AUTHORIZED DOCUMENTATION

Guía del usuario

October 31, 2008

Novell®
Identity Audit

1.0

www.novell.com

Información legal

Novell, Inc. no otorga ninguna garantía respecto al contenido y el uso de esta documentación y específicamente renuncia a cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Asimismo, Novell, Inc. se reserva el derecho a revisar esta publicación y a realizar cambios en su contenido en cualquier momento, sin obligación de notificar tales cambios a ninguna persona o entidad.

Además, Novell, Inc. no ofrece ninguna garantía con respecto a ningún software y rechaza específicamente cualquier garantía explícita o implícita de comercialización o adecuación para un fin determinado. Por otra parte, Novell, Inc. se reserva el derecho a realizar cambios en cualquiera de las partes o en la totalidad del software de Novell en cualquier momento, sin obligación de notificar tales cambios a ninguna persona ni entidad.

Los productos o la información técnica que se proporcionan bajo este Acuerdo pueden están sujetos a los controles de exportación de Estados Unidos o a la legislación sobre comercio de otros países. Usted acepta acatar las regulaciones de los controles de exportaciones y obtener todas las licencias necesarias para exportar, reexportar o importar bienes. De la misma forma, acepta no realizar exportaciones ni reexportaciones a las entidades que se incluyan en las listas actuales de exclusión de exportaciones de EE.UU., así como a ningún país terrorista o sometido a embargo, tal y como queda recogido en las leyes de exportación de los EE.UU. Asimismo, se compromete a no usar el producto para fines prohibidos, como la creación de mísiles o armas nucleares, químicas o biológicas. Consulte la página Web de International Trade Services de Novell (http://www.novell.com/info/exports/) para obtener más información sobre la exportación del software de Novell. Novell no se responsabiliza de la posibilidad de que usted no pueda obtener los permisos de exportación necesarios.

Novell, Inc. posee derechos de propiedad intelectual relacionados con la tecnología que representa el producto descrito en este documento. En concreto, y sin limitación, estos derechos de propiedad intelectual pueden incluir una o más de las patentes de EE. UU. que aparecen en la página Web de Novell sobre patentes legales (http://www.novell.com/company/legal/patents/), y una o más patentes adicionales o solicitudes de patentes pendientes en EE. UU. y en otros países.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
EE. UU.
www.novell.com

Documentación en línea: para acceder a la documentación en línea más reciente acerca de éste y otros productos de Novell, visite la página Web de documentación de Novell (http://www.novell.com/documentation).

Marcas comerciales de Novell

Para obtener información sobre las marcas comerciales de Novell, consulte la lista de marcas registradas y marcas de servicio de Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiales de otros fabricantes

Todas las marcas comerciales de otros fabricantes son propiedad de sus propietarios respectivos.

Tabla de contenido

Acerca de esta guía

En esta guía se describe la instalación y configuración de Novell® Identity Audit.

Audiencia

Esta guía está dirigida a los administradores de Novell Identity Audit.

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, o bien diríjase a www.novell.com/documentation/feedback.html e introduzca ahí sus comentarios.

Actualizaciones de la documentación

Para obtener la versión más reciente de la *Guía de Novell Identity Audit 1.0*, visite el sitio Web de documentación de Identity Audit (http://www.novell.com/documentation/identityaudit).

Convenciones de la documentación

En la documentación de Novell, los símbolos mayor que (>) se utilizan para separar acciones dentro de un paso y elementos en una ruta de referencia cruzada.

Un símbolo de marca comercial (®, ™, etc.) indica una marca comercial de Novell. Un asterisco (*) sirve para identificar una marca comercial de otro fabricante.

Introducción

1

Novell® Identity Audit facilita la elaboración de informes y supervisión de eventos para el entorno de Novell Identity and Security Management, además de Novell eDirectory™, Novell Identity Manager, Novell Access Manager, Novell Modular Authentication Services (NMAS™), Novell SecureLogin y Novell SecretStore®.

1.1 Descripción general del producto

Novell Identity Audit 1.0 es una herramienta ligera y fácil de usar para recopilar, agregar y almacenar eventos de Novell Identity Manager, Novell Access Manager, Novell eDirectory y otros productos y tecnologías de seguridad e identidad de Novell. Entre las funciones principales se incluyen:

- Interfaces de elaboración de informes y administración basadas en Web
- Herramienta de búsqueda de eventos completos que lleva a cabo la búsqueda entre diversos campos de evento.
- Salida de evento seleccionada para varios canales
- Motor integrado Jasper Reports para permitir el uso de herramientas de código abierto con el fin de personalizar los informes incluidos o de crear nuevos informes.
- Base de datos integrada que elimina la necesidad de administración o licencias de bases de datos externas
- Herramientas sencillas e intuitivas de gestión de datos

1.1.1 Comparación con Novell Audit 2.0.2

Novell Identity Audit 1.0 está diseñado como un producto de sustitución para la línea de productos de Novell Audit, cuya compatibilidad general será posible en febrero de 2009. Se puede establecer una equiparación con Identity Audit en cuanto a funciones, pero además incluye mejoras importantes en cuanto a arquitectura, elaboración de informes y gestión de datos. Novell Identity Audit 1.0 es una sustitución de paso para el Servidor de registro con seguridad de Novell Audit 2.0.2 para los productos de la línea de productos de la Gestión de identidades y seguridad de acceso y de seguridad. Debido a que Novell Identity Audit utiliza una nueva base de datos integrada, los clientes deben conservar los eventos existentes de Novell Audit en la base de datos archivada de Novell Audit, en lugar de intentar migrar datos heredados.

El componente del cliente Novell Audit, también conocido como Agente de la plataforma, se sigue utilizando como el mecanismo de transferencia de datos de Novell Identity Audit. Éste continuará siendo compatible, de acuerdo con los ciclos de vida de los productos Access Management y Novell Identity que sigan empleando el Agente de la plataforma.

1.1.2 Comparación con Novell Sentinel

Novell Identity Audit se integra en una fundación tecnológica sólida, ya que la mayor parte del código subyacente se comparte con Novell Sentinel. Sin embargo, Sentinel recopila datos de una gama más amplia de dispositivos, admite una velocidad de eventos superior e incluye más herramientas que Novell Identity Audit. Sentinel también ofrece funciones adicionales de Security Information and Event Management (SIEM), como paneles en tiempo real, correlación de múltiples eventos, seguimiento de incidentes, soluciones automáticas y recopilación de datos de productos no pertenecientes a Novell. Identity Audit está diseñado para integrarse en implementaciones futuras de Sentinel.

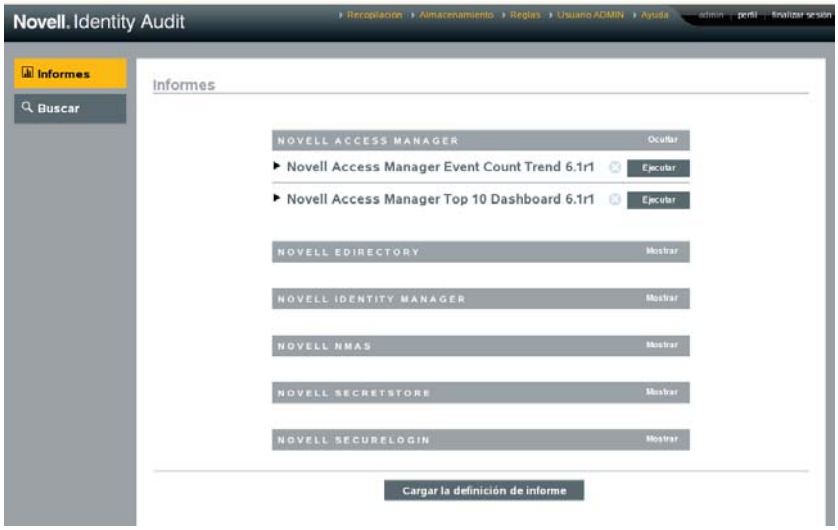
Novell Identity Audit 1.0 no forma parte de la plataforma CMP (Compliance Management Platform) de Novell y no incluye las funciones avanzadas de integración de seguridad e identidad que se ofrecen en dicha plataforma. Actualmente, Sentinel 6.1 es el componente de monitorización y auditoría de identidad de la CMP.

1.2 Interfaz

La interfaz Web de Novell Identity Audit permite desarrollar las siguientes tareas:

- Cargar, ejecutar, ver y suprimir informes
- Buscar eventos
- Editar detalles del perfil de usuario
- Crear, editar y eliminar usuarios, así como asignar derechos administrativos (sólo administradores)
- Configurar la recopilación de datos y ver el estado de orígenes de eventos (sólo administrador)
- Configurar el almacenamiento de datos y ver el estado de la base de datos (sólo administradores)
- Crear reglas de filtrado y configurar acciones asociadas para enviar los datos de evento coincidentes a los canales de salida (sólo para los administradores).

Figura 1-1 *Interfaz de Novell Identity Audit (vista de administrador)*



La interfaz se actualiza automáticamente cada 30 segundos para mostrar las actualizaciones de otros usuarios, si procede.

La interfaz está disponible en varios idiomas (inglés, francés, alemán, italiano, japonés, portugués, español, chino simplificado y chino tradicional). La interfaz aparece en el idioma por defecto del navegador, pero el usuario puede seleccionar otro idioma al entrar en la sesión.

Nota: Aunque la interfaz está localizada en los idiomas de bytes dobles, la versión actual de Identity Audit no procesa los datos de evento de bytes dobles.

1.3 Arquitectura

Identity Audit recopila datos de diferentes aplicaciones de Gestión de identidades y seguridad de acceso de Novell. Estos servidores de la aplicación están configurados para generar registros de eventos y cada uno aloja un Agente de plataforma, que forma parte de la aplicación Novell Audit. El Agente de plataforma reenvía los datos de evento al conector de Audit que se encuentra en el servidor Identity Audit.

El Conector de Audit pasa eventos al componente de recopilación de datos, que analiza dichos eventos y los ubica en el bus de comunicaciones, que es el segmento principal del sistema y, además, actúa como intermediario en todas las comunicaciones que se establecen entre los componentes. El conjunto de reglas de filtrado se encarga de evaluar los eventos entrantes como parte de la recopilación de datos. Dichas reglas filtran eventos y los envían a los canales de salida como un archivo, una transmisión de syslog, un

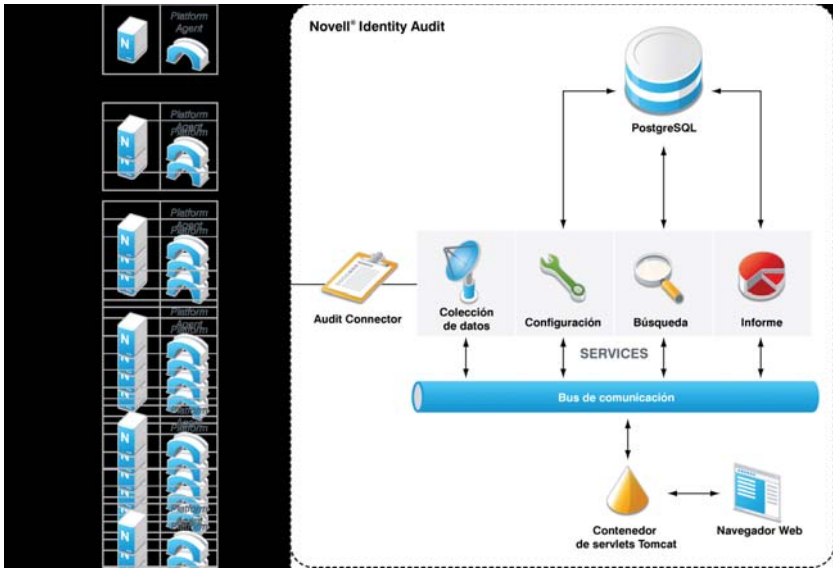
Además, todos los eventos se almacenan en la base de datos de Identity Audit (impulsado por PostgreSQL*) en tablas de partición.

El componente Configuración recupera, añade y modifica la información de configuración como la recopilación de datos, los ajustes de almacenamiento, las definiciones de reglas y las de informes. También gestiona la autenticación del usuario.

El componente de búsqueda realiza búsquedas indexadas rápidas y recupera los eventos de la base de datos para presentarle los conjuntos de resultados al usuario.

El componente de generación de informes ejecuta los informes y formatea los resultados del informe.

