Guía de instalación y configuración

NetIQ Sentinel 7.0.1

March 2012

Información legal

Para obtener más información, póngase en contacto con NetIQ en:

1233 West Loop South, Houston, Texas 77027

U.S.A

www.netiq.com

Tabla de contenido

Acerca de esta guía

Esta guía proporciona una introducción a NetIQ Sentinel y explica la forma de instalar, migrar y configurar Sentinel.

Usuarios a los que va dirigida

Esta guía está dirigida a administradores y consultores de Sentinel.

Comentarios

Nos gustaría recibir sus comentarios y sugerencias acerca de este manual y del resto de la documentación incluida con este producto. Utilice la función de comentarios del usuario situada en la parte inferior de las páginas de la documentación en línea.

Actualizaciones de la documentación

Para obtener la versión más reciente de la *Guía de instalación y configuración de NetIQ Sentinel 7.0.1*, visite el sitio Web de documentación de Sentinel (http://www.novell.com/documentation/sentinel70).

Documentación adicional

La documentación técnica de Sentinel se divide en varios volúmenes distintos. Son los siguientes:

- Sentinel Overview Guide (Guía de descripción general de Sentinel) (http://www.novell.com/documentation/sentinel70/s70_overview/data/bookinfo.html)
- Sentinel Quick Start Guide (Guía de inicio rápido de Sentinel) (http://www.novell.com/documentation/sentinel70/s70_quickstart/data/s70_quickstart.html)
- Sentinel Administration Guide (Guía de administración de Sentinel) (http://www.novell.com/documentation/sentinel70/s70_admin/data/bookinfo.html)
- Sentinel User Guide (Guía del usuario de Sentinel) (http://www.novell.com/documentation/sentinel70/s70_user/data/bookinfo.html)
- Sentinel Link Overview Guide (Guía de descripción general de Sentinel Link) (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Eventos de auditoría interna de Sentinel (http://www.novell.com/documentation/sentinel70/s70_auditevents/data/bookinfo.html)
- SDK de Sentinel (http://www.novell.com/developer/develop_to_sentinel.html)

  El sitio de SDK de Sentinel proporciona información sobre cómo crear sus propios módulos auxiliares (plug-ins).

Contacto con Novell y NetIQ

Sentinel es ahora un producto de NetIQ, si bien Novell sigue manejando muchas funciones de asistencia.

- Sitio Web de Novell (http://www.novell.com)
- Sitio Web de NetIQ (http://www.netiq.com)
- Asistencia técnica (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Autoasistencia (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Sitio de descarga de revisión (http://download.novell.com/index.jsp)
- Foros de asistencia de la comunidad de Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Sentinel TIDs (http://support.novell.com/products/sentinel)
- Sitio Web del módulo auxiliar (plug-in) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **Lista de notificación por correo electrónico:** Inscríbase a través del sitio Web de módulos auxiliares de Sentinel

Cómo contactar con asistencia para ventas

Para cualquier pregunta sobre nuestros productos, precios y capacidades, póngase en contacto con su representante local. Si no puede contactar con su representante local, comuníquese con nuestro equipo de Asistencia para ventas.

Oficinas mundiales: Ubicaciones de las oficinas de NetIQ (http://www.netiq.com/about_netiq/officelocations.asp)

Estados Unidos y Canadá: 888-323-6768

Correo electrónico: info@netiq.com

Sitio Web: www.netiq.com

Instalación

Utilice la siguiente información para instalar Sentinel:

1 Cumplimiento de los requisitos del sistema

En las siguientes secciones se describen los requisitos de compatibilidad de hardware, sistema operativo, navegador, conectores admitidos y orígenes de eventos para Sentinel.

1.1 Requisitos del sistema y plataformas compatibles

NetIQ admite Sentinel en los sistemas operativos descritos en esta sección. NetIQ también admite Sentinel en sistemas con pequeñas actualizaciones a estos sistemas operativos, como por ejemplo parches de seguridad y correcciones (hotfixes). Sin embargo, no es posible ejecutar Sentinel en sistemas que hayan realizado importantes actualizaciones de estos sistemas operativos hasta que NetIQ no haya probado y certificado dichas actualizaciones.

1.1.1 Sistemas operativos y plataformas compatibles

El servidor Sentinel, el gestor de recopiladores y el motor de correlación son compatibles con los siguientes sistemas operativos y plataformas:

Categoría	Requisito
Sistema operativo	Sentinel es compatible con los siguientes sistemas operativos: ◆ SUSE Linux Enterprise Server (SLES) 11 SP1 de 64 bits * ◆ Red Hat Enterprise Linux for Servers (RHEL) 6 de 64 bits * Sentinel 7 no se admite en las instalaciones Open Enterprise Server de SLES.
Plataforma virtual	NetIQ proporciona dispositivos que instalan un servidor SLES 11 SP1 de 64 bits y Sentinel en las siguientes plataformas virtuales: ◆ VMWare ESX 4.0 ◆ Xen 4.0
Imágenes ISO en DVD	NetIQ proporciona un archivo de imagen ISO en DVD que instala SLES 11 SP1 de 64 bits y Sentinel en: ◆ Servidor Hyper-V 2008 R2 ◆ Hardware sin sistema operativo instalado

1.1.2 Requisitos del hardware

Las recomendaciones de hardware para una implementación de Sentinel pueden variar en función de la implementación individual, por lo que se recomienda consultar con NetIQ Consulting Services (servicios de consultoría) o con algún socio de NetIQ Sentinel antes de finalizar la arquitectura de Sentinel.

- "Servidor de Sentinel" en la página 12
- "Gestor de recopiladores" en la página 13
- "Motor de correlación" en la página 14

Servidor de Sentinel

En esta sección se enumeran los requisitos de hardware recomendados para un sistema de producción que albergue 90 días de datos en línea. Estas recomendaciones suponen un tamaño medio de eventos de 600 bytes. Las recomendaciones de almacenamiento local y en red incluyen un buffer del 20 % por encima de las estimaciones reales de almacenamiento. NetIQ recomienda integrar un buffer en caso de que las estimaciones sean inexactas o que alguno de los servidores experimente mayor actividad con el tiempo.

Utilice los siguientes requisitos de hardware para ejecutar el servidor Sentinel con todos los componentes de Sentinel instalados en un solo servidor:

Categoría	100 EPS	2500 EPS	5000 EPS
CPU	Un procesador Intel Xeon X5570 2,93 GHz (4 núcleos de CPU)	Dos CPU Intel Xeon X5470 3,33 GHz (4 núcleos) CPUs (8 núcleos en total)	Dos CPU Intel Xeon X5470 3,33 GHz (4 núcleos) CPUs (8 núcleos en total)
Almacenamiento local (30 días)	2 unidades de 256 GB, 7200 RPM (hardware RAID con caché de 256 MB)	8 unidades de 7200 RPM, x 1.2 TB (RAID 10 en hardware con 256 MB de caché)	16 unidades de 15000 RPM, x 1.2 TB, (RAID 10 en hardware con 512 MB de caché) o una red de área de almacenamiento equivalente (SAN)
Almacenamiento en red (90 días)	2 x 128 GB	4 x 1 TB	8 x 1 TB
Memoria	**Otras instalaciones:** 4 GB **Instalación de imagen ISO en DVD:** 4.5 GB	16 GB	24 GB

NOTE: Sentinel es compatible en procesadores Intel Xeon x86 de 64 bits y AMD Opteron, pero no con los procesadores puros de 64 bits como Itanium.

Siga estas pautas para obtener un rendimiento óptimo del sistema:

- El almacenamiento local debe tener espacio suficiente para guardar como mínimo 5 días de datos, incluyendo tanto datos de eventos como datos en bruto. Para obtener más información sobre la forma de calcular los requisitos de almacenamiento de datos, consulte la Sección 1.1.5, “Estimación de requisitos de almacenamiento de datos”, en la página 16.
- El almacenamiento en red contiene el total de 90 días, e incluye una copia totalmente comprimida de los datos de eventos en el almacenamiento local. Se guarda una copia de los datos de eventos en el almacenamiento local para buscar e informar de datos de rendimiento. El tamaño de almacenamiento local puede disminuirse si preocupan los costes de almacenamiento. Sin embargo, debido al gasto de descompresión, se producirá una disminución estimada del 70% en el rendimiento de búsqueda y creación de informes en los datos que normalmente estarían en el almacenamiento local.
- Debe configurar la ubicación de almacenamiento en red en una red SAN externa de varias unidades o en un almacenamiento con interconexión a la red (NAS).
- El volumen de estado regular recomendado es del 80 % del número máximo de EPS con licencia. NetIQ recomienda añadir otras instancias de Sentinel si se alcanza el límite.

Gestor de recopiladores

Utilice los siguientes requisitos de hardware para ejecutar el gestor de recopiladores en un sistema diferente del servidor Sentinel en un entorno de producción:

Categoría	Mínimo	Recomendación
CPU	Un procesador Intel Xeon L5240 de 3 GHz (de 2 núcleos)	Un procesador Intel Xeon X5570 2,93-GHz (4 núcleos de CPU)
Espacio de disco	10 GB (RAID 1)	20 GB (RAID 1)
Memoria	1.5 GB	4 GB
Número estimado (EPS)	500	2.000

Motor de correlación

Utilice los siguientes requisitos del sistema para ejecutar el motor de correlación en un sistema diferente del servidor Sentinel en un entorno de producción:

Categoría	Mínimo	Recomendación
CPU	Un procesador Intel Xeon L5240 de 3 GHz (de 2 núcleos)	Un procesador Intel Xeon X5570 2,93-GHz (4 núcleos de CPU)
Espacio de disco	10 GB (no se requiere RAID)	10 GB (no se requiere RAID)
Memoria	1.5 GB	4 GB
Número estimado (EPS)	500	2500

1.1.3 Plataformas de bases de datos compatibles

Sentinel incluye un sistema de almacenamiento basado en archivos integrado y una base de datos, que son todo lo necesario para ejecutar Sentinel. Sin embargo, si utiliza la función opcional de sincronización de datos para copiar datos a un almacén de datos, Sentinel admite el uso de Oracle versión 11g R2 o Microsoft SQL Server 2008 R2 como almacén de datos.

1.1.4 Navegadores compatibles

La interfaz Web de Sentinel está optimizada para una visualización a una resolución de 1280 x 1024 o superior en los siguientes navegadores compatibles:

NOTE: Para cargar correctamente las aplicaciones del cliente de Sentinel, debe tener instalado en su sistema el módulo auxiliar (plug-in) de Sun Java.

Plataforma	Navegador
Windows 7	◆ Firefox 5, 6, 7, 8, 9 y 10 ◆ Internet Explorer 8 y 9 * Para obtener más información sobre Internet Explorer 8, consulte "Requisitos previos para Internet Explorer" en la página 15.
SLES 11 SP1 y RHEL 6	◆ Firefox 5, 6, 7, 8, 9 y 10 Para obtener más información, consulte la "Actualización manual de la versión de Firefox" en la página 15.

Requisitos previos para Internet Explorer

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* > *pestaña 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*.

Actualización manual de la versión de Firefox

Sentinel admite Firefox versiones 5 a 10; sin embargo, el sistema SLES 11 SP1 se envía con Firefox versión 3.6*x*. Realice los siguientes pasos para actualizar manualmente la instalación de SLES 11 SP1 para que incluya una versión compatible de Firefox:

1. Abra YaST.
2. Seleccione *Software* > *Repositorios de software* para mostrar la ventana de Repositorios de software configurados.
3. Haga clic en *Añadir* para abrir la ventana Tipo de medio.
4. Seleccione la opción para *Especificar URL* y haga clic en *Siguiente*.

   Se mostrará la ventana Dirección URL del repositorio.
5. Introduzca el enlace del Repositorio de software (http://download.opensuse.org/repositories/mozilla/SLE_11/) en el cuadro de texto de dirección URL y luego haga clic en *Siguiente*.

   Se descargará el repositorio de software.
6. Haga clic en *Aceptar* para actualizar el repositorio de software.
7. Haga clic en *Gestión de software* para abrir la ventana de YaST2.
8. Introduzca `Firefox` en el cuadro de texto *Buscar*.

   Se mostrará la lista de paquetes de Firefox.
9. Seleccione los paquetes necesarios para la versión compatible de Firefox que desea instalar.

Si selecciona un paquete que está en conflicto con la versión existente, se mostrará un cuadro de diálogo de advertencia. Seleccione la opción que corresponda y luego haga clic en el botón *Aceptar. Inténtelo de nuevo*.

10 Haga clic en *Aceptar.*

1.1.5 Estimación de requisitos de almacenamiento de datos

Sentinel se utiliza para retener datos en bruto durante un largo período de tiempo con el fin de cumplir los requisitos legales y de otro tipo. Sentinel utiliza compresión para ayudarle a utilizar el espacio de almacenamiento local o de red de forma eficaz. Sin embargo, los requisitos de almacenamiento podrían aumentar de forma significativa transcurrido un largo período de tiempo.

