Guía de inicio rápido de NetIQ Sentinel 7.0.1

Marzo de 2012

Novell®

Inicio

Utilice la siguiente información para instalar y poner en marcha Sentinel de una forma rápida.

Cumplimiento de los requisitos del sistema

Compruebe que cumple los requisitos mínimos del sistema para instalar Sentinel.

Requisitos de hardware para 500 EPS:

- **Memoria:** 6.7 GB
- **Disco duro:** 4 controladores RMP de 7,2K y 500 GB, ejecutándose en unidad RAID 1 con caché de 256 MB o área de red de almacenamiento (SAN) equivalente
- **Procesadores:** Una CPU Intel Xeon X5470 de 3,33 GHz (4 núcleos)

Sistemas operativos:

- SUSE Linux Enterprise Server (SLES) 11 SP1
- Red Hat Enterprise Linux (RHEL) 6

Máquinas virtuales:

- VMWare ESX 4.0
- Xen 4.0
- Sólo archivo de imagen ISO del servidor Hyper-V 2008 R2DVD

Imágenes ISO en DVD:

- Servidor Hyper-V 2008 R2
- Hardware sin sistema operativo instalado

Para conocer los requisitos de hardware si el número de EPS es superior o inferior a 500 EPS, consulte “Cumplimiento de los requisitos del sistema” en la *Guía de instalación y configuración de NetIQ Sentinel 7.0.1*.

Instalación de Sentinel

Puede instalar Sentinel como instalación independiente o como dispositivo.

Instalación en hardware:

La instalación estándar de Sentinel instala todos los componentes de Sentinel en un equipo. Si desea realizar una instalación personalizada o instalar Sentinel como usuario diferente de `root`, consulte “Instalación de Sentinel” en la *Guía de instalación y configuración de NetIQ Sentinel 7.0.1*.

Cómo instalar Sentinel:

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 Utilice el comando siguiente para extraer el archivo de instalación:

```
tar xfz <install_filename>
```

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

3 Utilice el comando siguiente para ejecutar el guión `install-sentinel`:

```
./install-sentinel
```

4 Especifique el número correspondiente al idioma deseado para la instalación y luego pulse Intro.

El valor por defecto es 3 para inglés.

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` (sí) o `y` para aceptar la licencia y continuar con la instalación.

Esta instalación puede tardar unos minutos en finalizar.

7 Cuando se le indique, introduzca 1 para continuar con la instalación estándar de Sentinel 7.0.

8 Especifique una contraseña dos veces para la cuenta de administrador por defecto que se creó durante la configuración.

Para obtener información detallada, consulte “Instalación de Sentinel” en la *Guía de instalación y configuración de NetIQ Sentinel 7.0.1*.

Instalación del dispositivo

El dispositivo está disponible para las plataformas virtuales VMware ESX, Xen y Hyper-V. También puede instalar el dispositivo en hardware. Las siguientes instrucciones corresponden al servidor VMware ESX. Para obtener instrucciones sobre las demás plataformas, consulte “Instalación del dispositivo” en la *Guía de instalación y configuración de NetIQ Sentinel 7.0.1*.

1 Descargue el archivo de instalación del dispositivo VMware.

El archivo correcto del dispositivo VMware tiene `vmx` en el nombre del archivo.

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 Novell SUSE Linux Enterprise Server.

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.

13 Asegúrese de que se haya seleccionado 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) en 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 Haga clic en *Next* (Siguiente) para guardar los ajustes de conexión 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 Novell SUSE Linux Enterprise Server, y luego haga clic en *Siguiente*.

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

20 Defina la contraseña de administrador de Sentinel y la contraseña de dbauser, y luego haga clic en *Siguiente*.

21 Haga clic en *Siguiente*. Se guardan los ajustes de conexiones de red.

Cuando finalice la instalación, anote la dirección IP del dispositivo que aparece en la consola.

Para obtener información de configuración posterior a la instalación, consulte "Configuración posterior a la instalación del dispositivo" en la *Guía de instalación y configuración de NetIQ Sentinel 7.0.1*.