Figura 1-2 *Arquitectura de Identity Audit*



Los usuarios interactúan con el servidor de Identity Audit y con todas sus funciones a través de un navegador Web, que establece conexión con un servidor Web de Apache Tomcat. El servidor Web realiza llamadas a varios componentes de Identity Audit a través del bus de comunicaciones.

Requisitos del sistema

2

Además de los requisitos de compatibilidad con el origen del evento, el navegador, el sistema operativo y el hardware que se describen a continuación, la instalación requiere un acceso como usuario root al sistema operativo con el fin de crear el usuario novell y el grupo novell, propietarios de los procesos de ejecución de Identity Audit.

2.1 Requisitos del hardware

Novell Identity Audit™ es compatible con procesadores Intel Xeon* y AMD Opteron* de 64 bits. No es compatible con procesadores de Itanium. Novell recomienda el siguiente hardware para un sistema de producción que mantendrá datos conectados durante 90 días:

- 1x Quad Core (x86-64)
- 16 GB de RAM
- 1,5 TB de espacio disponible en disco: 3 x 500 GB (3 utilizables), 10 K RPM unidades en la configuración RAID de hardware.
  - 2/3 del espacio de disco disponible aproximadamente se usan para los archivos de la base de datos.
  - 1/3 del espacio de disco disponible aproximadamente se usa para el índice de búsqueda y para los archivos temporales.
  - La capacidad de almacenamiento disponible para los datos archivados que se han eliminado de la base de datos es pequeña, pero Novell recomienda que los datos archivados se muevan a otro medio.

Tabla 2-1 *Rendimiento*

Métrica	Valor	Descripción
Eventos por segundo (eps): modo fijo	100	Velocidad media del evento durante operaciones normales
Eventos por segundo (eps): pico	500	Velocidad del evento de pico durante un remate (hasta 10 minutos)

Métrica	Valor	Descripción
Eventos por segundo (eps): pico por aplicación	300	Velocidad del evento de pico según el tipo de aplicación de Novell ◆ Las velocidades de eventos normalmente son bajas (inferiores a 15 eps) para el gestor de Identity, SecureLogin, SecretStore® y NMAS™). ◆ Las velocidades de eventos pueden ser muy altas en eDirectory™ y Access Manager. El filtrado de eventos se debe implementar para garantizar una velocidad que se pueda gestionar. ◆ Incluso durante el momento cumbre del evento, ninguna aplicación puede enviar más de esta cantidad de eventos por segundo.
Datos con conexión	90 días o 750 millones de eventos	La cantidad de datos que Identity Audit puede almacenar a una velocidad fija de 100 eps con la capacidad de almacenamiento recomendada.

2.2 Sistemas operativos compatibles

Se certifica que Identity Audit puede ejecutarse en el servidor SuSE Linux Enterprise Server™ 10 SP1 y SP2 de 64 bits.

2.3 Navegadores compatibles

Identity Audit admite los siguientes navegadores. Puede que otros navegadores no muestren la información de la forma prevista.

Tabla 2-2 *Navegadores Web compatibles con Novell Identity Audit*

Navegador Web y versión
Mozilla Firefox 2
Mozilla Firefox 3
Microsoft Internet Explorer 7

El rendimiento de las búsquedas y la visualización de los informes parecen variar en función del navegador. Novell ha experimentado un rendimiento especial con Mozilla Firefox 3.

2.4 Agente de plataforma admitido

Identity Audit 1.0 admite la recopilación de eventos de registro de muchas aplicaciones compatibles con Novell Audit y su Agente de plataforma. Para los orígenes de eventos de 32 bits, se necesita la versión 2.0.2 FP6 (2.0.2.55) del Agente de plataforma o posterior para Identity Audit. Para las fuentes de eventos de 64 bits, se necesita la versión 2.0.2 FP6 del Agente de plataforma.

Nota: Algunas aplicaciones de Novell se incluyen agrupadas con una versión anterior del Agente de la plataforma. La versión recomendada incluye importantes correcciones de errores, por ello Novell recomienda actualizar el Agente de la plataforma.

2.5 Orígenes de eventos admitidos

Identity Audit admite la recopilación de datos de las aplicaciones de Gestión de identidades y seguridad de acceso de Novell. Algunas aplicaciones necesitan un nivel de parche específico para recopilar los datos correctamente.

Tabla 2-3 *Aplicaciones compatibles con Novell Identity Audit*

Aplicación
Access Manager 3.0 de Novell
Novell eDirectory 8.8.3 con el parche de utilidades de eDirectory que se encuentra en el Sitio Web de asistencia de Novell (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~).
Gestor de identidades 3.6 de Novell
Novell NMAS 3.1
Novell SecretStore 3.4
Novell SecureLogin 6.0

Instalación

3

Este capítulo explica cómo instalar Novell Identity Audit y configurar los orígenes de eventos para enviar datos a este programa. En dichas instrucciones, se presupone que se cumplen los requisitos mínimos para cada componente de sistema. Para obtener más información, consulte Capítulo 2, "Requisitos del sistema", en la página 13.

3.1 Instalación de Novell Identity Audit

El paquete de instalación de Identity Audit instala todo lo necesario para ejecutar este programa: el bus de mensajes y aplicación de Identity Audit, la base de datos para almacenar eventos, la información de configuración, la interfaz de usuario basada en la Web y el servidor de informes. Existen dos opciones de instalación: una instalación simple que puede ejecutarse como usuario root o una instalación de varios pasos que utiliza el modo root lo menos posible.

3.1.1 Instalación rápida (como usuario root)

La instalación simple debe ejecutarse como usuario root.

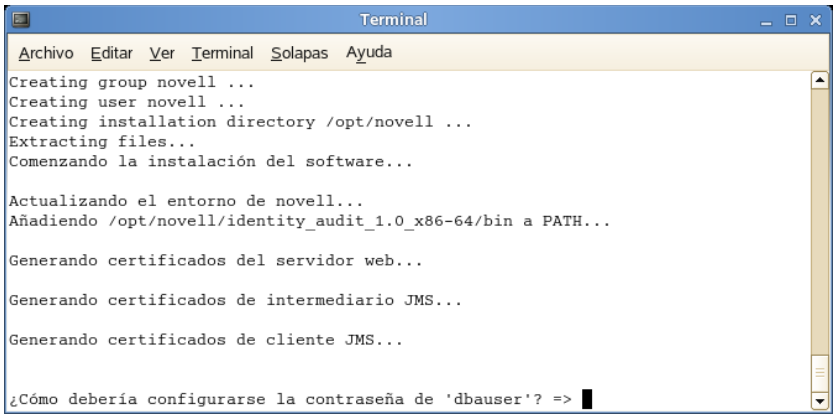
1. Entre como usuario `root` en el servidor en el que desea instalar Identity Audit.
2. Descargue o copie `identity_audit_1.0_x86-64.tar.gz` en un directorio temporal.
3. Extraiga el guión de instalación del archivo por medio del siguiente comando:

   ```
   tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup/root_install_all.sh
   ```
4. Ejecute el guión `root_install_all.sh` por medio del siguiente comando:

   ```
   identity_audit_1.0_x86-64/setup/root_install_all.sh identity_audit_1.0_x86-64.tar.gz
   ```
5. Introduzca un número para elegir un idioma.

   El Acuerdo de licencia de usuario se muestra en el idioma seleccionado.
6. Lea la licencia de usuario final e introduzca `1` o `y` si acepta los términos y desea continuar con la instalación.

   La instalación comenzará. En caso de que el idioma seleccionado no esté disponible para el instalador (por ejemplo, español), el instalador continuará en inglés.



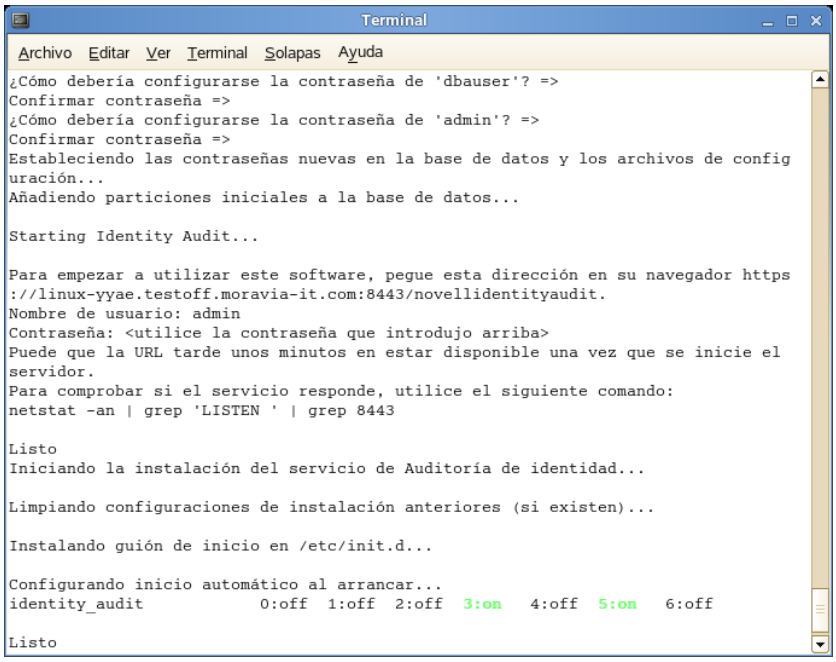
Se crearán el usuario de Novell y el grupo de Novell, en caso de que aún no existan.

7 Introduzca la contraseña para el administrador de la base de datos (dbauser).

8 Confirme la contraseña para el administrador de la base de datos (dbauser).

9 Introduzca la contraseña del usuario ADMIN.

10 Confirme la contraseña del usuario ADMIN.



Las credenciales de dbauser se emplean para crear tablas y particiones en la base de datos de PostgreSQL. Identity Audit está configurado para iniciarse con los niveles del tiempo de ejecución 3 y 5 (modo multiusuario con reinicio en la consola o con el modo X-Windows).

Una vez que se inicie el servicio Identity Audit, puede entrar en la URL especificada al finalizar la instalación (https://hostIP:8443/novellidentityaudit). El sistema empezará a procesar los eventos de auditoría interna inmediatamente y estará totalmente operativo en cuanto configure los orígenes del evento para enviar los datos a Identity Audit.

3.1.2 Instalación non-root

Si la directiva administrativa prohíbe la ejecución del proceso de instalación completa como usuario `root`, la instalación podrá ejecutarse en dos pasos. La primera parte del proceso de instalación debe desarrollarse con un acceso de nivel de raíz y la segunda se lleva a cabo como usuario administrativo de Identity Audit (creado durante la primera parte).

1. Entre como usuario `root` en el servidor en el que desea instalar Identity Audit.
2. Descargue o copie `identity_audit_1.0_x86-64.tar.gz` al directorio `/tmp`.
3. A menos que el usuario de Novell y el grupo de Novell ya existan en el servidor:
   1. Extraiga el guión para crear el usuario de Novell y el grupo de Novell desde el archivo tar de Identity Audit. Por ejemplo:
      ```
      tar xfz identity_audit_1.0_x86-64.tar.gz
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
   2. Como `root`, ejecute el guión por medio de este comando:
      ```
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
      El usuario de Novell y el grupo de Novell reconocerán los procesos de instalación y ejecución de Identity Audit.
4. Cree un directorio para Identity Audit. Por ejemplo:

   mkdir -p /opt/*novell*
5. Configure el directorio para que el usuario de Novell y el grupo de Novell lo reconozcan. Por ejemplo:
   ```
   chown -R novell:novell /opt/novell
   ```
6. Entre en la sesión como usuario de Novell:
   ```
   su novell
   ```
7. Extraiga el archivo tar de Identity Audit al directorio que acaba de crear. Por ejemplo:
   ```
   cd /opt/novell
   tar xfz /tmp/identity_audit_1.0_x86-64.tar.gz
   ```
8. Ejecute el guión de instalación. Por ejemplo:
   ```
   /opt/novell/identity_audit_1.0_x86-64/setup/install.sh
   ```
9. Introduzca un número para elegir un idioma.

   El Acuerdo de licencia de usuario se muestra en el idioma seleccionado.
10. Lea la licencia de usuario final e introduzca `1` o `y` si acepta los términos y desea continuar con la instalación.

