **Sentinel principal** (Interfaz principal) de Sentinel como usuario con la función de administrador.

3 Seleccione **Descargas**.

4 Haga clic en **Descargar instalador** de la sección Instalador de Collector Manager.

5 Guarde el archivo del instalador en el servidor de Collector Manager o Correlation Engine correspondiente.

6 Copie el archivo en una ubicación temporal.

7 Extraiga el contenido del archivo.

8 Ejecute el guión siguiente:

Para Collector Manager:

```
./install-cm
```

Para Correlation Engine:

```
./install-ce
```

9 Siga las instrucciones que aparecen en pantalla para finalizar el procedimiento de instalación.

10 (Condicional) En el caso de instalaciones personalizadas, ejecute el comando siguiente para sincronizar las configuraciones entre el servidor Sentinel, Collector Manager y Correlation Engine:

```
/opt/novell/sentinel/setup/configure.sh
```

Actualización del sistema operativo

Esta versión de Sentinel incluye un conjunto de comandos que debe utilizar durante el procedimiento de actualización de sistema operativo. Estos comandos garantizan que Sentinel funcione correctamente después de actualizar el sistema operativo.

Nota: Debe actualizar Sentinel antes de actualizar el sistema operativo.

Siga los pasos que se muestran a continuación para actualizar el sistema operativo:

1 En el servidor de Sentinel en el que desea actualizar el sistema operativo, entre a la sesión como uno de los siguientes usuarios:

- Usuario `root`
- Usuario no root

2 Abra un indicador de comandos y cambie al directorio donde extrajo el archivo de instalación de Sentinel.

3 Detenga los servicios de Sentinel:

```
rcsentinel stop
```

4 (Condicional) Si Sentinel estaba en modo FIPS antes de la actualización del sistema operativo, los archivos de base de datos NSS deben actualizarse manualmente ejecutando el siguiente comando:

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Siga las instrucciones en pantalla para actualizar la base de datos NSS.

Proporcione permisos totales al usuario `novell` para los siguientes archivos:

```
cert9.db
key4.db
pkcs11.txt
```

5 Actualice el sistema operativo.

6 (Condicional) Si utiliza Mozilla Network Security Services (NSS) 3.29, no se instalan dos archivos RPM dependientes `libfreebl3-hmac` y `libsoftokn3-hmac`. Instale de forma manual los siguientes archivos RPM: `libfreebl3 hmac` y `libsoftokn3 hmac`.

7 (Condicional) Para RHEL 7.*x*, ejecute el siguiente comando para comprobar si existen errores en la base de datos RPM:

```
rpm -qa --dbpath <install_location>/rpm | grep novell
```

Ejemplo: `# rpm -qa --dbpath /custom/rpm | grep novell`

7a Si existen errores, ejecute el comando siguiente para solucionarlos:

`rpm --rebuilddb --dbpath <install_location>/rpm`

Ejemplo: `# rpm --rebuilddb --dbpath /custom/rpm`

7b Ejecute el comando que se menciona en el paso 7 para asegurarse de que no hay ningún error.

8 Repita este procedimiento en:

- Instancias de Collector Manager
- Instancias de Correlation Engine
- Instancias de NetFlow Collector Manager

9 Reinicie el servicio Sentinel:

`rcsentinel restart`

Este paso no es aplicable a la alta disponibilidad (HA) de Sentinel.

29 Actualización del dispositivo Sentinel

Los procedimientos descritos en este capítulo le guiarán por el proceso de actualización del dispositivo Sentinel. Puede optar por actualizar Sentinel sin actualizar el sistema operativo SLES o actualizar tanto Sentinel como el sistema operativo SLES. Dado que el dispositivo Sentinel 8.2 incluye SLES 12 SP 3, se ha dejado de utilizar el canal de actualizaciones de SLES 11 y se eliminará cuando SUSE finalice la compatibilidad general con SLES 11. Por lo tanto, debe actualizar al dispositivo Sentinel 8.2, que incluye el sistema operativo SLES 12 SP3 para poder seguir recibiendo actualizaciones del sistema operativo. Debe actualizar Sentinel antes de actualizar el sistema operativo.

Actualización de Sentinel

Actualización de Sentinel mediante el canal de actualización de dispositivos

Puede actualizar Sentinel mediante Zypper. Zypper es un gestor de paquetes de línea de comandos que permite llevar a cabo una actualización interactiva del dispositivo. En casos donde se requiere la interacción del usuario para completar la actualización, por ejemplo, una actualización de acuerdo de licencia de usuario final, debe actualizar el dispositivo de Sentinel mediante Zypper.

Para actualizar el dispositivo mediante el canal de actualización de dispositivos:

1. Realice una copia de seguridad de su configuración y luego cree una exportación de ESM.

   Para obtener más información, consulte “Backing Up and Restoring Data (Copia de seguridad y restauración de datos)” en la *Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.

2. (Condicional) Si ha personalizado los ajustes de configuración en los archivos `server.xml`, `collector_mgr.xml` o `correlation_engine.xml`, asegúrese de que ha creado los archivos de propiedades adecuados con el nombre de obj-component id para estar seguro de que las personalizaciones se mantendrán después de la actualización. Para obtener más información, consulte “Maintaining Custom Settings in XML Files” (Cómo mantener los ajustes personalizados en los archivos XML) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

3. Entre a la consola de la aplicación como usuario `root`.

4. Ejecute el comando siguiente:

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

5. (Condicional) Si el programa de instalación muestra un mensaje en el que se le solicita que debe determinar una dependencia para el paquete OpenSSH, introduzca la opción adecuada para volver a la versión anterior del paquete OpenSSH.
6. (Condicional) Si el programa de instalación muestra un mensaje que indica el cambio en la arquitectura ncgOverlay, introduzca la opción adecuada para aceptar el cambio de arquitectura.
7. (Condicional) Si el programa de instalación muestra un mensaje en el que se le indica que debe determinar una dependencia para ciertos paquetes del dispositivo, introduzca la opción adecuada para desinstalar los paquetes dependientes.
8. Pulse `S` para continuar.
9. Pulse `sí` para aceptar el acuerdo de licencia.
10. Reinicie la aplicación Sentinel.
11. (Condicional) Si Sentinel está instalado en un puerto personalizado, o si Collector Manager o Correlation Engine están en modo FIPS, ejecute el comando siguiente:

    ```
    /opt/novell/sentinel/setup/configure.sh
    ```
12. Borre la memoria caché del navegador web para ver la versión más reciente de Sentinel.
13. Borre la caché de Java Web Start en los equipos cliente para utilizar la versión más reciente de las aplicaciones Sentinel.

    La caché de Java Web Start se puede borrar con el comando `javaws -clearcache` o desde Control Center de Java. Para obtener más información, vaya al sitio http://www.java.com/es/download/help/plugin_cache.xml.
14. (Condicional) Si se ha actualizado la base de datos PostgreSQL a una versión importante (por ejemplo, de 8.0 a 9.0 o de 9.0 a 9.1), elimine los archivos PostgreSQL antiguos de la base de datos PostgreSQL. Para obtener información sobre si se ha actualizado la base de datos PostgreSQL, consulte las notas de la versión de Sentinel.

    14a Cambie al usuario novell.

    ```
    su novell
    ```

    14b Busque en la carpeta `bin`:

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

    14c Elimine todos los archivos postgreSQL antiguos mediante el siguiente comando:

    ```
    ./delete_old_cluster.sh
    ```
15. (Condicional) Para actualizar Collector Manager o Correlation Engine, siga del Paso 3 alPaso 11 .
16. (Condicional) Si utiliza la autenticación Kerberos, habilite AES256 en Java Runtime Environment, ya que la carpeta `java` se reemplaza con archivos por defecto durante la actualización. Para habilitar AES256 en Java Runtime Environment, complete los siguientes pasos:

    16a Descargue Java Cryptography Extension (JCE) 8 en la siguiente ubicación: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

    16b Extraiga los dos archivos `*.jar` y cópielos en el directorio `/opt/novell/sentinel/jdk/jre/lib/security`.

    16c Reinicie Sentinel.
17. (Condicional) Si ejecuta Sentinel en un entorno de alta disponibilidad, repita estos pasos en todos los nodos del clúster.

18 (Condicional) Para actualizar el sistema operativo, consulte “Actualización del sistema operativo” en la página 162.

19 Reinicie Sentinel.

Actualización de Sentinel mediante SMT

En entornos protegidos en los que el dispositivo debe ejecutarse sin acceso directo a Internet, debe configurar el dispositivo con la herramienta SMT (Subscription Management Tool), que le permite actualizar el dispositivo a las versiones más recientes disponibles.

1 Asegúrese de que la aplicación está configurada con SMT.

Para obtener más información, consulte la “Configuración del dispositivo con SMT” en la página 108.

2 Realice una copia de seguridad de su configuración y luego cree una exportación de ESM.

Para obtener más información, consulte “Backing Up and Restoring Data (Copia de seguridad y restauración de datos)” en la *Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.

3 (Condicional) Si ha personalizado los ajustes de configuración en los archivos `server.xml`, `collector_mgr.xml` o `correlation_engine.xml`, asegúrese de que ha creado los archivos de propiedades adecuados con el nombre de obj-component id para estar seguro de que las personalizaciones se mantendrán después de la actualización. Para obtener más información, consulte “Maintaining Custom Settings in XML Files” (Cómo mantener los ajustes personalizados en los archivos XML) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

4 Entre a la consola de la aplicación como usuario `root`.

5 Actualice el repositorio para la actualización:

```
zypper ref -s
```

6 Compruebe si la aplicación está habilitada para la actualización:

```
zypper lr
```

7 (Opcional) Compruebe las actualizaciones disponibles para la aplicación:

```
zypper lu
```

8 (Opcional) Compruebe los paquetes que incluyen las actualizaciones disponibles para la aplicación:

```
zypper lp -r SMT-http_<smt_server_fqdn>:<package_name>
```

9 Actualice la aplicación:

```
zypper up -t patch -r SMT-http_<smt_server_fqdn>:<package_name>
```

10 Reinicie el dispositivo.

```
rcsentinel restart
```

11 (Condicional) Si Sentinel está instalado en un puerto personalizado, o si Collector Manager o Correlation Engine están en modo FIPS, ejecute el comando siguiente:

```
/opt/novell/sentinel/setup/configure.sh
```

12 (Condicional) Para actualizar Collector Manager o Correlation Engine, siga del Paso 4 alPaso 11 .

13 (Condicional) Si utiliza la autenticación Kerberos, habilite AES256 en Java Runtime Environment, ya que la carpeta `java` se reemplaza con archivos por defecto durante la actualización. Para habilitar AES256 en Java Runtime Environment, complete los siguientes pasos:

13a Descargue Java Cryptography Extension (JCE) 8 en la siguiente ubicación: `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`

13b Extraiga los dos archivos `*.jar` y cópielos en el directorio `/opt/novell/sentinel/jdk/jre/lib/security`.

13c Reinicie Sentinel.

14 (Condicional) Si ejecuta Sentinel en un entorno de alta disponibilidad, repita estos pasos en todos los nodos del clúster.

15 (Condicional) Para actualizar el sistema operativo, consulte “Actualización del sistema operativo” en la página 162.

16 Reinicie Sentinel.

Actualización del sistema operativo

Debe actualizar el sistema operativo después de actualizar Sentinel. Después de actualizar el sistema operativo, debe configurar el dispositivo para aprovechar las nuevas funciones de Sentinel Appliance Manager. Sentinel Appliance Manager proporciona una interfaz de usuario sencilla basada en la Web que le ayuda a configurar y administrar el dispositivo. Esta carpeta reemplaza a la funcionalidad existente de WebYast.

Para actualizar el sistema operativo y configurar el dispositivo:

1 Actualice Sentinel. Para obtener más información, consulte el “Actualización de Sentinel” en la página 159.

2 Detenga los servicios de Sentinel:

```
rcsentinel stop
```

3 (Condicional) Si Sentinel estaba en modo FIPS antes de la actualización del sistema operativo, los archivos de base de datos NSS deben actualizarse manualmente ejecutando el siguiente comando:

```
certutil -K -d sql:/etc/opt/novell/sentinel/3rdparty/nss -X
```

Siga las instrucciones en pantalla para actualizar la base de datos NSS.

Proporcione permisos totales al usuario `novell` para los siguientes archivos:

```
cert9.db
key4.db
pkcs11.txt
```

4 (Condicional) Si utiliza Mozilla Network Security Services (NSS) 3.29, no se instalarán dos archivos RPM dependientes `libfreebl3-hmac` y `libsoftokn3-hmac`. Instale de forma manual los siguientes archivos RPM: `libfreebl3 hmac y libsoftokn3 hmac`.

5 Descargue el instalador de SLES 12 SP3 y la utilidad posterior a la actualización desde el sitio Web de Micro Focus Patch Finder. Para obtener la función de alta disponibilidad de Sentinel, descargue también el archivo SLES 12 SP3 HA.

6 Siga las instrucciones de instalación para actualizar el sistema operativo. Para obtener la función de alta disponibilidad de Sentinel, cuando se le solicite la instalación de productos complementarios adicionales, seleccione la ubicación en la que ha descargado el archivo SLES 12 SP3 HA y continúe con la actualización.

   Para obtener más información sobre la actualización a SLES 12 SP3, consulte la documentación de SLES.

7 Durante el proceso de actualización, SLES cambia el nombre del archivo `/etc/sysctl.conf` a `/etc/sysctl.conf.rpmsave` como una copia de seguridad y crea un nuevo archivo `/etc/sysctl.conf`. Después de la actualización, copie el contenido del archivo `/etc/sysctl.conf.rpmsave` en el archivo`/etc/sysctl.conf`. Abra el archivo `sysctl.conf` y busque `# Added by sentinel vm.max_map_count`. Desplace este ajuste a la línea siguiente, como se indica a continuación:

   Cambio

   ```
   net.core.wmem_max = 67108864# Added by sentinel vm.max_map_count : 65530
   vm.max_map_count = 262144
   ```

   a

   ```
   net.core.wmem_max = 67108864
   # Added by sentinel vm.max_map_count : 65530
   vm.max_map_count = 262144
   ```

8 (Condicional) Para obtener la función de alta disponibilidad de Sentinel, siga los pasos indicados en las secciones siguientes:

   - “Configuración de destinos iSCSI” en la página 218
   - “Configuración de iniciadores iSCSI” en la página 219
   - “Configuración del clúster de HA” en la página 220

9 Para configurar el dispositivo, ejecute la utilidad posterior a la actualización desde el indicador de comandos:

   9a Desempaquete el archivo:

   `tar -xvf <nombre de archivo del instalador de la utilidad posterior a la actualización>.tar.gz`

   9b Acceda al directorio en el que ha extraído la utilidad:

   `cd <nombre de archivo del instalador de la utilidad posterior a la actualización>`

   9c Para configurar el dispositivo, ejecute el siguiente guión:

   `./appliance_SLESISO_post_upgrade.sh`

   Nota: No ejecute este guión de forma remota, ya que este conlleva una nueva configuración de red.

   9d Siga las instrucciones que aparecen en pantalla para completar la configuración.

   Este guión configura de nuevo los paquetes instalados y configura los paquetes para la gestión de dispositivos.

10 Mediante el código de registro existente, regístrese de nuevo para recibir las actualizaciones más recientes del sistema operativo y Sentinel. Para obtener más información, consulte el “Registro para recibir actualizaciones” en la página 106.

30 Configuraciones posteriores a la actualización

En este capítulo se especifican las configuraciones que se deben realizar tras la actualización.

Protección de datos en Elasticsearch

Sentinel utiliza Kibana, una consola de análisis y búsqueda basada en navegador, que ayuda a visualizar eventos y alertas en consolas. Sentinel almacena e indexa alertas en Elasticsearch. Puede configurar Sentinel para almacenar e indexar también eventos de Elasticsearch a fin de aprovechar las funciones visualización de eventos. Las consolas de Sentinel acceden a los datos de Elasticsearch para presentar eventos y alertas en consolas. Para garantizar que en las consolas solo se muestren los datos que puede ver la función de un usuario y evitar el acceso no autorizado a los datos de Elasticsearch, debe instalar el módulo auxiliar (plug-in) de seguridad de Elasticsearch. Para obtener más información, consulte “Protección de datos en Elasticsearch” en la página 79.

Configuración de visualizaciones de eventos

Sentinel proporciona visualizaciones de eventos que presentan datos en gráficos, tablas y mapas. Estas visualizaciones facilitan la visualización y el análisis de grandes volúmenes de datos, como eventos, eventos de flujo IP y alertas. También puede crear sus propias visualizaciones y consolas.

Sentinel hace uso de Kibana, una consola de búsqueda y análisis basada en navegador, que le ayuda a buscar y visualizar eventos. Kibana accede a los datos del almacén de datos de visualización (Elasticsearch) para presentar los eventos en las consolas. Sentinel incluye por defecto un nodo de Elasticsearch. Debe habilitar la visualización de eventos para almacenar e indexar los eventos en Elasticsearch. Para obtener más información, consulte “Configuración del almacén de datos de visualización” en la página 43.