Acceso a la interfaz Web de Sentinel

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

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

`https://<Dirección_IP_servidor_Sentinel>:8443`

El puerto 8443 es el valor por defecto.

Recopilación de datos

La recopilación de datos se produce a través de conectores y recopiladores. Por defecto, Sentinel tiene instalados y configurados algunos conectores y recopiladores.

Por defecto, existen servidores syslog de TCP, UDP y SSL instalados en el servidor Sentinel. Si utiliza el dispositivo, los servidores syslog se configuran automáticamente cuando comienzan a recibir eventos del archivo syslog local.

Puede configurar dispositivos syslog, como el servidor Linux, para enviar información a estos servidores syslog. Además, puede configurar otros conectores para que Sentinel pueda recopilar datos.

- "Configuración de un servidor Linux para enviar información de syslog a Sentinel" en la página 3
- "Configuración de recopilación de datos para Windows" en la página 3
- "Configuración de conectores y recopiladores adicionales" en la página 6

Configuración de un servidor Linux para enviar información de syslog a Sentinel

El servidor Sentinel contiene un servidor de orígenes de eventos de syslog previamente configurado que escucha cualquier conexión entrante a estos puertos:

- **TCP:** 1468
- **UDP:** 1514
- **SSL:** 1443

Utilice la siguiente información para configurar un servidor Linux para que envíe eventos al servidor de orígenes de eventos de syslog de TCP.

Para configurar el archivo de syslog en Linux:

1 Abra el archivo `/etc/syslog-ng/syslog-ng.conf`.

2 Añada las siguientes líneas de código al final del archivo `syslog-ng.conf`.

```
# Forward all messages to Sentinel:
#
destination d_slm { tcp("127.0.0.1"
port(1468)); };
log { source(src); destination(d_slm); };
```

3 Cambie el valor de TCP a la dirección IP del servidor Linux.

4 Guarde y cierre el archivo.

5 Reinicie el servicio syslog:

```
/etc/init.d/syslog restart
```

Para obtener información sobre cómo configurar dispositivos para que envíen información al conector de Syslog, consulte la documentación del conector de Syslog que encontrará en la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Configuración de recopilación de datos para Windows

Si tiene un sistema Windows del que desea recopilar datos, debe configurar un Conector de eventos de Windows (WMI). El conector de eventos de Windows está instalado en el gestor de recopiladores y recibe eventos del Servicio de recopilación de eventos de Windows instalado en el servidor de Windows.

- "Configuración del conector de eventos de Windows" en la página 3
- "Instalación del servicio de recopilación de eventos de Windows en el servidor Windows" en la página 4
- "Configuración del Servicio de recopilación de eventos de Windows" en la página 5

Configuración del conector de eventos de Windows

1 Entre en la interfaz Web de Sentinel.

`https://<Dirección_IP_servidor_Sentinel>:8443`

El puerto 8443 es el valor por defecto.

2 Haga clic en *Aplicaciones* en la barra de herramientas y luego haga clic en *Lanzar el Centro de control*.

3 Acceda al Centro de control de Sentinel con el nombre de usuario y contraseña de administrador y luego haga clic en *Entrada*.

4 En la barra de herramientas, haga clic en *Gestión de orígenes de eventos* > *Vista activa*.

5 Añada un recopilador específico de Windows al gestor de recopiladores.

Debe tener configurado un recopilador específico de Windows para poder añadir el conector de eventos de Windows.

5a Haga clic con el botón derecho del ratón en el gestor de recopiladores y luego haga clic en *Añadir recopilador*.

5b Seleccione*Microsoft* en la columna*Proveedor* y luego seleccione la versión de Windows o Active Directory en la columna Versión.

5c Haga clic en *Siguiente*.

5d Seleccione los guiones que desea visualizar y luego haga clic en *Siguiente*.

5e Cambie cualquiera de los parámetros de configuración y después haga clic en *Siguiente*.

5f Defina parámetros de configuración adicionales para el recopilador y luego haga clic en *Finalizar*.