Para superar los problemas de limitación de costes de los grandes sistemas de almacenamiento, puede usar sistemas de almacenamiento de datos económicos para almacenar los datos a largo plazo. Los sistemas de almacenamiento basados en cinta representan la solución más común y rentable. No obstante, las cintas no permiten el acceso aleatorio a los datos almacenados, que resulta necesario para realizar búsquedas rápidas. Por ello, resulta recomendable un planteamiento híbrido para el almacenamiento de datos a largo plazo, en el que los datos que se han de buscar están disponibles en un sistema de almacenamiento de acceso aleatorio y los datos que queremos conservar, y no buscar, se guardan en un medio alternativo y económico, como una cinta. Para obtener instrucciones para la aplicación de este planteamiento híbrido, consulte "Using Sequential-Access Storage for Long Term Data Storage" (Uso de almacenamiento de acceso secuencial para el almacenamiento de datos a largo plazo) en *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1).

Para determinar la cantidad de espacio de almacenamiento de acceso aleatorio necesario para Sentinel, haga primero una estimación del número de días de datos que necesita buscar con regularidad o sobre los que necesita ejecutar informes. Debe tener suficiente espacio en el disco duro ya sea a nivel local en el equipo de Sentinel o a distancia en el protocolo Server Message Block (SMB) o el protocolo CIFS, el sistema de archivos de red (NFS) o en una SAN para que Sentinel los utilice con fines de archivado de datos.

Debe tener el siguiente espacio adicional en el disco duro aparte de los requisitos mínimos:

- Para acomodar las velocidades de datos superiores a las esperadas.
- Para copiar datos desde la cinta y de nuevo a Sentinel para realizar búsquedas y generar informes sobre los datos históricos.

Utilice las siguientes fórmulas para estimar la cantidad de espacio necesario para almacenar datos:

- **Almacenamiento de eventos local (parcialmente comprimidos):** {tamaño medio en bytes por evento} x {número de días} x {eventos por segundo} x 0.00008 = espacio total de almacenamiento (GB) necesario

  Los tamaños de evento típicos tienen de 300 a 1000 bytes.
- **Almacenamiento de eventos en red (totalmente comprimidos):** {tamaño medio en bytes por evento} x {número de días} x {eventos por segundo} x 0.00001 = espacio total de almacenamiento (GB) necesario
- **Almacenamiento de datos en bruto (totalmente comprimidos tanto en almacenamiento local como en red):** {tamaño medio en bytes por registro de datos en bruto} x {número de días} x {eventos por segundo} x 0.000003 = espacio total de almacenamiento (GB) necesario

  El tamaño medio típico de datos en bruto para los mensajes de syslog es de 200 bytes.

- **Tamaño total de almacenamiento local (con almacenamiento en red habilitado):** {Tamaño de almacenamiento local de eventos para el número de días deseado} + {Tamaño de almacenamiento de datos en bruto durante un día) = Espacio total de almacenamiento (GB) necesario

  Si está activado el almacenamiento en red, los datos de eventos normalmente se copian al almacenamiento en red al cabo de 2 días. Para obtener más información, consulte "Configuring Data Storage" (Configuración de almacenamiento de datos) en la *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1).

- **Tamaño total de almacenamiento local (con el almacenamiento en red deshabilitado):**

  {Tamaño de almacenamiento local de eventos} + {Tamaño de almacenamiento de datos en bruto para el tiempo de retención) = Espacio total de almacenamiento (GB) necesario

- **Tamaño total de almacenamiento en red:** {Tamaño de almacenamiento en red de eventos para el tiempo de retención} + {Tamaño de almacenamiento de datos en bruto para el tiempo de retención} = Espacio total de almacenamiento (GB) necesario

---

NOTE:

- Los coeficientes de cada fórmula representan ((segundos por día) x (GB por byte) x relación de compresión).
- Estas cifras son sólo estimaciones y dependen del tamaño de los datos de eventos así como del tamaño de los datos comprimidos.
- Parcialmente comprimidos significa que los datos están comprimidos, pero no el índice de los datos. Totalmente comprimidos significa que tanto los datos de eventos como los datos del índice están comprimidos. La relación de compresión de los datos de eventos es por lo general de 10:1. La relación de compresión del índice es por lo general de 5:1. El índice se utiliza para optimizar la búsqueda a través de los datos.

Puede usar las fórmulas anteriores para determinar cuánto espacio de almacenamiento se requiere para un sistema de almacenamiento de datos a largo plazo, como por ejemplo una cinta.

1.1.6 Estimación de utilización de E/S del disco

Utilice las siguientes fórmulas para estimar el nivel de utilización del disco en el servidor a diversas velocidades de EPS.

- **Datos escritos en el disco (kilobytes por segundo):** (tamaño medio de eventos en bytes + tamaño medio de datos en bruto en bytes) x (eventos por segundo) x 0,002 coeficiente de compresión = datos escritos por segundo en el disco

  Por ejemplo, a 500 EPS, para un tamaño medio de eventos de 758 bytes y un tamaño medio de datos en bruto de 490 bytes en el archivo de registro, los datos escritos en el disco se determinan de la siguiente manera:

  (758 bytes + 490 bytes) x 500 EPS x 0,002 = ~1100 KB

- **Número de peticiones de E/S en el disco (transferencias por segundo):** (tamaño medio de eventos en bytes + tamaño medio de datos en bruto en bytes) x (eventos por segundo) x 0,00002 coeficiente de compresión = Peticiones de E/S por segundo en el disco

  Por ejemplo, a 500 EPS, para un tamaño medio de eventos de 758 bytes y un tamaño medio de datos en bruto de 490 bytes en el archivo de registro, el número de peticiones de E/S por segundo en el disco se determina de la siguiente manera:

(758 bytes + 490 bytes) x 500 EPS x 0,00002 = ~10 transferencias por segundo

- **Número de bloques escritos por segundo en el disco:** (tamaño medio de eventos en bytes + tamaño medio de datos en bruto en bytes) x (eventos por segundo) x 0,003 coeficiente de compresión = Bloques escritos por segundo en el disco

  Por ejemplo, a 500 EPS, para un tamaño medio de eventos de 758 bytes y un tamaño medio de datos en bruto de 490 bytes en el archivo de registro, el número de bloques escritos por segundo en el disco se determina de la siguiente manera:

  (758 bytes + 490 bytes) x 500 EPS x 0,003 = ~1800 bloques por segundo

- **Lectura de datos del disco por segundo al realizar una búsqueda:** (tamaño medio de eventos en bytes + tamaño medio de datos en bruto en bytes) x (número de eventos que coinciden con una consulta en millones) x 0,40 coeficiente de compresión = kilobytes leídos por segundo del disco

  Por ejemplo, a 5 millones de eventos coincidentes con la consulta de búsqueda, para un tamaño medio de eventos de 758 bytes y un tamaño medio de datos en bruto de 490 bytes en el archivo de registro, la lectura de datos por segundo en el disco se determina de la siguiente manera:

  (758 bytes + 490 bytes) x 5 x 0,4 = ~500 KB

1.1.7 Estimación de uso del ancho de banda de la red

Utilice las siguientes fórmulas para estimar el uso de ancho de banda de la red entre el servidor Sentinel y el gestor de recopiladores remoto a diferentes números de eventos por segundo (EPS):

{tamaño medio de eventos en bytes + tamaño medio de datos en bruto en bytes} x {eventos por segundo} x 0,0003 coeficiente de compresión = ancho de banda de la red en Kbps (kilobits por segundo)

Por ejemplo, a 500 EPS para un tamaño medio de eventos de 758 bytes y un tamaño medio de datos en bruto de 490 bytes en el archivo de registro, el uso de ancho de banda de la red se determina de la siguiente manera:

(758 bytes + 490 bytes} x 500 EPS x 0,0003 = ~175 Kbps

1.1.8 Entorno virtual

Sentinel se ha probado a fondo en servidores VMware ESX y la compatibilidad es total. Al configurar un entorno virtual, los equipos virtuales deben tener 2 o más CPU. Para obtener resultados de rendimiento comparables 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 recomendaciones para equipos físicos, consulte la Sección 1.1, “Requisitos del sistema y plataformas compatibles”, en la página 11.

1.2 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 la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

1.3 Puertos utilizados

1.3.1 Servidor de Sentinel

Puertos locales

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

Puertos	Descripción
TCP 5432	Se utiliza para la base de datos PostgreSQL. No es necesario abrir este puerto por defecto. No obstante, si crea informes utilizando Sentinel SDK, entonces deberá abrir este puerto. Para obtener más información, consulte el sitio Web de SDK de módulos auxiliares (plug-in) de Sentinel (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).
TCP 27017	Se utiliza para la base de datos de configuración Inteligencia de seguridad.
TCP 28017	Se utiliza para la interfaz 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.

Puertos de red

Sentinel utiliza diferentes 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 estándar, es necesario configurar el sistema operativo en el que va a instalar Sentinel para poder abrir los puertos en el cortafuegos.

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

Puertos	Descripción
TCP 1099 y 2000	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	Se utiliza para las conexiones de Audit.
UDP 1514	Se utiliza para los mensajes de syslog.
TCP 8443	Se utiliza para la comunicación de HTTPS.
TCP 1443	Se utiliza para los mensajes de syslog con SSL cifrado.
TCP 61616	Se utiliza para la comunicación entre los gestores de recopiladores y el servidor.
TCP 10013	Utilizados por el Centro de control de Sentinel y Solution Designer.
TCP 1468	Se utiliza para los mensajes de syslog.
TCP 10014	Lo utilizan los gestores de recopiladores remotos con el fin de conectar con el servidor a través de un proxy de SSL. Sin embargo, esto es poco común. Por defecto, los gestores de recopiladores remotos utilizan el puerto SSL 61616 para conectar con el servidor.

Puertos específicos del dispositivo del servidor Sentinel

Además de los puertos anteriores, están abiertos los siguientes puertos en el dispositivo del servidor Sentinel.

Puertos	Descripción
TCP 22	Se utiliza para el acceso mediante secure shell al dispositivo Sentinel
TCP 54984	Lo utiliza la consola de gestión del dispositivo de Sentinel (WebYaST). También lo utiliza el dispositivo Sentinel para el servicio de actualización.
TCP 289	Se reenvía a 1289 para las conexiones de Audit.
UDP 443	Se remite a 8443 para la comunicación HTTPS.
UDP 514	Se reenvía a 1514 para los mensajes de syslog.
TCP 1290	Este es el puerto de Sentinel Link al que se permite conectar a través del cortafuegos de SuSE.
UDP y TCP 40000 - 41000	Puertos que pueden utilizarse al configurar los servidores de recopilación de datos, como syslog. Sentinel no escucha estos puertos por defecto.

1.3.2 Gestor de recopiladores

Puertos de red

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

Puertos	Descripción
TCP 1289	Se utiliza para las conexiones de Audit.
UDP 1514	Se utiliza para los mensajes de syslog.
TCP 1443	Se utiliza para los mensajes de syslog con SSL cifrado.
TCP 1468	Se utiliza para los mensajes de syslog.
TCP 1099 y 2000	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).

Puertos específicos del dispositivo del gestor de recopiladores

Además de los puertos anteriores, los siguientes puertos están abiertos en el dispositivo del gestor de recopiladores de Sentinel.

Puertos	Descripción
TCP 22	Se utiliza para el acceso mediante secure shell al dispositivo Sentinel
TCP 54984	Lo utiliza la consola de gestión del dispositivo de Sentinel (WebYaST). También lo utiliza el dispositivo Sentinel para el servicio de actualización.
TCP 289	Se reenvía a 1289 para las conexiones de Audit.
UDP 514	Se reenvía a 1514 para los mensajes de syslog.
TCP 1290	Este es el puerto de Sentinel Link al que se permite conectar a través del cortafuegos de SuSE.
UDP y TCP 40000 - 41000	Puertos que pueden utilizarse al configurar los servidores de recopilación de datos, como syslog. Sentinel no escucha estos puertos por defecto.

1.3.3 Motor de correlación

Puertos de red

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

Puertos	Descripción
TCP 1099 y 2000	Los utilizan conjuntamente las herramientas de supervisión para conectar con el proceso del servidor Sentinel utilizando las Extensiones de gestión de Java (JMX).

Puertos específicos del dispositivo del motor de correlación

Además de los puertos anteriores, los siguientes puertos están abiertos en el dispositivo del motor de correlación de Sentinel.

Puertos	Descripción
TCP 22	Se utiliza para el acceso mediante secure shell al dispositivo Sentinel
TCP 54984	Lo utiliza la consola de gestión del dispositivo de Sentinel (WebYaST). También lo utiliza el dispositivo Sentinel para el servicio de actualización.

2 Instalación de Sentinel

Sentinel puede instalarse como instalación independiente o como dispositivo. El instalador independiente instala Sentinel en un sistema operativo SUSE Linux Enterprise Server (SLES) 11 SP1 o Red Hat Enterprise Linux (RHEL) 6 existente. El instalador del dispositivo instala tanto el sistema operativo SLES 11 SP1 de 64 bits como Sentinel.