Nota: Algunas de las consolas de Sentinel que utilizan Kibana no se cargan después de actualizar a Sentinel 8.2. Este problema se produce porque las versiones de Elasticsearch y Kibana se han actualizado a Sentinel 8.2 y el archivo de índice de Kibana existente no es compatible con las

versiones actualizadas de Elasticsearch y Kibana. Para solucionar este problema, debe eliminar manualmente el archivo de índice de Kibana existente y volver a crear un nuevo archivo de índice Kibana. Para obtener más información, consulte el artículo de Knowledge Base 7022736.

Configuración de la recopilación de datos de flujo IP

Sentinel utiliza ahora ArcSight SmartConnectors que ayudan a supervisar la red empresarial mediante la recopilación de datos de flujo IP, además de datos de NetFlow. Los SmartConnectors recopilan datos de flujo IP como eventos, lo que permite:

- Utilizar instancias existentes de Collector Manager para recopilar datos de flujo IP. Ya no necesitará utilizar instancias de NetFlow Collector Manager para recopilar datos de NetFlow.
- Aprovechar los datos de flujos IP en varias áreas de Sentinel, como visualizaciones, encaminamiento de eventos, federación de datos, informes y correlación.
- Aplique directivas de retención de datos a los datos de flujo IP, lo le permite almacenar estos datos durante el tiempo deseado.

Después de actualizar a Sentinel, puede seguir utilizando las funciones de NetFlow u optar por configurar la recopilación de datos de flujo IP. Sin embargo, con la disponibilidad de las funciones de visualización y recopilación de datos de flujo IP, las funciones de NetFlow disponibles anteriormente, incluidas las vistas de NetFlow, se han dejado de utilizar y se eliminarán en el futuro para mejorar la experiencia del usuario.

Una vez que haya habilitado la recopilación de datos de flujo IP:

- Los datos de flujo IP se recopilarán como eventos y, por lo tanto, se tendrán en cuenta para el recuento de EPS.
- Se perderán los datos de NetFlow recopilados antes de habilitar el flujo IP. El sistema NetFlow obsoleto contaba con un máximo de retención de 3 días. Puede conservar los eventos de flujo IP durante el tiempo que sea necesario.
- No puede migrar los datos de NetFlow recopilados antes de habilitar el flujo IP en la función de flujo IP.
- No se puede recuperar la configuración a menos que se instale de nuevo Sentinel.
- Saldrá de Sentinel Main y deberá entrar de nuevo.

Para configurar la recopilación de datos de flujo IP:

1. Instale y configure ArcSight SmartConnector. Durante la configuración, asegúrese de configurar los SmartConnectors pertinentes que recopilan datos de flujo IP.

   Para obtener información sobre la configuración de SmartConnectors, consulte la documentación de Generic Universal CEF Collector en el sitio Web de módulos auxiliares (plug-ins) de Sentinel.
2. En **Sentinel Main** > **Recopilación** > **Flujo IP**, seleccione **Recopilar datos de flujo IP** y, a continuación, haga clic en **Habilitar**.

Nota: Dado que los eventos de flujo IP ahora se envían a Collector Manager, ya no es necesario utilizar las instancias de NetFlow Collector Manager. Por lo tanto, puede desinstalar las instancias existentes de NetFlow Collector Manager. Para obtener más información, consulte “Desinstalación de NetFlow Collector Manager” en la página 234.

Configuración posterior a la actualización de Sentinel Scalable Data Manager

Instalación del módulo auxiliar (plug-in) de Elasticsearch

Además de los nodos de Elasticsearch externos, Sentinel ahora incluye por defecto un nodo de Elasticsearch local para la visualización de datos. Por lo tanto, debe instalar un módulo auxiliar (plug-in) de Elasticsearch para el nodo de Elasticsearch local. Para obtener más información, consulte “Instalación del módulo auxiliar (plug-in) de Elasticsearch” en la página 80.

Al actualizar las instancias de Elasticsearch y Kibana utilizadas Sentinel, debe implantar de nuevo los módulos auxiliares (plug-ins) de seguridad de Elasticsearch en los nodos de Elasticsearch existentes. Para obtener información sobre cómo implantar de nuevo el módulo auxiliar (plug-in) de seguridad de Elasticsearch, consulte “Nueva implantación del módulo auxiliar (plug-in) de Elasticsearch” en la página 84.

Presentación de aplicaciones de Spark en YARN

Durante la actualización de Sentinel, se actualizan también algunos de los archivos de la aplicación Spark. Debe volver a enviar las aplicaciones Spark con estos archivos actualizados llevando a cabo los pasos siguientes:

1. Entre en el servidor SSDM como usuario `novell` y copie los archivos en el servidor de historial de Spark donde está instalado HDFS NameNode:

   ```
   cd /etc/opt/novell/sentinel/scalablestore
   ```

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

   donde <*directorio_de_destino*> es cualquier directorio donde desee colocar los archivos copiados. Además, asegúrese de que el usuario `hdfs` dispone de permisos totales para este directorio.

2. Entre en el servidor <*hdfs_node*> como usuario root y cambie la propiedad de los archivos copiados al usuario `hdfs`:

   ```
   cd <directorio_de_destino>
   ```

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

   Asigne el permiso ejecutable al guión `manage_spark_jobs.sh`.

3. Asegúrese de que las tareas de Spark han finalizado el procesamiento de todos los datos:

   Vaya a la interfaz de usuario Web de ResourceManager de YARN y vea cada aplicación Spark de Sentinel. Los datos de la aplicación Spark Streaming mostrarán la reducción de la tasa de entrada a cero cuando se hayan procesado todos los datos desde Kafka.

4. Ejecute el siguiente comando para detener el procesamiento de datos:

   ```
   ./manage_spark_jobs.sh stop
   ```

5 Borre el punto de comprobación de procesamiento de datos:

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

donde `/chispa/checkpoint` es el directorio de punto de comprobación.

6 Ejecute el siguiente guión para volver a enviar las tareas de Spark:

```
./manage_spark_jobs.sh start
```

El comando anterior tardará un rato en finalizar el proceso de envío.

7 (Opcional) Ejecute el siguiente comando para verificar el estado de las tareas de Spark enviadas:

```
./manage_spark_jobs.sh status
```

8 Reanude el reenvío de eventos a Kafka para que Spark inicie el procesamiento de los mismos:

8a En Sentinel principal, haga clic en **Storage** (Almacenamiento) > **Scalable Storage** (Almacenamiento ampliable) > **Advanced Configuration** (Configuración avanzada) > **Kafka** (Kafka).

8b Defina la siguiente propiedad como falsa:

```
pause.events.tokafka
```

8c Haga clic en **Guardar**.

Habilitación de funciones de Sentinel

Cuando actualiza desde SSDM 8.0.*x.x*, algunas de las funciones de Sentinel añadidas en Sentinel 8.1 y versiones posteriores no están disponibles por defecto. Debe habilitar manualmente las funciones del archivo `/etc/opt/novell/sentinel/config/ui-configuration.properties`.

1 Entre en el servidor de Sentinel como el usuario `novell`.

2 Abra el archivo `/etc/opt/novell/sentinel/config/ui-configuration.properties`.

3 Cambie el ajuste de las siguientes propiedades a falso:

```
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 Actualice el navegador de Sentinel.

Actualización de los paneles y visualizaciones en Sentinel Scalable Data Manager

Debe actualizar las consolas y las visualizaciones después de actualizar SSDM para que se apliquen las mejoras incluidas en la versión más reciente de las consolas y las visualizaciones.

Cuando se actualiza SSDM, las consolas y visualizaciones no se actualizan de forma predeterminada. Sin embargo, puede actualizarlas manualmente tras la actualización. Puede actualizar las consolas y las visualizaciones eliminando las ya existentes y ejecutando el guión `load_kibana_data.sh`, que instala las consolas y visualizaciones más recientes.

Importante: Se perderán las personalizaciones que haya realizado en las consolas y visualizaciones una vez las actualice.

Para actualizar las visualizaciones y consolas:

1. Inicie sesión en la interfaz Web de SSDM y diríjase a la Visualización de eventos.
2. En la Visualización de eventos, diríjase a **Ajustes** > **Objetos** > **Consolas**.
3. Seleccione las consolas que desea actualizar y haga clic en **Suprimir**.
4. Haga clic en **Visualizaciones**. Seleccione las visualizaciones que desea actualizar y haga clic en **Suprimir**.
5. Salga de la sesión en la interfaz Web de Sentinel.
6. Entre en el servidor de SSDM como el usuario `novell`.
7. Diríjase al directorio `/opt/novell/sentinel/bin`.
8. Ejecute el guión `load_kibana_data.sh` empleando el siguiente comando:

   ```
   ./load_kibana_data.sh http://<dirección ip>:<puerto>> <alerts/events/misc>
   ```

   Por ejemplo:

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

   ```
   ./load_kibana_data.sh http://127.0.0.1:9200 events
   ```
9. Inicie sesión en la interfaz Web de SSDM y diríjase a la Visualización de eventos para ver las consolas y visualizaciones actualizadas.

Adición del controlador JDBC DB2

Después de actualizar a Sentinel, añada el controlador JDBC correcto y configúrelo para la recopilación y sincronización de datos. Siga estos pasos para hacerlo:

1. Copie la versión correcta del controlador IBM DB2 JDBC (`db2jcc-*.jar`) para su versión de base de datos DB2 en la carpeta `/opt/novell/sentinel/lib`.
2. Asegúrese de definir la propiedad y los permisos necesarios para el archivo de controlador.
3. Configure este controlador para la recopilación de datos. Para obtener más información, consulte la documentación del conector de base de datos.

Configuración de las propiedades de federación de datos en la aplicación Sentinel

Siga este procedimiento tras actualizar la aplicación Sentinel, de modo que la federación de datos no muestre ningún error en el entorno si hay dos o más tarjetas NIC configuradas:

1. En el servidor del solicitante autorizado, añada la siguiente propiedad al archivo `/etc/opt/novell/sentinel/config/configuration.properties` de este modo:

   ```
   sentinel.distsearch.console.ip=<una de las direcciones IP del solicitante autorizado>
   ```
2. En el servidor de origen de datos, añada la siguiente propiedad al archivo `/etc/opt/novell/sentinel/config/configuration.properties` de este modo:

   ```
   sentinel.distsearch.target.ip=<una de las direcciones IP del origen de datos>
   ```
3. Reinicie Sentinel:

```
rcsentinel restart
```

4 Entre en el servidor del solicitante autorizado y haga clic en Integración. Si el origen de datos que desea añadir ya existe, suprímalo y añádalo de nuevo con una de las direcciones IP que especificó en el paso 2.

   Del mismo modo, añada solicitantes autorizados utilizando las direcciones IP especificadas en el paso 1.

Registro del dispositivo Sentinel para recibir actualizaciones

Si ha actualizado el sistema operativo, debe volver a registrar el dispositivo Sentinel para recibir las actualizaciones más recientes del sistema operativo y Sentinel. Puede utilizar la clave de registro existente para volver a registrarse a fin de recibir actualizaciones. Para registrar el dispositivo, consulte “Registro para recibir actualizaciones” en la página 106.

Actualización de bases de datos externas para la sincronización de datos

A partir de Sentinel 8.x, el tamaño del campo de evento `Mensaje (msj)` se ha aumentado de 4000 a 8000 caracteres para dar cabida a más información en el campo.

Si ha creado una directiva de sincronización de datos en las versiones anteriores de Sentinel que sincroniza el campo de evento Mensaje (msj) con una base de datos externa, debe aumentar el tamaño de la columna asignada correspondiente en la base de datos externa en consecuencia.

Nota: El paso anterior solo es aplicable si va a actualizar versiones anteriores de Sentinel a 8.x.

Nueva autenticación de Sentinel en modo de autenticación múltiple

Si se actualiza el servidor de Sentinel en modo MFA, las instancias existentes de NetFlow Collector Manager no se autentican automáticamente en el servidor de Sentinel. Debe realizar los siguientes pasos para volver a autenticar manualmente las instancias de NetFlow Collector Manager en el servidor de Sentinel.

Para volver a autenticar Sentinel en modo MFA:

1 Entre en el equipo de NetFlow Collector Manager.

2 Vaya a `/opt/novell/sentinel/setup`.

3 Ejecute el guión `configure.sh`.

   Se le solicitará que entre en el servidor de Sentinel.

4 Especifique el nombre de usuario y la contraseña de LDAP.

5 Proporcione el ID y el secreto de cliente de Sentinel.

   Para recuperar el secreto de cliente de Sentinel y el ID de cliente de Sentinel, vaya a la siguiente dirección URL:

   `https://Sentinel_FQDN:port/SentinelAuthServices/oauth/clients`

Dónde:

- `Sentinel_FQDN` es el nombre de dominio completo del servidor de Sentinel.

  Por ejemplo, `abc.netiq.com`

  donde `abc` es el nombre de host del servidor de Sentinel y `netiq.com` es el nombre de dominio.

- `Puerto` es el puerto que utiliza Sentinel (normalmente 8443).

La dirección URL especificada utiliza la sesión actual de Sentinel para recuperar el secreto de cliente de Sentinel y el ID de cliente de Sentinel.

31 Actualización de módulos auxiliares (plug-in) de Sentinel

Las instalaciones de actualizaciones de Sentinel no actualizan los módulos auxiliares (plug-ins) a menos que uno de los módulos auxiliares no sea compatible con la versión más reciente de Sentinel.

Los módulos auxiliares (plug-in) nuevos y actualizados de Sentinel, incluidos los paquetes de soluciones, se cargan con frecuencia en el sitio Web de módulos auxiliares (plug-ins) de Sentinel . Para obtener las correcciones de defectos, documentación y mejoras más recientes de un módulo auxiliar (plug-in), descargue e instale la versión más reciente de dicho módulo auxiliar. Para obtener más información sobre cómo instalar un módulo auxiliar (plug-in), consulte la documentación específica del módulo auxiliar en cuestión.

VI Migración de datos desde el almacenamiento tradicional

La migración de datos de Sentinel con almacenamiento tradicional permite aprovechar los datos de Sentinel existentes y el tiempo que ha invertido en ellos. Para migrar datos de Sentinel con almacenamiento tradicional, la versión de Sentinel en los servidores de origen y de destino debe ser la misma. Por ejemplo, si desea migrar datos de Sentinel 8.1 (origen) a Sentinel 8.2, debe actualizar Sentinel 8.1 a Sentinel 8.2 y, a continuación, iniciar el proceso de migración de datos.

En esta sección, se proporciona información acerca de la migración de datos existentes al componente de almacén de datos que desee.

32 Migración de datos al almacenamiento ampliable

Puede tener un solo servidor Sentinel o varios servidores de Sentinel con almacenamiento tradicional. El proceso de migración de datos que debe seguir depende de cómo desea realizar la configuración y el mantenimiento de la implantación de Sentinel.

Tabla 32-1 *Proceso de migración de datos para la implementación de Sentinel*

Implementación de Sentinel	Proceso de migración
Dispone de un único servidor de Sentinel y tiene previsto actualizar el servidor de Sentinel existente al almacenamiento ampliable.	Migre los datos de eventos y en bruto del almacenamiento tradicional en el almacenamiento ampliable después de actualizar el servidor de Sentinel y habilitar el almacenamiento ampliable. Para obtener más información, consulte la Capítulo 34, “Migración de datos”, en la página 185.
Dispone de un único servidor de Sentinel con almacenamiento tradicional y desea configurar otro servidor de Sentinel para el almacenamiento ampliable para poder utilizar todas las funciones de Sentinel.	Utilice la utilidad de copia de seguridad y restauración para migrar datos de Sentinel con almacenamiento tradicional a Sentinel con almacenamiento ampliable. Para obtener información acerca del uso de la utilidad de copia de seguridad y restauración, consulte “Backing Up and Restoring Data” (Copia de seguridad y restauración de datos) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Implementación de Sentinel	Proceso de migración
Tiene una configuración multinivel que dispone de varios servidores Sentinel y va a configurar un nuevo servidor de Sentinel o utilizar uno de los servidores existentes para el almacenamiento ampliable; necesita migrar datos de configuración además de los datos de eventos y datos en bruto.	En una configuración de varios niveles, puede identificar uno de los servidores tradicionales de Sentinel que disponga de la mayoría de los datos y, a continuación, utilizar la utilidad de copia de seguridad y restauración para migrar los datos. Si necesita realizar copias de seguridad de los datos desde el resto de los servidores de Sentinel, debe migrar los datos de configuración, los datos de eventos y datos en bruto desde los servidores a través de un enfoque diferente que se describe más adelante en esta sección. Debe también volver a crear manualmente cierta parte de la configuración. No es posible utilizar la utilidad de copia de seguridad y restauración para migrar los datos de varios servidores, ya que la utilidad anula los datos existentes cuando realiza la restauración. Por ejemplo, si ya ha recuperado datos desde un servidor y, a continuación, intenta restaurar los datos del servidor B, esta utilidad reemplaza los datos ya restaurados desde el servidor A. Por lo tanto, para comprender el proceso de migración de datos implicado, siga las instrucciones proporcionadas en las secciones siguientes en el mismo orden: ◆ Datos que puede migrar ◆ Migración de datos de configuración ◆ Migración de datos ◆ Datos de NetFlow y alertas de migración ◆ Actualización de clientes de Sentinel ◆ Importación de la configuración de ESM

Datos que puede migrar

Puede migrar los datos de eventos, los datos en bruto y algunos de los datos de configuración. Se debe volver a crear manualmente el resto de la configuración, que no se puede migrar.

Tabla 32-2 Configuraciones que se pueden migrar y que tiene que volver a crear

Configuraciones que se pueden migrar	Configuraciones que debe volver a crear
◆ Reglas de correlación ◆ Acciones ◆ Asignaciones ◆ Filtros ◆ Fuentes de amenazas ◆ Configuración de ESM ◆ Alertas excepto los datos de la Base de conocimientos ◆ NetFlow	◆ Arrendatarios, Funciones, Usuarios y Configuración LDAP ◆ Eventos y alertas de reglas de encaminamiento ◆ Directivas de retención de alerta y datos ◆ Consolas ◆ Vistas en tiempo real ◆ Información de identidad ◆ Configuración de titulares ◆ Configuración de módulo auxiliar de acciones e integrador ◆ Configuración de seguridad

Migración de datos de configuración

Antes de migrar los datos de eventos, primero debe migrar los datos de configuración al servidor Sentinel de destino. Puede realizar una copia de cierta parte de la configuración mediante el uso de Solution Designer y las opciones de exportación e importación de Gestión de orígenes de eventos (ESM). Se debe volver a crear manualmente el resto de los datos de configuración, que no se pueden copiar ni exportar.

- "Copia de seguridad de datos en el servidor de origen" en la página 179
- "Restauración de datos en el servidor de destino" en la página 180

Copia de seguridad de datos en el servidor de origen

Debe realizar una copia de seguridad los datos necesarios mediante el uso de varias opciones de Sentinel.

- "Uso de paquetes de soluciones" en la página 179
- "Uso de la opción de configuración de exportación de ESM" en la página 180

Uso de paquetes de soluciones

Realice una copia de la siguiente configuración del servidor de origen utilizando Solution Designer:

Tabla 32-3 Datos de configuración

	Datos	Notas
❒	Reglas de correlación	Cree controles independientes para cada instancia de Correlation Engine y así poder migrar las reglas por separado a las instancias de Correlation Engine específicas.

	Datos	Notas
❒	Acciones	Solo puede realizar copias de seguridad de acciones JavaScript y no de acciones heredadas como la lista dinámica y la creación de incidencias.
❒	Enriquecimiento de eventos	Sentinel también realiza una copia de seguridad de las asignaciones asociadas a los campos de evento. Por lo tanto, no es necesario volver a crear las asignaciones asociadas después de restaurar los datos de enriquecimiento de eventos.
❒	Filtros	Realiza una copia de seguridad de todos los filtros personalizados.
❒	Fuentes de información	El paquete de soluciones solo realiza copias de seguridad de los complementos de las fuentes, pero no la de la configuración de estos.

Para obtener información acerca de la copia de seguridad de datos en Solution Designer, consulte la sección "Creating Solution Packs" (Creación de paquetes de soluciones) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Uso de la opción de configuración de exportación de ESM

Realice una copia de seguridad de la configuración de recopilación de datos mediante la opción de configuración de exportación de ESM. Para obtener más información, consulte la sección "Exporting Configurations" (Exportación de configuraciones) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Restauración de datos en el servidor de destino

- "Instalación de los datos de configuración del paquete de soluciones" en la página 180
- "Volver a crear la configuración de forma manual" en la página 180

Instalación de los datos de configuración del paquete de soluciones

Importe los datos de configuración de los cuales realizó una copia de seguridad en el servidor de origen utilizando Solution Designer. Para obtener más información, consulte "Installing Content from Solution Packs" (Instalación de contenido de los paquetes de soluciones) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Cambie el nombre de los nombres de objetos como los filtros, las acciones y las reglas de correlación. Por defecto, todos los filtros son públicos al importarlos en el servidor de destino. Vuelva a asignar manualmente el permiso para cada filtro.

Volver a crear la configuración de forma manual

Además de los datos de configuración que se han importado del paquete de soluciones, se deben volver a crear manualmente todas las demás configuraciones. Para obtener más información acerca de las configuraciones que deba volver a crear manualmente, consulte la sección Tabla 32-2, "Configuraciones que se pueden migrar y que tiene que volver a crear", en la página 179.

Migración de datos de eventos y datos en bruto

Para migrar datos de eventos y en bruto, consulte Migración de datos.

Datos de NetFlow y alertas de migración

Puede utilizar la utilidad de copia de seguridad y restauración para migrar datos de NetFlow y alertas desde el servidor de origen al servidor de destino. Con respecto a las alertas, esta utilidad restaura los eventos que activaron la alerta. Sin embargo, no restaura la información de la base de conocimiento y la regla de correlación asociada.

Utilice los siguientes comandos para realizar copias de seguridad de y restaurar datos de NetFlow y alertas:

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

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

Con respecto a los datos de NetFlow y las alertas, dispone de una opción para redefinir o para realizar una adición al final de los datos existentes. Elija la opción que desee.

Aunque el comando anterior realiza copias de seguridad de y restaura los datos de inteligencia de seguridad, no puede utilizar estos datos la inteligencia de seguridad no está disponible en SSDM.

Para obtener información acerca del uso de la utilidad de copia de seguridad y restauración, consulte "copia de seguridad y restauración de datos" en la *Guía de administración de Sentinel*.

Actualización de clientes de Sentinel

Debe actualizar las configuraciones de Collector Manager, Correlation Engine y NetFlow Collector Manager existentes de forma que empiecen a comunicarse con el servidor Sentinel de destino. Para obtener más información, consulte la sección "Updating Sentinel Clients" (Actualización de clientes de Sentinel) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Nota: Aunque ya haya migrado los datos de eventos del servidor de origen, debe ejecutar de nuevo el guión de migración de datos para migrar los datos de eventos que puedan haber llegado durante o después de este proceso de migración de datos. Para obtener más información, consulte la Capítulo 34, "Migración de datos", en la página 185.

Importación de la configuración de ESM

Importe la configuración de recopilación de datos utilizada en el servidor de origen mediante la opción de configuración de importación en la interfaz de usuario ESM. Para obtener más información, consulte la sección "Importing Configurations" (Importación de configuraciones) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

33 Migración de datos a Elasticsearch

Sentinel almacena datos en el almacenamiento tradicional basado en archivos e indexa por defecto los datos de forma local en el servidor de Sentinel. Al habilitar la visualización de eventos, Sentinel almacena e indexa los datos en Elasticsearch, además de en el almacenamiento tradicional basado en archivos. En las consolas, solo se muestran los eventos procesados después de habilitar la visualización de eventos. Para ver los eventos existentes presentes en el almacenamiento basado en archivos, debe migrar los datos del almacenamiento basado en archivos a Elasticsearch. Para migrar datos a Elasticsearch, consulte Capítulo 34, “Migración de datos”, en la página 185.

34 Migración de datos

Puede utilizar el guión `data_uploader.sh` para migrar los datos a uno de los siguientes componentes de almacenamiento de datos:

- **Kafka:** Puede migrar datos de eventos y en bruto a Kafka. Ejecute el guión de forma individual para los datos de eventos y datos en bruto. El guión migra los datos a los temas de Kafka.

  Puede especificar personalizaciones, como la compresión de datos durante la migración, el envío de datos en lotes, etc. Para especificar estas personalizaciones, cree un archivo de propiedades y añadir las propiedades requeridas en formato valor-clave. Por ejemplo, puede añadir propiedades de la siguiente forma:

  ```
  compression.type=lz4

  batch.size=20000
  ```

  Para obtener información acerca de las propiedades de Kafka, consulte la sección Kafka documentation (Documentación de Kafka). Defina las propiedades y sus valores según su criterio debido a que el guión no valida estas propiedades.

  Nota: Asegúrese de que el servidor de Sentinel pueda resolver todos los nombres de host de intermediario de Kafka con direcciones IP válidas para todo el clúster de Kafka. Si no se ha configurado el DNS para habilitar esto, añada los nombres de host de intermediario de Kafka al archivo `/etc/hosts` del servidor de Sentinel.

- **Elasticsearch:** Solo puede migrar datos de eventos en Elasticsearch. Antes de migrar los datos, asegúrese de que ha habilitado la visualización de eventos. Para obtener más información, consulte “Habilitación de la visualización de eventos” en la página 125.

El guión transfiere datos para el rango de datos (desde y a) que especifique. Al ejecutar el guión, se muestran los parámetros obligatorios y opcionales que debe especificar para iniciar la migración de datos y también la información sobre las propiedades correspondientes que se deben utilizar para el componente de almacenamiento de datos deseado.

El guión debe ejecutarse como usuario novell. Por lo tanto, asegúrese de que los directorios de datos y los archivos que especifique dispongan de los permisos adecuados para el usuario novell. Por defecto, el guión migra los datos desde el almacenamiento principal. Si desea migrar los datos desde el almacenamiento secundario, especifique la vía adecuada para el almacenamiento secundario cuando se ejecute el guión.

Para migrar los datos:

1. Entre en el servidor de Sentinel como el usuario novell.
2. Ejecute el guión siguiente:

   ```
   /opt/novell/sentinel/bin/data_uploader.sh
   ```

3. Siga las instrucciones en pantalla y ejecute el guión de nuevo con los parámetros necesarios.

Los datos migrados tendrán el período de retención que se haya definido en el servidor de destino.

Una vez que finalice la migración de datos, el guión registra el estado, como las particiones que se han migrado correctamente, las particiones que no se han podido migrar, el número de eventos migrados, etc. Para las particiones con fecha del día actual y el día anterior, el estado de transferencia de datos se mostrará IN_PROGRESS teniendo en cuenta los eventos que puedan entrar más tarde.

Vuelva a ejecutar el guión cuando no se haya completado correctamente la migración de datos o el estado de migración de datos de las particiones aún indique IN_PROGRESS. Al volver a ejecutar el guión, se comprueba primero el archivo de estado para conocer las particiones que ya se han migrado y, a continuación, se siguen migrando solo las restantes. El guión mantiene los registros en el directorio /`var/opt/novell/sentinel/log/data_uploader.log` con el fin de solucionar problemas.

VII Implantación de Sentinel para alta disponibilidad

En esta sección se proporciona información acerca de la instalación de Sentinel en modo de alta disponibilidad Activo-Pasivo, que permite a Sentinel realizar un failover a un nodo de clúster redundante en caso de producirse un fallo del hardware o software. Para obtener más información sobre cómo implementar la alta disponibilidad y la recuperación tras fallos en el entorno Sentinel, póngase en contacto con el servicio de Asistencia técnica de .

Nota: La configuración de alta disponibilidad (HA) solo se admite en el servidor de Sentinel. Sin embargo, las instancias de Collector Manager y Correlation Engine aún pueden comunicarse con el servidor Sentinel de alta disponibilidad.

35 Conceptos

Alta disponibilidad se refiere a una metodología de diseño destinada a mantener la disponibilidad de un sistema para su utilización en la máxima medida posible. La intención es reducir al mínimo las causas de tiempo de inactividad, como por ejemplo fallos del sistema y mantenimiento y minimizar el tiempo que se tarda en detectar y recuperarse de los eventos que producen tiempo de inactividad cada vez que ocurran. En la práctica, se hace necesario contar con un medio automatizado para detectar y recuperarse rápidamente los eventos que causan tiempo de inactividad a medida que se deben obtener niveles más altos de disponibilidad.

Para obtener más información acerca de la alta disponibilidad, consulte la SUSE High Availability Guide (Guía de alta disponibilidad de SUSE).

Sistemas externos

Sentinel es una aplicación compleja multinivel que depende de y proporciona una amplia variedad de servicios. Por otro lado, se integra con varios sistemas de terceros externos para la recopilación de datos, uso compartido de datos y resolución de incidencias. La mayoría de soluciones de alta disponibilidad (HA) permiten a los encargados de implementarlas declarar dependencias entre los servicios que deben estar altamente disponibles, pero esto solo se aplica a los servicios que se ejecutan en el propio clúster. Los sistemas externos a Sentinel como los orígenes de eventos deben configurarse por separado para tener la disponibilidad que requiere la organización, y también deben configurarse para manejar correctamente situaciones en las que Sentinel no está disponible durante un cierto período de tiempo, como por ejemplo cuando se produce un evento de failover. Si los derechos de acceso están muy restringidos, por ejemplo, si se utilizan sesiones autenticadas para enviar o recibir datos entre un sistema de terceros y Sentinel, entonces el sistema de terceros debe configurarse para aceptar las sesiones procedentes de cualquier nodo del clúster o para iniciar sesión en cualquier nodo del clúster (para este fin, Sentinel debe configurarse con una dirección IP virtual).

Almacenamiento compartido

Todos los clústeres de alta disponibilidad (HA) requieren alguna forma de almacenamiento compartido que permita mover rápidamente los datos de aplicaciones de un nodo de clúster a otro en caso de fallo del nodo de origen. El almacenamiento en sí debería tener una alta disponibilidad; eso se consigue por lo general mediante la tecnología de Red de área de almacenamiento (SAN) conectada a los nodos del clúster mediante una red de Canal de fibra. Otros sistemas utilizan Almacenamiento con interconexión a la red (NAS), iSCSI u otras tecnologías que permiten el

montaje remoto de almacenamiento compartido. El requisito fundamental del almacenamiento compartido es que el clúster pueda mover de forma transparente el almacenamiento desde un nodo de clúster que ha fallado a un nuevo nodo de clúster.

Existen dos planteamientos básicos que puede usar Sentinel para el almacenamiento compartido. El primero localiza todos los componentes (binarios de aplicaciones, configuración y datos de eventos) en el almacenamiento compartido. Al producirse el failover, el almacenamiento se desmonta del nodo principal y se mueve al nodo de reserva, el cual carga toda la aplicación y la configuración desde el almacenamiento compartido. El segundo planteamiento almacena los datos de eventos en el almacenamiento compartido, pero los binarios de la aplicación y la configuración residen en cada nodo del clúster. Al producirse el failover, solo los datos de eventos se mueven al nodo de reserva.

Cada uno de estos planteamientos tiene ventajas y desventajas, pero el segundo permite a la instalación de Sentinel utilizar vías de instalación estándar compatibles con FHS, permite la verificación de paquetes RPM y también la aplicación de parches en caliente y la reconfiguración con el fin de reducir al mínimo el tiempo de inactividad.

Esta solución le guiará en un ejemplo del proceso de instalación en un clúster que utiliza almacenamiento compartido iSCSI y localiza los binarios de la aplicación/la configuración en cada nodo del clúster.

Supervisión de servicios

Un componente clave de cualquier entorno de alta disponibilidad es una forma sistemática y fiable de supervisar los recursos que deben tener una alta disponibilidad, junto con cualquier recurso del que dependen. EL SLE HAE utiliza un componente denominado Resource Agent para llevar a cabo esta supervisión: el trabajo de Resource Agent consiste en proporcionar el estado de cada recurso, y además (cuando se le pida) iniciar o detener dicho recurso.

Los Resource Agents deben proporcionar un estado fiable de los recursos supervisados para prevenir cualquier tiempo de inactividad innecesario. Los falsos positivos (cuando se considera que un recurso ha fallado, pero de hecho se recupera por sí solo) pueden provocar una migración del servicio (y el tiempo de inactividad asociado) cuando en realidad no es necesario y los falsos negativos (cuando el Resource Agent informa que un recurso está funcionando correctamente cuando de hecho no lo está) pueden impedir el uso adecuado del servicio. Por otro lado, la supervisión externa de un servicio puede ser bastante difícil; un puerto de servicio Web podría responder a un ping sencillo, por ejemplo, pero podría no ofrecer datos correctos cuando se envía una consulta real. En muchos casos, la funcionalidad de autocomprobación debe integrarse en el propio servicio para proporcionar una medida verdaderamente exacta.

Esta solución proporciona un OCF Resource Agent básico para Sentinel capaz de supervisar y detectar un fallo importante de hardware, del sistema operativo o del sistema Sentinel. En este momento las capacidades de supervisión externas de Sentinel se basan en la investigación de puertos IP y existe cierta posibilidad de que se produzcan lecturas de falsos positivos y negativos. Tenemos previsto mejorar en el futuro tanto Sentinel como Resource Agent con el fin de mejorar la exactitud de este componente.

Fencing

Dentro de un clúster de alta disponibilidad (HA), se supervisan de forma constante los servicios cruciales y se reinician automáticamente en otros nodos en caso de fallo. Esta automatización puede presentar problemas, no obstante, si ocurre algún problema de comunicación con el nodo principal;

aunque el servicio que se ejecuta en dicho nodo parece estar inactivo, de hecho sigue ejecutándose y escribiendo datos en el almacenamiento compartido. En ese caso, comenzar un nuevo conjunto de servicios en un nodo de reserva podría dañar fácilmente los datos.

Los clústeres utilizan una variedad de técnicas denominadas de forma colectiva "fencing" que impiden que esto suceda, incluidas SBD (Split Brain Detection) y STONITH (Shoot The Other Node In The Head). El objetivo principal es prevenir que se dañen los datos en el almacenamiento compartido.

36 Requisitos del sistema

Al asignar recursos de clúster para ofrecer compatibilidad con una instalación de alta disponibilidad (HA), tenga en cuenta los siguientes requisitos:

- ❒ (Condicional) Para instalaciones de dispositivos de alta disponibilidad (HA), asegúrese de que el dispositivo HA de Sentinel tenga disponible una licencia válida. El dispositivo HA de Sentinel es un dispositivo ISO que incluye los siguientes paquetes:
  - Sistema operativo: SLES 12 SP3
  - Paquete de Extensión de alta disponibilidad de SLES (SLES HAE)
  - Software de Sentinel (incluido HA rpm)
- ❒ (Condicional) Para instalaciones tradicionales de HA, asegúrese de que están disponibles los siguientes elementos:
  - Sistema operativo: SLES 11 SP4 o SLES 12 SP1 o versiones posteriores
  - Imagen ISO de SLES HAE con licencias válidas
  - Instalador de Sentinel (archivo TAR)
- ❒ (Condicional) Si utiliza el sistema operativo SLES con kernel versión 3.0.101 o posterior, debe cargar manualmente el controlador de vigilancia en el equipo. Para buscar el controlador de vigilancia adecuado para el hardware de su equipo, póngase en contacto con su proveedor de hardware. Para cargar el controlador de vigilancia, realice lo siguiente:
  1. En el indicador de comandos, ejecute el siguiente comando para cargar el controlador de vigilancia en la sesión actual:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```

  2. En el archivo `/etc/init.d/boot.local`, añada la siguiente línea para garantizar que el equipo cargue automáticamente el controlador de vigilancia cada vez que se arranque:

     ```
     /sbin/modprobe -v --ignore-install <watchdog driver name>
     ```
- ❒ Asegúrese de que cada nodo de clúster que alberga servicios de Sentinel cumpla los requisitos especificados en el Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 37.
- ❒ Asegúrese de que haya espacio de almacenamiento compartido suficiente para los datos y la aplicación Sentinel.
- ❒ Asegúrese de utilizar una dirección IP virtual para los servicios que se pueda migrar de un nodo a otro al producirse el failover.
- ❒ Asegúrese de que el dispositivo de almacenamiento compartido cumpla los requisitos de características de tamaño y rendimiento especificados en el Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 37. Utilice una máquina virtual de SLES estándar configurada con destinos iSCSI como almacenamiento compartido.

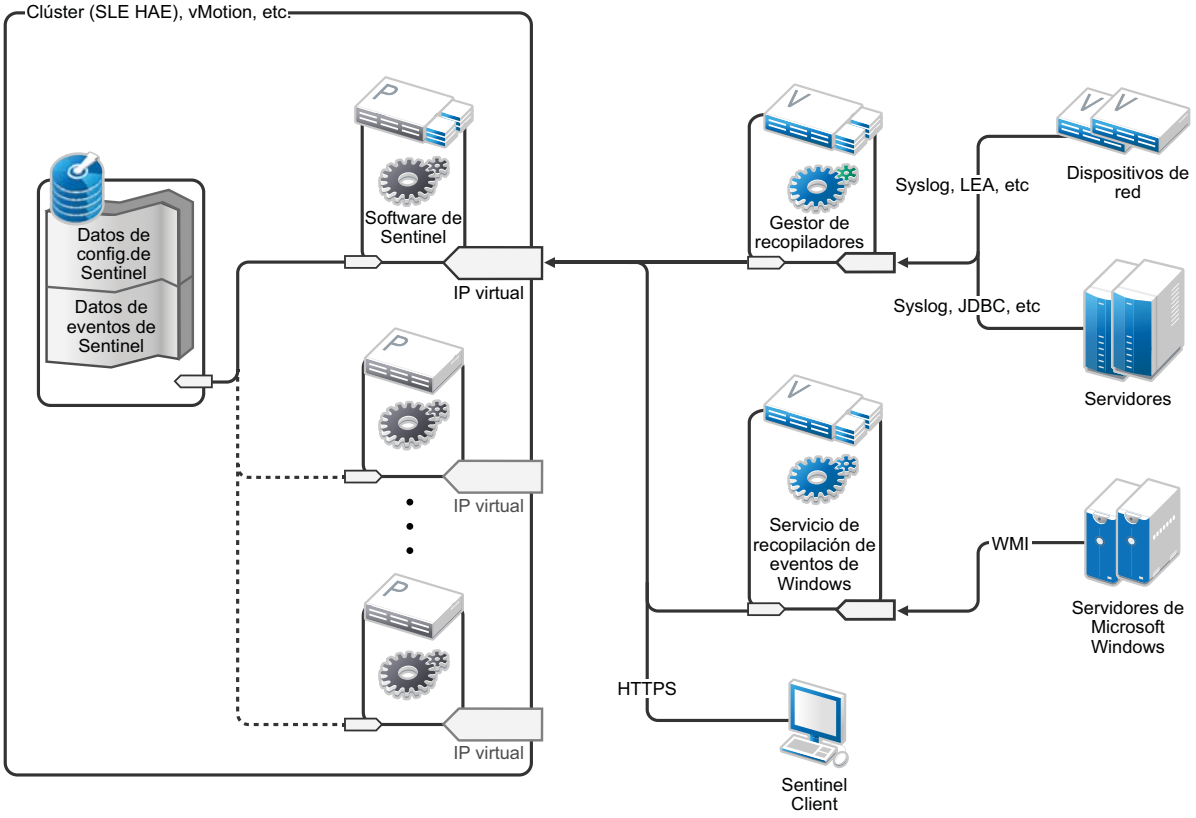
  Para iSCSI, debe usar la unidad de transferencia de mensajes (MTU) más grande que sea compatible con su hardware. Las MTU de mayor tamaño optimizan el rendimiento del almacenamiento. Sentinel podría tener problemas si la latencia y el ancho de banda para almacenamiento son inferiores al valor recomendado.

- ❒ Asegúrese de tener como mínimo dos nodos de clúster que cumplan los requisitos de recursos para ejecutar Sentinel en el entorno del cliente. Es recomendable utilizar dos máquinas virtuales SLES.
- ❒ Asegúrese de crear un método de comunicación de los nodos del clúster con el almacenamiento compartido, como FibreChannel para una SAN. Utilice una dirección IP específica para conectarse con el destino iSCSI.
- ❒ Asegúrese de tener una dirección IP virtual que se pueda migrar desde un nodo del clúster a otro para que sirva como dirección IP externa de Sentinel.
- ❒ Asegúrese de tener al menos una dirección IP por nodo del clúster para las comunicaciones internas del clúster. Puede utilizar una dirección IP de unidifusión sencilla, pero es preferible la multidifusión para los entornos de producción.

37 Instalación y configuración

En este capítulo se proporcionan los pasos de instalación y configuración de Sentinel en un entorno de alta disponibilidad (HA).

El siguiente diagrama representa una arquitectura de alta disponibilidad (HA) activa-pasiva.



Config inicial

Configure el hardware del equipo, el hardware de red, el hardware de almacenamiento, los sistemas operativos, las cuentas de usuario y demás recursos básicos del sistema de acuerdo con los requisitos documentados para Sentinel y los requisitos locales del cliente. Pruebe los sistemas para garantizar su funcionamiento y estabilidad adecuados.

Utilice la siguiente lista de verificación como guía para realizar la instalación y configuración inicial.

	Elementos de la lista de verificación
?	Las características de CPU, RAM y espacio en el disco para cada nodo del clúster deben cumplir los requisitos del sistema definidos en el Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 37 en base al número de eventos esperado.
?	Las características de espacio en el disco y E/S para los nodos de almacenamiento deben cumplir los requisitos del sistema definidos en el Capítulo 5, “Cumplimiento de los requisitos del sistema”, en la página 37 en función del número de eventos esperado y de las directivas de retención de datos del almacenamiento principal y secundario.
?	Si desea configurar cortafuegos en el sistema operativo para limitar el acceso a Sentinel y al clúster, consulte el Capítulo 8, “Puertos utilizados”, en la página 63 para obtener detalles sobre qué puertos deben estar disponibles dependiendo de la configuración local y de los orígenes que enviarán los datos de eventos.
?	Asegúrese de que todos los nodos del clúster tengan sincronizada la hora. Puede usar NTP o una tecnología similar para este propósito.
?	◆ El clúster requiere una resolución de nombre de host fiable. Introduzca todos los nombres de host del clúster interno en el archivo `/etc/hosts` a fin de garantizar la continuidad del clúster en caso de fallo del DNS. ◆ Asegúrese de no asignar un nombre de host a una dirección IP de retrobucle. ◆ Al configurar el nombre de host y el nombre de dominio durante la instalación del sistema operativo, deseleccione la opción**Assign Hostname to Loopback IP** (Asignar nombre de host a IP de retrobucle).

Puede utilizar la siguiente configuración:

- (Condicional) Para instalaciones tradicionales de HA:
  - Dos máquinas virtuales de nodo de clúster que ejecutan SLES 11 SP4 or SLES 12 SP1 o versiones posteriores.
  - (Condicional) Puede instalar X Windows si requiere configurar la interfaz gráfica de usuario. Defina los guiones de arranque para iniciarse sin X (nivel de ejecución 3), de manera que pueda iniciarlos solo cuando sea necesario.
- (Condicional) Para instalaciones de dispositivos HA: dos máquinas virtuales de nodo de clúster basadas en dispositivos ISO HA. Para obtener información sobre la instalación del dispositivo ISO HA, consulte la “Instalación de Sentinel” en la página 102.
- Los nodos tendrán una NIC para acceso externo y otra para comunicaciones iSCSI.
- Configure las NIC externas con direcciones IP que permitan el acceso remoto a través de SSH o similar. Para este ejemplo, utilizaremos 172.16.0.1 (node01) y 172.16.0.2 (node02).
- Cada nodo debe tener suficiente espacio de disco para el sistema operativo, binarios de Sentinel y datos de configuración, software del clúster, espacio temporal, etc. Consulte los requisitos del sistema SLES y SLES HAE, así como los requisitos de la aplicación Sentinel.

- Una máquina virtual que ejecuta SLES 11 SP4 o SLES 12 SP1 o versiones posteriores que está configurada con destinos iSCSI para almacenamiento compartido
  - (Condicional) Puede instalar X Windows si requiere configurar la interfaz gráfica de usuario. Defina los guiones de arranque para iniciarse sin X (nivel de ejecución 3), de manera que pueda iniciarlos solo cuando sea necesario.
  - Los nodos tendrán dos NICS: una para acceso externo y otra para comunicaciones iSCSI.
  - Configure las NIC externas con una dirección IP que permita el acceso remoto a través de SSH o similar. Por ejemplo, 172.16.0.3 (almacenamiento03).
  - El sistema debería tener espacio suficiente para el sistema operativo, espacio temporal, un gran volumen para almacenamiento compartido para albergar datos de Sentinel, y una pequeña cantidad de espacio para una partición SBD. Consulte los requisitos del sistema SLES, así como los requisitos de almacenamiento de datos de eventos de Sentinel.

Nota: En un clúster de producción, puede usar direcciones IP internas, no encaminables en tarjetas NIC independientes (posiblemente un par de ellas, para ofrecer redundancia) para las comunicaciones internas del clúster.

Configuración de almacenamiento compartido

Configure su almacenamiento compartido y asegúrese de que pueda montarlo en cada nodo del clúster. Si utiliza FibreChannel y una SAN, quizá necesite proporcionar conexiones físicas además de una configuración adicional. Sentinel utiliza este almacenamiento compartido para almacenar las bases de datos y los datos de eventos. Asegúrese de que el almacenamiento compartido tenga un tamaño adecuado en función del número de eventos previsto y de las directivas de retención de datos

Tenga en cuenta el siguiente ejemplo de instalación de almacenamiento compartido:

Una implementación típica podría usar una SAN rápida conectada mediante FibreChannel a todos los nodos del clúster, con una matriz RAID de gran tamaño para almacenar datos de eventos locales. Se podría utilizar una NAS independiente o un nodo iSCSI para el almacenamiento secundario más lento. Siempre que el nodo del clúster pueda montar el almacenamiento principal como dispositivo de bloques normal, podrá ser utilizado por la solución. El almacenamiento secundario también puede montarse como dispositivo de bloques, o bien podría ser un NFS o volumen CIFS.

Nota: Configure el almacenamiento compartido y pruebe a montarlo en cada nodo del clúster. Sin embargo, la configuración del clúster manejará el montaje real del almacenamiento.

Lleve a cabo el procedimiento siguiente para crear destinos iSCSI albergados por una máquina virtual de SLES:

1. Conéctese a `storage03`, la máquina virtual que creó durante la Config inicial e inicie una sesión en la consola.
2. Ejecute el siguiente comando para crear un archivo en blanco de cualquier tamaño para el almacenamiento principal de Sentinel:

   ```
   dd if=/dev/zero of=/localdata count=<file size> bs=<bit size>
   ```

   Por ejemplo, ejecute el comando siguiente para crear un archivo de 20 GB lleno de ceros copiados desde el pseudodispositivo `/dev/zero`:

   ```
   dd if=/dev/zero of=/localdata count=20480000 bs=1024
   ```

3 Repita los pasos 1 y 2 para crear un archivo para el almacenamiento secundario del mismo modo.

Por ejemplo, ejecute el comando siguiente para el almacenamiento secundario:

```
dd if=/dev/zero of=/networkdata count=20480000 bs=1024
```

Nota: Para este ejemplo creó dos archivos con las mismas características de tamaño y rendimiento para representar los dos discos. Para una implementación de producción, puede crear el almacenamiento principal en una red SAN rápida y el almacenamiento secundario en un volumen iSCSI, NFS o CIFS más lento.

Lleve a cabo los pasos descritos en las siguientes secciones para configurar los dispositivos de iniciador y destino iSCSI:

- “Configuración de destinos iSCSI” en la página 198
- “Configuración de iniciadores iSCSI” en la página 200

Configuración de destinos iSCSI

Lleve a cabo el siguiente procedimiento para configurar los archivos `localdata` y `networkdata` como destinos iSCSI.

Para obtener más información sobre la configuración de destinos iSCSI, consulte la sección Creating iSCSI Targets with YaST (Crear destinos iSCSI con YaST) en la documentación de SUSE.

1 Ejecute YaST desde la línea de comandos (o utilice la interfaz gráfica del usuario, si lo prefiere): `/sbin/yast`

2 Seleccione **Dispositivos de red** > **Configuración de red**.

3 Asegúrese de que esté seleccionada la pestaña **Descripción general**.

4 Seleccione la NIC secundaria en la lista que aparece y luego desplácese hacia delante para Editar y pulse `Intro`.

5 En la pestaña **Dirección**, asigne la dirección IP estática 10.0.0.3. Esta será la dirección IP de comunicaciones iSCSI internas.

6 Haga clic en **Siguiente** y después en **Aceptar**.

7 (Condicional) En la pantalla principal:

- Si utiliza SLES 11 SP4, seleccione **Servicios de red** > **Destino iSCSI**.
- Si utiliza SLES 12 SP1 o versiones posteriores, seleccione **Network Services** (Servicios de red) > **iSCSI LIO Target** (Destino iSCSI LIO).

  Nota: Si no se encuentra esta opción, diríjase a **Software** > **Gestión de Software** > **Servidor LIO iSCSI** e instale el paquete iSCSI LIO.

  ---

8 (Condicional) Si se le solicita, instale el software requerido:

- Para SLES 11 SP4: `iscsitarget RPM`
- Para SLES 12 SP1 o versiones posteriores: `iscsiliotarget RPM`

9 (Condicional) Si utiliza SLES 12 SP1 o versiones posteriores, realice los siguientes pasos en todos los nodos del clúster:

9a Ejecute el comando siguiente para abrir el archivo que contiene el nombre del iniciador iSCSI:

```
cat /etc/iscsi/initiatorname.iscsi
```

9b Tome nota del nombre del iniciador que se utilizará para la configuración de iniciadores iSCSI:

Por ejemplo:

```
InitiatorName=iqn.1996-04.de.suse:01:441d6988994
```

Estos nombres del iniciador se utilizarán durante la configuración del cliente de destino iSCSI.

10 Haga clic en **Servicio**, seleccione la opción**When Booting** (En el arranque) para asegurarse de que el servicio se inicia al arrancar el sistema operativo.

11 Seleccione la pestaña **Global**, deseleccione **Sin autenticación** para habilitar la autenticación y, a continuación, especifique las credenciales necesarias para la autenticación entrante y saliente.

La opción**Sin autenticación** está habilitada por defecto. Sin embargo, debe habilitar la autenticación para asegurarse de que la configuración sea segura.

12 Haga clic en **Destinos** y luego en **Añadir** para añadir un nuevo destino.

El destino iSCSI generará automáticamente una ID y después presentará una lista vacía de LUN (unidades) que están disponibles.

13 Haga clic en **Añadir** para añadir un nuevo LUN.

14 Deje el número LUN 0, y después busque en el cuadro de diálogo **Vía** (en Type=fileio) y seleccione el archivo `/localdata` que ha creado. Si tiene un disco dedicado para almacenamiento, especifique un dispositivo de bloque, como por ejemplo `/dev/sdc`.

15 Repita los pasos 13 y 14, añada LUN 1 y seleccione `/networkdata` en esta ocasión.

16 (Condicional) Si utiliza SLES 11 SP4, lleve a cabo los pasos siguientes:

16a Deje las demás opciones en sus valores por defecto, haga clic en **Aceptar** y, a continuación, haga clic en **Siguiente**.

16b (Condicional) Si ha habilitado la autenticación en el paso 11, proporcione las credenciales de autenticación.

Seleccione un cliente, seleccione **Editar Aut.** > **Autenticación entrante** y especifique el nombre de usuario y contraseña.

17 (Condicional) Si utiliza SLES 12 SP1 o versiones posteriores, lleve a cabo los pasos siguientes:

17a Deje las demás opciones en sus valores por defecto y haga clic en **Siguiente**.

17b Haga clic en **Añadir**. Cuando se le pida el nombre del cliente, especifique el nombre del iniciador que ha copiado en el paso 9. Repita este paso para añadir todos los nombres de cliente mediante la especificación de los nombres del iniciador.

Se mostrará la lista de nombres de los clientes en la lista de clientes.

17c (Condicional) Si ha habilitado la autenticación en el paso 11, proporcione las credenciales de autenticación.

Seleccione un cliente, seleccione **Editar Aut.** > **Autenticación entrante** y especifique el nombre de usuario y contraseña. Repita este paso para todos los clientes.

18 Haga clic de nuevo en **Siguiente** para seleccionar las opciones de autenticación por defecto, y luego en **Finalizar** para salir de la configuración. Elija Aceptar si se le pide reiniciar iSCSI.

19 Salga de YaST.

Nota: Este procedimiento expone dos destinos iSCSI del servidor en la dirección IP 10.0.0.3. En cada nodo del clúster, asegúrese de que pueda montar el dispositivo de almacenamiento compartido de datos locales.

Configuración de iniciadores iSCSI

Lleve a cabo el siguiente procedimiento para formatear los dispositivos del iniciador iSCSI.

Para obtener más información acerca de la configuración de iniciadores iSCSI, consulte la sección Configuring the iSCSI Initiator(Configuración del iniciador iSCSI) en la documentación de SUSE.

1. Conéctese a uno de los nodos del clúster (node01) e inicie YaST.
2. Seleccione **Dispositivos de red** > **Configuración de red**.
3. Asegúrese de que esté seleccionada la pestaña **Descripción general**.
4. Seleccione la NIC secundaria de la lista que aparece y luego desplácese hacia delante para Editar y pulse Intro.
5. Haga clic en **Dirección**, asigne la dirección IP estática 10.0.0.1. Esta será la dirección IP de comunicaciones internas de iSCSI.
6. Seleccione **Siguiente** y después **Aceptar**.
7. Haga clic en **Network Services** (Servicios de red) > **iSCSI Initiator** (Iniciador de iSCSI).
8. Si se le solicita, instale el software necesario (`iscsiclient` RPM).
9. Haga clic en **Service** (Servicio), seleccione **When Booting** (Al arrancar) para asegurarse de que el servicio iSCSI se inicia durante el arranque.
10. Haga clic en **Discovered Targets** (Destinos descubiertos) y seleccione **Discovery** (Descubrimiento).
11. Especifique la dirección IP de destino (10.0.0.3) de iSCSI.

    (Condicional) Si ha habilitado la autenticación en el paso 11 en “Configuración de destinos iSCSI” en la página 198, deseleccione **Sin autenticación**. En el campo **Autenticación saliente**, escriba el nombre de usuario y la contraseña que ha configurado durante la configuración de destino iSCSI.

    Haga clic en **Siguiente.**
12. Seleccione el destino iSCSI descubierto con la dirección IP 10.0.0.3 y después seleccione**Log In** (Entrar).
13. Realice los siguientes pasos:

    13a Cambie a Automático en el menú desplegable **Inicio**.

    13b (Condicional) Si ha habilitado la autenticación, deseleccione **Sin autenticación**.

    El nombre de usuario y la contraseña que ha especificado en el paso 11 deben aparecer en la sección **Autenticación saliente**. Si no se muestran estas credenciales, introduzca las credenciales en esta sección.

    13c Haga clic en **Siguiente.**
14. Cambie a la pestaña **Connected Targets** (Destinos conectados) para garantizar que se establezca la conexión con el destino.
15. Salga de la configuración. Esta acción debería haber montado los destinos iSCSI como dispositivos de bloque en el nodo del clúster.
16. En el menú principal YaST, seleccione **System** (Sistema) > **Partitioner** (Particionador).
17. En la vista del sistema, debería ver nuevos discos duros de los siguientes tipos (por ejemplo, `/dev/sdb` y `/dev/sdc`) en la lista:
    - En SLES 11 SP4: IET-VIRTUAL-DISK
    - En SLES 12 SP1 o versiones posteriores: LIO-ORG-FILEIO

Desplácese hacia el primero de la lista (que debería ser el almacenamiento principal), selecciónelo y pulse Intro.

18 Seleccione **Add**(Añadir) para añadir una nueva partición al disco vacío. Dé formato al disco como partición principal, pero no lo monte. Asegúrese de que esté seleccionada la opción **No montar partición**.

19 Seleccione **Siguiente** y luego **Finalizar** después de revisar los cambios que se realizarán.

El disco formateado (por ejemplo, `/dev/sdb1`) debería estar ya listo. Se conoce como `/dev/<SHARED1>` en los siguientes pasos de este procedimiento.

20 Regrese al **Particionador** y repita el proceso de creación de particiones/formato (pasos 16-19) para `/dev/sdc` o sea cual sea el dispositivo de bloque que corresponda con el almacenamiento secundario. Esto debe dar lugar a una partición `/dev/sdc1` o disco formateado similar (denominado `/dev/<NETWORK1>` a continuación).

21 Salga de YaST.

22 (Condicional) Si realiza una instalación tradicional de HA, cree un punto de montaje y pruebe el montaje de la partición local de la siguiente manera (el nombre exacto del dispositivo dependerá de la implementación específica):

```
# mkdir /var/opt/novell
# mount /dev/<SHARED1> /var/opt/novell
```

Debe poder crear archivos en la nueva partición y verlos siempre que esté montada.

23 (Condicional) Si realiza una instalación tradicional de HA, para desmontarla:

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

24 (Condicional) Para las instalaciones de dispositivos de alta disponibilidad, repita los pasos 1 a 15 para asegurarse de que cada nodo del clúster se pueda montar en el almacenamiento compartido local. Reemplace la dirección IP del nodo del paso 5 por otra diferente para cada nodo del clúster.

25 (Condicional) Para las instalaciones de dispositivos de alta disponibilidad, repita los pasos 1 a 15, 22 y 23 para asegurarse de que cada nodo del clúster se pueda montar en el almacenamiento compartido local. Reemplace la dirección IP del nodo del paso 6 por otra diferente para cada nodo del clúster.

Instalación de Sentinel

Hay dos opciones para instalar Sentinel: instalar cada uno de los componentes de Sentinel en el almacenamiento compartido usando la opción `--location` para redirigir la instalación de Sentinel a donde sea que se haya montado el almacenamiento compartido, o poner solo los datos variables de la aplicación en el almacenamiento compartido.

Instale Sentinel en cada nodo del clúster que pueda alojarlo. Después de instalar Sentinel por primera vez, debe llevar a cabo una instalación completa, incluidos los archivos binarios de la aplicación, la configuración y todos los almacenes de datos. Para las instalaciones posteriores en otros nodos del clúster, solo instalará la aplicación. Los datos de Sentinel estarán disponibles una vez que haya montado el almacenamiento compartido.

Instalación del primer nodo

- “Instalación tradicional de HA” en la página 202
- “Instalación de un dispositivo HA de Sentinel” en la página 202

Instalación tradicional de HA

1. Conéctese a uno de los nodos de clúster (node01) y abra la ventana de la consola.
2. Descargue el instalador de Sentinel (un archivo tar.gz) y guárdelo en `/tmp` en el nodo de clúster.
3. Lleve a cabo los siguientes pasos para iniciar la instalación:
   - **3a** Ejecute los comandos siguientes:

     ```
     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** Especifique `2` para seleccionar Configuración personalizada cuando se le pida seleccionar el método de configuración.
4. Ejecute la instalación, configurando el producto como corresponda.
5. Inicie Sentinel y pruebe las funciones básicas. Puede usar la dirección IP de nodo de clúster externa estándar para acceder al producto.
6. Apague Sentinel y desmonte el almacenamiento compartido mediante los siguientes comandos:

   ```
   rcsentinel stop
   umount /var/opt/novell
   ```

   Este paso eliminará los guiones de inicio automático de manera que el clúster pueda gestionar el producto.

   ```
   cd /
   insserv -r sentinel
   ```

Instalación de un dispositivo HA de Sentinel

El dispositivo HA de Sentinel incluye el software de Sentinel ya instalado y configurado. Para configurar el software Sentinel para HA, realice los siguientes pasos:

1. Conéctese a uno de los nodos de clúster (node01) y abra la ventana de la consola.
2. Acceda al directorio siguiente:

   ```
   cd /opt/novell/sentinel/setup
   ```

3. Registre la configuración:
   - **3a** Ejecute el comando siguiente:

     ```
     ./configure.sh --record-unattended=/tmp/install.props --no-start
     ```

     En este paso se registra la configuración en el archivo`install.props`, que se requiere para configurar los recursos del clúster mediante el guión `install-resources.sh`.
   - **3b** Especifique `2` para seleccionar Configuración personalizada cuando se le pida seleccionar el método de configuración.
   - **3c** Cuando se le pida introducir la contraseña, especifique `2` para introducir una contraseña nueva.

     Si especifica `1`, el archivo `install.props` no almacena la contraseña.

4 Apague Sentinel utilizando el siguiente comando:

```
rcsentinel stop
```

Este paso eliminará los guiones de inicio automático de manera que el clúster pueda gestionar el producto.

```
insserv -r sentinel
```

5 Mueva la carpeta de datos de Sentinel al almacenamiento compartido utilizando los siguientes comandos. Este movimiento permite que los nodos utilicen la carpeta de datos de Sentinel a través del almacenamiento compartido.

```
mkdir -p /tmp/new
```

```
mount /dev/<SHARED1> /tmp/new
```

```
mv /var/opt/novell/* /tmp/new
```

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

6 Verifique el desplazamiento de la carpeta de datos de Sentinel al almacenamiento compartido utilizando los siguientes comandos:

```
mount /dev/<SHARED1>  /var/opt/novell/
```

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

Instalación de nodos posteriores

- “Instalación tradicional de HA” en la página 203
- “Instalación de un dispositivo HA de Sentinel” en la página 204

Repita la instalación en otros nodos:

El instalador inicial de Sentinel crea una cuenta de usuario para su uso por parte del producto, que utiliza la siguiente ID de usuario disponible en el momento de la instalación. Las instalaciones posteriores en modo sin supervisión tratarán de usar la misma ID para la creación de la cuenta, pero existe la posibilidad de que surjan conflictos (si los nodos del clúster no son idénticos en el momento de la instalación). Se recomienda encarecidamente realizar una de las siguientes acciones:

- Sincronizar la base de datos de la cuenta en todos los nodos del clúster (manualmente a través de LDAP o similar), asegurándose de que se produzca la sincronización antes de realizar instalaciones posteriores. En ese caso, el instalador detectará la presencia de la cuenta de usuario y utilizará la existente.
- Observe el resultado de las instalaciones posteriores sin supervisión: se emitirá una advertencia si no fue posible crear la cuenta de usuario con la misma ID de usuario.

Instalación tradicional de HA

1 Conéctese a cada nodo del clúster adicional (node02) y abra una ventana de consola.

2 Ejecute los comandos siguientes:

```
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
```

Instalación de un dispositivo HA de Sentinel

1. Conéctese a cada nodo del clúster adicional (node02) y abra una ventana de consola.
2. Ejecute el comando siguiente:

   ```
   insserv -r sentinel
   ```

3. Detenga los servicios de Sentinel.

   ```
   rcsentinel stop
   ```

4. Elimine el directorio de Sentinel.

   ```
   rm -rf /var/opt/novell/*
   ```

Al finalizar el proceso, Sentinel deberá estar instalado en todos los nodos, pero es probable que no funcione correctamente en ninguno de ellos salvo el primero hasta que varias claves estén sincronizadas, lo que sucederá cuando se configuren los recursos del clúster.

Instalación del clúster

Debe instalar el software del clúster solo para instalaciones tradicionales de alta disponibilidad (HA). El dispositivo HA de Sentinel incluye el software de clúster y no requiere instalación manual.

Utilice el siguiente procedimiento para configurar la extensión de alta disponibilidad de SLES con una superposición de Resource Agents específica de Sentinel:

1. Instale el software de clúster en cada nodo.
2. Registre cada nodo del clúster con el gestor de clústeres.
3. Verifique que cada nodo del clúster aparezca en la consola de gestión de clústeres.

   Nota: El OCF Resource Agent para Sentinel es un guión shell sencillo que ejecuta una variedad de comprobaciones para verificar si Sentinel es funcional. Si no utiliza el OCF Resource Agent para supervisar Sentinel, debe desarrollar una solución de supervisión similar para el entorno de clúster local. Para desarrollar una propia, revise el Resource Agent existente, almacenado en el archivo `Sentinelha.rpm` en el paquete de descarga de Sentinel.

   ---

4. Instale el software central SLE HAE de acuerdo con la Documentación de SLE HAE.Para obtener información sobre la instalación de productos complementarios de SLES, consulte la Guía de implantación.
5. Repita el paso 4 en todos los nodos del clúster. El producto complementario instalará el software de comunicaciones y gestión de clústeres central, además de cualquier Resource Agent que se utilice para supervisar los recursos del clúster.

6 Instale un RPM adicional para proporcionar los Resource Agent de clúster adicionales específicos de Sentinel. El RPM puede encontrarse en el archivo `novell-Sentinelha-<versión_Sentinel>*.rpm` incluido en el paquete de descarga por defecto de Sentinel, que desempaquetó para instalar el producto.

7 En cada nodo del clúster, copie el archivo `novell-Sentinelha-<versión_Sentinel>*.rpm` en el directorio `/tmp` y luego ejecute los siguientes comandos:

```
cd /tmp

rpm -i novell-Sentinelha-<Sentinel_version>*.rpm
```

Configuración del clúster

Debe configurar el software del clúster para registrar cada nodo del clúster como miembro del clúster. Dentro del proceso de configuración, también puede configurar recursos de fencing y STONITH (Shoot The Other Node In The Head) a fin de garantizar la uniformidad en el clúster.

Importante: Los procedimientos descritos en esta sección utilizan comandos `rcopenais` y `openais`, que funcionan solo con SLES 11 SP4. Para SLES 12 SP2 y versiones posteriores, utilice el comando `systemctl pacemaker.service`.

Por ejemplo, para el comando `/etc/rc.d/openais start`, utilice el comando `systemctl start pacemaker.service`.

Utilice el siguiente procedimiento para la configuración del clúster:

Para esta solución, debe utilizar direcciones IP privadas para las comunicaciones internas del clúster y utilizará unidifusión para minimizar la necesidad de solicitar direcciones de multidifusión de un administrador de red. Debe utilizar además un destino iSCSI configurado en la misma máquina virtual de SLES que alberga el almacenamiento compartido para que sirva como dispositivo SBD (Split Brain Detection) para fines de fencing.

Configuración de SBD

1 Conéctese a `storage03` e inicie una sesión de la consola. Use el siguiente comando para crear un archivo en blanco de cualquier tamaño:

```
dd if=/dev/zero of=/sbd count=<file size> bs=<bit size>
```

Por ejemplo, ejecute el comando siguiente para crear un archivo de 1 MB lleno de ceros copiados desde el pseudodispositivo `/dev/zero`:

```
dd if=/dev/zero of=/sbd count=1024 bs=1024
```

2 Ejecute YaST desde la línea de comandos o la interfaz gráfica del usuario: `/sbin/yast`

3 Seleccione **Servicios de red** > **Destino iSCSI**.

4 Haga clic en **Destinos** y seleccione el destino existente.

5 Seleccione**Editar**. La interfaz del usuario presentará una lista de LUN (unidades) que están disponibles.

6 Seleccione **Añadir** para añadir un LUN nuevo.

7 Deje el número LUN 2. Busque en el cuadro de diálogo **Vía** y seleccione el archivo `/sbd` que ha creado.

8 Deje las demás opciones en sus valores por defecto y luego seleccione **Aceptar** y después **Siguiente**; a continuación haga clic de nuevo en **Siguiente** para seleccionar las opciones de autenticación por defecto.

9 Haga clic en **Finalizar** para salir de la configuración. Si es necesario, reinicie los servicios. Salga de YaST.

Nota: Los pasos siguientes requieren que cada nodo del clúster sea capaz de resolver el nombre de host de todos los demás nodos del clúster (el servicio de sincronización de archivos csync2 fallará si no es el caso). Si no se configura el DNS o no está disponible, añada entradas para cada host en el archivo `/etc/hosts` que enumeren cada dirección IP junto con su nombre de host (tal como lo indica el comando de nombre de host). Asegúrese además de no asignar un nombre de host a una dirección IP de retrobucle.

Realice los siguientes pasos para exponer un destino iSCSI para el dispositivo SBD en el servidor en la dirección IP 10.0.0.3 (storage03).

Configuración de nodos

Conéctese a un nodo del clúster (node01) y abra una consola:

1 Ejecute YaST.

2 Abra **Network Services** (Servicios de red) > **iSCSI Initiator** (Iniciador de iSCSI).

3 Seleccione **Connected Targets** (Destinos conectados) y luego el destino iSCSI que configuró anteriormente.

4 Seleccione la opción **Log Out** (Salir) para salir del destino.

5 Cambie a la pestaña **Destinos descubiertos** y seleccione el **Destino** y vuelva a entrar para actualizar la lista de dispositivos (deje la opción de inicio **automático** y deseleccione **Sin autenticación**).

6 Seleccione **OK** para salir de la herramienta del Iniciador de iSCSI.

7 Abra**System** (Sistema) > **Partitioner** (Particionador) e identifique el dispositivo SBD como el 1MB IET-VIRTUAL-DISK. Aparecerá como **/dev/sdd** o similar; observe cuál.

8 Salga de YaST.

9 Ejecute el comando `ls -l /dev/disk/by-id/` y observe la ID del dispositivo que está vinculada al nombre del dispositivo identificado anteriormente.

10 (Condicional) Ejecute uno de los comandos siguientes:

- Si utiliza SLES 11 SP4:

  `sleha-init`

- Si utiliza SLES 12 SP1 o versiones posteriores:

  `ha-cluster-init`

11 Cuando se le pregunte a qué dirección de red desea vincularlo, especifique la dirección IP de NIC externa (172.16.0.1).

12 Acepte la dirección de multidifusión y el puerto por defecto. Más tarde sobrescribiremos estos valores.

13 Introduzca `s` para habilitar SBD y luego especifique `/dev/disk/by-id/<device id>`, donde`<device id>` es el ID que identificó anteriormente (puede usar el tabulador para completar automáticamente la vía).

14 (Condicional) Introduzca `N` cuando se le indique lo siguiente:

```
Do you wish to configure an administration IP? [y/N]
```

Para configurar una dirección IP de administración, proporcione la dirección IP virtual durante“Configuración de recursos” en la página 209

15 Complete el asistente y asegúrese de que no se generen errores.

16 Inicie YaST.

17 Seleccione **High Availability** (Alta disponibilidad) > **Cluster** (Clúster) (o simplemente Clúster en algunos sistemas).

18 En el cuadro de la izquierda, asegúrese de que se haya seleccionado **Communication Channels** (Canales de comunicación).

19 Desplácese hasta la línea superior de configuración y cambie la selección de **udp** a **udpu** (esto inhabilita multidifusión y selecciona unidifusión).

20 Seleccione la opción para **Add a Member Address** (Añadir una dirección de miembro) y especifique este nodo (172.16.0.1), luego repita y añada el otro o los otros nodos del clúster: 172.16.0.2.

21 Seleccione **Finalizar** para completar la instalación.

22 Salga de YaST.

23 Ejecute el comando `/etc/rc.d/openais restart` para reiniciar los servicios de clúster con el nuevo protocolo de sincronización.

Conéctese a cada nodo de clúster adicional (node02) y abra una consola:

1 Ejecute YaST.

2 Abra **Network Services** (Servicios de red) > **iSCSI Initiator** (Iniciador de iSCSI).

3 Seleccione **Connected Targets** (Destinos conectados) y luego el destino iSCSI que configuró anteriormente.

4 Seleccione la opción **Log Out** (Salir) para salir del destino.

5 Cambie a la pestaña **Destinos descubiertos** y seleccione el **Destino** y vuelva a entrar para actualizar la lista de dispositivos (deje la opción de inicio **automático** y deseleccione **Sin autenticación**).

6 Seleccione **OK** para salir de la herramienta del Iniciador de iSCSI.

7 (Condicional) Ejecute uno de los comandos siguientes:

- Si utiliza SLES 11 SP4:

  `sleha-join`

- Si utiliza SLES 12 SP1 o versiones posteriores:

  `ha-cluster-join`

8 Introduzca la dirección IP del primer nodo del clúster.

(Condicional) Si el clúster no se inicia correctamente, realice los siguientes pasos:

1 Ejecute el comando `crm status` para comprobar si se han unido los nodos. Si no se han unido los nodos, reinicie todos los nodos del clúster.

2 Copie manualmente el archivo `/etc/corosync/corosync.conf` de `node01` a `node02`, o ejecute `csync2 -x -v` en el `node01`, o bien configure manualmente el clúster en `node02` a través de YaST.

3 (Condicional) Si se produce un error a la hora de sincronizar todos los archivos cuando ejecuta el comando `csync2 - x - v` en el paso 1, lleve a cabo el procedimiento siguiente:

3a Borre la base de datos csync2 del directorio `/var/lib/csync2` de todos los nodos.

3b En todos los nodos, actualice la base de datos csync2 con el fin de que coincida con el sistema de archivos, pero sin marcar ningún elemento para su sincronización con otros servidores:

```
csync2 -cIr /
```

3c En el nodo activo, realice lo siguiente:

3c1 Encuentre todas las diferencias entre los nodos activos y pasivos, y marque esas diferencias para la sincronización:

```
csync2 -TUXI
```

3c2 Restaure la base de datos para forzar al nodo activo a anular cualquier conflicto:

```
csync2 -fr /
```

3c3 Inicie la sincronización en todos los nodos:

```
csync2 -xr /
```

3d En todos los nodos, compruebe que se sincronizan todos los archivos:

```
csync2 -T
```

Este comando solo muestra los archivos que no se han sincronizado.

4 Ejecute el siguiente comando en `node02`:

Para SLES 11 SP4:

```
/etc/rc.d/openais start
```

Para SLES 12 SP1 y versiones posteriores:

```
systemctl start pacemaker.service
```

(Condicional) Si el servicio `xinetd` no añade correctamente el nuevo servicio `csync2`, el guión no funcionará correctamente. El servicio `xinetd` es necesario para que el otro nodo pueda sincronizar los archivos de configuración del clúster hasta este nodo. Si ve errores como `csync2 run failed`, podría tener este problema.

Para solucionar este problema, ejecute el comando`kill -HUP `cat /var/run/xinetd.init.pid` y luego vuelva a ejecutar el guión `sleha-join`.

5 Ejecute `crm_mon` en cada nodo del clúster para verificar que el clúster funcione correctamente. También puede usar "hawk", la consola Web, para verificar el clúster. El nombre de usuario por defecto es `hacluster` y la contraseña `linux`.

(Condicional) Dependiendo de su entorno, realice las siguientes tareas para modificar otros parámetros:

1 Para asegurarse de que un fallo en un nodo de un clúster formado por dos nodos no detenga inesperadamente todo el clúster, defina la opción global de clúster `no-quorum-policy` en `ignore`:

```
crm configure property no-quorum-policy=ignore
```

Nota: Si el clúster tiene más de dos nodos, no defina esta opción.

2 Para asegurarse de que el gestor de recursos permita a los recursos ejecutarse en su lugar y desplazarse, defina la opción global de clúster `default-resource-stickiness` en 1:

```
crm configure property default-resource-stickiness=1
```

Configuración de recursos

Resource Agents se suministra por defecto con SLE HAE. Si no utiliza SLE HAE, deberá supervisar estos recursos adicionales utilizando otra tecnología:

- Un recurso de sistema de archivos correspondiente al almacenamiento compartido que utiliza el software.
- Un recurso de dirección IP que se corresponde con la dirección IP virtual por la que se accederá a los servicios.
- El software de la base de datos PostgreSQL que almacena la configuración y los metadatos de eventos.

Utilice el siguiente procedimiento de configuración de recursos:

El guión `crm` le ayuda a configurar el clúster. El guión envía variables de configuración relevantes desde el archivo de configuración sin supervisión generado dentro de la instalación de Sentinel. Si no generó el archivo de configuración, o si desea cambiar la configuración de los recursos, puede usar el siguiente procedimiento de configuración para editar el guión según corresponda.

1. Conéctese al nodo original en el que se instaló Sentinel.

   Nota: Debe ser el nodo en el que ejecutó la instalación completa de Sentinel.

2. Edite el guión para que aparezca de la siguiente manera, donde `<SHARED1>` es el volumen compartido que creó anteriormente:

   ```
   mount /dev/<SHARED1> /var/opt/novell

   cd /usr/lib/ocf/resource.d/novell

   ./install-resources.sh
   ```

3. (Condicional) Podría tener problemas con los nuevos recursos incluidos en el clúster. Si experimenta este problema, ejecute el siguiente comando en node02:

   Para SLES 11 SP4:

   ```
   /etc/rc.d/openais start
   ```

   Para SLES 12 SP1:

   ```
   systemctl start pacemaker.service
   ```

4. El guión `install-resources.sh` le pedirá algunos valores, principalmente la dirección IP virtual que desea que utilicen las personas para acceder a Sentinel y el nombre del dispositivo del almacenamiento compartido, y luego creará automáticamente los recursos de clúster necesarios. Tenga en cuenta que el guión requiere que el volumen compartido ya esté montado y también requiere que esté presente el archivo de instalación sin supervisión que se creó durante la instalación de Sentinel (`/tmp/install.props`). No es necesario que ejecute este guión en ningún nodo instalado salvo el primero; todos los archivos de configuración relevantes se sincronizarán automáticamente en los otros nodos.
5. Si su entorno varía con respecto a esta solución recomendada por , puede editar el archivo `resources.cli` (en el mismo directorio) y modificar las definiciones primitivas desde aquí. Por ejemplo, la solución recomendada utiliza un simple recurso de Sistema de archivos; quizá desee usar un recurso cLVM que emplee más funciones de clúster.
6. Después de ejecutar el guión shell, puede emitir un comando de `estado de crm` y el resultado debería ser similar a:

   ```
   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 En este punto, los recursos relevantes de Sentinel deben configurarse en el clúster. Puede examinar cómo se configuran y agrupan en la herramienta de gestión del clúster, por ejemplo ejecutando el estado de crm.

Configuración de almacenamiento secundario

Realice los siguientes pasos para configurar el almacenamiento secundario de manera que Sentinel pueda migrar particiones de eventos a otro almacenamiento menos costoso:

Nota: Este proceso es opcional y el almacenamiento secundario no necesita ser de alta disponibilidad de la misma forma que configuró el resto del sistema. Puede usar cualquier directorio, montado a partir de una SAN o no, un volumen NFS o CIFS.

1 En la interfaz principal de Sentinel, en la barra de menú de la parte superior, haga clic en **Almacenamiento**.

2 Seleccione **Configuración**.

3 Seleccione uno de los botones circulares de almacenamiento secundario no configurados.

Utilice un destino iSCSI sencillo como ubicación de almacenamiento compartido en red, con prácticamente la misma configuración que el almacenamiento principal. En su entorno de producción, sus tecnologías de almacenamiento podrían ser diferentes.

Utilice el siguiente procedimiento para configurar el almacenamiento secundario para su uso en Sentinel:

Nota: En el destino iSCSI, el destino se montará como directorio para su uso como almacenamiento secundario. Debe configurar el montaje como recurso del sistema de archivos de forma similar a como se configuró el sistema de archivos de almacenamiento principal. Esto no se configuró automáticamente dentro del guión de instalación de recursos, ya que había otras variaciones posibles.

1 Revise los pasos anteriores para determinar qué partición se creó para su uso como almacenamiento secundario (`/dev/<NETWORK1>`, o algo parecido a`/dev/sdc1`). Si es necesario, cree un directorio vacío en el que se pueda montar la partición (por ejemplo `/var/opt/netdata`).

2 Configure el sistema de archivos de red como recurso de clúster; utilice la interfaz principal de Sentinel o ejecute el comando:

```
crm configure primitive sentinelnetfs ocf:heartbeat:Filesystem params device="/
dev/<NETWORK1>" directory="<PATH>" fstype="ext3" op monitor interval=60s
```

donde `/dev/<NETWORK1>` es la partición que se creó en la sección Configuración de almacenamiento compartido anterior, y <PATH> es cualquier directorio local en el que se puede montar.

3. Añada el nuevo recurso al grupo de recursos gestionados:

```
 crm resource stop sentinelgrp
 crm configure delete sentinelgrp
 crm configure group sentinelgrp sentinelip sentinelfs sentinelnetfs sentineldb
sentinelserver
 crm resource start sentinelgrp
```

4. Puede conectarse al nodo que alberga actualmente los recursos (utilice `estado de crm` o `Hawk`) y asegúrese de que el almacenamiento secundario esté montado correctamente (utilice el comando `mount`).
5. Inicie sesión en la interfaz principal de Sentinel.
6. Seleccione **Storage** (Almacenamiento) y después **Configuration** (Configuración) y, a continuación, seleccione la **SAN (montada localmente**) en Almacenamiento secundario no configurado.
7. Introduzca la vía en la que se ha montado el almacenamiento secundario, por ejemplo `/var/opt/netdata`.

Utilice versiones sencillas de los recursos necesarios como, por ejemplo, Filesystem Resource Agent. Puede elegir recursos de clúster más sofisticados como cLVM (una versión de volumen lógico del sistema de archivos) si es necesario.

38 Configuración de la función de alta disponibilidad (HA) de Sentinel como SSDM

En este capítulo se proporciona información sobre cómo configurar una instalación de alta disponibilidad (HA) de Sentinel como SSDM. Estas instrucciones son aplicables a instalaciones tradicionales y de dispositivos.

Para configurar la función de alta disponibilidad de Sentinel como SSDM:

1. Instale y configure el almacenamiento ampliable para Sentinel. Para obtener más información, consulte el Capítulo 13, “Instalación y configuración del almacenamiento ampliable”, en la página 87.
2. Habilite el almacenamiento ampliable en el nodo activo. Para obtener más información, consulte la sección “Enabling Scalable Storage Post-Installation” (Habilitación del almacenamiento ampliable después de la instalación) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).
3. Ejecute el siguiente comando en el nodo activo:

   ```
   csync2 -x -v
   ```

   Esto sincronizará la configuración de SSDM con todos los nodos pasivos.
4. (Condicional) Si se produce un error a la hora de sincronizar todos los archivos cuando ejecuta el comando `csync2 - x - v` en el paso 3, realice los siguientes pasos:

   4a Borre la base de datos csync2 (en el directorio `/var/lib/csync2`) en todos los nodos.

   4b Ejecute el comando siguiente en todos los servidores para actualizar la base de datos csync2 con el fin de que coincida con el sistema de archivos, pero sin marcar ningún elemento para su sincronización con otros servidores:

   ```
   csync2 -cIr /
   ```

   4c Ejecute el siguiente comando para buscar todas las diferencias entre el servidor autorizado y los servidores remotos y marque para efectuar la sincronización:

   ```
   csync2 -TUXI
   ```

   4d Ejecute el siguiente comando para restaurar la base de datos con el fin de obligar al servidor actual a ser ganador en cualquier conflicto:

   ```
   csync2 -fr /
   ```

   4e Ejecute el siguiente comando para iniciar una sincronización con todos los demás servidores:

   ```
   csync2 -xr /
   ```

   4f Ejecute el siguiente comando para verificar que todos los archivos están sincronizados:

   ```
   csync2 -T
   ```

   Este comando no mostrará ningún archivo en caso de que la sincronización se realice correctamente.

39 Actualización de Sentinel con alta disponibilidad (HA)

Al actualizar Sentinel en un entorno HA, debe actualizar primero los nodos pasivos del clúster y luego actualizar el nodo de clúster activo.

Requisitos previos

- Descargue el programa de instalación más reciente desde el sitio Web de descargas.
- Si utiliza el sistema operativo SLES con kernel versión 3.0.101 o posterior, debe cargar manualmente el controlador de vigilancia en el equipo. Para buscar el controlador de vigilancia adecuado para el hardware de su equipo, póngase en contacto con su proveedor de hardware. Para cargar el controlador de vigilancia, realice lo siguiente:
  1. En el indicador de comandos, ejecute el siguiente comando para cargar el controlador de vigilancia en la sesión actual:

     `/sbin/modprobe -v --ignore-install <watchdog driver name>`
  2. Añada la siguiente línea al archivo `/etc/init.d/boot.local` para asegurarse de que el equipo cargue automáticamente el controlador de vigilancia durante cada inicio:

     `/sbin/modprobe -v --ignore-install <watchdog driver name>`

Actualización de una instalación tradicional de HA de Sentinel

En esta sección se proporciona información acerca de cómo actualizar una instalación tradicional de Sentinel y, además, acerca de la actualización del sistema operativo en este tipo de instalación.