    La instalación comenzará. En caso de que el idioma seleccionado no esté disponible para el instalador (por ejemplo, español), éste continuará en inglés.

```
Comenzando la instalación del software...

Actualizando el entorno de novell...
Añadiendo /opt/novell/identity_audit_1.0_x86-64/bin a PATH...

Generando certificados del servidor web...

Generando certificados de intermediario JMS...

Generando certificados de cliente JMS...


¿Cómo debería configurarse la contraseña de 'dbauser'? =>
```

11 Introduzca la contraseña para el administrador de la base de datos (dbauser)

12 Confirme la contraseña para el administrador de la base de datos (dbauser)

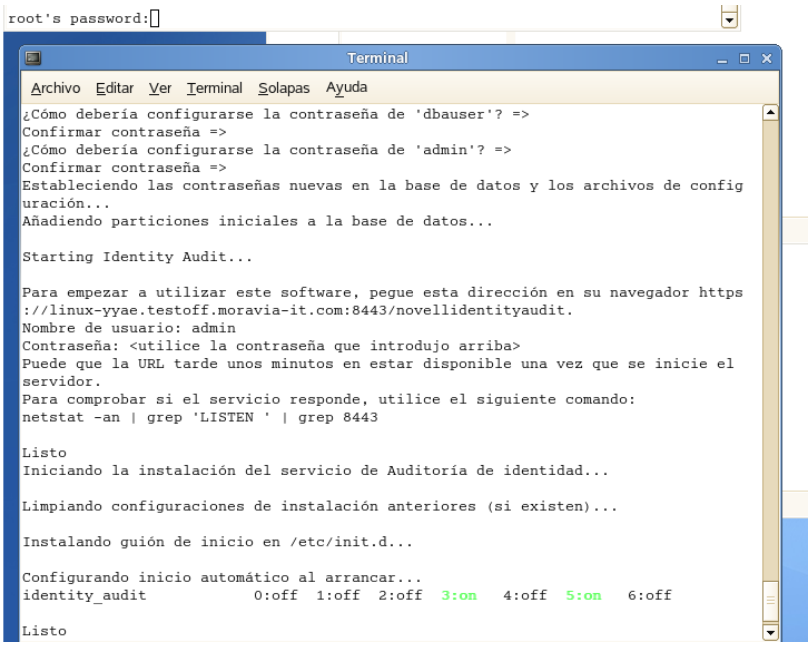
13 Introduzca la contraseña del usuario ADMIN.

14 Confirme la contraseña del usuario ADMIN.

15 Cierre la sesión y vuelva a iniciarla como usuario de Novell. De este modo, se cargarán los cambios realizados por el guión `install.sh` en la variable de entorno PATH.

16 Ejecute el guión `root_install_service.sh` para habilitar el inicio de Identity Audit como servicio. Este paso requiere un acceso de nivel `raíz`. Por ejemplo:

```
sudo /opt/novell/identity_audit_1.0_x86-64/setup/
root_install_service.sh
```



17 Introduzca la contraseña del usuario `root`.

Identity Audit está configurado para iniciarse con los niveles del tiempo de ejecución 3 y 5 (modo multiusuario con reinicio en la consola o con el modo X-Windows).

Una vez que se inicie el servicio Identity Audit, puede registrarse en la URL especificada al finalizar la instalación (https://hostIP:8443/novellidentityaudit). El sistema empezará a procesar los eventos de auditoría interna inmediatamente y estará totalmente operativo en cuanto configure los orígenes del evento para enviar los datos a Identity Audit.

3.2 Configuración de orígenes de eventos

Identity Audit 1.0 admite la recopilación de eventos de registro de las aplicaciones compatibles con el producto anterior de Novell Audit y su Agente de plataforma. Antes de finalizar los pasos de esta sección, asegúrese de que los productos de Novell de los que dispone son compatibles. Para obtener más información, consulte Sección 2.4, “Agente de plataforma admitido”, en la página 14.

3.2.1 Instalación del Agente de plataforma

El Agente de plataforma se debe corresponder, al menos, con la versión mínima recomendada para Identity Audit. Para obtener más información, consulte Sección 2.4, “Agente de plataforma admitido”, en la página 14. El Agente de plataforma adecuado (32 o 64 bits) debe instalarse o actualizarse en todos los equipos de orígenes de eventos. El Agente de plataforma se incluye con la descarga de Novell Audit que se encuentra disponible en el sitio Web de descarga de Novell (http://download.novell.com).

Para instalar o actualizar el Agente de plataforma de 32 bits:

1. Descargue el archivo `iso` para la versión Audit 2.0.2 FP6 o posterior en el directorio /tmp del equipo del origen de eventos.
2. Cree un directorio para Audit. Por ejemplo, `mkdir -p audit202fp6`
3. Entre a la sesión como usuario `Root`.
4. Montar el archivo `iso` de Audit.

   ```
   mount -o loop ./NAudit202.iso./audit202fp6
   ```
5. Ir al directorio `audit202fp6`
6. Vaya al directorio apropiado del sistema operativo del origen del evento. Por ejemplo:

   ```
   cd Linux
   ```
7. Ejecute `pinstall.lin`

   ```
   ./pinstall.lin
   ```
8. Lea el Acuerdo de licencia y escriba `y` si está de acuerdo con los términos.
9. Escriba `P` para instalar el Agente de plataforma.
10. Escriba `Y` para mantener las configuraciones anteriores del archivo `logevent.conf`.

    El Agente de plataforma está instalado.
11. Para verificar que la versión del Agente de plataforma es correcta, introduzca el siguiente comando:

    ```
    rpm -qa | grep AUDT
    ```

La versión de novell-AUDTplatformagent debe ser, como mínimo, la versión compatible que se enumera en Sección 2.4, “Agente de plataforma admitido”, en la página 14.

Para instalar o actualizar el Agente de plataforma de 64 bits, descargue NAudit 2.0.2 FP6 y siga las instrucciones que se incluyen en el parche.

3.2.2 Configuración del Agente de plataforma

Después de la instalación, se debe configurar el Agente de plataforma para enviar datos al servidor de Identity Audit y, si lo desea, para enviar firmas del evento desde los orígenes de los eventos.

Advertencia: La configuración del Agente de plataforma para generar firmas puede afectar de forma negativa al rendimiento de los equipos del origen del evento.

Para configurar el Agente de plataforma:

1. Registrarse en el equipo del origen del evento.
2. Abra el archivo `logevent` para editarlo. La ubicación del archivo depende del sistema operativo:
   - Linux: `/etc/logevent.conf`
   - Windows: `C:\WINDOWS\logevent.cfg`
   - NetWare: `SYS:\etc\logevent.cfg`
   - Solaris: `/etc/logevent.conf`
3. Ajustar LogHost a la dirección IP del servidor de Identity Audit.
4. Ajustar LogEnginePort=1289. (Añada esta entrada en caso de que aún no exista).
5. Si desea que el origen del evento envíe firmas de eventos, introduzca LogSigned=always.
6. Guarde el archivo.
7. Reinicie el Agente de plataforma. El método varía en función del sistema operativo y de la aplicación. Reinicie el equipo o consulte la documentación específica de la aplicación que se encuentra en el sitio Web de documentación de Novell (http://www.novell.com/documentation) para obtener más instrucciones.

3.2.3 Configuración del nivel de auditoría.

Los eventos para los que cada aplicación crea informes están configurados de forma diferente para cada una de las aplicaciones que controla Identity Audit. Las URL que aparecen a continuación contienen más información sobre cada aplicación.

- Access Manager (http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b8cvd2l.html#b8cvd2l)
- eDirectory (http://www.novell.com/documentation/novellaudit20/index.html?page=/documentation/novellaudit20/novellaudit20/data/b296n3h.html)
- Gestor de identidades (http://www.novell.com/documentation/idm36/idm_sentinel/data/bookinfo.html)
- NMAS (http://www.novell.com/documentation/nmas32/admin/index.html?page=/documentation/nmas32/admin/data/ahefojr.html)

- SecretStore (http://www.novell.com/documentation/secretstore33/index.html?page=/documentation/secretstore33/nssadm/data/bsqdjxv.htm)
- SecureLogin (http://www.novell.com/documentation/securelogin60/index.html (see the Auditing link))

3.3 Inicio

El usuario administrativo creado durante la instalación puede acceder a la aplicación de Identity Audit y crear más usuarios, ejecutar informes cargados con anterioridad, cargar nuevos informes, llevar a cabo búsquedas de eventos y mucho más.

Para entrar en Identity Audit:

1. Abra un navegador Web compatible. Para obtener más información, consulte Sección 2.3, “Navegadores compatibles”, en la página 14.
2. Vaya a la página de inicio de sesión de Identity Audit (https://hostIP:8443/novellidentityaudit).
3. Si es la primera vez que ha accedido a Identity Audit, recibirá un certificado como presentación. Tiene que aceptarlo para continuar.
4. Introduzca `admin`.
5. Introduzca la contraseña de administrador que configuró durante la instalación.
6. Seleccione el idioma de la interfaz de Identity Audit (inglés, portugués, francés, italiano, alemán, español, japonés, chino tradicional o chino simplificado).
7. Haga clic en *Entrar*.

3.4 Desinstalación

Para limpiar completamente la instalación de Identity Audit, debe ejecutar el guión de desinstalación y, a continuación, desarrollar una serie de pasos de limpieza.

1. Acceda al servidor de Identity Audit como `root`.
2. Detener el servicio de Identity Audit:
   ```
   /etc/init.d/identity_audit stop
   ```
3. Ejecute el guión de desinstalación:
   ```
   /opt/novell/identity_audit_1.0_x86-64/setup/
   root_uninstall_service.sh
   ```
4. Eliminar el directorio principal de Identity Audit y sus contenidos.
   ```
   rm -rf /opt/novell/identity_audit_1.0_x86-64
   ```
5. Los pasos finales dependen de si desea mantener cualquier información relacionada con el grupo y usuario de Novell.
   - Si no desea mantener información relacionada con el usuario de Novell, ejecute el siguiente comando para eliminar el usuario, el directorio personal y el grupo:
     ```
     userdel -r novell && groupdel novell
     ```
   - Si desea mantener el usuario de Novell y su directorio personal, pero desea eliminar todos los ajustes relacionados con Identity Audity, siga los siguientes pasos:
     1. Elimine las siguientes entradas de la variable de entorno para Identity Audit desde el perfil del usuario de Novell (en `~novell/.bashrc`):

```
APP_HOME=/opt/novell/identity_audit_1.0_x86-64 export
PATH=$APP_HOME/bin:$PATH
```

2. Elimine la entrada dbauser del archivo de `~novell/.pgpass`.
   `*:*:*:dbauser:`*`contraseña`*

Nota: Aunque el texto de la contraseña de dbauser es claro, sólo pueden ver el contenido de este archivo los usuarios de novell y los usuarios root, quienes aún cuentan con permiso de acceso pleno a todas las funciones del servidor de Identity Audit.

Búsqueda

4

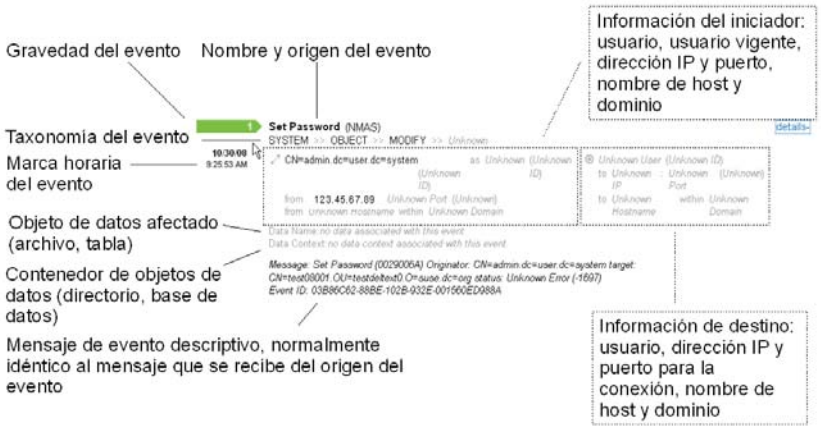
Esta sección describe las funciones de búsqueda de Novell® Identity Audit.

4.1 Descripción general de la búsqueda de eventos

Novell Identity Audit permite realizar búsquedas en los eventos. La búsqueda incluye todos los datos en línea que se encuentran actualmente en la base de datos, pero se excluyen los eventos internos generados por Identity Audit, a menos que el usuario seleccione la opción *Incluir eventos del sistema*. Por defecto, los eventos se almacenan en función del algoritmo de relevancia del motor de búsqueda.