En esta sección se describe el procedimiento para una instalación independiente del servidor Sentinel en un sistema SLES 11 SP1 o en RHEL 6. Para realizar una instalación como dispositivo, consulte el Capítulo 5, “Instalación del dispositivo”, en la página 41.

2.1 Métodos de instalación

Para la instalación independiente, hay disponibles los siguientes métodos:

- **Interactivo:** la instalación se lleva a cabo con datos que introduce el usuario. Durante la instalación, puede registrar opciones de instalación (valores introducidos por el usuario o valores por defecto) en un archivo, que posteriormente puede utilizarse para una instalación silenciosa.
- **Silencio:** puede usar esta opción si se han registrado previamente las opciones de instalación. La instalación silenciosa se refiere al archivo que tiene los datos de instalación registrados y realiza la instalación con los valores capturados en el archivo. La instalación silenciosa es efectiva cuando desea instalar numerosas réplicas de la misma configuración en su entorno. Para obtener más información, consulte Sección 2.5, “Instalación silenciosa”, en la página 29.

Tanto la instalación interactiva como silenciosa de Sentinel pueden realizarse como usuario `root` o como usuario diferente de root.

2.1.1 Instalación estándar y personalizada

Al instalar Sentinel, tiene a su disposición las siguientes configuraciones:

- **Estándar:** en esta configuración, la instalación utiliza valores por defecto para establecer la configuración. Sólo se requiere la intervención del usuario para introducir la contraseña. Para obtener más información sobre la instalación de Sentinel con la configuración estándar, consulte la Sección 2.4.1, “Configuración estándar”, en la página 26.
- **Personalizada:** en esta configuración, la instalación le indica que especifique valores para establecer la configuración. Puede seleccionar valores por defecto o especificar los valores necesarios. Para obtener más información sobre la instalación de Sentinel con una configuración personalizada, consulte la Sección 2.4.2, “Configuración personalizada”, en la página 27.

Configuración estándar	Configuración personalizada
Se instala con una clave de evaluación por defecto de 90 días.	Le permite realizar la instalación con una clave de licencia de 90 días 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.
Autentica los usuarios con la base de datos interna.	Ofrece la opción de autenticar usuarios con la base de datos interna o mediante autenticación LDAP.

2.1.2 Componentes instalados

Existen numerosos componentes en Sentinel. Todos los componentes siguientes se instalan por defecto:

- Servidor de Sentinel
- Motor de correlación
- Gestor de recopiladores

Es posible instalar motores de correlación y gestores de recopiladores adicionales en diferentes sistemas.

2.2 Antes de empezar

Verifique que haya realizado las siguientes tareas antes de iniciar la instalación:

- Verifique que el hardware y el software cumplen los requisitos del sistema enumerados en la Sección 1.1, “Requisitos del sistema y plataformas compatibles”, en la página 11.
- 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 Parte V, “Desinstalación”, en la página 99.

- Para obtener un rendimiento, estabilidad y fiabilidad óptimos del servidor Sentinel, utilice el archivo ext3 en SLES y el archivo ext4 en RHEL. Para obtener más información sobre los sistemas de archivos, consulte Overview of File Systems in Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) (Descripción de los sistemas de archivos en Linux) en la *Storage Administration Guide* (Guía de administración del almacenamiento).
- Configure los ajustes de red de manera que el sistema tenga una dirección IP y un nombre de host válidos.
- Obtenga su clave de licencia del Centro de atención al cliente de Novell (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) si piensa instalar la versión con licencia.
- Sincronice el tiempo utilizando el protocolo de tiempo de red (NTP).
- Asegúrese de que los puertos enumerados en la Sección 1.3, “Puertos utilizados”, en la página 19 estén abiertos en el cortafuegos.
- Para obtener un rendimiento óptimo, los ajustes de memoria deben ser adecuados 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 realizar una instalación mínima o sin GUI, 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
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof
  - net-tools
  - openssl
  - python-libs
  - sed
  - zlib

2.3 Opciones de instalación

`./install-sentinel --help` muestra las siguientes opciones:

Opciones	Valor	Descripción
--location	Directorio	Especifica un directorio diferente de root (/) para instalar Sentinel.
-m, --manifest	Nombre de archivo	Especifica un archivo de inventario del producto que se utilizará en lugar del archivo de inventario por defecto.
--no-configure		Especifica que no se debe configurar el producto después de la instalación.
-n, --no-start		Especifica que no se debe iniciar o reiniciar Sentinel después de la instalación o configuración.
-r, --recordunattended	Nombre de archivo	Especifica un archivo para registrar los parámetros que se pueden utilizar para una instalación sin supervisión.
-u, --unattended	Nombre de archivo	Utiliza parámetros del archivo especificado para instalar Sentinel en sistemas sin supervisión.
-h, --help		Muestra las opciones que se pueden utilizar al instalar Sentinel.
-l, --log-file	Nombre de archivo	Registra los mensajes del registro en un archivo.
--no-banner		Anula la visualización de un mensaje de banda.
-q, --quiet		Muestra menos mensajes.
-v, --verbose		Muestra todos los mensajes durante la instalación.

2.4 Instalación interactiva

2.4.1 Configuración estándar

1. Descargue el archivo de instalación de Sentinel de la página Web de descargas de Novell (http://download.novell.com/index.jsp):
   - **1a** En el campo *Product or Technology* (Producto o Tecnología), examine y seleccione *SIEM-Sentinel*.
   - **1b** Haga clic en *Buscar*.
   - **1c** Haga clic en el botón de la columna *Download* (Descargar) para obtener una versión de *Evaluación de Sentinel 7.0*.
   - **1d** Haga clic en *proceed to download* (continuar con la descarga), y luego especifique su nombre de usuario y contraseña.
   - **1e** Haga clic en *download* (descargar) para obtener la versión de instalación de su plataforma.
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 sentinel_server-7.0.0.0.x86_64
```

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 de 90 días incluida en el instalador. Esta clave de licencia activa todo el conjunto de funciones del producto durante un período de prueba de 90 días. En cualquier momento durante el período de prueba 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 Web de Sentinel, especifique la siguiente dirección URL en el navegador Web:

```
https://<IP_Address_Sentinel_server>:8443.
```

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

2.4.2 Configuración personalizada

Si va a instalar Sentinel con una configuración personalizada, puede especificar la clave de licencia, cambiar la contraseña para diferentes usuarios y especificar valores para puertos diferentes que se utilizan para interactuar con los componentes internos.

1 Descargue el archivo de instalación de Sentinel de la página Web de descargas de Novell (http://download.novell.com/index.jsp):

1a En el campo *Product or Technology* (Producto o Tecnología), examine y seleccione *SIEM-Sentinel*.

1b Haga clic en *Buscar*.

1c Haga clic en el botón de la columna *Download* (Descargar) para obtener una versión de *Evaluación de Sentinel 7.0*.

1d Haga clic en *proceed to download* (continuar con la descarga), y luego especifique su nombre de usuario y contraseña.

1e Haga clic en *download* (descargar) para obtener la versión de instalación de su plataforma.

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 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>
```

4 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.

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

6 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.

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

8 Introduzca `1` para usar la clave de licencia de evaluación por defecto de 90 días.

O bien

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

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

10 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.

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

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

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

14 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`.

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 Web de Sentinel, especifique la siguiente dirección URL en el navegador Web:

`https://<IP_Address_Sentinel_server>:8443.`

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

2.5 Instalación silenciosa

La instalación silenciosa o sin supervisión de Sentinel resulta útil si tiene que instalar más de un servidor de Sentinel en su implantación. En tal caso, puede registrar los parámetros de instalación durante la instalación interactiva y luego ejecutar el archivo registrado en todos los demás servidores. Puede registrar los parámetros de instalación mientras instala Sentinel con la configuración estándar o personalizada.

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 Sección 2.4.1, “Configuración estándar”, en la página 26 o bien la Sección 2.4.2, “Configuración personalizada”, en la página 27.

1. Descargue los archivos de instalación de la página Web de descargas de Novell (http://download.novell.com/index.jsp).
2. Entre como usuario `root` en el servidor en el que desea instalar Sentinel.
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 instalar Sentinel en el modo silencioso:

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

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

   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 Web de Sentinel, especifique la siguiente dirección URL en el navegador Web:

`https://<IP_Address_Sentinel_server>:8443.`

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

2.6 Instalación de Sentinel como usuario diferente de root

Si la directiva de su organización no le permite ejecutar la instalación completa de Sentinel como usuario `root`, puede realizar la instalación de Sentinel como un usuario diferente. En esta instalación, algunos pasos se realizan como usuario `root` y luego se continúa la instalación de Sentinel como otro usuario diferente creado por el usuario `root`. Por último, el usuario `root` finaliza la instalación.

1. Descargue los archivos de instalación de la página Web de descargas de Novell (http://download.novell.com/index.jsp).
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 comendo para cambiar al nuevo usuario de `novell` diferente de root recién creado: `novell`:

   ```
   su novell
   ```
7. (Condicional) Para realizar una instalación interactiva:

   7a Especifique el siguiente comando:

   ```
   ./install-sentinel
   ```

   Para instalar Sentinel en una ubicación diferente de la ubicación por defecto, especifique la opción --location junto con el comando. Por ejemplo:.

   ```
   ./install-sentinel --location=/foo
   ```

   7b Continúe con el Paso 9.
8. (Condicional) Para realizar una instalación silenciosa:

   8a Especifique el siguiente comando:

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

   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. La instalación puede tardar algunos 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 Sección 2.4.1, “Configuración estándar”, en la página 26.
   - Si decide continuar con la configuración personalizada, continúe con el Paso 7 al Paso 14 de la Sección 2.4.2, “Configuración personalizada”, en la página 27.

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 Web de Sentinel, especifique la siguiente dirección URL en el navegador Web:

`https://<IP_Address_Sentinel_server>:8443.`

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

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

   ```
   ./configure.sh
   ```

2 Especifique `1` para llevar a cabo una configuración estándar o bien `2` para realizar una configuración personalizada de Sentinel.

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

4 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.

5 Introduzca `1` para usar la clave de licencia de evaluación por defecto de 90 días.

   O bien

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

6 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 7.
   - Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 7.

7 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 8.
- Si desea cambiar la contraseña existente, introduzca `2`, especifique la nueva contraseña, confírmela y luego continúe con el Paso 8.

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.

8 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 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 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.

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

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

11 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`.

3 Instalación de gestores de recopiladores adicionales

Por defecto, Sentinel instala un gestor de recopiladores. Dependiendo del entorno, quizá necesite más de un gestor de recopiladores. Utilice la siguiente información para instalar gestores de recopiladores.

IMPORTANT: No puede instalar otro gestor de recopiladores o motor de correlación en el mismo servidor donde se está ejecutando Sentinel.

3.1 Ventajas de los gestores de recopiladores adicionales

La instalación de más de un gestor de recopiladores en una red distribuida aporta varias ventajas:

- **Mejora del rendimiento del sistema:** los gestores de recopiladores adicionales 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 los gestores de recopiladores se encuentran ubicados 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:** El gestor de recopiladores remoto puede 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.

3.2 Antes de empezar

Verifique 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 Sección 1.1, “Requisitos del sistema y plataformas compatibles”, en la página 11.

- ❒ Sincronice el tiempo utilizando el protocolo de tiempo de red (NTP).
- ❒ Un gestor de recopiladores requiere conectividad de red con el puerto de bus de mensajes (61616) en el servidor Sentinel Antes de instalar el gestor de recopiladores, asegúrese de que todos los ajustes del cortafuegos y de red puedan comunicarse a través de este puerto.

3.3 Instalación de un gestor de recopiladores adicional

Debe instalar el gestor de recopiladores remoto en un sistema diferente de donde está instalado Sentinel o el motor de correlación remoto.

1. Lance la interfaz Web de Sentinel especificando la siguiente dirección URL en el navegador Web:

   `https://<IP_Address_Sentinel_server>:8443.`

   El valor <*dirección_IP_servidor_Sentinel*> es la dirección IP o el nombre de DNS del servidor Sentinel y 8443 es el puerto por defecto del servidor 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. En el encabezado Gestor de recopiladores, haga clic en *Descargar instalador*.
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. Por ejemplo:

   `cd sentinel_collector_mgr-7.0.0.0.x86_64`
7. Especifique el siguiente comando para instalar el gestor de recopiladores de Sentinel:

   `./install-cm`

   El guion de instalación comprueba primero si hay memoria y espacio disponibles en el disco. Si hay menos de 1.5 GB de memoria disponible, el guión cierra la instalación de forma automática.
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 podría tardar unos segundos en solicitar el tipo de configuración.
11. Cuando se le indique, especifique 1 para continuar con la configuración estándar.
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. Especifique el nombre de usuario y la contraseña del gestor de recopiladores.

    El nombre de usuario y la contraseña se almacenan en el archivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` ubicado en el servidor de Sentinel.

    Por ejemplo:

    `collectormanager=1c51ae55`

En este ejemplo, `collectormanager` es el nombre de usuario y el valor correspondiente es la contraseña.