Importante: Los procedimientos descritos en esta sección utilizan comandos `rcopenais` y `openais`, que funcionan solo con SLES 11 SP4. Para SLES 12 SP2 y versiones posteriores, utilice el comando `systemctl pacemaker.service`.

Por ejemplo, para el comando `/etc/rc.d/openais start`, utilice el comando `systemctl start pacemaker.service`.

Actualización de HA de Sentinel

1 Habilite el modo de mantenimiento en el clúster:

```
crm configure property maintenance-mode=true
```

El modo de mantenimiento le ayuda a evitar interrupciones en los recursos del clúster en ejecución durante la actualización de Sentinel. Este comando se puede ejecutar desde cualquier nodo del clúster.

2 Compruebe si el modo de mantenimiento está activo:

```
crm status
```

El estado de los recursos del clúster debería ser sin gestionar.

3 Actualice el nodo del clúster pasivo:

3a Detenga la pila del clúster:

```
rcopenais stop
```

Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando accesibles y se evitan las barreras de nodos.

3b Entre como usuario `root` en el servidor en el que desea actualizar Sentinel.

3c Extraiga los archivos de instalación del archivo tar:

```
tar xfz <install_filename>
```

3d Ejecute el comando siguiente en el directorio donde extrajo los archivos de instalación:

```
./install-sentinel --cluster-node
```

3e Cuando finalice la actualización, reinicie la pila del clúster:

```
rcopenais start
```

Repita el Paso 3 para todos los nodos del clúster pasivos.

3f Elimine los guiones de inicio automático de manera que el clúster pueda gestionar el producto.

```
cd /
insserv -r sentinel
```

4 Actualice el nodo del clúster activo:

4a Realice una copia de seguridad de su configuración y luego cree una exportación de ESM.

Para obtener más información sobre la copia de seguridad de datos, consulte la sección “Backing Up and Restoring Data” (Copia de seguridad y restauración de datos) en la *Sentinel Administration Guide (Guía de administración de NetIQ Sentinel 7.1)*.

4b Detenga la pila del clúster:

```
rcopenais stop
```

Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando accesibles y se evitan las barreras de nodos.

4c Entre como usuario `root` en el servidor en el que desea actualizar Sentinel.

4d Ejecute el siguiente comando para extraer los archivos de instalación del archivo tar:

```
tar xfz <install_filename>
```

4e Ejecute el comando siguiente en el directorio donde extrajo los archivos de instalación:

```
./install-sentinel
```

4f Cuando finalice la actualización, inicie la pila del clúster:

```
rcopenais start
```

4g Elimine los guiones de inicio automático de manera que el clúster pueda gestionar el producto.

```
cd /
insserv -r sentinel
```

4h Ejecute el siguiente comando para sincronizar cualquier cambio que se haya hecho en los archivos de configuración:

```
csync2 -x -v
```

5 Inhabilite el modo de mantenimiento en el clúster:

```
crm configure property maintenance-mode=false
```

Este comando se puede ejecutar desde cualquier nodo del clúster.

6 Compruebe si el modo de mantenimiento está inactivo:

```
crm status
```

El estado de los recursos del clúster debería ser iniciado.

7 (Opcional) Compruebe si Sentinel se actualizó correctamente:

```
rcsentinel version
```

Actualización del sistema operativo

En esta sección se proporciona información acerca de cómo actualizar el sistema operativo a una versión superior, por ejemplo la actualización de SLES 11 a SLES 12, en un clúster HA de Sentinel. Cuando se actualiza el sistema operativo, debe realizar algunas tareas de configuración para asegurarse de que HA de Sentinel funciona correctamente después de actualizar el sistema operativo.

Realice los pasos descritos en las secciones siguientes:

- “Actualización del sistema operativo” en la página 217
- “Configuración de destinos iSCSI” en la página 218
- “Configuración de iniciadores iSCSI” en la página 219
- “Configuración del clúster de HA” en la página 220

Actualización del sistema operativo

Para actualizar el sistema operativo:

1 Entre como usuario `root` en cualquier nodo del clúster de HA de Sentinel.

2 Ejecute el siguiente comando para habilitar el modo de mantenimiento en el clúster:

```
crm configure property maintenance-mode=true
```

El modo de mantenimiento le ayuda a evitar interrupciones en los recursos del clúster en ejecución durante la actualización del sistema operativo.

3 Ejecute el siguiente comando para comprobar si el modo de mantenimiento está activo:

```
crm status
```

El estado de los recursos del clúster debería ser sin gestionar.

4 Asegúrese de que Sentinel se ha actualizado a la versión 8.2 o posterior en todos los nodos del clúster.

5 Asegúrese de que todos los nodos del clúster se hayan registrado en SLES y SLESHA.

6 Realice los pasos siguientes para actualizar el sistema operativo en el nodo del clúster pasivo:

6a Ejecute el siguiente comando para detener la pila del clúster:

`rcopenais stop`

Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando inaccesibles y se evitan las barreras de nodos.

6b Actualice el sistema operativo. Para obtener más información, consulte la sección Actualización del sistema operativo.

7 Repita el paso 6 en todos los nodos pasivos para actualizar el sistema operativo.

8 Repita el paso 6 en el nodo activo para actualizar el sistema operativo en él.

9 Repita el paso 6b para actualizar el sistema operativo en el almacenamiento compartido.

10 Asegúrese de que el sistema operativo en todos los nodos del clúster se actualiza a SLES12 SP3.

Configuración de destinos iSCSI

Para configurar destinos iSCSI:

1 En el almacenamiento compartido, compruebe si está instalado el paquete iSCSI LIO. Si todavía no está instalado, diríjase a la gestión de software de YaST2 e instale el paquete iSCSI LIO (`isccilioTarget` RPM).

2 Realice los siguientes pasos en todos los nodos del clúster:

2a Ejecute el comando siguiente para abrir el archivo que contiene el nombre del iniciador iSCSI:

```
cat /etc/iscsi/initiatorname.iscsi
```

2b Tome nota del nombre del iniciador que se utilizará para la configuración de iniciadores iSCSI:

Por ejemplo:

```
InitiatorName=iqn.1996-04.de.suse:01:441d6988994
```

Estos nombres del iniciador se utilizarán durante la configuración del cliente de destino iSCSI.

3 Haga clic en **Servicio**y seleccione la opción**En el arranque** para asegurarse de que el servicio se inicia al arrancar el sistema operativo.

4 Seleccione la pestaña **Global**, deseleccione **Sin autenticación** para habilitar la autenticación y, a continuación, especifique el nombre de usuario y contraseña requeridos para la autenticación entrante y saliente.

La opción**Sin autenticación** está habilitada por defecto. Sin embargo, debe habilitar la autenticación para asegurarse de que la configuración sea segura.

5 Haga clic en **Destinos** y en **Añadir** para añadir un nuevo destino.

6 Haga clic en **Añadir** para añadir un nuevo LUN.

7 Deje el número LUN 0, busque en el cuadro de diálogo **Vía** (en Type=fileio) y seleccione el archivo `/localdata` que ha creado. Si tiene un disco dedicado para almacenamiento, especifique un dispositivo de bloque, como por ejemplo `/dev/sdc`.

8 Repita los pasos 6 y 7, añada LUN 1 y seleccione `/networkdata` en esta ocasión.

9 Repita los pasos 6 y 7, añada LUN 2 y seleccione `/sbd` en esta ocasión.

10 Deje las demás opciones en sus valores por defecto. Haga clic en **Siguiente.**

11 Haga clic en **Añadir**. Cuando se le pida el nombre del cliente, especifique el nombre del iniciador que ha copiado en el paso 2. Repita este paso para añadir todos los nombres de cliente mediante la especificación de los nombres del iniciador.

Se mostrará la lista de nombres de los clientes en la lista de clientes.

12 (Condicional) Si ha habilitado la autenticación en el paso 4, proporcione las credenciales de autenticación que ha especificado en dicho paso.

   Seleccione un cliente, seleccione **Edit Auth** (Editar aut.) > **Incoming Authentication** (Autenticación entrante) y especifique el nombre de usuario y contraseña. Repita este paso para todos los clientes.

13 Haga clic de nuevo en **Siguiente** para seleccionar las opciones de autenticación por defecto, y luego en **Finalizar** para salir de la configuración. Si se le solicita, reinicie iSCSI.

14 Salga de YaST.

Configuración de iniciadores iSCSI

Para configurar los iniciadores iSCSI:

1 Conéctese a uno de los nodos del clúster (node01) e inicie YaST.

2 Haga clic en **Network Services** (Servicios de red) > **iSCSI Initiator** (Iniciador de iSCSI).

3 Si se le solicita, instale el software necesario (`iscsiclient` RPM).

4 Haga clic en **Servicio** y seleccione **Al arrancar** para asegurarse de que el servicio iSCSI se inicia durante el arranque.

5 Haga clic en **Destinos descubiertos**.

   Nota: Si se muestran todos los destinos iSCSI ya existentes, suprima esos destinos.

   Seleccione **Descubrimiento** para añadir un nuevo destino iSCSI.

6 Especifique la dirección IP de destino (10.0.0.3) de iSCSI.

   (Condicional) Si ha habilitado la autenticación en el paso 4 en “Configuración de destinos iSCSI” en la página 218, deseleccione **Sin autenticación**. En la sección **Autenticación saliente**, introduzca las credenciales de autenticación que ha especificado durante la configuración de destinos iSCSI.

   Haga clic en **Siguiente.**

7 Seleccione el destino iSCSI descubierto con la dirección IP 10.0.0.3 y después seleccione **Entrar**.

8 Realice los siguientes pasos:

   8a Cambie a Automático en el menú desplegable **Inicio**.

   8b (Condicional) Si ha habilitado la autenticación, deseleccione **Sin autenticación**.

   El nombre de usuario y la contraseña que ha especificado deben aparecer en la sección **Autenticación saliente**. Si no se muestran estas credenciales, introduzca las credenciales en esta sección.

   8c Haga clic en **Siguiente.**

9 Cambie a la pestaña **Destinos conectados** para garantizar que se establezca la conexión con el destino.

10 Salga de la configuración. Esta acción debería haber montado los destinos iSCSI como dispositivos de bloque en el nodo del clúster.

11 En el menú principal YaST, seleccione **System** (Sistema) > **Partitioner** (Particionador).

12 En la vista del sistema, debería ver nuevos discos duros del tipo LIO-ORG: FILEIO (por ejemplo, `/dev/sdb` y `/dev/sdc`) en la lista, junto con discos ya formateados (por ejemplo, `/dev/sdb1` o `/dev / < SHARED1`).

13 Repita los pasos del 1 al 12 en todos los nodos.

Configuración del clúster de HA

Para configurar el clúster de HA:

1. Inicie YaST2 y acceda a **Alta disponibilidad** > **Clúster**.
2. Si se le solicita, instale el paquete de HA y determine las dependencias.

   Después de la instalación del paquete de HA, se muestran los canales de comunicación del clúster.
3. Asegúrese de seleccionar `Unidifusión` como la opción de transporte.
4. Seleccione **Agregar una dirección de miembro** y especifique la dirección IP del nodo y, a continuación, repita este proceso para añadir todas las demás direcciones IP de nodo de clúster.
5. Asegúrese de seleccionar la opción **Generar automáticamente ID de nodo**.
6. Asegúrese de que el servicio HAWK esté habilitado en todos los nodos. Si no está habilitado, ejecute el siguiente comando para habilitarlo:

   ```
   service hawk start
   ```
7. Ejecute el comando siguiente:

   ```
   ls -l /dev/disk/by-id/
   ```

   Se muestra el ID de partición SBD. Por ejemplo, `scsi-1LIO-ORG_FILEIO:33caaa5a-a0bc-4d90-b21b-2ef33030cc53`.

   Copie el ID.
8. Abra el archivo sbd (`/etc/sysconfig/sbd`) y cambie el ID de `SBD_DEVICE` por el ID que ha copiado en el paso 7.
9. Ejecute el siguiente comando para reiniciar el servicio Pacemaker:

   ```
   rcpacemaker restart
   ```
10. Ejecute los comandos siguientes para eliminar los guiones de inicio automático, de forma que el clúster pueda gestionar el producto.

    ```
    cd /
    ```

    ```
    insserv -r sentinel
    ```
11. Repita los pasos del 1 a 10 en todos los nodos del clúster.
12. Ejecute el siguiente comando para sincronizar cualquier cambio que se haya hecho en los archivos de configuración:

    ```
    csync2 -x -v
    ```
13. Ejecute el siguiente comando para inhabilitar el modo de mantenimiento en el clúster:

    ```
    crm configure property maintenance-mode=false
    ```

    Este comando se puede ejecutar desde cualquier nodo del clúster.
14. Ejecute el siguiente comando para comprobar si el modo de mantenimiento está inactivo:

    ```
    crm status
    ```

    El estado de los recursos del clúster debería ser iniciado.

Actualización de una instalación de dispositivo HA de Sentinel

Puede actualizar una instalación de dispositivo de alta disponibilidad de Sentinel mediante el parche Zypper.

Importante: Los procedimientos descritos en esta sección utilizan comandos `rcopenais` y `openais`, que funcionan solo con SLES 11 SP4. Para SLES 12 SP2 y versiones posteriores, utilice el comando `systemctl pacemaker.service`.

Por ejemplo, para el comando `/etc/rc.d/openais start`, utilice el comando `systemctl start pacemaker.service`.

- "Actualización del dispositivo de alta disponibilidad de Sentinel mediante Zypper" en la página 221

Actualización del dispositivo de alta disponibilidad de Sentinel mediante Zypper

Debe registrar todos los nodos del dispositivo mediante Sentinel Appliance Manager antes de realizar la actualización. Para obtener más información, consulte la "Registro para recibir actualizaciones" en la página 106. Si no registra el dispositivo, Sentinel mostrará una advertencia en amarillo.

1. Habilite el modo de mantenimiento en el clúster.

   ```
   crm configure property maintenance-mode=true
   ```

   El modo de mantenimiento le ayuda a evitar interrupciones en los recursos del clúster en ejecución durante la actualización del software de Sentinel. Este comando se puede ejecutar desde cualquier nodo del clúster.

2. Compruebe si el modo de mantenimiento está activo.

   ```
   crm status
   ```

   El estado de los recursos del clúster debería ser sin gestionar.

3. Actualice el nodo del clúster pasivo:

   3a Detenga la pila del clúster.

   ```
   rcopenais stop
   ```

   Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando inaccesibles y se evitan las barreras de nodos.

   3b Descargue las actualizaciones del dispositivo HA de Sentinel.

   ```
   zypper -v patch
   ```

   3c (Condicional) Si el programa de instalación muestra un mensaje en el que se le solicita que debe determinar una dependencia para el paquete OpenSSH, introduzca la opción adecuada para volver a la versión anterior del paquete OpenSSH.

   3d (Condicional) Si el programa de instalación muestra un mensaje que indica el cambio en la arquitectura ncgOverlay, introduzca la opción adecuada para aceptar el cambio de arquitectura.

   3e (Condicional) Si el programa de instalación muestra un mensaje en el que se le indica que debe determinar una dependencia para ciertos paquetes del dispositivo, introduzca la opción adecuada para desinstalar los paquetes dependientes.

3f Cuando finalice la actualización, inicie la pila del clúster.

```
rcopenais start
```

4 Repita el paso 3 para todos los nodos pasivos del clúster.

5 Actualice el nodo del clúster activo:

5a Realice una copia de seguridad de su configuración y luego cree una exportación de ESM.

Para obtener más información sobre la copia de seguridad de los datos, consulte "Backing Up and Restoring Data" (Copia de seguridad y restauración de datos) en *Sentinel Administration Guide (Guía de administración de NetIQ Sentinel)*.

5b Detenga la pila del clúster.

```
rcopenais stop
```

Al detener la pila del clúster, se garantiza que los recursos del clúster sigan estando inaccesibles y se evitan las barreras de nodos.

5c Descargue las actualizaciones del dispositivo HA de Sentinel.

```
zypper -v patch
```

5d (Condicional) Si el programa de instalación muestra un mensaje en el que se le solicita que debe determinar una dependencia para el paquete OpenSSH, introduzca la opción adecuada para volver a la versión anterior del paquete OpenSSH.

5e (Condicional) Si el programa de instalación muestra un mensaje que indica el cambio en la arquitectura ncgOverlay, introduzca la opción adecuada para aceptar el cambio de arquitectura.

5f (Condicional) Si el programa de instalación muestra un mensaje en el que se le indica que debe determinar una dependencia para ciertos paquetes del dispositivo, introduzca la opción adecuada para desinstalar los paquetes dependientes.