6 Añada el conector de eventos de Windows al recopilador que creó en el Paso 5:

6a Haga clic con el botón derecho del ratón en el recopilador y luego haga clic en *Agregar conector*.

6b Seleccione el conector de eventos de Windows y luego haga clic en *Siguiente*.

6c Configure los ajustes de red para el servidor del conector de eventos de Windows y luego haga clic en *Siguiente*.

6d Configure los ajustes de SSL y luego haga clic en *Siguiente*.

6e Seleccione la forma de gestionar el conector de eventos de Windows:

- **Manualmente:** seleccione esta opción para gestionar manualmente el origen de eventos.
- **Automática:** seleccione esta opción para sincronizar automáticamente con Active Directory.

6f Haga clic en *Siguiente*.

6g Especifique las credenciales del usuario que se emplearon para conectar con el Servicio de recopilación de eventos de Windows y para conectar con el origen de eventos.

6h Especifique los parámetros de configuración y luego haga clic en *Finalizar*.

7 Añada un origen de evento para los sistemas Windows de los que desea recopilar datos.

7a Haga clic con el botón derecho del ratón en el conector de eventos de Windows y luego haga clic en *Añadir origen de eventos*.

7b Especifique la dirección IP o el nombre de host del sistema Windows

O bien

Seleccione un sistema Windows de Active Directory y luego haga clic en *Siguiente*.

7c Seleccione un modo de conexión para el origen de eventos y luego haga clic en *Siguiente*.

7d Especifique los parámetros de configuración del origen de eventos y luego haga clic en *Finalizar*.

Instalación del servicio de recopilación de eventos de Windows en el servidor Windows

1 Compruebe que haya creado una cuenta de usuario en el servidor de Windows que cuente con los derechos adecuados para ejecutar el Servicio de recopilación de eventos de Windows y para recopilar eventos de los registros de eventos de Windows de los sistemas Windows remotos. Estos derechos son:

- Permiso para acceder a los registros de eventos de Windows
- Permisos de WMI
- Permisos de DOCM
- Los derechos de lectura, escritura y supresión de ACL deben estar asignados al grupo de Usuarios distribuidos de COM para todos los tipos de registros de eventos.
- Permiso de lectura del registro de eventos de seguridad
- El usuario debe tener privilegios administrativos para instalar el Agente de Windows
- El usuario debe tener el derecho de *Entrada como servicio*.

Para obtener más información, consulte la documentación del conector de eventos de Windows en la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html). En los capítulos 4 y 5 encontrará la información relativa a los permisos.

2 Copie el archivo `WindowsEvent-CollectionService.msi` del archivo `.zip` del conector de eventos de Windows al servidor de Windows donde desea instalar el Servicio de recopilación de eventos de Windows.

3 Haga doble clic en el archivo `WindowsEvent-CollectionService.msi` para lanzar el Asistente de configuración del servicio de recopilación de eventos de Windows.

4 En la página de bienvenida haga clic en *Siguiente*.

5 (Condicional) Lea la advertencia sobre el límite de asistencia y luego haga clic en *Siguiente*.

6 Acepte la licencia del usuario final y luego haga clic en *Siguiente*.

7 Utilice la siguiente información para personalizar la configuración del Servicio de recopilación de eventos de Windows:

Funciones adicionales: seleccione las funciones que desea instalar. No todas las funciones están instaladas por defecto. Las funciones son:

- **Servicio de recopilación:** instala el Servicio de recopilación de eventos de Windows que se comunica con Sentinel.
- **Documentación:** instala la documentación que se suministra con el conector.

Ubicación: (opcional) cambie la ubicación de instalación por defecto haciendo clic en *Examinar* y seleccionando una nueva ubicación. La ubicación de instalación por defecto es `Archivos de programa\Novell\SentinelWECS`.

Uso del disco: (opcional) haga clic en *Utilización del disco* para determinar si hay suficiente espacio disponible en el disco para instalar el Servicio de recopilación de eventos de Windows.