14 Acepte el certificado de forma permanente cuando se le indique.

La instalación del gestor de recopiladores remoto de Sentinel ha finalizado.

3.4 Cómo añadir un usuario personalizado para un gestor de recopiladores

Sentinel recomienda utilizar el nombre de usuario del gestor de recopiladores por defecto de `collectormanager`. No obstante, si tiene instalados varios gestores de recopiladores remotos y desea identificarlos por separado, puede crear nuevos usuarios:

1 Acceda al servidor como el usuario que tiene acceso a los archivos de instalación de Sentinel.

2 Abra el archivo `activemqgroups.properties`.

El archivo se encuentra en el directorio `/<install_dir>/etc/opt/novell/sentinel/config/`.

3 Añada el nuevo gestor de recopiladores en la sección `cm`, separado por una coma. Por ejemplo:

```
cm=collectormanager,cmuser1,cmuser2,...
```

4 Guarde y cierre el archivo.

5 Abra el archivo `activemqusers.properties`.

Este archivo se encuentra en el directorio `/<install_dir>/etc/opt/novell/sentinel/config/`.

6 Añada la contraseña del usuario que creó en el Paso 3.

La contraseña puede ser cualquier cadena aleatoria. Por ejemplo:

```
system=c7f34372ecd20d831cceb29e754e5ac9
collectormanager=1c51ae56
cmuser1=1b51de55
cmuser2=1a51ce57
```

7 Guarde y cierre el archivo.

8 Reinicie el servidor Sentinel.

4 Instalación de motores de correlación adicionales

Sentinel instala por defecto un motor de correlación. Para los entornos que tienen un gran número de reglas de correlación o números de eventos muy elevados, podría ser beneficioso instalar más de un motor de correlación. Para obtener información sobre los números de eventos recomendados por motor de correlación, consulte Motor de correlación en el Capítulo 1, "Cumplimiento de los requisitos del sistema", en la página 11.

IMPORTANT: No es posible instalar otro gestor de recopiladores u otro motor de correlación en el servidor en el que se está ejecutando Sentinel.

4.1 Antes de empezar

Verifique 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 Sección 1.1, "Requisitos del sistema y plataformas compatibles", en la página 11.
- ❒ Sincronice el tiempo utilizando el protocolo de tiempo de red (NTP).
- ❒ Un motor de correlación requiere conectividad de red con el puerto de bus de mensajes (61616) en el servidor Sentinel. Antes de instalar el motor de correlación, asegúrese de que todos los ajustes del cortafuegos y de red puedan comunicarse a través de este puerto.

4.2 Instalación de un motor de correlación adicional

Debe instalar un motor de correlación remoto en un sistema diferente del que está instalado Sentinel o un gestor de recopiladores remoto.

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

```
https://<IP_Address_Sentinel_server>:8443.
```

El valor <*dirección_IP_servidor_Sentinel*> es la dirección IP o el nombre de DNS del servidor Sentinel y 8443 es el puerto por defecto del servidor 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. En el encabezado Motor de correlación, haga clic en *Descargar instalador*.
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. Por ejemplo:

   ```
   cd sentinel_correlation_engine-7.0.0.0.x86_64
   ```
7. Especifique el siguiente comando para instalar el motor de correlación de Sentinel:

   ```
   ./install-ce
   ```

   El guion de instalación comprueba primero si hay memoria y espacio disponibles en el disco. Si hay menos de 1.5 GB de memoria disponible, el guión cierra la instalación de forma automática.
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 indique, especifique 1 para continuar con la configuración estándar.
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. Especifique el nombre de usuario y la contraseña del motor de correlación.

    El nombre de usuario y la contraseña se almacenan en el archivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` ubicado en el servidor de Sentinel.

    Por ejemplo:

    ```
    correlationengine=68790d7a
    ```

    En este ejemplo, `correlationengine` es el nombre de usuario y el valor correspondiente es la contraseña.
14. Acepte el certificado de forma permanente cuando se le indique.

    La instalación del motor de correlación remoto de Sentinel ha finalizado.

4.3 Cómo añadir un usuario personalizado para el motor de correlación

Sentinel recomienda utilizar el nombre de usuario del motor de correlación por defecto de `correlationengine`. No obstante, si ha instalado varios motores de correlación y desea identificarlos por separado, puede crear nuevos usuarios:

1. Acceda al servidor como el usuario que tiene acceso a los archivos de instalación de Sentinel.
2. Abra el archivo `activemqgroups.properties`.

   Este archivo se encuentra en el directorio `/<install_dir>/etc/opt/novell/sentinel/config/`.
3. Añada el nuevo usuario del motor de correlación en la sección `admin`, separado por una coma. Por ejemplo:

   ```
   admins=system,correlationengine,ceuser1,ceuser2,...
   ```
4. Guarde y cierre el archivo.
5. Abra el archivo `activemqusers.properties`.

   Este archivo se encuentra en el directorio `/<install_dir>/etc/opt/novell/sentinel/config/`.
6. Añada la contraseña del usuario que creó en el Paso 3.

   La contraseña puede ser cualquier cadena aleatoria. Por ejemplo:

   ```
   system=c7f34372ecd20d831cceb29e754e5ac9
   correlationengine=68790d7a
   ceuser1=69700c6d
   ceuser2=70701b5c
   ```
7. Guarde y cierre el archivo.
8. Reinicie el servidor Sentinel.

5 Instalación del dispositivo

El dispositivo Sentinel es un dispositivo de software listo para ejecutarse basado en SUSE Studio. El dispositivo combina un sistema operativo SUSE Linux Enterprise Server (SLES) 11 SP 1 reforzado y el servicio de actualización integrado del software de Sentinel para proporcionar una experiencia fácil y transparente al usuario, que permite a los clientes aprovechar su inversión actual. El dispositivo de software puede instalarse en hardware o en un entorno virtual.

5.1 Antes de empezar

Asegúrese de haber realizado las siguientes tareas antes de instalar el dispositivo.

- ❒ Verifique que se cumplen los requisitos de hardware. Para obtener más información, consulte Sección 1.1, “Requisitos del sistema y plataformas compatibles”, en la página 11.
- ❒ Obtenga su clave de licencia del Centro de atención al cliente de Novell (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) si piensa instalar la versión con licencia.
- ❒ Obtenga el código de registro del Centro de atención al cliente de Novell (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) para registrarse para obtener actualizaciones de software.

5.2 Instalación del dispositivo VMware

5.2.1 Instalación de Sentinel

Para importar e instalar la imagen del dispositivo de Sentinel en un servidor VMware ESX:

1. Descargue el archivo de instalación del dispositivo VMware del sitio Web de descargas de Novell (http://download.novell.com/index.jsp).

   El archivo correcto del dispositivo VMware tiene `vmx` en el nombre del archivo. Por ejemplo, `sentinel_server_7.0.0.0.x86_64.vmx.tar.gz`
2. Establezca un almacén de datos de ESX en el que se pueda instalar la imagen del dispositivo.
3. Entre como usuario Administrador en el servidor en el que desea instalar el dispositivo.
4. Utilice el siguiente comando para extraer la imagen comprimida del dispositivo desde el equipo donde está instalado VM Converter:

   ```
   tar zxvf <install_file>
   ```

   Reemplace <*archivo_instalación*> por el nombre real del archivo.
5. Para importar la imagen de VMware al servidor ESX, utilice el VMware Converter y siga las instrucciones en pantalla del asistente de instalación.
6. Entre en el equipo del servidor ESX.
7. Seleccione la imagen de VMware importada del dispositivo y haga clic en el icono de *encendido*.
8. Seleccione el idioma deseado y luego, haga clic en *Siguiente*.
9. Seleccione la disposición del teclado y haga clic en *Siguiente*.
10. Lea y acepte el acuerdo de licencia de software de SUSE Linux Enterprise Server (SLES) 11 SP1.
11. Lea y acepte el acuerdo de licencia del usuario final de NetIQ Sentinel.
12. En la pantalla Nombre de host y Nombre de dominio, especifique los valores correspondientes y asegúrese de que esté seleccionada la opción *Assign Hostname to Loopback IP* (Asignar nombre de host a IP de retrobucle).
13. Haga clic en *Siguiente*. Se guardará la información configurada de nombre de host.
14. Realice una de las siguientes acciones:
    - Para usar los ajustes de conexión de red actuales, seleccione *Use Following Configuration* (Usar la siguiente configuración) en la página Configuración de red II y luego haga clic en *Siguiente*.
    - Para cambiar los ajustes de conexión de red, seleccione *Change* (Cambiar), realice los cambios necesarios y haga clic en *Siguiente*.

    Se guardan los ajustes de conexiones de red.
15. Establezca la fecha y la hora y luego haga clic en *Siguiente*.

    Para cambiar la configuración de NTP después de la instalación utilice YaST en la línea de comandos del dispositivo. Puede usar WebYast para cambiar la fecha y la hora, pero no la configuración de NTP.

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

    ```
    rcntp restart
    ```
16. Defina la contraseña `root` y luego haga clic en *Siguiente*.

La instalación comprueba si hay memoria y espacio disponible en el disco. Si la memoria disponible es inferior a 2.5 GB, la instalación no le permitirá continuar y el botón *Siguiente* aparece atenuado.

Si hay entre 2.5 GB y 6.7 GB de memoria disponible, la instalación muestra un mensaje que indica que hay menos memoria de la recomendada. Cuando aparezca este mensaje, haga clic en *Siguiente* para continuar con la instalación.

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

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.

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

19 Pase a la Sección 5.5, “Configuración del dispositivo posterior a la instalación”, en la página 52.

5.2.2 Instalación del gestor de recopiladores

Para importar e instalar la imagen del dispositivo en el servidor VMWare ESX:

1 Descargue el archivo de instalación del dispositivo VMware del sitio Web de descargas de Novell (http://download.novell.com/index.jsp).

El archivo correcto del dispositivo VMware tiene `vmx` en el nombre del archivo. Por ejemplo, `sentinel_colletor_manager_7.0.0.0.x86_64.vmx.tar.gz`

2 Establezca un almacén de datos de ESX en el que se pueda instalar la imagen del dispositivo.

3 Entre como usuario Administrador en el servidor en el que desea instalar el dispositivo.

4 Utilice el siguiente comando para extraer la imagen comprimida del dispositivo desde el equipo donde está instalado VM Converter:

```
tar zxvf <install_file>
```

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

5 Para importar la imagen de VMware al servidor ESX, utilice el VMware Converter y siga las instrucciones en pantalla del asistente de instalación.

6 Entre en el equipo del servidor ESX.

7 Seleccione la imagen de VMware importada del dispositivo y haga clic en el icono de *encendido*.

8 Especifique el nombre de host/la dirección IP del servidor Sentinel al que debe conectarse el gestor de recopiladores.

9 Especifique el número de puerto del servidor de comunicaciones. El puerto del bus de mensajes por defecto es `61616`.

10 Especifique el nombre de usuario de JMS, que representa el nombre de usuario del gestor de recopiladores. El nombre de usuario por defecto es `collectormanager`.

11 Especifique la contraseña del usuario de JMS.

El nombre de usuario y la contraseña se almacenan en el archivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` ubicado en el servidor de Sentinel.

12 (Opcional) Para verificar la contraseña, consulte la siguiente línea en `activemqusers.properties`.

```
collectormanager=<password>
```

En este ejemplo, `collectormanager` es el nombre de usuario y el valor correspondiente es la contraseña.

13 Haga clic en *Siguiente*.

14 Acepte el certificado cuando se le indique.

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

Cuando haya finalizado la instalación, se muestra un mensaje que indica que el dispositivo es el gestor de recopiladores de Sentinel, junto con la dirección IP. Además, muestra la dirección IP de la interfaz del usuario del servidor Sentinel.

5.2.3 Instalación del motor de correlación

La instalación del dispositivo del motor de correlación es similar a la del dispositivo del gestor de recopiladores.

1 Descargue el archivo de instalación del dispositivo VMware del sitio Web de descargas de Novell (http://download.novell.com/index.jsp).

El archivo correcto del dispositivo de motor de correlación de VMware tiene `vmx` en el nombre del archivo. Por ejemplo, `sentinel_correlation_engine_7.0.0.0.x86_64.vmx.tar.gz`

2 Establezca un almacén de datos de ESX en el que se pueda instalar la imagen del dispositivo.

3 Entre como usuario Administrador en el servidor en el que desea instalar el dispositivo.

4 Especifique el siguiente comando para extraer la imagen comprimida del dispositivo desde el equipo donde está instalado VM Converter:

```
tar zxvf <install_file>
```

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

5 Para importar la imagen de VMware al servidor ESX, utilice el VMware Converter y siga las instrucciones en pantalla del asistente de instalación.

6 Entre en el equipo del servidor ESX.

7 Seleccione la imagen de VMware importada del dispositivo y haga clic en el icono de *encendido*.

8 Especifique el nombre de host/la dirección IP del servidor Sentinel al que debería conectarse el motor de correlación.

9 Especifique el número de puerto del servidor de comunicaciones. El puerto del bus de mensajes por defecto es `61616`.

10 Especifique el nombre de usuario de JMS, que representa el nombre de usuario del motor de correlación. El nombre de usuario por defecto es `correlationengine`.