La información básica del evento incluye el nombre del evento, el origen, la fecha, la gravedad, la información sobre el iniciador (representado por el icono de una flecha) e información acerca del destino (representado por el icono de una diana).

Figura 4-1 *Campos de eventos*



4.2 Ejecución de una búsqueda de evento

Los usuarios pueden ejecutar búsquedas simples y avanzadas.

- Sección 4.2.1, “Búsqueda básica”, en la página 26
- Sección 4.2.2, “Búsqueda avanzada”, en la página 27

4.2.1 Búsqueda básica

Se ejecuta una búsqueda básica entre todos los campos de evento de Tabla 4-1 en la página 30. Algunas búsquedas básicas de muestra incluyen lo siguiente:

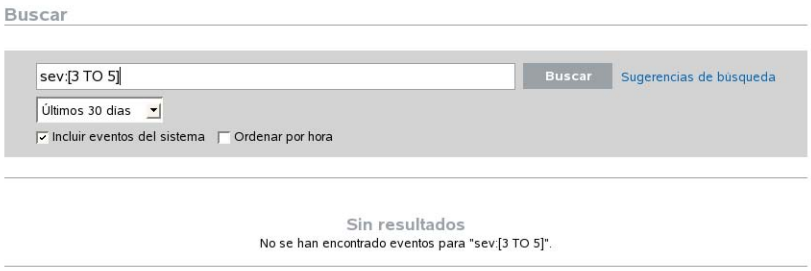
- `root`
- `127.0.0.1`
- `Bloquear*`
- `driverset0`

Nota: Si la hora no está sincronizada entre el equipo del usuario y el servidor de Identity Audit (por ejemplo, un equipo va 25 minutos atrasado), es posible que obtenga resultados que no desea al realizar la búsqueda. Las búsquedas como *La última hora* o *Las últimas 24 horas* se basan en la hora del equipo del usuario final.

---

1. Haga clic en el enlace *Buscar* situado a la izquierda.

   Identity Audit está configurado para ejecutar una búsqueda por defecto para eventos que no pertenecen al sistema con una gravedad comprendida entre 3 y 5 la primera vez que el usuario hace clic en el enlace *Buscar*. De lo contrario, por defecto, volverá al último término de búsqueda que el usuario haya introducido.



2. Para realizar una búsqueda diferente, escriba un término de búsqueda en el campo de búsqueda (por ejemplo, `admin`). La búsqueda no distingue entre mayúsculas y minúsculas.
3. Seleccione el período de tiempo para el que desea que se realice la búsqueda. La mayoría de las configuraciones de tiempo se explican por sí solas y el período predeterminado es *Los últimos 30 días*.
   - La opción *Personalizar* le permite seleccionar las fechas y horas de inicio y de finalización de la consulta. La fecha de inicio debe ser anterior a la fecha final y la hora se basa en
   - *Todos los períodos* busca en todos los datos de la base de datos.

4 Seleccione *Incluir eventos del sistema* para que se incluyan los eventos que se generan como resultado de las operaciones del sistema Identity Audit.

5 Seleccione *Ordenar por hora*

Nota: La clasificación por hora lleva más tiempo que la clasificación por relevancia, que es la predeterminada.

---

6 Haga clic en *Buscar*.

Todos los campos del índice se buscan para encontrar el texto específico. Un icono giratorio indica que se está realizando la búsqueda.

Aparecen los resúmenes de evento.

4.2.2 Búsqueda avanzada

Mediante la búsqueda avanzada se puede buscar un valor determinado en un campo o campos de evento específicos. Los criterios de búsqueda avanzada se basan en los nombres abreviados de cada campo de evento y la lógica de búsqueda del índice. La siguiente tabla describe los campos, facilita los nombres abreviados para la búsqueda avanzada e indica si los campos se pueden ver en la vista de eventos detallada o la básica.

Para buscar un valor en un campo determinado, use el nombre corto del campo (para obtener más información, consulte Tabla 4-1 en la página 30), dos puntos y el valor. Por ejemplo, para buscar un intento de autenticación de user2 en Identity Audit, introduzca el siguiente texto en el campo de búsqueda:

- `evt:authentication AND sun:user2`
- `pn:NMAS AND sev:5`
- `sip:123.45.67.89 AND evt:"Ajustar contraseña"`

Se pueden combinar diferentes criterios de búsqueda avanzada por medio de los siguientes operadores booleanos:

- AND (debe escribirse con mayúsculas)
- OR (debe escribirse con mayúsculas)

- NOT (debe escribirse con mayúsculas y no se puede utilizar como criterio exclusivo de búsqueda)
- +
- -

Los caracteres especiales deben establecerse como secuencia de escape con un símbolo \:
`+ - && || ! ( ) { } [ ] ^ " ~ * ? : \`

Los criterios de búsqueda avanzada se rigen por los criterios de búsqueda del paquete de código abierto Apache Lucene. Para obtener más información sobre los criterios de búsqueda, visite la página Web: Lucene Query Parser Syntax (http://lucene.apache.org/java/2_3_2/queryparsersyntax.html).

4.3 Visualización de los resultados de búsqueda

La búsqueda ofrece como resultado un conjunto de eventos. Los usuarios pueden ver información de eventos detallada o básica, así como configurar el número de resultados por página. Los resultados de búsqueda se muestran por lotes. El tamaño predeterminado de los lotes es de 25 resultados, pero esto se puede modificar fácilmente.

- Sección 4.3.1, “Vista básica del evento”, en la página 28
- Sección 4.3.2, “Vista del evento con detalles”, en la página 29
- Sección 4.3.3, “Definir los resultados de búsqueda”, en la página 29

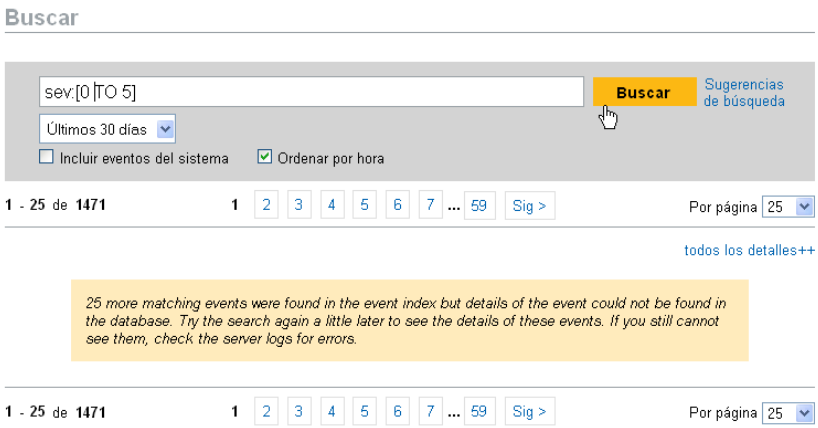
4.3.1 Vista básica del evento

La información de los eventos se clasifica en Información de iniciador e Información de destino. Si determinados datos no están disponibles para un campo de evento en concreto, los campos se etiquetan como *Desconocidos*.

Figura 4-2 *Vista básica del evento*

De forma ocasional, el motor de búsqueda puede indexar los eventos más rápido que si se insertaran en la base de datos. En caso de que el usuario ejecute una búsqueda que le devuelva eventos que no se han incluido en la base de datos, el usuario obtendrá un mensaje en el que se le indicará que algunos números de eventos coinciden con la solicitud de búsqueda pero no se pueden encontrar en la base de datos. Por norma general, si la búsqueda se realiza posteriormente, los eventos se encontrarán en la base de datos y la búsqueda se realizará con éxito.

Figura 4-3 *Eventos indexados que aún no se encuentran en la base de datos.*



4.3.2 Vista del evento con detalles

Los usuarios pueden ver detalles adicionales sobre cualquier evento haciendo clic en el enlace *detalles* situado en el lateral derecho de la página. Los detalles de todos los eventos de una página pueden ampliarse o contraerse a través de los enlaces All Details++ o *All Details--*. Esta preferencia se mantiene mientras navega por varias páginas de resultados o ejecuta nuevas búsquedas.

Figura 4-4 *Vista del evento con detalles*

El evento anterior muestra el mismo evento que en Figura 4-2 en la página 28, pero con una vista ampliada que muestra campos de datos adicionales que pueden haberse publicado.

4.3.3 Definir los resultados de búsqueda

Después de ver los resultados de una búsqueda, puede que sea necesario volver a definir los resultados y añadir criterios adicionales de búsqueda. Por ejemplo, puede que aparezca el nombre del usuario iniciador varias veces en los resultados de búsqueda y desee ver más eventos de dicho iniciador.

Para filtrar los resultados de búsqueda de un valor específico que aparezca en los resultados de búsqueda:

1. Identifique los criterios del filtro que desee aplicar en los resultados de la búsqueda.
2. Haga clic en el valor (por ejemplo, el nombre de host de destino test1900) mediante el cual desearía filtrar los resultados.

Sugerencia: Así se añade el valor al filtro con el operador AND. Para añadir el valor al filtro con un operador NOT, pulse la tecla Alt mientras hace clic en el valor.

3 Haga clic en *Buscar*.

Algunos campos no se pueden seleccionar para restringir la búsqueda de esta forma:

- EventTime
- Mensaje
- Cualquier campo relacionado con el Generador de informes
- Cualquier campo relacionado con el observador
- Cualquier campo con un valor `Desconocido`

4.4 Campos de eventos

Cada evento contiene campos que pueden o no publicarse en función del evento determinado. Los valores para dichos campos de eventos se pueden visualizar mediante una búsqueda o mediante la ejecución de un informe. Cada campo contiene un nombre abreviado que se usa en las búsquedas avanzadas. Los valores para la mayoría de dichos campos se muestran en la vista detallada del evento. Otros valores también se ven en la vista básica del evento.

Tabla 4-1 *Campos de eventos*

Campo	Nombre abreviado	Descripción	Visible en la Vista básica	Visible en la Vista detallada
Gravedad	gra	Gravedad del evento en una escala de 0 (informativo) a 5 (crítico)	X	X

Campo	Nombre abreviado	Descripción	Visible en la Vista básica	Visible en la Vista detallada
EventTime	dt	Marca de hora del evento Puede ser la marca de hora del servidor Identity Audit o la marca de hora original del origen del evento (si está habilitado “marca de evento de confianza”).	X	X
EventName	evt	Nombre abreviado del evento	X	X
Mensaje	msg	Mensaje detallado del evento		X
NombreProducto	pn	Producto que generó el evento; origen del evento. Se muestra después del nombre del evento.	X	X
InitUserName	sun	Nombre de usuario del usuario que inició el evento	X	X
InitUserID	iuid	ID de usuario del usuario que inició el evento		X
InitUserDomain	rv35	Dominio del usuario que inició el evento Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		
InitHostName	shn	Nombre del host del equipo desde el que se inició el evento	X	X
InitHostDomain	rv42	Dominio del equipo desde el que se inició el evento	X	X
InitIP	sip	Dirección IP del equipo desde el que se inició el evento		X
InitServicePort	spint	Número de puerto desde el que se inició el evento (por ejemplo, HTTP)		X
InitServicePortName	sp	Tipo de puerto desde el que se inició el evento (por ejemplo, HTTP)		X
TargetUserName	dun	Nombre de usuario del usuario de destino del evento	X	X
TargetUserID	tuid	ID de usuario del usuario de destino del evento		X
TargetUserDomain	rv35	Dominio del usuario de destino del evento Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		X
TargetHostName	dhn	Nombre del host del equipo de destino del evento	X	X
TargetHostDomain	rv45	Dominio del equipo de destino del evento	X	X

Campo	Nombre abreviado	Descripción	Visible en la Vista básica	Visible en la Vista detallada
TargetIP	dip	Dirección IP del equipo de destino del evento		X
TargetServicePort	dpint	Número del puerto de destino del evento (por ejemplo, 80)		X
TargetServicePortName	dp	Tipo del puerto de destino del evento (por ejemplo, HTTP)		X
TargetTrustName	ttn	Función del usuario de destino del evento (por ejemplo, administrador financiero) Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		
TargetTrustID	ttid	ID numérico que representa la función del usuario de destino del evento Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		
TargetTrustDomain	ttd	Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		
EffectiveUserName	euname	El nombre del usuario al que InitUser está representando (`root` que emplea `su`, por ejemplo); sigue al *Nombre de usuario del iniciador (ID del usuario iniciador) como aparece* en la vista detallada del evento.		X
EffectiveUserID	euid	ID numérico del usuario al que InitUser está representando (`root` que emplea `su`, por ejemplo)		X
ObserverHostName	sn	Nombre del host del equipo que remitió el evento al sistema de gestión de eventos de información de seguridad (por ejemplo, el nombre del host de un servidor syslog) Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		
ObserverHostDomain	obsdom	Dominio del equipo que remitió el evento al sistema de gestión de eventos de información de seguridad (por ejemplo, el dominio de un servidor syslog) Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		
ObserverIP	obsip	Dirección IP del equipo que remitió el evento al sistema de gestión de eventos de información de seguridad (por ejemplo, la dirección IP de un servidor syslog) Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		