5g Cuando finalice la actualización, inicie la pila del clúster.

```
rcopenais start
```

5h Ejecute el siguiente comando para sincronizar cualquier cambio que se haya hecho en los archivos de configuración:

```
csync2 -x -v
```

6 Inhabilite el modo de mantenimiento en el clúster.

```
crm configure property maintenance-mode=false
```

Este comando se puede ejecutar desde cualquier nodo del clúster.

7 Compruebe si el modo de mantenimiento está inactivo.

```
crm status
```

El estado de los recursos del clúster debería ser iniciado.

8 (Opcional) Compruebe si Sentinel se actualizó correctamente:

```
rcsentinel version
```

9 (Condicional) Para actualizar el sistema operativo, consulte "Actualización del sistema operativo" en la página 162.

40 Recuperación de datos y copias de seguridad

El clúster de failover de alta disponibilidad descrito en este documento proporciona un nivel de redundancia para que, si un servicio falla en un nodo del clúster, se producirá automáticamente el failover y la recuperación en otro nodo del clúster. Cuando sucede un evento de este tipo, es importante devolver el nodo fallido al estado operativo de manera que se pueda restaurar la redundancia de sistema y protegerlo en caso de otro fallo. En esta sección se describe la restauración del nodo fallido en una variedad de condiciones de fallo.

Copia de seguridad

Si bien el clúster de failover de alta disponibilidad descrito en este documento proporciona un nivel de redundancia, sigue siendo importante realizar una copia de seguridad tradicional de la configuración y los datos, que haría muy fácil la recuperación en caso de pérdida o daño de los mismos. En la sección “Backing Up and Restoring Data” (Copia de seguridad y recuperación de datos) de *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel) se describe cómo usar las herramientas integradas en Sentinel para crear una copia de seguridad. Estas herramientas deben usarse en el nodo activo del clúster porque el nodo pasivo del clúster no tendrá el acceso necesario al dispositivo de almacenamiento compartido. Sería posible usar en su lugar otras herramientas comerciales de copia de seguridad disponibles que podrían tener requisitos diferentes sobre en qué nodo se pueden usar.

Recuperación

Fallo temporal

Si se trató de un fallo temporal y no parece que haya daños en la aplicación o el software del sistema operativo y la configuración, entonces será posible devolver el nodo al estado operativo eliminando simplemente el fallo temporal, por ejemplo reiniciando el nodo. Puede utilizarse la interfaz del usuario de gestión del clúster para recuperar la configuración inicial del servicio en ejecución al nodo del clúster original, si así lo desea.

Daño del nodo

Si el fallo dio lugar a daños en la aplicación o el software del sistema operativo o en la configuración presente en el sistema de almacenamiento del nodo, será necesario reinstalar el software. La repetición de los pasos de adición de un nodo al clúster descrita anteriormente en este documento

devolverá el nodo a un estado operativo. Puede utilizarse la interfaz del usuario de gestión del clúster para recuperar la configuración inicial del servicio en ejecución al nodo del clúster original, si así lo desea.

Configuración de datos del clúster

Si se producen daños en los datos del dispositivo de almacenamiento compartido de forma que no es posible recuperar este dispositivo, los daños producidos afectarían a todo el clúster de manera que no se podrá recuperar automáticamente al usar el clúster de failover de alta disponibilidad descrito en este documento. La sección “Backing Up and Restoring Data” (Copia de seguridad y restauración de datos) de *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel) describe cómo usar las herramientas integradas de Sentinel para restaurarlo a partir de una copia de seguridad. Estas herramientas deben usarse en el nodo activo del clúster porque el nodo pasivo del clúster no tendrá el acceso necesario al dispositivo de almacenamiento compartido. Sería posible usar en su lugar otras herramientas comerciales de copia de seguridad y restauración disponibles que podrían tener requisitos diferentes sobre en qué nodo se pueden usar.

VIII Apéndices

A Solución de problemas

En esta sección se enumeran los problemas que podrían ocurrir durante la instalación y las medidas para solucionar dichos problemas.

La instalación falló debido a una configuración de red incorrecta

Durante el primer arranque, si el instalador detecta que los ajustes de red son incorrectos, se muestra un mensaje de error. Si la red no está disponible, falla la instalación de Sentinel en el dispositivo.

Para solucionar este problema, configure adecuadamente los ajustes de red. Para verificar la configuración, utilice el comando `ipconfig` para devolver la dirección IP válida y utilice el comando `hostname -f` para devolver el nombre de host válido.

El UUID no se crea para instancias de Correlation Engine o Collector Manager con imagen.

Si crea una imagen de un servidor de Collector Manager (por ejemplo, mediante ZENworks Imaging) y restaura las imágenes en otros equipos, Sentinel no identifica de forma exclusiva las nuevas instancias de Collector Manager. Esto sucede debido a que existen UUID duplicados.

Debe generar un nuevo UUID siguiendo estos pasos en los sistemas de Collector Manager recién instalados:

1. Suprima el archivo `host.id` o `sentinel.id` ubicado en la carpeta `/var/opt/novell/sentinel_/data`.
2. Reinicie Collector Manager.

   Collector Manager genera de forma automática el UUID.

La interfaz principal de Sentinel está en blanco en Internet Explorer después de entrar a la sesión

Si el nivel de Seguridad de Internet se configura en Alto, aparece una página en blanco después de entrar en Sentinel y el navegador podría bloquear la ventana emergente de descarga de archivos. Para salvar este problema, deberá fijar primero el nivel de seguridad en Medio-alto y luego cambiar a nivel Personalizado de la siguiente manera:

1. Desplácese a **Herramientas > Opciones de Internet > Seguridad** y fije el nivel de seguridad en **Medio-alto**.
2. Asegúrese de que no esté seleccionada la opción **Herramientas > Vista de compatibilidad**.
3. Desplácese a **Herramientas > Opciones de Internet > pestaña Seguridad> Nivel personalizado**, luego desplácese a la sección **Descargas** y elija **Habilitar** en la opción **Pedir intervención del usuario automática para descargas de archivo**.

Sentinel no se lanza en Internet Explorer 11 en Windows Server 2012 R2

Al utilizar Windows Server 2012 R2, Sentinel no se lanza en Internet Explorer 11 debido a las configuraciones de seguridad por defecto de esta versión del navegador. Debe añadir manualmente Sentinel a la lista de sitios de confianza antes de lanzar Sentinel.

Para añadir Sentinel a la lista de sitios de confianza

1. Abra Internet Explorer 11.
2. Haga clic en el icono de **configuración** > **Opciones de Internet** > pestaña **Seguridad** > **Sitios de confianza** > **Sitios**.
3. Añada el host de Sentinel a la lista de sitios de confianza.

Sentinel no puede ejecutar informes locales con una licencia EPS por defecto

Si su entorno tiene la licencia por defecto de 25 EPS y ejecuta un informe, este presentará el siguiente error: `License for Distributed Search feature is expired` (La licencia de la función de búsqueda distribuida ha caducado).

Para ejecutar informes en el mismo JVM que Sentinel, realice los siguientes pasos:

1. Entre en el servidor de Sentinel y abra el archivo `/etc/opt/novell/sentinel/config/obj-component.JasperReportingComponent.properties`.
2. Localice la propiedad `reporting.process.oktorunstandalone`.
3. (Condicional) Si la propiedad no se encuentra en el archivo, añádala.
4. Defina la propiedad en `false` (falso). Por ejemplo:

   ```
   reporting.process.oktorunstandalone=false
   ```
5. Reinicie Sentinel.

Es necesario iniciar manualmente la sincronización en la configuración de alta disponibilidad de Sentinel después de convertir el nodo activo al modo FIPS 140-2

Problema: Al convertir el nodo activo al modo FIPS 140-2 en la configuración de alta disponibilidad de Sentinel, la sincronización para convertir todos los nodos pasivos al modo FIPS 140-2 no se realiza por completo. Debe iniciar manualmente la sincronización.

Solución: Sincronice manualmente todos los nodos pasivos al modo FIPS 140-2 de la siguiente forma:

1. Entre a la sesión como usuario root en el nodo activo.
2. Abra el archivo `/etc/csync2/csync2.cfg`.
3. Cambie la línea siguiente:

   ```
   include /etc/opt/novell/sentinel/3rdparty/nss/*;
   ```

   a

   ```
   include /etc/opt/novell/sentinel/3rdparty/nss;
   ```
4. Guarde el archivo `csync2.cfg`.
5. Ejecute el comando siguiente para iniciar la sincronización de forma manual:

   ```
   csync2 -x -v
   ```

La interfaz principal de Sentinel muestra una página en blanco tras la conversión a Sentinel Scalable Data Manager

Problema: Después de habilitar SSDM, cuando se entra a la interfaz principal de Sentinel, el navegador mostrará una página en blanco.

Solución: Cierre el navegador y entre de nuevo a la interfaz principal de Sentinel. Este problema solo ocurre en una ocasión: la primera vez que entra a la interfaz principal de Sentinel después de habilitar SSDM.

Falta el panel Campos de evento en la página Programación cuando se editan algunas búsquedas guardas

Problema: Cuando se edita una búsqueda guardada que se actualizó de Sentinel 7.2 a una versión posterior, la página Programación no muestra el panel **Campos de evento**, usado para especificar campos de salida en el archivo CSV de informe de la búsqueda.

Solución: Después de actualizar Sentinel, vuelva a crear y programar la búsqueda para ver el panel **Campos de evento** en la página Programación.

Sentinel no devuelve ningún evento correlacionado cuando se buscan eventos para la regla implantada con la búsqueda de número de activaciones por defecto

Problema: Sentinel no devuelve ningún evento correlacionado cuando se buscan todos los eventos correlacionados que se generaron después de implantar o habilitar la regla, haciendo clic en el icono situado junto a **Número de activaciones** en el panel **Estadísticas de actividad** de la página de resumen de correlaciones para dicha regla.

Solución: Cambie el valor del campo **Desde** en la página de búsqueda de eventos por una hora anterior a la que se muestra en el campo y vuelva a hacer clic en **Buscar**.

La consola de inteligencia de seguridad muestra una duración de línea de base no válida al regenerar una línea de base

Problema: Durante la regeneración de la línea de base de inteligencia de seguridad, las fechas de inicio y fin de la línea de base son incorrectas y se muestra 1/1/1970.

Solución: Las fechas correctas se actualizan al finalizar la regeneración de la línea de base.

El servidor Sentinel se apaga al ejecutar una búsqueda si hay muchos eventos en una sola partición

Problema: El servidor Sentinel se apaga al ejecutar una búsqueda si hay muchos eventos indexados en una sola partición.

Solución: Cree directivas de retención de modo que haya al menos dos particiones abiertas en un día. El hecho de tener más de una partición abierta contribuye a reducir el número de eventos indexados en las particiones.

Puede crear directivas de retención que filtren los eventos en función del campo `estzhour`, que rastrea la hora del día. Por lo tanto, puede crear una directiva de retención con el filtro `estzhour:[0 TO 11]` y otra con el filtro `estzhour:[12 TO 23]`.

Para obtener más información, consulte "Configuring Data Retention Policies" (Configuración de directivas de retención de datos) en la *Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Error al utilizar el guion report_dev_setup.sh para configurar los puertos de Sentinel para excepciones de cortafuegos en las instalaciones actualizadas de dispositivos Sentinel

Problema: Sentinel muestra un error cuando se utiliza el guion `report_dev_setup.sh` para configurar los puertos de Sentinel para excepciones de cortafuegos.

Solución: Siga estos pasos para configurar los puertos de Sentinel para excepciones de cortafuegos:

1. Abra el archivo `/etc/sysconfig/SuSEfirewall2`.
2. Cambie la línea siguiente:

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   a

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Reinicie Sentinel.

B Desinstalación

En este apéndice se proporciona información sobre la desinstalación de Sentinel y otras tareas posteriores a la desinstalación.

Lista de verificación de desinstalación

Utilice la siguiente lista de verificación para desinstalar Sentinel:

- ❒ Desinstale el servidor Sentinel.
- ❒ Desinstale Collector Manager y Correlation Engine, si los hay.
- ❒ Lleve a cabo las tareas posteriores a la desinstalación para finalizar la desinstalación de Sentinel.

Desinstalación de Sentinel

Hay disponible un guión de desinstalación que le ayudará a eliminar una instalación de Sentinel. Antes de ejecutar una nueva instalación, debe ejecutar todos los pasos siguientes para asegurarse de que no quedan archivos ni ajustes del sistema procedentes de una instalación anterior.

Advertencia: Estas instrucciones implican la modificación de valores de configuración y archivos del sistema operativo. Si no está familiarizado con la modificación de estos valores de configuración y archivos del sistema, póngase en contacto con el administrador del sistema.

Desinstalación del servidor de Sentinel

Siga los pasos indicados a continuación para desinstalar el servidor Sentinel:

1. Entre en Sentinel como usuario `root`.

   Nota: No es posible desinstalar el servidor Sentinel como usuario diferente de root si la instalación la llevó a cabo el usuario `root`. Sin embargo, un usuario diferente de root puede desinstalar el servidor Sentinel si la instalación fue realizada por un usuario diferente de root.

   ---

2. Acceda al siguiente directorio:

   ```
   <sentinel_installation_path>/opt/novell/sentinel/setup/
   ```

3. Ejecute el comando siguiente:

   ```
   ./uninstall-sentinel
   ```

4 Cuando se le indique que vuelva a confirmar que desea continuar con la desinstalación, pulse s.

El guión detiene primero el servicio y luego lo elimina por completo.

Desinstalación de Collector Manager y Correlation Engine.

Siga los pasos indicados a continuación para desinstalar Collector Manager y Correlation Engine:

1 Entre en el equipo de Collector Manager y Correlation Engine como usuario `root`.

Nota: No es posible desinstalar las instancias remotas de Collector Manager o Correlation Engine como usuario diferente de root, si la instalación se realizó como usuario `root`. Sin embargo, un usuario diferente de root puede realizar la desinstalación, si la instalación la llevó a cabo un usuario diferente de root.

---

2 Vaya a la siguiente ubicación:

```
/opt/novell/sentinel/setup
```

3 Ejecute el comando siguiente:

```
./uninstall–sentinel
```

El guión muestra una advertencia que indica que Collector Manager o Correlation Engine y todos los datos asociados se eliminarán por completo.

4 Introduzca s para eliminar Collector Manager o Correlation Engine.

El guión detiene primero el servicio y luego lo elimina por completo. No obstante, aún podría visualizarse el icono de Collector Manager y Correlation Engine en la interfaz principal de Sentinel.

5 (Condicional) Si ha habilitado la visualización de eventos, debe implantar de nuevo el módulo auxiliar (plug-in) de seguridad de Elasticsearch. Para obtener más información, consulte “Nueva implantación del módulo auxiliar (plug-in) de Elasticsearch” en la página 84.

6 Lleve a cabo los siguientes pasos adicionales para suprimir manualmente Collector Manager y Correlation Engine en la interfaz principal de Sentinel:

Collector Manager:

1. Acceda a **Gestión de orígenes de eventos > Vista activa**.
2. Haga clic con el botón derecho en la instancia de Collector Manager que desee suprimir y, a continuación, haga clic en **Suprimir**.

Correlation Engine:

1. Acceda a la interfaz **Sentinel principal** como administrador.
2. Amplíe **Correlación** y luego seleccione la instancia de Correlation Engine que desea suprimir.
3. Haga clic en el botón **Suprimir** (icono de papelera).

Desinstalación de NetFlow Collector Manager

Siga los pasos indicados a continuación para desinstalar NetFlow Collector Manager:

1 Entre en el equipo de NetFlow Collector Manager.

Nota: Debe acceder con el mismo permiso de usuario que utilizó para instalar NetFlow Collector Manager.

---

2 Cambie al directorio siguiente:

```
/opt/novell/sentinel/setup
```

3 Ejecute el comando siguiente:

```
./uninstall–sentinel
```

4 Introduzca s para desinstalar Collector Manager.

El guión detiene primero el servicio y luego lo desinstala por completo.

Tareas posteriores a la desinstalación

La desinstalación del servidor Sentinel no supone la eliminación del usuario administrador de Sentinel del sistema operativo. Necesitará eliminarlo manualmente.

Después de desinstalar Sentinel, se conservan algunos ajustes del sistema. Es necesario eliminar estos ajustes antes de llevar a cabo una nueva instalación de Sentinel, en particular si se encuentran errores en la desinstalación de Sentinel.

Para eliminar manualmente los ajustes del sistema de Sentinel:

1 Entre a la sesión como usuario `root`.

2 Asegúrese de que todos los procesos de Sentinel están detenidos.

3 Elimine el contenido de `/opt/novell/sentinel` (o la carpeta en la que haya instalado el software de Sentinel).

4 Asegúrese de que nadie haya iniciado una sesión como usuario del sistema operativo del administrador de Sentinel (novell por defecto); a continuación, elimine el usuario, el directorio personal y el grupo.

```
userdel -r novell
```

```
groupdel novell
```

5 Reinicie el sistema operativo.