11 Especifique la contraseña del usuario de JMS.

El nombre de usuario y la contraseña se almacenan en el archivo/<*install_dir*>/etc/opt/novell/sentinel/config/activemqusers.properties ubicado en el servidor de Sentinel.

12 (Opcional) Para verificar la contraseña, consulte la siguiente línea del archivo `activemqusers.properties`:

```
correlationengine=<password>
```

En este ejemplo, `correlationengine` es el nombre de usuario y el valor correspondiente es la contraseña.

13 Haga clic en *Siguiente*.

14 Acepte el certificado cuando se le indique.

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

Cuando haya finalizado la instalación, se muestra un mensaje que indica que el dispositivo es el motor de correlación de Sentinel, junto con la dirección IP. Además, muestra la dirección IP de la interfaz del usuario del servidor Sentinel.

5.3 Instalación del dispositivo Xen

5.3.1 Instalación de Sentinel

1 Descargue el archivo de instalación del dispositivo virtual Xen del sitio Web de descargas de Novell (http://download.novell.com/index.jsp) en `/var/lib/xen/images`.

El nombre de archivo correcto del dispositivo virtual Xen contiene `xen`. Por ejemplo, `Sentinel_7.0.0.0.x86_64.xen.tar.gz`

2 Especifique el siguiente comando para desempaquetar el archivo:

```
tar -zxvf <install_file>
```

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

3 Cambie al nuevo directorio de instalación. El directorio tiene los siguientes archivos:

- *<nombre_archivo>*`.raw`
- *<nombre_archivo>*`.xenconfig`

4 Abra el archivo *<nombre_archivo>*`.xenconfig` utilizando el editor de texto.

5 Modifique el archivo de la siguiente manera:

- Especifique la vía completa al archivo `.raw` en el ajuste `disk`.
- Especifique el ajuste de puente para la configuración de red. Por ejemplo, `"bridge=br0"` o `"bridge=xenbr0"`.
- Especifique los valores para `name` y `memory`.

Por ejemplo:

```
# -*- mode: python; -*-
name="Sentinel_7.0.0.0.x86_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/sentinel_7.0.0.0.x86_64/
sentinel_7.0.0.0.x86_64.raw,xvda,w" ]
vif=[ "bridge=br0" ]
```

6 Después de modificar el archivo *<nombredearchivo>*`.xenconfig`, especifique el siguiente comando para crear la máquina virtual:

```
xm create <file_name>.xenconfig
```

7 (Opcional) Para verificar si se ha creado la máquina virtual, especifique el siguiente comando:

```
xm list
```

La máquina virtual aparece en la lista que se genera.

Por ejemplo, si ha configurado `name="Sentinel_7.0.0.0.x86_64"`en el archivo `.xenconfig`, entonces la máquina virtual aparece con ese nombre.

8 Para iniciar la instalación, especifique el siguiente comando:

```
xm console <vm name>
```

Reemplace <*nombre_vm*> por el nombre especificado en el ajuste de nombre en el archivo `.xenconfig`, que también es el valor devuelto en el paso 7. Por ejemplo:

```
xm console Sentinel_7.0.0.0.x86_64
```

La instalación comprueba primero si hay memoria y espacio disponible en el disco. Si hay menos de 2.5 GB de memoria disponible, la instalación se cancela de forma automática. Si hay entre 2.5 GB y 6.7 GB de memoria disponible, la instalación muestra un mensaje que indica que hay menos memoria de la recomendada. Escriba `y` si desea continuar con la instalación o `n` si no es así.

9 Seleccione el idioma deseado y luego, haga clic en *Siguiente*.

10 Seleccione la disposición del teclado y haga clic en *Siguiente*.

11 Lea y acepte el acuerdo de licencia de software de SUSE Linux Enterprise Server (SLES) 11 SP1.

12 Lea y acepte el acuerdo de licencia del usuario final de NetIQ Sentinel.

13 En la pantalla Nombre de host y Nombre de dominio, especifique los valores correspondientes y asegúrese de que esté seleccionada la opción *Assign Hostname to Loopback IP* (Asignar nombre de host a IP de retrobucle).

14 Seleccione *Siguiente*. Se guardará la información configurada de nombre de host.

15 Realice una de las siguientes acciones:

- Para usar los ajustes de conexión de red actuales, seleccione la opción *Use the following configuration* (Usar la siguiente configuración) de la pantalla de *Network Configuration II* (Configuración de red II).
- Para cambiar los ajustes de conexión de red, seleccione *Change* (Cambiar) y luego realice los cambios necesarios.

16 Seleccione *Siguiente*. Se guardan los ajustes de conexiones de red.

17 Establezca la fecha y la hora y haga clic en *Siguiente*, seguido de la opción para *Finalizar*

Para cambiar la configuración de NTP después de la instalación utilice YaST en la línea de comandos del dispositivo. Puede usar WebYast para cambiar la fecha y la hora, pero no la configuración de NTP.

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

```
rcntp restart
```

18 Defina la contraseña `root` de SUSE Enterprise Server y luego haga clic en *Siguiente*.

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

La instalación de Sentinel continúa y finaliza. Puede tardarse unos minutos en iniciar todos los servicios después de la instalación, porque el sistema lleva a cabo una inicialización única. Espere a que termine la instalación antes de entrar en el servidor.

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

20 Pase a la Sección 5.5, “Configuración del dispositivo posterior a la instalación”, en la página 52.

5.3.2 Instalación del gestor de recopiladores

Puede instalar el gestor de recopiladores como dispositivo en un sistema Linux habilitado para Xen que cumpla los requisitos mínimos de hardware para el gestor de recopiladores. Para obtener más información, consulte Sección 1.1.2, "Requisitos del hardware", en la página 12.

1. Realice el Paso 1 al Paso 14 de la Sección 5.3.1, "Instalación de Sentinel", en la página 45.

   El nombre de archivo correcto del archivo de instalación del dispositivo virtual Xen del gestor de recopiladores es `sentinel_collector_manager_7.0.0.0.x86_64.xen.tar.gz`
2. En la pantalla Configuración de red II, seleccione *Cambiar* y especifique la dirección IP de la máquina virtual en la que desea instalar el dispositivo adicional de gestor de recopiladores.
3. Especifique la máscara de subred de la dirección IP especificada.
4. Seleccione *Siguiente*. Se guardan los ajustes de conexiones de red.
5. Establezca la fecha y la hora y luego seleccione *Siguiente*.

   Para cambiar la configuración de NTP después de la instalación utilice YaST en la línea de comandos del dispositivo. Puede usar WebYast para cambiar la fecha y la hora, pero no la configuración de NTP.

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

   ```
   rcntp restart
   ```
6. Defina la contraseña `root` de SUSE Enterprise Server, y luego seleccione *Siguiente*.
7. Especifique el nombre de host/la dirección IP del servidor Sentinel al que debería conectarse el motor de correlación.
8. Especifique el número de puerto del servidor de comunicaciones. El puerto del bus de mensajes por defecto es `61616`.
9. Especifique el nombre de usuario de JMS, que representa el nombre de usuario del gestor de recopiladores. El nombre de usuario por defecto es `collectormanager`.
10. Especifique la contraseña del usuario de JMS.

    El nombre de usuario y la contraseña se almacenan en el archivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` ubicado en el servidor de Sentinel.
11. (Opcional) Para verificar la contraseña, consulte la siguiente línea del archivo `activemqusers.properties`:

    ```
    collectormanager=<password>
    ```

    En este ejemplo, `collectormanager` es el nombre de usuario y el valor correspondiente es la contraseña.
12. Seleccione *Siguiente* para finalizar la instalación.

    Cuando haya finalizado la instalación, aparecerá un mensaje que indica que este dispositivo es el gestor de recopiladores de Sentinel, junto con la dirección IP.

5.3.3 Instalación del motor de correlación

Puede instalar el motor de correlación como dispositivo en un sistema Linux habilitado para Xen que cumpla los requisitos mínimos de hardware para el motor de correlación. Para obtener más información, consulte Sección 1.1.2, "Requisitos del hardware", en la página 12.

1. Realice el Paso 1 al Paso 14 de la Sección 5.3.1, "Instalación de Sentinel", en la página 45.

   El nombre de archivo correcto del archivo de instalación del dispositivo virtual Xen del motor de correlación es `sentinel_correlation_engine_7.0.0.0.x86_64.xen.tar.gz`
2. En la pantalla Network Configuration II (Configuración de red II), seleccione *Change* (Cambiar) y especifique la dirección IP de la máquina virtual en la que desea instalar el dispositivo del motor de correlación.
3. Especifique la máscara de subred de la dirección IP especificada.
4. Seleccione *Siguiente*. Se guardan los ajustes de conexiones de red.
5. Establezca la fecha y la hora y luego seleccione *Siguiente*.

   Para cambiar la configuración de NTP después de la instalación utilice YaST en la línea de comandos del dispositivo. Puede usar WebYast para cambiar la fecha y la hora, pero no la configuración de NTP.

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

   ```
   rcntp restart
   ```
6. Defina la contraseña `root` de SUSE Enterprise Server, y luego seleccione *Siguiente*.
7. Especifique el nombre de host/la dirección IP del servidor Sentinel al que debería conectarse el motor de correlación.
8. Especifique el número de puerto del servidor de comunicaciones. El puerto del bus de mensajes por defecto es `61616`.
9. Especifique el nombre de usuario de JMS, que representa el nombre de usuario del motor de correlación. El nombre del usuario por defecto es `correlationengine`.
10. Especifique la contraseña del usuario de JMS.
11. Haga clic en *Siguiente*.

    El nombre de usuario y la contraseña se almacenan en el archivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` ubicado en el servidor de Sentinel.
12. Para verificar la contraseña, consulte la siguiente línea del archivo `activemqusers.properties`:

    ```
    correlationengine=<password>
    ```

    En este ejemplo, `correlationengine` es el nombre de usuario y el valor correspondiente de la contraseña.
13. Acepte el certificado cuando se le indique.
14. Haga clic en *Siguiente* para completar la instalación.

    Cuando la instalación haya finalizado, mostrará un mensaje que indica que el dispositivo es el motor de correlación de Sentinel, junto con la dirección IP. Además, muestra la dirección IP de la interfaz del usuario del servidor Sentinel.

5.4 Instalación del dispositivo en hardware

Antes de instalar el dispositivo en el hardware, asegúrese de que la imagen de disco ISO del dispositivo se haya descargado desde el sitio de asistencia, y que se haya desempaquetado y esté disponible en un DVD.

IMPORTANT: La instalación en hardware utilizando la imagen ISO en disco (desde cero e Hyper-V) requiere una memoria mínima de 4,5 GB para poder finalizar la instalación. Para obtener más información sobre los requisitos de hardware, consulte la Sección 1.1.2, “Requisitos del hardware”, en la página 12.

5.4.1 Instalación de Sentinel

1. Arranque el equipo físico de la unidad de DVD con el DVD.
2. Siga las instrucciones en pantalla del asistente de instalación.
3. Ejecute la imagen del dispositivo en el DVD seleccionando la entrada superior del menú de arranque.

   La instalación comprueba primero si hay memoria y espacio disponible en el disco. Si hay menos de 2.5 GB de memoria disponible, la instalación se cancela de forma automática. Si hay entre 2.5 GB y 6.7 GB de memoria disponible, la instalación muestra un mensaje que indica que hay menos memoria de la recomendada. Escriba `y` si desea continuar con la instalación o `n` si no es así.
4. Seleccione el idioma deseado y luego, haga clic en *Siguiente*.
5. Seleccione la disposición del teclado y haga clic en *Siguiente*.
6. Lea y acepte el acuerdo de licencia del software de SUSE Enterprise Server.
7. Lea y acepte el acuerdo de licencia del usuario final de NetIQ Sentinel.
8. Seleccione *Siguiente*.
9. En la pantalla Nombre de host y Nombre de dominio, especifique los valores correspondientes y asegúrese de que esté seleccionada la opción *Assign Hostname to Loopback IP* (Asignar nombre de host a IP de retrobucle).
10. Seleccione *Siguiente*. Se guarda la configuración del nombre de host.
11. Realice una de las siguientes acciones:
    - Para usar los ajustes de conexión de red actuales, seleccione la opción *Use the following configuration* (Usar la siguiente configuración) de la página de Network Configuration II (Configuración de red II).
    - Para cambiar los ajustes de conexión de red, seleccione *Change* (Cambiar) y luego realice los cambios necesarios.
12. Seleccione *Siguiente*. Se guardan los ajustes de conexiones de red.
13. Establezca la fecha y la hora y luego haga clic en *Siguiente*.

Para cambiar la configuración de NTP después de la instalación utilice YaST en la línea de comandos del dispositivo. Puede usar WebYast para cambiar la fecha y la hora, pero no la configuración de NTP.