Campo	Nombre abreviado	Descripción	Visible en la Vista básica	Visible en la Vista detallada
ReporterHostName	rn	Nombre del host del equipo que informó del evento a un observador Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		
ReporterHostDomain	repdom	Dominio del equipo que informó del evento a un observador Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		
ReporterIP	repip	Dirección IP del equipo que informó del evento a un observador Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		
SensorType	st	El designador de caracteres únicos para el tipo de sensor (N=red, H=host, O=sistema operativo, A e I=eventos de auditoría de Identity Audit, P=eventos de rendimiento de Identity Audit). Se puede buscar, pero no se puede mostrar en ninguna vista de evento.		
DataName	es	Nombre del objeto de datos del que se informa en el evento (por ejemplo, el nombre del archivo o el nombre de la tabla de la base de datos)		X
DataContext	rv36	El contenedor para el objeto de datos del nombre de archivo (por ejemplo, un directorio para el archivo o una instancia de base de datos par una tabla de la base de datos).		X
TaxonomyLevel1	rv50	Clasificación de destino para el evento. Se muestra debajo del nombre del evento con el siguiente formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel2	rv51	Clasificación de subdestino para el evento. Se muestra debajo del nombre del evento con el siguiente formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

Campo	Nombre abreviado	Descripción	Visible en la Vista básica	Visible en la Vista detallada
TaxonomyLevel3	rv52	Información de la acción para el evento. Se muestra debajo del nombre del evento con el siguiente formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel4	rv53	Información detallada para el evento. Se muestra debajo del nombre del evento con el siguiente formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

Algunos campos están acortados. Si se acortan los campos, se puede buscar una palabra concreta en el campo sin necesidad de un carácter general. Los campos están acortados de acuerdo con los espacios y otros caracteres especiales. Para estos campos, se eliminan artículos como "un" o "el" del índice de búsqueda.

- EventName
- Mensaje
- NombreProducto
- Nombre de archivo
- DataContext
- TaxonomyLevel1
- TaxonomyLevel2
- TaxonomyLevel3
- TaxonomyLevel4

Generación de informes

5

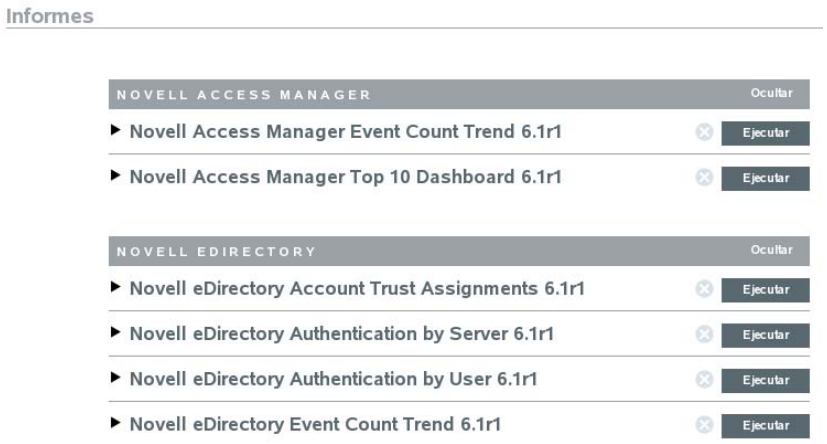
Este capítulo describe cómo ejecutar, ver y gestionar informes en Novell® Identity Audit.

5.1 Descripción general

Identity Audit se instala con una serie de plantillas de informe relacionadas con aplicaciones de Novell. Cualquier usuario de Identity Audit puede ejecutar un informe utilizando los parámetros que desee (como las fecha de inicio y finalización) y los resultados del mismo se guardan con el nombre que elija el usuario. Después de la ejecución del informe, cualquier usuario de Identity Audit puede recuperar los resultados y verlos como un archivo PDF.

Los informes se organizan por categorías. Identity Audit se instala con informes para cada origen de evento compatible.

Figura 5-1 *Informes organizados por categorías*



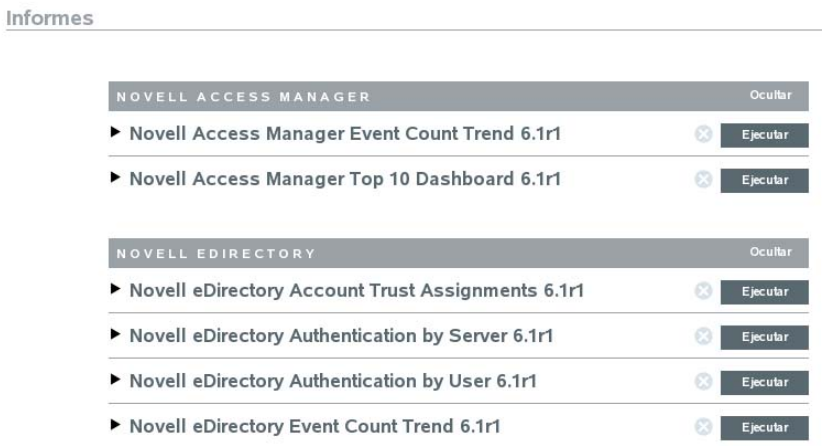
5.2 Ejecución de informes

Identity Audit está instalado junto con un conjunto de informes organizados en varias categorías de productos. Los informes se ejecutan de forma asíncrona, de manera que los usuarios puedan continuar sus tareas en la aplicación mientras se ejecuta el informe. Todos los usuarios pueden ver los resultados del informe en PDF en cuanto éste termine de ejecutarse.

Muchas definiciones de informes incluyen parámetros. Al usuario se le pide que defina lo anterior antes de ejecutar informes. En función de la forma en la que el desarrollador del informe lo diseñara, los parámetros de dicho informe pueden ser texto, números, valores booleanos o fechas. Un parámetro puede contar con un valor por defecto o una lista de selección basados en los valores que se encuentran en la base de datos de Identity Audit.

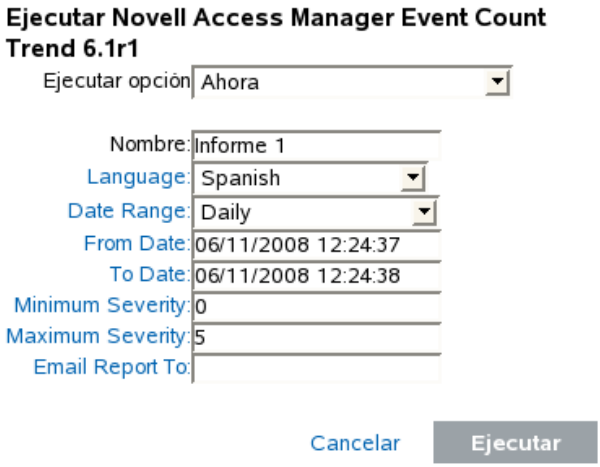
Para ejecutar un informe:

1 En Identity Audit, haga clic en *Informes* para ver los informes disponibles.



Si lo desea, haga clic en la definición del informe para ampliarla. Si ve *Informe de muestra*, puede hacer clic en *Ver* para saber cómo aparece el informe completo con un conjunto de datos de muestra.

2 Seleccione el informe que desea ejecutar y haga clic en *Ejecutar*.



3 Programe la ejecución del informe. En caso de que el informe se vaya a ejecutar con posterioridad, será necesario que establezca también la hora de inicio.

- Ahora: éste es el valor por defecto. Se encarga de ejecutar el informe de forma inmediata.
- Una vez: este valor se encarga de ejecutar el informe una vez en la fecha y hora especificadas.
- Diariamente: este valor se encarga de ejecutar el informe una vez al día a la hora especificada.

- Semanalmente: este valor se encarga de ejecutar el informe una vez a la semana y el mismo día a la hora especificada.
- Mensualmente: este valor se encarga de ejecutar el informe el mismo día con carácter mensual comenzado en la fecha y hora especificadas. Por ejemplo, si la fecha y hora de inicio es el 28 de octubre a las 14:00 horas, el informe se ejecutará todos los días 28 del mes a las 14:00 horas.

Nota: Todos los ajustes temporales se basan en la hora local del navegador.

---

4 Introduzca un nombre para identificar los resultados del informe.

No es necesario que el nombre del informe sea único, ya que el nombre de usuario y la hora también se usan a efectos de identificación de los resultados del informe.

5 Elija el idioma en el que desea que se muestre el informe (inglés, francés, alemán, italiano, japonés, chino tradicional o simplificado, español o portugués).

6 Seleccione el tipo de informe. Todos los períodos temporales se basan en la hora local del navegador.

- Diariamente: el informe muestra los eventos comprendidos entre la media noche del día en curso hasta las 11:59 del mismo día. Si en dicho momento son las 8:00, el informe mostrará 8 horas de datos.
- Semanalmente: el informe muestra eventos desde la media noche del lunes de la semana en curso hasta el final del día en curso.
- Mensualmente: el informe muestra eventos desde la media noche del primer día del mes en curso hasta el final del día en curso.
- Rango de fecha personalizado: para realizar este ajuste exclusivamente, será necesario que también establezca una fecha de inicio y final a continuación.
- Día anterior: el informe muestra eventos desde la media noche de ayer hasta las 11:59 de ayer.

7 En caso de que haya seleccionado un rango de fecha personalizado, defina la fecha de inicio (en Fecha) y la fecha final (hasta Fecha) para el informe.

Nota: Si se selecciona Diariamente, Semanalmente, Mensualmente o Día anterior para el tipo de informe, se ignoran dichos ajustes temporales.

---

8 Establezca los eventos de gravedad mínima de forma que se incluyan en el informe.

9 Establezca los eventos de gravedad máxima de forma que se incluyan en el informe.

10 Si se va a enviar este informe a uno o varios usuarios, introduzca las direcciones de correo electrónico pertinentes separadas por comas.

Nota: Para habilitar el envío de informes, el administrador debe configurar el relevo de envío en *Reglas>Configuración*.

---

11 Haga clic en *Ejecutar*.

Se crea una entrada con los resultados del informe y se envía a los destinatarios especificados.

5.3 Visualización de informes

Los usuarios de Identity Audit pueden visualizar informes en la aplicación Identity Audit. Otros usuarios pueden recibir informes.Archivos `pdf` en el correo electrónico.

1 Para ver la lista de los resultados del informe, haga clic en *Ver*. Todos los informes ejecutados anteriormente aparecen con el nombre de informe definido por el usuario, el usuario que los ejecutó y la hora a la que se llevó a cabo la operación.

2 Haga clic en *mostrar parámetros* para ver los valores exactos utilizados para ejecutar el informe.

- Para el tipo de informe, D=Diariamente, S=Semanalmente, M=Mensualmente, RF=Rango de fecha personalizado y DA=Día anterior.
- Para el idioma, en=inglés, fr=francés, de=alemán, it=italiano, ja=japonés, pt=portugués de Brasil, es=español, zh=chino simplificado y zh_TW=chino tradicional.

3 Haga clic en *Ver* en los resultados del informe que desee consultar. Los resultados del informe se muestran en una ventana nueva con formato `pdf`.

Sugerencia: Los resultados del informe se organizan desde los más nuevos a los más antiguos.

5.4 Gestión de informes

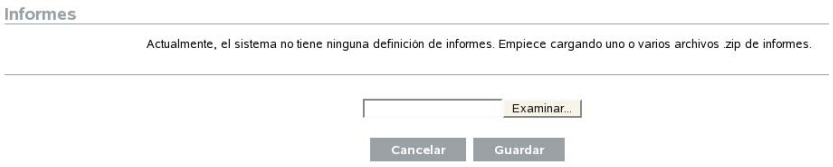
Los usuarios de Identity Audit pueden añadir, suprimir, actualizar y programar informes.