8 Haga clic en *Siguiente*.

9 Defina la cuenta de servicio que utiliza el Servicio de recopilación de eventos de Windows para conectar con los orígenes de eventos de Windows externos.

Cuenta del sistema local: seleccione esta opción para ejecutar el Servicio de recopilación de eventos de Windows como usuario de cuenta del sistema local. Si selecciona esta opción, deberá especificar las credenciales del usuario al implantar el conector de eventos de Windows en el gestor de recopiladores.

El nombre de esta cuenta: Seleccione esta opción para ejecutar el Servicio de recopilación de eventos de Windows como usuario o dominio específico. Utilice las credenciales del usuario que tiene derechos para ejecutar el Servicio de recopilación de eventos de Windows.

El sistema del Servicio de recopilación de eventos de Windows debe tener acceso para leer el registro de eventos de Windows en cada sistema de origen de eventos que estará bajo supervisión. Por lo tanto, los usuarios que se creen deben tener asignados los permisos adecuados en cada sistema de origen de eventos.

Iniciar el servicio una vez instalado: seleccione esta opción si desea iniciar el Servicio de recopilación de eventos de Windows tan pronto como finalice la instalación.

10 Haga clic en *Siguiente*.

11 Haga clic en *Instalar* para instalar el Servicio de recopilación de eventos de Windows.

12 Haga clic en *Finalizar* para salir del asistente de configuración.

Una vez que esté instalado el Servicio de recopilación de eventos de Windows, debe configurarse para su funcionamiento.

Configuración del Servicio de recopilación de eventos de Windows

1 Abra el archivo `eventManagement.config` mediante un editor de archivos.

La ubicación por defecto del archivo es`Archivos de programa\Novell\SentinelWECS`.

2 En la sección <`cliente`>, copie la línea `endPoint address` y péguela debajo de la línea existente. Reemplace la dirección IP existente por la dirección IP del servidor (Gestor de recopiladores) donde se conecta el Servicio de recopilación de eventos de Windows y el número de puerto a través del cual se comunica con el conector.

Por ejemplo:

```
<client>
    <!-- Additional collectors/plugins can be
added with different host/
port configurations -->
     <!-- <endPoint address="tcp://
127.0.0.1:1024"
behaviorConfiguration="localhost" />-->
     <endPoint address="tcp://
<IP_address_Sentinel_server:<port_number>"
behaviorConfiguration="localhost" />-->
  </client>
```

3 Puede configurar tantos conectores como desee repitiendo el Paso 2. Puede configurar un agente con varios conectores o un agente con un solo conector.

4 Guarde y cierre el archivo `eventManagement.config`.

5 Abra la ventana de servicio para iniciar el Servicio de recopilación de eventos de Windows.

5a Haga clic en *Inicio* > *Ejecutar* para abrir el cuadro de diálogo Ejecutar.

5b Escriba `services.msc` y haga clic en *Aceptar*.

6 Seleccione *Servicio de recopilación de eventos de Windows de Sentinel*, luego haga clic con el botón derecho del ratón y seleccione *Inicio* para iniciar el Servicio de recopilación de eventos de Windows.

7 Cierre la ventana del servicio.

Para obtener más información sobre Microsoft Active Directory, el recopilador de Windows y el Conector de eventos de Windows (WMI), consulte la página Web de módulos auxiliares (plug-ins) de Windows (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Configuración de conectores y recopiladores adicionales

Los conectores y recopiladores disponibles se instalan en el servidor Sentinel durante la instalación de Sentinel. No obstante, a menudo hay disponibles otros conectores y recopiladores nuevos o actualizados.

Consulte la página Web de módulos auxiliares (plug-ins) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) para obtener versiones actualizadas de los conectores y recopiladores.

Si necesita configurar un conector o un recopilador que no esté configurado por defecto, consulte "Cómo añadir componentes adicionales a Sentinel" en la *Guía de instalación y configuración de NetIQ Sentinel 7.0.1*.

Pasos siguientes

Ahora ya está instalado Sentinel. Hay dos guías que 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 los usuarios que realizan 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).

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 base a 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.