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

```
rcntp restart
```

14 Defina la contraseña `root` y luego haga clic en *Siguiente*.

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

16 Introduzca el nombre de usuario y la contraseña en la consola para entrar en el dispositivo.

El valor por defecto del nombre de usuario es `root` y la contraseña es la contraseña definida en el Paso 14.

17 Detenga el servidor Sentinel:

```
service sentinel stop
```

18 Introduzca el siguiente comando para restablecer la interfaz del usuario para crear una pantalla nueva en YaST:

```
reset
```

19 Para instalar el dispositivo en el servidor físico, ejecute el siguiente comando:

```
/sbin/yast2 live-installer
```

Pueden 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.

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

21 Pase a la Sección 5.5, “Configuración del dispositivo posterior a la instalación”, en la página 52.

5.4.2 Instalación del gestor de recopiladores

Puede instalar el gestor de recopiladores como dispositivo en un sistema que cumpla los requisitos mínimos de hardware para el gestor de recopiladores. Para obtener más información, consulte Sección 1.1.2, “Requisitos del hardware”, en la página 12.

1 Realice el Paso 1 al Paso 14 de la Sección 5.4.1, “Instalación de Sentinel”, en la página 49.

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

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

La instalación intenta conectarse al servidor con las credenciales especificadas. Si introdujo cualquiera de los valores de forma incorrecta, la instalación mostrará un error.

4 Especifique el nombre de usuario de JMS, que representa el nombre de usuario del gestor de recopiladores. El nombre del usuario por defecto es `collectormanager`.

5 Especifique la contraseña del usuario de JMS.

6 Haga clic en *Siguiente*.

El nombre de usuario y la contraseña se almacenan en el archivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` ubicado en el servidor de Sentinel.

7 Para verificar la contraseña, consulte la siguiente línea en el archivo `activemqusers.properties`:

```
collectormanager=<password>
```

En este ejemplo, `collectormanager` es el nombre de usuario y el valor correspondiente es la contraseña.

8 Acepte el certificado cuando se le indique.

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

Cuando haya finalizado la instalación, aparecerá un mensaje que indica que este dispositivo es el gestor de recopiladores de Sentinel, junto con la dirección IP. Además, muestra la dirección IP de la interfaz del usuario del servidor Sentinel.

5.4.3 Instalación del motor de correlación

Puede instalar el motor de correlación como dispositivo en un sistema que cumpla los requisitos mínimos de hardware para el motor de correlación. Para obtener más información, consulte Sección 1.1.2, “Requisitos del hardware”, en la página 12.

1 Realice el Paso 1 al Paso 14 en la Sección 5.4.1, “Instalación de Sentinel”, en la página 49.

2 Especifique el nombre de host/la dirección IP de servidor Sentinel al que debe conectarse el motor de correlación.

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

4 Especifique el nombre de usuario de JMS, que representa el nombre de usuario del motor de correlación. El nombre de usuario por defecto es `correlationengine`.

5 Especifique la contraseña del usuario de JMS.

6 Haga clic en *Siguiente*.

El nombre de usuario y la contraseña se almacenan en el archivo `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` ubicado en el servidor de Sentinel.

7 Para verificar la contraseña, consulte la siguiente línea del archivo `activemqusers.properties` :

```
correlationengine=<password>
```

En este ejemplo, `correlationengine` es el nombre de usuario y el valor correspondiente de la contraseña.

8 Acepte el certificado cuando se le indique.

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

Cuando la instalación haya finalizado, se mostrará un mensaje que indica que el dispositivo es el motor de correlación de Sentinel, junto con la dirección IP. Además, muestra la dirección IP de la interfaz del usuario del servidor Sentinel.

10 Pase al Sección 5.5, “Configuración del dispositivo posterior a la instalación”, en la página 52.

5.5 Configuración del dispositivo posterior a la instalación

5.5.1 Instalación de VMware Tools

Para que Sentinel funcione de forma eficaz en el servidor VMware, debe instalar VMware Tools. VMware Tools es un conjunto de utilidades que mejora el rendimiento del sistema operativo del equipo virtual. Además, mejora la gestión del equipo virtual. Para obtener más información sobre la instalación de VMware Tools, consulte VMware Tools for Linux Guests (https://www.vmware.com/support/ws55/doc/ws_newguest_tools_linux.html#wp1127177) (VMware Tools para sistemas Linux invitados).

Para obtener más información sobre la documentación de VMware, consulte el Manual del usuario de la estación de trabajo (http://www.vmware.com/pdf/ws71_manual.pdf).

5.5.2 Acceso a la interfaz Web de dispositivo

Para entrar en la consola Web del dispositivo e inicializar el software:

1. Abra un navegador Web y acceda a https://<*dirección_IP*>:8443, donde 8443 es el puerto por defecto del servidor Sentinel. Se mostrará la página Web de Sentinel.

   Se muestra la dirección IP del dispositivo en la consola del dispositivo después de que finalice la instalación y se reinicie el servidor.
2. Configure el dispositivo Sentinel para el almacenamiento y la recopilación de datos.

   Para obtener más información sobre la configuración del dispositivo, consulte *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1).
3. Regístrese para obtener actualizaciones.

   Para obtener más información, consulte Sección 5.9, “Registro para recibir actualizaciones”, en la página 54.

5.6 Configuración de WebYaST

La interfaz del usuario del dispositivo Sentinel está equipada con WebYaST, que es una consola remota basada en la Web para controlar los dispositivos basados en SUSE Linux Enterprise. Puede acceder, configurar y supervisar los dispositivos de Sentinel mediante WebYaST. El siguiente procedimiento describe brevemente los pasos necesarios para configurar WebYaST. Para obtener más información acerca de la configuración detallada, consulte *WebYaST User Guide (Guía del usuario de WebYaST)* (http://www.novell.com/documentation/webyast/).

1. Entre en el dispositivo de Sentinel.
2. Haga clic en *Appliance* (Dispositivo).
3. Configure el servidor de Sentinel para recibir actualizaciones tal como se describió en Sección 5.9, “Registro para recibir actualizaciones”, en la página 54.
4. Haga clic en *Siguiente* para finalizar la instalación inicial.

5.7 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 apoderado de paquetes integrado en Centro de servicios al cliente de Novell que proporciona funciones clave de dicho centro.

5.7.1 Requisitos previos

- Obtenga las credenciales del Centro de servicios al cliente de Novell para Sentinel para obtener actualizaciones de Novell. Para obtener información sobre la forma de obtener credenciales, comuníquese con Asistencia de Novell (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup).
- Asegúrese de que SLES 11 SP1 esté instalada con los siguientes paquetes en el equipo donde desea instalar la herramienta SMT:
  - htmldoc
  - smt
  - perl-DBIx-Transaction
  - perl-File-Basename-Object
  - pertl-DBIx-Migration-Director
  - perl-MIME-Lite
  - perl-Text-ASCIITable
  - smt-support
  - yast2-smt
  - yum-metadata-parser
  - createrepo
  - sle-smt-release-cd
  - sle-smt_en
  - 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 (http://www.novell.com/documentation/smt11/):
  - 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.

5.7.2 Configuración del dispositivo

Para obtener información sobre cómo configurar el dispositivo con SMT, consulte la sección "Configuring Clients to Use SMT" (Configuración de clientes para usar SMT) (http://www.novell.com/documentation/smt11/smt_sle_11_guide/?page=/documentation/smt11/smt_sle_11_guide/data/smt_client.html) en la documentación de Subscription Management Tool.

5.8 Inicio y detención del servidor mediante la interfaz basada en la Web

Puede iniciar y detener el servidor de Sentinel utilizando la interfaz basada en la Web de la siguiente manera:

1. Entre en el dispositivo de Sentinel.
2. Haga clic en *Appliance* (Dispositivo) para lanzar WebYaST.
3. Haga clic en *System Services* (Servicios del sistema).
4. Para detener el servidor de Sentinel, haga clic en *detener*.
5. Para iniciar el servidor de Sentinel, haga clic en *iniciar*.

5.9 Registro para recibir actualizaciones

1. Entre en el dispositivo de Sentinel.
2. Haga clic en *Appliance* (Dispositivo) para lanzar WebYaST.
3. Haga clic en *Registration* (Registro).
4. Especifique la ID del correo electrónico en la que desea recibir actualizaciones y luego especifique el nombre del sistema y el código de registro del dispositivo.
5. Haga clic en *Guardar*.

6 Resolución de problemas en la instalación

En esta sección se enumeran los problemas que podrían ocurrir durante la instalación y las medidas para solucionar dichos problemas.

6.1 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.

6.2 El UUID no se crea para gestores de recopiladores con imagen o motores de correlación.

Si crea una imagen de un servidor del gestor de recopiladores (por ejemplo, mediante ZENworks Imaging) y restaura las imágenes en otros equipos, Sentinel no identifica de forma exclusiva las nuevas instancias del gestor de recopiladores. Esto sucede debido a que existen UUID duplicados.

Debe generar un nuevo UUID siguiendo estos pasos en los sistemas del gestor de recopiladores recién instalados:

1. Suprima el archivo `host.id` o `sentinel.id` ubicado en la carpeta `/var/opt/novell/sentinel_/data`.
2. Reinicie el gestor de recopiladores.

   El gestor de recopiladores genera de forma automática el UUID.

7 Pasos siguientes

Después de instalar Sentinel, dos guías le ayudarán a configurar Sentinel: la *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1) y la *NetIQ Sentinel 7.0.1 User Guide* (Guía del usuario de NetIQ Sentinel 7.0.1).

La Guía de administración incluye información de configuración para realizar tareas que solo puede realizar un usuario que tenga derechos administrativos. Por ejemplo:

- "Configuración de usuarios y funciones"
- "Configuración del almacenamiento de datos"
- "Configuración de la recopilación de datos"
- "Búsqueda y generación de informes de eventos en un entorno distribuido"

Para obtener más información sobre estas y otras tareas de administración, consulte la *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1).

La guía del usuario incluye instrucciones para ayudar a los usuarios a realizar tareas en Sentinel. Por ejemplo:

- "Búsqueda de eventos"
- "Análisis de tendencias en los datos"
- "Generación de informes"
- "Configuración de incidencias"

Para obtener más información sobre estas y otras tareas, consulte la *NetIQ Sentinel 7.0.1 User Guide* (Guía del usuario de NetIQ Sentinel 7.0.1).

También puede configurar Sentinel para analizar sus eventos, añadir datos utilizando reglas de correlación, configurar líneas de base, configurar flujos de trabajo para que actúen en función de la información y mucho más. Utilice la información de la *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1) para ayudarle a configurar estas funciones de Sentinel.

II Configuración

Después de instalar Sentinel, podrá configurarlo para ejecutarlo en su entorno.

8 Acceso a la interfaz Web de Sentinel

Una vez instalado Sentinel, puede acceder a la interfaz Web de Sentinel para realizar tareas de administración y configurar Sentinel para la recopilación de datos.

1. Abra un navegador Web y acceda a la dirección https://<*dirección IP*>:8443, donde 8443 es el puerto por defecto del servidor Sentinel.
2. (Condicional) La primera vez que acceda a Sentinel, acepte el certificado cuando se le indique.

   Al aceptar el certificado se muestra la página de inicio de sesión de Sentinel
3. Especifique el nombre de usuario y la contraseña del administrador de Sentinel
4. Haga clic en *Entrar a la sesión*.

   Se muestra la interfaz basada en la Web de NetIQ Sentinel.

9 Cómo añadir componentes adicionales de Sentinel

Por defecto, Sentinel tiene instalados y configurados un conector y un recopilador de syslog, además de diferentes conectores de auditoría y diversos recopiladores de productos de Novell. En las siguientes secciones se explica cómo instalar y configurar conectores y recopiladores adicionales.

9.1 Instalación de conectores y recopiladores

Por defecto, todos los recopiladores y conectores distribuidos están instalados en Sentinel 7. Si se distribuye un nuevo recopilador o conector después del lanzamiento de Sentinel 7, deberá instalar los archivos del recopilador o del conector antes de configurarlos.

9.1.1 Instalación de un recopilador

1. Descargue el recopilador de la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).
2. Acceda a la interfaz Web de Sentinel en la dirección https://<*dirección IP*>:8443, donde 8443 es el puerto por defecto del servidor Sentinel.
3. Haga clic en *aplicaciones* en la barra de herramientas y luego haga clic en *Aplicaciones*.
4. Haga clic en *Lanzar el Centro de control* para lanzar el Centro de control de Sentinel.
5. 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)*.
6. Busque y seleccione el archivo de recopilador que descargó en el Paso 1, y luego haga clic en *Siguiente*.
7. Siga las indicaciones restantes y luego haga clic en *Finalizar*.