- Sección 5.4.1, “Añadir informes”, en la página 39
- Sección 5.4.2, “Renombrar los resultados del informe”, en la página 41
- Sección 5.4.3, “Supresión de informes”, en la página 41
- Sección 5.4.4, “Actualización de las definiciones de informes”, en la página 41

5.4.1 Añadir informes

Identity Audit viene cargado previamente con los informes, pero se pueden cargar los complementos nuevos del informe (archivos `.zip` especiales que incluyen la definición del informe y los metadatos) pueden cargarse en Identity Audit. Si no hay informes en el sistema, aparece la siguiente pantalla:

Figura 5-2 *No se han cargado informes.*



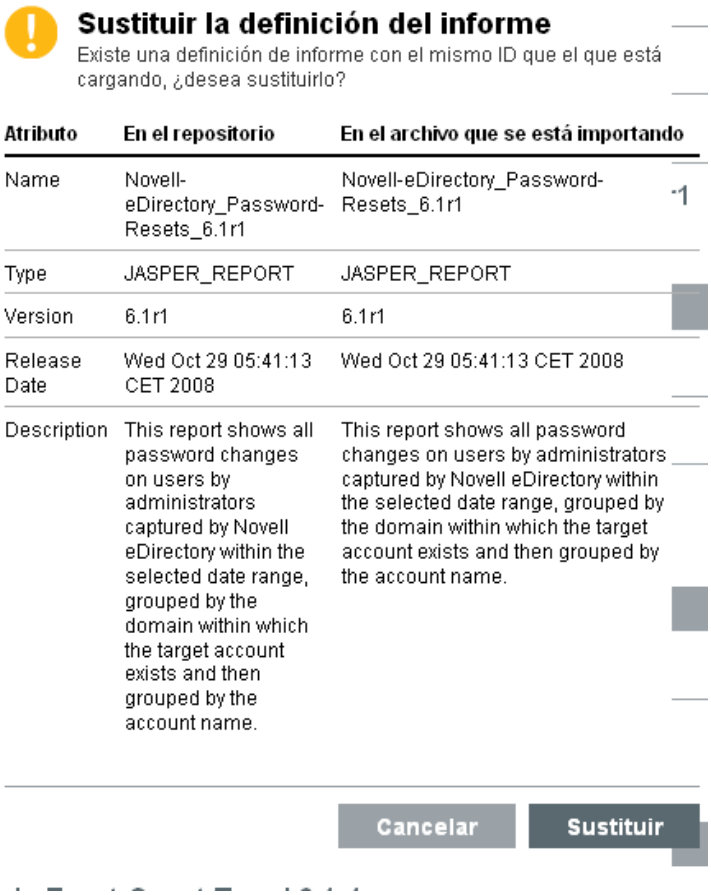
Para añadir un informe:

1. Haga clic en el botón *Informes*, situado en el lateral izquierdo de la pantalla.
2. Haga clic en el botón *Cargar informe*.
3. Busque la ubicación del archivo `.zip` del módulo auxiliar del informe en el equipo local.

4 Haga clic en *Abrir*.

5 Haga clic en *Guardar*.

6 En caso de que el mismo informe ya exista en el repositorio del informe (basado en el ID exclusivo del informe), Identity Audit muestra los detalles de ambos informes en el sistema y el que se está importando. El usuario puede decidir si desea sustituir el informe existente. En el caso siguiente, el informe importado es de la misma versión que el informe existente.



7 La nueva definición de informe se añade a la lista por orden alfabético y puede ejecutarse de forma inmediata, si se desea.

Descarga de informes nuevos o actualizados

Los informes nuevos o actualizados por Novell se pueden descargar en el sitio Web de contenido de Novell (http://support.novell.com/products/identityaudit/identityaudit10.html).

Creación de informes nuevos

Los usuarios pueden modificar o escribir mediante JasperForge* iReport. un diseñador de informes gráficos para los informes de Jasper. iReport es una herramienta de desarrollo de informes de origen abierto que se encuentra disponible para su descarga en JasperForge.org (http://jasperforge.org/plugins/project/project_home.php?group_id=83) (desde el momento en el que se publica).

Los informes modificados o nuevos pueden incluir campos adicionales de la base de datos que no se encuentran en la interfaz Web de Identity Audit. Se deben ajustar a los requisitos de formato y de archivo de los complementos del informe. Para obtener información adicional sobre los requisitos relacionados con los campos de la base de datos, archivos y formatos para los complementos de los informes, consulte el sitio Web de Sentinel SDK (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

5.4.2 Renombrar los resultados del informe

Se pueden renombrar los resultados del informe (pero no las definiciones del informe) en la interfaz de Identity Audit.

1. Haga clic en el botón *Informes*, situado en el lateral izquierdo de la pantalla.
2. Haga clic en el nombre de un informe para ampliarlo.
3. Haga clic en el nombre de los resultados de un informe si desea renombrarlo.
4. Escriba la nueva contraseña.
5. Haga clic en *Renombrar*.

5.4.3 Supresión de informes

Los usuarios pueden suprimir un resultado de informe establecido o una definición de informe. Si se suprime una definición de informe, todos los resultados asociados del informe se suprimirán también.

Si se suprime un informe en progreso, se cancela la consulta de la base de datos.

5.4.4 Actualización de las definiciones de informes

Los usuarios pueden cargar informes actualizados en Identity Audit para sustituir un informe existente. Para obtener más información, consulte Sección 5.4.1, “Añadir informes”, en la página 39.

Recopilación de datos

6

Los administradores pueden configurar y supervisar la recopilación de datos de Novell® Identity Audit. Identity Audit se instala con la capacidad de recopilar datos de una serie de aplicaciones de Novell por medio del agente de la plataforma de Novell Audit. Para obtener más información acerca de las versiones compatibles del Agente de la plataforma, consulte Sección 2.4, “Agente de plataforma admitido”, en la página 14.

6.1 Configuración de orígenes de eventos

Aunque Identity Audit está preconfigurado para aceptar datos de varias aplicaciones de Novell, los servidores de aplicación deben estar configurados (orígenes de eventos) para enviar los datos al servidor Identity Audit. Esto forma parte de la instalación básica de Identity Audit. Para obtener más información, consulte Sección 3.2, “Configuración de orígenes de eventos”, en la página 21.

6.2 Estado de la recopilación de datos

Los administradores pueden habilitar o inhabilitar la recopilación de datos tanto a nivel general como por aplicación. Además, también pueden ver información de actividad sobre cada aplicación.

1. Entre en Identity Audit como administrador.
2. Haga clic en *Recopilación* en la esquina superior derecha de la página.

3. Habilitar o inhabilitar la colección general de datos mediante el servidor de Audit.
4. Habilitar o inhabilitar la recopilación de datos específica de una aplicación desde los orígenes de eventos.
5. Haga clic en *mostrar detalles* para ver más información sobre las conexiones activas de cada aplicación.

Los cambios de esta página surten efecto inmediatamente.

- Sección 6.2.1, “Servidor de Audit”, en la página 44
- Sección 6.2.2, “Orígenes de eventos”, en la página 45

6.2.1 Servidor de Audit

En la sección *Servidor de Audit*, los administradores pueden habilitar o inhabilitar la recopilación de datos a nivel general mediante las opciones "Activar" o "Desactivar". También se muestra el estado de actividad del servidor de Audit.

Activo: un indicador verde significa que el servidor de Audti está activo (está funcionando, se está escuchando en un puerto y no tiene errores sin resolver).

Error: un indicador rojo significa que hay un problema en el servidor de Audit. Para obtener información adicional, consulte los archivos `server0.*.log`.

Desconectado: un indicador gris significa que los administradores han utilizado el servidor de Audit sin conexión.

6.2.2 Orígenes de eventos

En la sección *Orígenes de eventos*, los administradores pueden habilitar la recopilación de datos a nivel de aplicación. Estos ajustes de configuración pueden afectar a la recopilación de datos para varios servidores (por ejemplo, varias instancias de eDirectory).

Nota: Estos ajustes de configuración habilitan (o inhabilitan) la recopilación de datos de Identity Audit desde las aplicaciones que se enumeran. No inician ni detienen servicios en el equipo del origen de eventos.

El estado de actividad de cada icono se indica mediante los colores rojo, amarillo, verde o negro. Para la mayoría de los estados, puede obtener información adicional si hace clic en *mostrar detalles*.

Activo: un indicador verde significa que el origen del evento está activo y que Identity Audit ha recibido datos que provienen de él.

Advertencia: un indicador amarillo indica una condición de advertencia. Una causa frecuente es que la aplicación está activada en Identity Audit, pero no ha enviado ningún dato. Por ejemplo, esto puede suceder si el Agente de plataforma del origen de eventos no está configurado correctamente para enviar datos a Identity Audit o si el registro de eventos no está habilitado para la aplicación. Haga clic en *Mostrar detalles* para obtener más información.

Error: un indicador rojo significa que el servidor de Identity Audit está generando un informe sobre un error al conectarse a esta aplicación o al recibir datos de ella. Haga clic en *Mostrar detalles* para obtener más información.

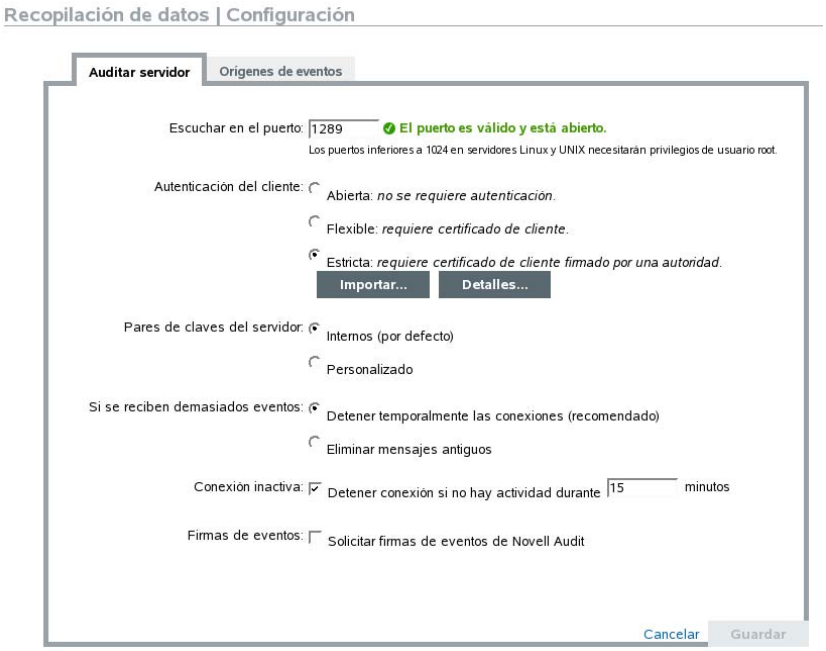
Desconectado: un indicador gris significa que se ha inhabilitado un origen de eventos. Identity Audit no está procesando ningún dato que proceda de él.

Para cada origen de evento conectado, Identity Audit muestra la velocidad calculada del evento para los eventos entrantes. La velocidad del evento se vuelve a calcular cada 60 segundos.

6.3 Opciones del servidor de auditoría

Los administradores pueden modificar algunas configuraciones relacionadas con el modo en que Identity Audit escucha los datos de las aplicaciones de origen del evento, incluidos el puerto en el que Identity Audit lleva a cabo la escucha y el tipo de autenticación existente entre el origen del evento e Identity Audit.

1. Entre en Identity Audit como administrador.
2. Haga clic en el enlace *Recopilación* en la parte superior de la pantalla.
3. Haga clic en el enlace *Configuración* en el lateral derecho de la pantalla.
4. Asegúrese de que *Servidor de auditoría* esté seleccionado.



5 Introduzca el puerto en el que el servidor de Identity Audit escuchará los mensajes procedentes de los orígenes de eventos. Para obtener más información, consulte Sección 6.3.1, “Configuración del puerto y reenvío de puerto”, en la página 47.

6 Establezca la autenticación adecuada del cliente y los valores de los pares de claves del servidor. Para obtener más información, consulte Sección 6.3.2, “Autenticación del cliente”, en la página 48.

7 Seleccione el comportamiento del servidor de Identity Audit cuando el búfer se llene de demasiados eventos.

Conexiones pausadas de forma temporal: este ajuste suelta las conexiones existentes y deja de aceptar las nuevas conexiones hasta que el búfer no tenga espacio para los nuevos mensajes. Mientras tanto, los orígenes de eventos almacenan los mensajes en la memoria caché.

Suelte los mensajes más antiguos: este valor de configuración suelta los mensajes más antiguos para aceptar los nuevos.