Para configurar el recopilador, consulte la documentación específica del recopilador en la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.1.2 Instalación de un conector

1. Descargue el conector correcto de la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).
2. Acceda a la interfaz Web de Sentinel en la dirección https://<*dirección IP*>:8443, donde 8443 es el puerto por defecto del servidor Sentinel.
3. Haga clic en *aplicación* en la barra de herramientas y luego haga clic en *Aplicaciones*.
4. Haga clic en *Lanzar el Centro de control* para lanzar el Centro de control de Sentinel.
5. En la barra de herramientas, seleccione *Gestión de orígenes de eventos* > *Vista activa* y luego haga clic en *Herramientas* > *Importar módulo auxiliar (plug-in)*.
6. Busque y seleccione el archivo de conector que descargó en el Paso 1, y luego haga clic en *Siguiente*.
7. Siga las indicaciones restantes y luego haga clic en *Finalizar*.

Para configurar el conector, consulte la documentación específica del conector en la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.2 Cómo añadir conectores y recopiladores adicionales

9.2.1 Cómo añadir recopiladores adicionales

Puede añadir recopiladores adicionales para normalizar los datos de otros orígenes.

1. Acceda a la interfaz Web de Sentinel en la dirección https://<*dirección IP*>:8443, donde 8443 es el puerto por defecto del servidor Sentinel.
2. Haga clic en *aplicación* en la barra de herramientas y luego haga clic en *Aplicaciones*.
3. Haga clic en *Lanzar el Centro de control* para lanzar el Centro de control de Sentinel.
4. En la barra de herramientas, seleccione *Gestión de orígenes de eventos* > *Vista activa*.
5. Haga clic con el botón derecho del ratón en el gestor de recopiladores y luego haga clic en *Añadir recopilador*.
6. Seleccione el recopilador de la columna *Proveedor* y haga clic en *Siguiente*.
7. Los campos son diferentes para cada recopilador, por lo que necesita seguir la documentación específica del recopilador para configurar el recopilador en este punto.

   La documentación del recopilador se encuentra en la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.2.2 Cómo añadir conectores adicionales

Puede añadir conectores adicionales para recopilar información de otros orígenes.

1. Acceda a la interfaz Web de Sentinel en la dirección https://<*dirección IP*>:8443, donde 8443 es el puerto por defecto de Sentinel.
2. Haga clic en *aplicación* en la barra de herramientas y luego haga clic en *Aplicaciones*.
3. Haga clic en *Lanzar el Centro de control* para lanzar el Centro de control de Sentinel.
4. En la barra de herramientas, seleccione *Gestión de orígenes de eventos* > *Vista activa*.
5. Haga clic con el botón derecho del ratón en el recopilador al que desea añadir el conector adicional y luego haga clic en *Agregar conector*.
6. Seleccione el conector deseado de la columna *Nombre* y luego haga clic en *Siguiente*.
7. Los campos son diferentes para cada conector, por lo que deberá seguir la documentación específica del conector para configurarlo en este momento.

   La documentación del conector se encuentra en la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

10 Gestión de datos

10.1 Estructura de directorio

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 encuentran en los siguientes directorios:
  - `/opt/novell/sentinel/bin`
  - `/opt/novell/sentinel/setup`
  - `/opt/novell/sentinel/3rdparty`
- Los archivos de registro se encuentran en el directorio `/var/opt/novell/sentinel/log`
- Los archivos de configuración se encuentran en el siguiente directorio `/etc/opt/novell/sentinel`
- El archivo de ID de proceso (PID) se encuentra en el directorio`/var/run/sentinel/server.pid`.

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

10.2 Consideraciones sobre almacenamiento

Al almacenar archivos de datos de Sentinel, asegúrese de que los archivos de datos se almacenen en una partición diferente de donde se encuentran los archivos ejecutables, de configuración y del sistema operativo. La ventaja de almacenar los datos por separado es que se permite crear fácilmente una imagen de un conjunto de archivos y recuperarlos en caso de que resulten dañados. Además, mejora el rendimiento general de los sistemas donde los sistemas de archivos más pequeños son más eficientes. Para obtener más información, consulte “Disk partitioning (Creación de particiones de disco)” (http://en.wikipedia.org/wiki/Disk_partitioning#Benefits_of_multiple_partitions).

Puede decidir instalar Sentinel en varias particiones o en una sola partición dependiendo de los siguientes tipos de instalación:

- Instalación independiente
- Instalación de dispositivo

10.2.1 Uso de una partición en una instalación independiente

Si va a instalar Sentinel como instalación independiente, podrá modificar la distribución en la partición 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 detallada en la Sección 10.1, “Estructura de directorio”, en la página 67. Al ejecutar el instalador, Sentinel se instala en los directorios creados previamente, lo que da lugar a una instalación que abarca varias particiones.

NOTE:

- Puede usar la opción`--location` mientras ejecuta el instalador para especificar una ubicación 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 los enlaces del sistema de archivos (por ejemplo, enlaces simbólicos) para la opción `--location`.

10.2.2 Uso de una partición en una instalación de dispositivo

Si va a instalar Sentinel utilizando una instalación de dispositivo, no es posible volver a configurar el sistema operativo antes de la instalación de Sentinel porque el sistema operativo se instala junto con Sentinel. Sin embargo, puede añadir una partición en el dispositivo y mover un directorio a la nueva partición mediante la herramienta YaST.

El siguiente procedimiento crea una partición nueva y mueve 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 al Centro de control 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.
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. Cambie al usuario `root`.

13 Ejecute el siguiente comando para reiniciar el dispositivo Sentinel:

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

11 Configuración de contenido predefinido

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 preinstalado en un Paquete central de soluciones de Sentinel. Para obtener más información, consulte "Using Solution Packs" (Uso de paquetes de soluciones) en la *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1).

El paquete de soluciones permite clasificar y agrupar el contenido en "controles" o conjuntos de directivas que se consideran como una unidad. Los controles del Paquete central de soluciones de Sentinel vienen preinstalados para proporcionarle este contenido predefinido, pero dichos controles deben implementarse formalmente o probarse mediante la IU basada en la Web 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 centrales de Sentinel 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 *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1).

12 Configuración de la hora

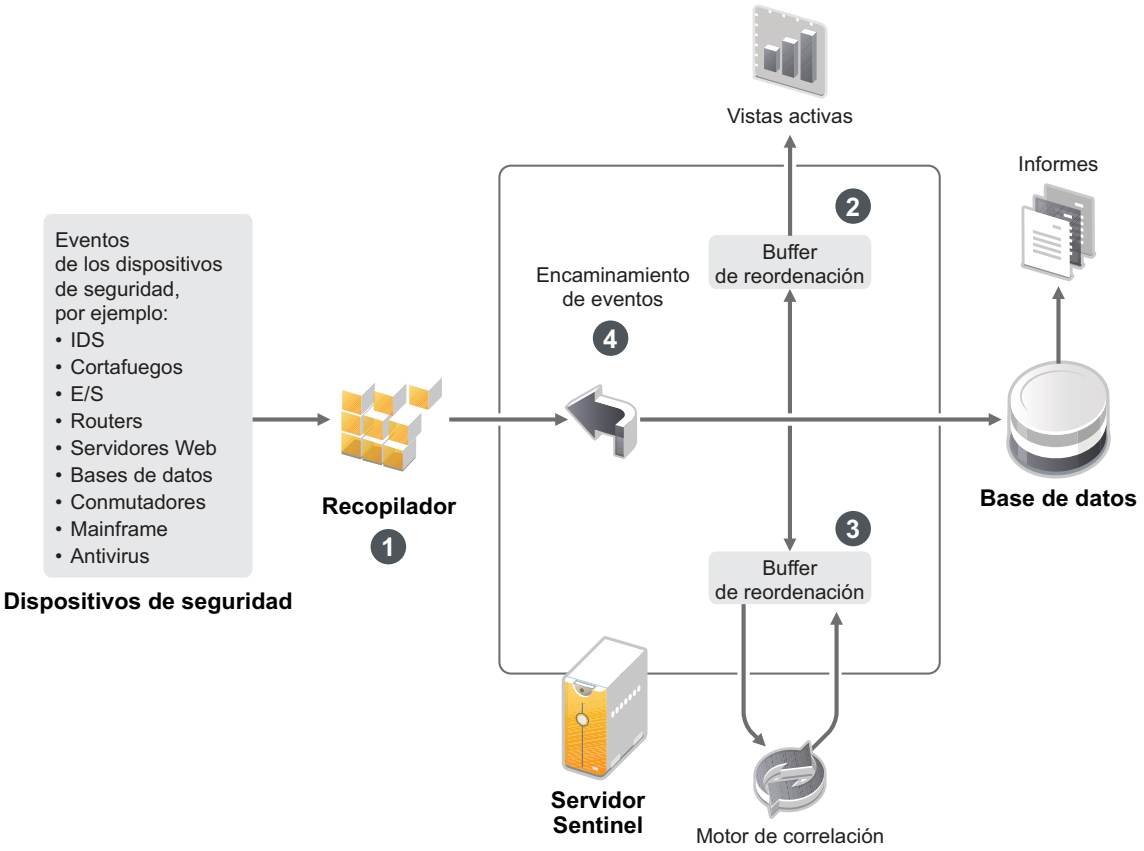
La hora de un evento es crucial para su procesamiento en Sentinel. Es importante para la generación de informes y para fines de auditoría, además de para el procesamiento en tiempo real.

12.1 Comprender el tiempo en Sentinel

Sentinel es un sistema distribuido compuesto de varios procesos que pueden encontrarse en diferentes partes de la red. Además, puede haber algún retraso introducido por el dispositivo. Para adaptarlo, los procesos de Sentinel reordenan los eventos en un flujo ordenado por tiempo antes de procesarlos.

En la siguiente ilustración se explica cómo Sentinel lleva a cabo esta operación:

Figura 12-1 *Hora de Sentinel*



1. Por defecto, la hora del evento se define en la hora del gestor de recopiladores. La hora ideal es la hora del dispositivo. Por lo tanto, es mejor definir la hora del evento en la hora del dispositivo si está disponible, es precisa y el recopilador la ha analizado adecuadamente.
2. Los eventos se ordenan en intervalos de 30 segundos para poder verlos en las Vistas activas. Por defecto, los eventos que tienen una marca horaria dentro de un intervalo de 5 minutos a partir de la hora del servidor (en el pasado o futuro) se procesan con normalidad. Los eventos que tienen marcas horarias de más de 5 minutos en el futuro no se muestran en las Vistas activas, pero se ingresan en el almacén de eventos Los eventos que tienen marcas horarias de más de 5 minutos y menos de 24 horas en el pasado 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. En el caso de que la hora del evento sea más de 30 segundos anterior a la hora del servidor, el motor de correlación no procesará los eventos.
4. Si la hora del evento es más de 5 minutos anterior a la hora del gestor de recopiladores (la hora correcta), los eventos se encaminan directamente al almacén de eventos.

12.2 Configuración de la hora en Sentinel

El motor de correlación 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 el gestor de recopiladores y deseleccione *Hora del origen de eventos predeterminado* en el origen de eventos del Gestor de orígenes de eventos. Sentinel utiliza el gestor de recopiladores 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 *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1).
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.

12.3 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, el gestor de recopiladores 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.

El segundo escenario es en general el más sencillo. Si se utilizan las IDs de zona horaria de formato largo o diferencias horarias, es posible convertir fácilmente al formato UTC para obtener la hora UTC canónica absoluta (guardada en DeviceEventTime), pero también se pueden calcular fácilmente 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 puede ser el más complicado, porque 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 el gestor de recopiladores. 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 el gestor de recopiladores al servidor Sentinel y se guarda en el almacén de eventos. La zona horaria en la que se encuentran el gestor de recopiladores 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 zona 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.

13 Información sobre licencias

En esta sección se describen las diferentes licencias de Sentinel y se ofrece información sobre la forma de gestionarlas.

13.1 Descripción de licencias de Sentinel

Sentinel tiene varias licencias a su disposición. Por defecto, Sentinel se suministra con la licencia de prueba.

13.1.1 Licencia de prueba

La licencia por defecto de Sentinel le permite usar todas las funciones empresariales de Sentinel durante el período de evaluación de 90 días. Un sistema que ejecute la licencia de prueba muestra un indicador en la interfaz Web que indica que se está utilizando la clave de licencia temporal. También muestra el número de días que quedan para que caduque la funcionalidad e indica la forma de actualizar a una licencia completa.

NOTE: La fecha de caducidad del sistema se basa en los datos más antiguos del sistema. Si restaura eventos antiguos en el sistema, se ajustará la fecha de caducidad en la forma correspondiente.

Después del período de prueba de 90 días, se inhabilitan la mayoría de funciones, aunque aún podrá acceder al sistema y actualizarlo para usar una clave de licencia empresarial.

Después de actualizar a una licencia empresarial, se restaura toda la funcionalidad. Para prevenir cualquier interrupción de la funcionalidad, debe actualizar el sistema a una licencia empresarial antes de la fecha de caducidad.

13.1.2 Licencias empresariales

Al adquirir Sentinel, recibe una clave de licencia a través del portal para clientes. Dependiendo de la licencia que adquiera, la clave de licencia habilita 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. Para añadir la clave de licencia al sistema, consulte la Sección 13.2.1, “Cómo añadir una clave de licencia mediante la interfaz Web”, en la página 78.