Advertencia: No existe ningún método compatible para recuperar los mensajes sueltos si selecciona la opción *Soltar los mensajes más antiguos*.

---

8 Seleccione *Conexión inactiva* para desconectar los orígenes de eventos que no han enviado datos durante un período de tiempo determinado.

Las conexiones del origen de eventos se volverán a crear automáticamente cuando empiecen a enviar datos de nuevo.

9 Especifique el número de minutos antes de desconectar la conexión inactiva.

10 Seleccione *Firmas de eventos* para recibir una firma con el evento.

Nota: Para recibir una firma, el Agente de plataforma del origen de evento debe configurarse correctamente. Para obtener más información, consulte Sección 6.1, “Configuración de orígenes de eventos”, en la página 43. .

11 Haga clic en *Guardar*.

6.3.1 Configuración del puerto y reenvío de puerto

El puerto predeterminado en el que Identity Audit escucha los mensajes de los Agentes de la plataforma es el 1289. Cuando se configura el puerto, el sistema comprueba si éste es válido y está abierto.

El enlace a puertos inferiores a 1.024 necesita privilegios "root". En su lugar, Novell recomienda que utilice un puerto superior a 1.024. Puede modificar los dispositivos de origen para enviar a un puerto superior o para usar la remisión de puertos en el servidor de Identity Audit.

Para modificar el origen del evento para enviar a un puerto diferente:

1 Regístrese en el equipo del origen del evento.

2 Abra el archivo `logevent` para editarlo. La ubicación del archivo depende del sistema operativo:

- Linux: `/etc/logevent.conf`
- Windows: `C:\WINDOWS\logevent.cfg`
- NetWare: `SYS:\etc\logevent.cfg`
- Solaris: `/etc/logevent.conf`

3 Defina el parámetro LogEnginePort para el puerto deseado.

4 Guarde el archivo.

5 Reinicie el Agente de plataforma. El método varía en función del sistema operativo y de la aplicación. Reinicie el equipo o consulte la documentación específica de la aplicación que se encuentra en el sitio Web de documentación de Novell (http://www.novell.com/documentation) para obtener más instrucciones.

Para configurar la remisión de puertos en el servidor de Identity Audit:

1 Entre en el sistema operativo del servidor de Identity Audit como `root` (o `su` para `root`).

2 Abra el archivo `/etc/init.d/boot.local` para editarlo.

3 Añada el siguiente comando casi al final del proceso de reinicio:

`iptables -A PREROUTING -t nat -p` *`protocol`* `--dport` *`incoming port`* `-j DNAT --to-destination` *`IP:rerouted port`*

donde el *protocolo* es tcp o udp, el *puerto de entrada* es el puerto al que llegan los mensajes y el *IP:puerto enrutado* es la dirección IP del equipo local y un puerto disponible superior a 1.024.

4 Guarde los cambios.

5 Reiniciar. Si no puede reiniciar inmediatamente, ejecute el comando `iptables` anterior desde la línea de comando.

6.3.2 Autenticación del cliente

Los orígenes de eventos envían sus datos mediante una conexión SSL y la configuración de la *Autenticación del cliente* para el servidor de Identity Audit determina el tipo de autenticación que se ejecuta para los certificados desde los Agentes de plataforma en los orígenes de eventos.

Abierto: No se requiere autenticación. Identity Audit no solicita, requiere ni valida ningún certificado del origen del evento.

Flexible: se necesita un certificado X.509 válido del origen del evento, pero este certificado no se valida. La autoridad certificadora no tiene que firmarlo.

Estricto: se necesita un certificado X.509 válido del origen de evento, el cual debe incluir la firma de una autoridad certificadora de confianza. Si el origen de evento no cuenta con un certificado válido, Identity Audit no aceptará sus datos de evento.

- "Creación de un archivo truststore" en la página 48
- "Importación de un archivo truststore" en la página 48
- "Par de claves del servidor" en la página 49

Creación de un archivo truststore

Para la autenticación estricta, debe disponer de un archivo truststore que contenga un certificado del origen de eventos o el certificado para la autoridad certificadora (CA) que ha firmado dicho certificado. Si cuenta con el certificado DER o PEM, puede crear el archivo truststore mediante la utilidad CreateTruststore que se incluye con Identity Audit.

1. Entrar en el servidor de Identity Audit como Novell.
2. Vaya a `/opt/novell/identity_audit_1.0_x86/data/updates/done`.
3. Descomprima el archivo `audit_connector.zip`.

   ```
   descomprimir audit_connector.zip
   ```
4. Copie `TruststoreCreator.sh` o `TruststoreCreator.bat` en el equipo con el certificado o copie el certificado en el equipo con la utilidad TruststoreCreator.
5. Ejecute la utilidad `TruststoreCreator.sh`.

   ```
   TruststoreCreator.sh -keystore /tmp/my.keystore -password
   password1 -certs /tmp/cert1.pem,/tmp/cert2.pem
   ```

   En este ejemplo, la utilidad TruststoreCreator crea un archivo de almacén de claves llamado `my.keystore` que contiene dos certificados (`cert1.pem` y `cert2.pem`). La contraseña *password1* lo protege.

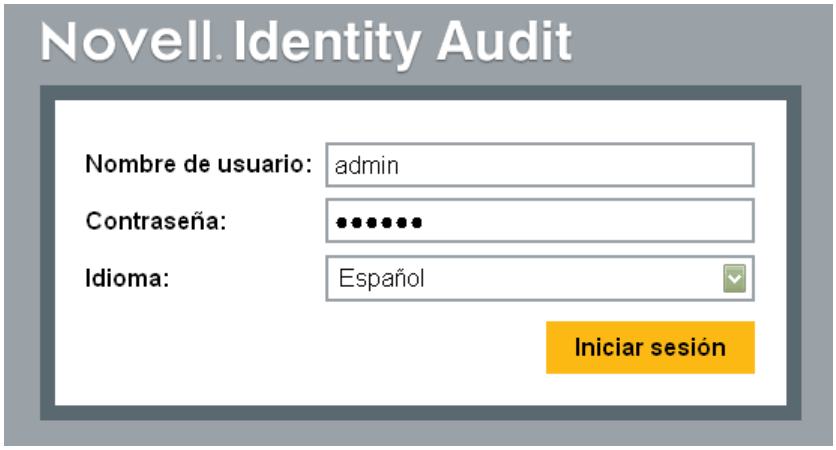
Importación de un archivo truststore

Para una autenticación estricta, el administrador puede importar un archivo truststore con el botón *Importar*. De esta forma se garantiza que sólo los orígenes de eventos autorizados envíen datos a Identity Audit. El archivo truststore debe incluir el certificado del origen de eventos o el certificado de la autoridad certificadora que lo ha firmado.

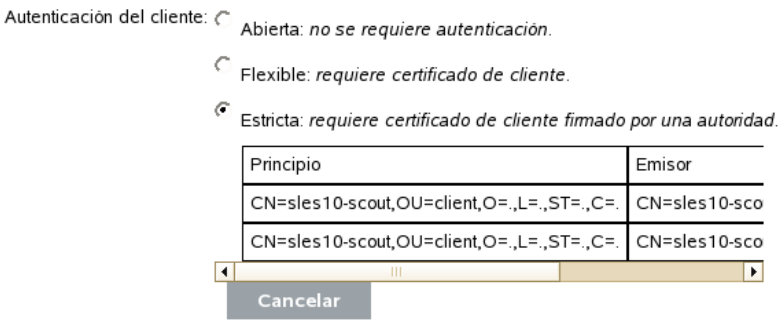
El siguiente procedimiento se debe ejecutar en el equipo que contenga el archivo truststore. Puede abrir el navegador Web en el equipo con el archivo truststore o mover dicho archivo a cualquier equipo con un navegador Web.

Para importar un archivo truststore:

1. Entre en Identity Audit como administrador.
2. Haga clic en el enlace *Recopilación* en la parte superior de la pantalla.
3. Haga clic en el enlace *Configuración* en el lateral derecho de la pantalla.
4. Asegúrese de que el *Servidor de auditoría* esté seleccionado.
5. Seleccione la opción *Estricta* en *Autenticación del cliente*.



6. Haga clic en *Examinar* y busque el archivo truststore (por ejemplo, `my.keystore`).
7. Introduzca la contraseña para el archivo de confianza.
8. Haga clic en *Importar*.
9. Haga clic en *Información* para obtener información adicional sobre el archivo truststore.



10. Haga clic en *Guardar*.

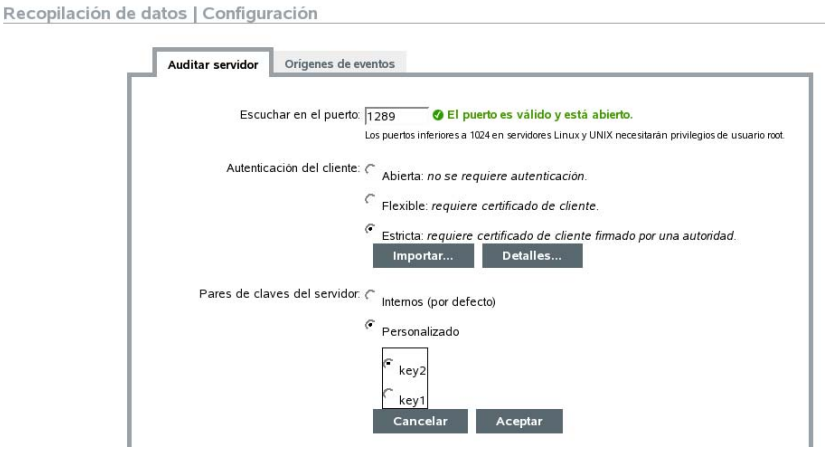
Después de que el archivo truststore se haya importado correctamente, puede hacer clic en *Información* para ver los certificados que se encuentran en dicho archivo.

Par de claves del servidor

Identity Audit está instalado junto con un certificado integrado que se utiliza para autenticar al servidor de Identity Audit para los orígenes de eventos. Se puede sobrescribir dicho certificado con un certificado que haya firmado la autoridad certificadora pública (CA).

Para reemplazar el certificado integrado:

1. Entre en Identity Audit como administrador.
2. Haga clic en el enlace *Recopilación* en la parte superior de la pantalla.
3. Haga clic en el enlace *Configuración* en el lateral derecho de la pantalla.
4. Asegúrese de que *Servidor de auditoría* esté seleccionado.
5. En *Par de claves del servidor*, seleccione la opción *Personalizar*.
6. Haga clic en *Examinar* para buscar el archivo truststore.
7. Introduzca la contraseña para el archivo de confianza.
8. Haga clic en *Importar*.



   En caso de que haya más de un par de claves público-privado en el archivo, seleccione el par que desee y haga clic en *Aceptar*.

9. Haga clic en *Información* para obtener información adicional sobre el par de claves del servidor.
10. Haga clic en *Guardar*.

6.4 Orígenes de eventos

La página *Orígenes de eventos* permite que los administradores configuren el tiempo establecido para los eventos procedentes de cada origen de eventos. La hora del evento se basa en la marca horaria del origen de eventos ("hora del evento trust") o en la marca horaria del servidor de Identity Audit. La marca horaria afecta al orden en el que aparecen los eventos al realizar una búsqueda en caso de que los haya ordenado por hora. La marca horaria también afecta a la hora que aparece en los informes. La operación por defecto es usar la hora del servidor de Identity Audit.

Nota: Se recomienda un servidor NTP para mantener la hora sincronizada en todos los equipos del sistema Identity Audit. En caso de que el servidor NTP se encuentre disponible, Novell recomienda almacenar la hora del evento en un archivo de confianza para cada aplicación. En caso de que no se encuentre disponible, Novell recomienda usar la hora del servidor de Identity Audit para todas las aplicaciones (que es el valor de configuración por defecto) a fin de corregir cualquier diferencia horaria entre los equipos.

Para modificar las opciones de hora del evento:

1. Entre en Identity Audit como administrador.
2. Haga clic en el enlace *Recopilación* en la parte superior de la pantalla.
3. Haga clic en el enlace *Configuración* en el lateral derecho de la pantalla.
4. Haga clic en *Origen del evento*.
5. Seleccione todas las aplicaciones para las que Identity Audit debería utilizar la marca de hora de la aplicación original.

   Para todas las demás, la marca de hora del servidor Identity Audit sustituye a la marca horaria de la aplicación original.