13.2 Cómo añadir una clave de licencia

NOTE: Para añadir, ver o suprimir una licencia, debe tener privilegios de administrador.

Puede añadir una clave de licencia mediante la interfaz Web o la línea de comandos.

- Sección 13.2.1, "Cómo añadir una clave de licencia mediante la interfaz Web", en la página 78
- Sección 13.2.2, "Cómo añadir una clave de licencia a través de la línea de comandos", en la página 78

13.2.1 Cómo añadir una clave de licencia mediante la interfaz Web

1. Acceda a la interfaz Web de Sentinel como administrador.
2. Haga clic en el enlace *Acerca de* en la esquina superior izquierda de la página.
3. Haga clic en la pestaña *Licencia*.
4. En la sección Licencias, haga clic en *Añadir licencia*.
5. Especifique la clave de licencia en el campo *Clave*. Una vez especificada la licencia, se muestra la siguiente información en la sección Vista previa:

   Funciones: Las funciones disponibles en la licencia.

   Host: Este campo es de uso exclusivamente interno de NetIQ.

   Serial: Este campo es de uso exclusivamente interno de NetIQ.

   Eps: Número de eventos incorporado a la clave de licencia. Más allá de este número, Sentinel generará advertencias pero seguirá recopilando datos.

   venció: Fecha de caducidad de la licencia. Debe especificar una clave de licencia válida antes de la fecha de caducidad para prevenir la interrupción de la funcionalidad.
6. Haga clic en *Guardar*.

13.2.2 Cómo añadir una clave de licencia a través de la línea de comandos

Puede añadir la licencia a través de la línea de comandos mediante el guión `softwarekey.sh`.

1. Entre en Sentinel como usuario `root`.
2. Cambie al directorio `/opt/novell/sentinel/bin`.
3. Introduzca el siguiente comando para cambiar al usuario novell:

   ```
   su novell
   ```
4. Especifique el siguiente comando para ejecutar el guión `softwarekey.sh`.

   ```
   ./softwarekey.sh
   ```
5. Introduzca 1 para insertar la clave de licencia.
6. Especifique la clave de licencia y luego pulse Intro.

14 Configuración de Sentinel para alta disponibilidad

Se han realizado pruebas en Sentinel que certifican que puede utilizarse en un entorno de alta disponibilidad y que es compatible con arquitecturas de recuperación tras fallos. NetIQ Consulting (servicios de consultoría) y los socios de NetIQ pueden ayudarle a implementar las funciones de alta disponibilidad y recuperación tras fallos de Sentinel.

Para habilitar los servidores de Sentinel para una alta disponibilidad, necesitará lo siguiente:

- Nodos de Sentinel duplicados, agrupados en clústeres.
- Acceso a almacenamiento de datos compartido.
- Direcciones IP virtuales que puedan utilizarse para cambiar de manera transparente entre un nodo que ha fallado y otro nodo.
- Guiones para iniciar, detener y supervisar la aplicación en función de las directivas definidas en las soluciones de agrupación en clúster. Puede utilizar soluciones de agrupación en clúster como Cluster Resource Agents o guiones init LSB en sistemas Linux Enterprise de alta disponibilidad.

En el mercado pueden existir numerosos paquetes que habilitan una alta disponibilidad. Se realizaron pruebas de Sentinel con la *Extensión de SUSE Linux Enterprise High Availability (HA)* (http://www.novell.com/products/highavailability/), unidades RAID de almacenamiento compartido y guiones personalizados. Esta arquitectura puede duplicarse entre centros de datos para garantizar la disponibilidad de todo tipo de elementos desde el servidor Sentinel hasta los gestores de recopiladores y los recopiladores.

Es necesario considerar la alta disponibilidad para orígenes de eventos de manera individual debido a la gran variedad de dispositivos que se pueden utilizar.

III Actualización de Sentinel

15 Actualización del servidor Sentinel

1. Realice una copia de seguridad de su configuración y, a continuación, cree una exportación de ESM.

   Para obtener más información sobre cómo realizar una copia de seguridad de los datos, consulte"Copia de seguridad y restauración de datos" en la *NetIQ Sentinel 7.0.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.0.1)*.

2. Descargue el programa de instalación más reciente del sitio de descargas de Novell (http://download.novell.com).

3. Entre como usuario `root` en el servidor en el que desea actualizar Sentinel.

4. 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.

5. Vaya al directorio donde extrajo el archivo de instalación.

6. Especifique el siguiente comando para actualizar Sentinel:

   ```
   ./install-sentinel
   ```

7. 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.

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

9. 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. Si pulsa n, la instalación se cancela. Para continuar con la actualización, pulse s.

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

10. (Condicional) Para actualizar los sistemas de gestor de recopiladores, consulte el Capítulo 17, "Actualización del gestor de recopiladores", en la página 87.

11. (Condicional) Para actualizar el sistema de motor de correlación, consulte el Capítulo 18, "Actualización del motor de correlación", en la página 89.

16 Actualización del dispositivo Sentinel

Este procedimiento le guía en la actualización del dispositivo Sentinel así como de los dispositivos de gestor de recopiladores y motor de correlación.

1. Entre en el dispositivo Sentinel como usuario con funciones de administrador.
2. ***Si desea actualizar el dispositivo Sentinel***, haga clic en *Dispositivo* para lanzar WebYaST.
3. ***Si desea actualizar un dispositivo de gestor de recopiladores o de motor de correlación***, especifique la dirección URL del equipo del gestor de recopiladores o del motor de correlación utilizando el puerto 54984 para lanzar WebYaST.
4. Realice una copia de seguridad de su configuración y, a continuación, cree una exportación de ESM.

   Para obtener más información sobre cómo realizar una copia de seguridad de los datos, consulte"Copia de seguridad y restauración de datos" en la *NetIQ Sentinel 7.0.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.0.1)*.
5. (Condicional) Si aún no ha registrado el dispositivo para actualizaciones automáticas, hágalo ahora.

   Para obtener más información, consulte Sección 5.9, "Registro para recibir actualizaciones", en la página 54.

   Si el dispositivo no está registrado, se mostrará una advertencia en amarillo para informarle de que la aplicación no está registrada.
6. Para comprobar si existen actualizaciones, haga clic en *Updates* (Actualizaciones).

   Se muestran las actualizaciones disponibles.
7. Seleccione y aplique las actualizaciones.

   Las actualizaciones pueden tardar unos minutos en finalizar. Una vez finalizada de forma satisfactoria la actualización, se mostrará la página de acceso de WebYaST.

   Antes de actualizar la aplicación, WebYaST detiene el servicio de Sentinel automáticamente. Cuando finalice la actualización, debe reiniciar este servicio manualmente.
8. Reinicie el servicio Sentinel utilizando la interfaz basada en la Web.

   Para obtener más información, consulte la Sección 5.8, "Inicio y detención del servidor mediante la interfaz basada en la Web", en la página 54.

17 Actualización del gestor de recopiladores

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 *NetIQ Sentinel 7.0.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.0.1)*.
2. Entre en la interfaz basada en la Web de Sentinel como usuario con funciones de administrador.
3. Seleccione *Descargas*.
4. Haga clic en *Descargar instalador* de la sección Instalador de gestor de recopiladores.

   Se muestra una ventana con opciones para abrir o guardar el archivo del instalador en el equipo local.
5. Guarde el archivo.
6. Copie el archivo en una ubicación temporal.
7. Extraiga el contenido del archivo.
8. Ejecute el guión siguiente:

   ./install-cm
9. Siga las instrucciones que aparecen en pantalla para finalizar el procedimiento de instalación.

18 Actualización del motor de correlación

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*NetIQ Sentinel 7.0.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.0.1)*.
2. Entre en la interfaz basada en la Web de Sentinel como usuario con funciones de administrador.
3. Seleccione *Descargas*.
4. Haga clic en *Descargar instalador* en la sección Instalador de motor de correlación.

   Se muestra una ventana con opciones para abrir o guardar el archivo del instalador en el equipo local.
5. Guarde el archivo.
6. Copie el archivo en una ubicación temporal.
7. Extraiga el contenido del archivo.
8. Ejecute el guión siguiente:

   ./install-ce
9. Siga las instrucciones que aparecen en pantalla para finalizar el procedimiento de instalación.

19 Actualización de módulos auxiliares (plug-in) de Sentinel

Los módulos auxiliares (plug-in) nuevos y actualizados de Sentinel se cargan con frecuencia en el sitio Web de módulos auxiliares de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html). Para obtener las correcciones de defectos, documentación y mejoras más recientes de un módulo auxiliar (plug-in), descargue la versión más reciente de dicho módulo auxiliar. Para obtener más información sobre cómo instalar o actualizar un módulo auxiliar (plug-in), consulte la documentación específica del módulo auxiliar en cuestión.

IV Migración

20 Escenarios de migración compatibles

En esta versión de Sentinel, no hay escenarios de migración compatibles. Debe realizar una nueva instalación de Sentinel en lugar de una migración o una actualización. No obstante, en breve se distribuirá una herramienta para migrar datos.

Para obtener instrucciones sobre la instalación, consulte Capítulo 2, “Instalación de Sentinel”, en la página 23.

21 Pasos siguientes

Después de instalar Sentinel, dos guías le ayudarán a configurar Sentinel: la *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1) y la *NetIQ Sentinel 7.0.1 User Guide* (Guía del usuario de NetIQ Sentinel 7.0.1).

La Guía de administración incluye información de configuración para realizar tareas que solo puede realizar un usuario que tenga derechos administrativos. Por ejemplo:

- "Configuración de usuarios y funciones"
- "Configuración del almacenamiento de datos"
- "Configuración de la recopilación de datos"
- "Búsqueda y generación de informes de eventos en un entorno distribuido"

Para obtener más información sobre estas y otras tareas de administración, consulte la *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1).

La guía del usuario incluye instrucciones para ayudar a los usuarios a realizar tareas en Sentinel. Por ejemplo:

- "Búsqueda de eventos"
- "Análisis de tendencias en los datos"
- "Generación de informes"
- "Configuración de incidencias"

Para obtener más información sobre estas y otras tareas, consulte la *NetIQ Sentinel 7.0.1 User Guide* (Guía del usuario de NetIQ Sentinel 7.0.1).

También puede configurar Sentinel para analizar sus eventos, añadir datos utilizando reglas de correlación, configurar líneas de base, configurar flujos de trabajo para que actúen en función de la información y mucho más. Utilice la información de la *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1) para ayudarle a configurar estas funciones de Sentinel.

V Desinstalación

Para desinstalar Sentinel debe realizar la siguientes tareas:

- Capítulo 22, “Desinstalación de Sentinel”, en la página 101
- Capítulo 23, “Tareas posteriores a la desinstalación”, en la página 103

22 Desinstalación de Sentinel

Hay disponible un guión de desinstalación que le ayudará a eliminar una instalación de Sentinel. Algunos archivos, como los archivos de registro, se mantienen en el sistema; de forma que, si lo desea, puede eliminarlos de forma manual. 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.

WARNING: 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.

22.1 Desinstalación del servidor de Sentinel

1. Entre en Sentinel como usuario `root`.

   NOTE: 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:

   ```
   /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.

22.2 Desinstalación del gestor de recopiladores remoto o del motor de correlación

1. Entre a la sesión como usuario `root`.

   NOTE: No es posible desinstalar un gestor de recopiladores remoto o un motor de correlación remoto 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 el gestor de recopiladores o el motor de correlación y todos los datos asociados se eliminarán por completo.

4 Introduzca s para eliminar el gestor de recopiladores o el motor de correlación.

El guión detiene primero el servicio y luego lo elimina por completo.

23 Tareas posteriores a la desinstalación

NOTE: La desinstalación del servidor Sentinel no supone la eliminación del usuario administrador del sistema operativo. Si desea eliminarlo, necesitará hacerlo manualmente.

23.1 Eliminación de la configuración del sistema de Sentinel

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.

23.1.1 Finalización de la desinstalación del motor de correlación

Después de ejecutar el guión de desinstalación del motor de correlación, el icono del motor de correlación se muestra aún en estado inactivo en la interfaz Web. Debe realizar los siguientes pasos adicionales para suprimir manualmente el motor de correlación en la interfaz Web:

1. Acceda a la interfaz Web de Sentinel como administrador.
2. Amplíe *Correlación* y luego seleccione el motor de correlación que desea suprimir.
3. Haga clic en el botón *Suprimir* (icono de papelera).

23.1.2 Finalización de la desinstalación del gestor de recopiladores

Después de ejecutar el guión de desinstalación del gestor de recopiladores, el icono del gestor de recopiladores se muestra aún en estado inactivo en la interfaz Web. Debe realizar los siguientes pasos adicionales para suprimir manualmente el gestor de recopiladores en la interfaz Web:

1. Acceda a *Gestión de orígenes de eventos* > *Vista activa*.
2. Haga clic con el botón derecho en el gestor de recopiladores que desee suprimir y, a continuación, haga clic en *Suprimir*.