Los cambios serán efectivos inmediatamente para todos los eventos entrantes nuevos. Puede que los eventos que ya estén en la cola tarden un tiempo en procesarse.

Almacenamiento de datos 7

Con la instalación de Novell® Identity Audit se instala una base de datos PostgreSQL con todas las tablas y usuarios necesarios para ejecutar Identity Audit. La base de datos también incluye procedimientos diseñados para administrar particiones de base de datos y archivar datos antiguos. Los administradores pueden gestionar el almacenamiento de base de datos y la configuración de archivado a través de la interfaz Web.

7.1 Actividad de la base de datos

La página de actividad del almacenamiento de datos, disponible sólo para administradores, muestra el buen estado de la base de datos teniendo en cuenta el número de particiones disponibles en la misma y la ejecución satisfactoria de los procedimientos de almacenamiento para crear nuevas particiones y archivar datos (si esta opción está configurada).

Para comprobar la actividad de la base de datos:

1. Entre en Identity Audit como administrador.
2. Haga clic en el enlace Almacenamiento, situado en la esquina superior derecha de la página.

   Se muestra la página de actividad.

Esta página muestra si varias de las funciones de la base de datos se encuentran en un estado correcto (verde), un estado de advertencia (amarillo) o un estado erróneo (rojo).

Base de datos en línea: este indicador muestra si el número previsto de particiones se encuentra en la base de datos para cada una de las tablas con particiones. El número previsto de particiones se basa en el número de días configurados para estar conectado (o el número de días desde la instalación, si se trata de una instalación reciente).

Si el número de particiones no coincide con el previsto, la página muestra el número de la tabla, el número de particiones previstas y el número real de particiones de la base de datos.

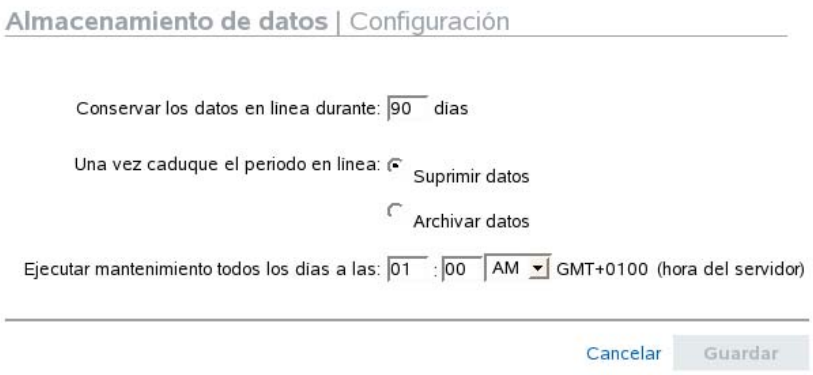
Tareas de la base de datos en línea el indicador aparece en rojo si se ha producido cualquier error la última vez que ejecutaron los procedimientos almacenados para añadir particiones y suprimir datos. En caso de que el archivado esté habilitado, el indicador sólo muestra si se han producido errores la última vez que se ejecutó la tarea de añadir particiones. En caso de errores, la página muestra el nombre, la marca horaria y la información asociada con la tarea que ha provocado el error.

Base de datos de archivos de reserva: este indicador sólo aparece en caso de que el archivado esté habilitado. En caso de que se vuelva rojo, significa que se ha producido algún error la última vez que se ejecutó el procedimiento de almacenamiento para archivar datos. En caso de errores, la página muestra el nombre, la marca horaria y la información asociada con la tarea que ha provocado el error.

7.2 Configuración del almacenamiento de datos

La base de datos es el repositorio para eventos entrantes, información de configuración y resultados de informes. Identity Audit proporciona procedimientos de gestión de bases de datos para evitar que la base de datos se llene. La página Almacenamiento de datos, a la que sólo pueden acceder los administradores, permite configurar diversos aspectos del almacenamiento de datos.

Figura 7-1 *Configuración del almacenamiento de datos*



Conservar los datos conectados para: los administradores pueden especificar el número de días durante los que se van a conservar los datos en la base de datos a efectos de elaboración de informes. El período mínimo es de un día y el número debe ser entero (no se admiten decimales).

Después de que caduque el período de conexión: después de que caduque el período de retención de datos en conexión, cualquier dato del evento que sea anterior al período de tiempo anterior, se suprimirá o moverá de la base de datos a un directorio de archivos.

Advertencia: Novell no admite la recuperación de los datos que se hayan suprimido, por tanto, tenga cuidado a la hora de seleccionar la opción Suprimir.

Archivar en este directorio de base de datos: Si se elige la opción *Archivar datos* , es necesario especificar la ubicación de un directorio existente en el que se vayan a archivar los datos. Este directorio debe existir de antemano y el usuario de Novell debe tener acceso de escritura al mismo. De forma predeterminada, esta ubicación se establece en /data/db_archive en el directorio principal de Identity Audit. El directorio por defecto se crea con los permisos adecuados durante la instalación de Identity Audit.

Importante: Novell recomienda que los archivos de almacenamiento se transfieran regularmente a una ubicación de almacenamiento a largo plazo para evitar que el disco duro se llene.

Prueba: si se elige la opción *Archivar datos* , el botón Prueba comprueba si el directorio de archivo existe y si el usuario de Novell tiene acceso de escritura al mismo.

Lleve a cabo un mantenimiento diario a las: especifique la hora del día a la que desea que se desarrollen las rutinas de mantenimiento. Esta hora se basa en la hora local del servidor de Identity Audit. A la hora establecida para el mantenimiento, se ejecuta un procedimiento almacenado para añadir particiones a la base de datos. Dos horas más tarde, se ejecuta un procedimiento almacenado para archivar o eliminar los datos correspondientes a una fecha anterior al número de días configurados.

El archivado de datos debe planificarse para una hora del día en la que el uso de la base de datos sea relativamente bajo.

Reglas

8

Este capítulo describe los canales de eventos que pueden utilizarse para enviar eventos desde Identity Audit a otro sistema.

8.1 Descripción general de las reglas

La interfaz de reglas ofrece la posibilidad de definir reglas para evaluar los eventos entrantes y entrega los eventos seleccionados a los canales de salida designados. Por ejemplo, cada evento con gravedad 5 se puede enviar por correo electrónico a una lista de distribución de un analista de seguridad o a un administrador.

Nota: Todos los eventos también se entregan a la base de datos.

Un evento de entrada se evalúa en comparación con la regla de filtrado en orden hasta que se encuentra una coincidencia y, a continuación, se ejecutan las acciones de entrega asociadas con la regla en cuestión:

Enviar por correo electrónico: enviar el evento a un usuario o usuarios con un relevo SMTP configurado.

Escritura en archivo: escritura del evento en un archivo determinado del servidor Identity Audit.

Envío a Syslog: Remitir el evento a un servidor syslog configurado

---

Sugerencia: las acciones asociadas procesan un evento cada vez. Por tanto, debería considerar las implicaciones de rendimiento al seleccionar el canal de salida al que se envían los eventos. Por ejemplo, la acción "Escritura en archivo" es la menos intensa en lo que respecta a recursos, por tanto, se puede utilizar para probar los criterios de regla a fin de determinar el volumen de datos antes de enviar una gran cantidad de eventos por correo electrónico o por syslog.

Además, al configurar la acción Enviar por correo electrónico, debería tener en cuenta la cantidad de eventos que un destinatario puede manejar de forma efectiva y ajustar el filtrado de la regla según corresponda.

El formato de la salida de eventos es JavaScript Object Notation (JSON), un formato de intercambio de datos de poco volumen. Los eventos se componen de nombres de archivos (como "evt" para el nombre de evento) seguidos de dos puntos y de un valor (como "Iniciar") separados por comas.

```
{"st":"I","evt":"Start","sev":"1","sres":"Collector","res":"Collec
torManager","rv99":"0","rv1":"0","repassetid":"0","rv77":"0","agen
t":"Novell SecureLogin","obsassetid":"0","vul":"0","port":"Novell
SecureLogin","msg":"Proceso iniciado para el colector Novell
```

SecureLogin (ID D892E9F0-3CA7-102B-B5A1-005056C00005).","dt":"1224204655689","id":"751D97B0-7E13-112B-B933-000C29E8CEDE","src":"D892E9F0-3CA7-102B-B5A2-005056C00004"}

8.2 Configuración de reglas

Las reglas de Identity Audit pueden configurarse para filtrar eventos teniendo en cuenta uno o varios de los campos que se pueden buscar. Para obtener una lista de los campos de eventos que se pueden buscar de Identity Audit, consulte Tabla 4-1 en la página 30. Cada regla se puede asociar a una o más acciones configuradas.

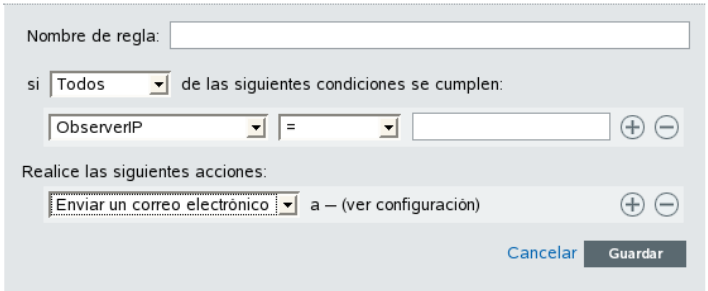
8.2.1 Criterios de filtro

Las reglas se pueden basar en cualquier campo de evento sujeto a búsqueda. Para obtener una lista de estos campos, consulte Tabla 4-1 en la página 30. Los operadores disponibles dependen del tipo de datos del campo del evento. Por ejemplo, la `subred de coincidencia` está disponible para las direcciones IP y el `regex de coincidencia` para los campos de texto.

8.2.2 Añadir una regla

Los administradores pueden añadir una regla basada en filtros y, a continuación, definir uno o más canales a los que remitir los eventos que coincidan con los criterios de la regla.

1. Entre en Identity Audit como administrador.
2. Haga clic en *Reglas* en la esquina superior derecha de la página.
3. Haga clic en *Añadir regla*.
4. Escriba un nombre de regla.
5. Si va a crear varias condiciones, seleccione *Todo* para unir las condiciones con el operador AND. Seleccione *Cualquiera* para unir las condiciones con un operador OR.
6. Seleccione el campo del evento, el operador y el valor para el filtro.



7 Seleccione una acción que se llevará a cabo en cada evento que coincida con los criterios del filtro.

   La información de la acción se basa en la información de configuración que aparece al hacer clic en el enlace *Configuración*.

8 Configurar acciones adicionales en función de sus necesidades.

9 Haga clic en *Guardar*.

8.2.3 Solicitud de reglas

Debido a que las reglas evalúan los eventos en orden hasta que se produce una coincidencia, Novell recomienda que ordene las reglas según corresponda. Las reglas cuya definición sea más precisa y las reglas más importantes deberían colocarse al principio de la lista. Cuando hay más de una regla, se pueden ordenar utilizando la opción de arrastrar y soltar.

Para volver a solicitar reglas:

1 Entre en Identity Audit como administrador.

2 Haga clic en *Reglas* en la esquina superior derecha de la página.

3 Pase sobre el icono hacia la izquierda de la numeración de la regla para habilitar la opción de arrastrar y soltar. Los cambios del cursor.

4 Arrastre la regla y suéltela en el lugar adecuado de la lista solicitada.

8.2.4 Supresión de una regla

Si ya existen eventos en cola para una acción o una serie de acciones cuando elimine una regla, puede que la cola tarde un tiempo en vaciarse después de desactivar la regla.

8.2.5 Activar o desactivar una regla

A la izquierda de cada regla, en la columna cuyo encabezado es Activar, hay un recuadro de verificación para activar la regla. Las reglas nuevas se activan de forma predeterminada. Si desactiva una regla, los eventos entrantes ya no se evaluarán conforme a dicha regla. Si ya existen eventos en cola para una acción o una serie de acciones, puede que la cola tarde un tiempo en vaciarse después de desactivar la regla.

8.3 Configuración de acciones

Un evento se entrega a uno o varios canales cuando coincide con los criterios que especifica una de las reglas. Antes de que los eventos puedan dirigirse hacia un canal, la acción de enviar a un canal debe configurarse con la información de conexión apropiada (y con las credenciales de autenticación, si es necesario para el relevo SMTP). Puede que el sistema Identity Audit sólo disponga de una conexión configurada por tipo de acción (por ejemplo, todos los eventos que se escriben en un archivo deben escribirse en el mismo archivo).

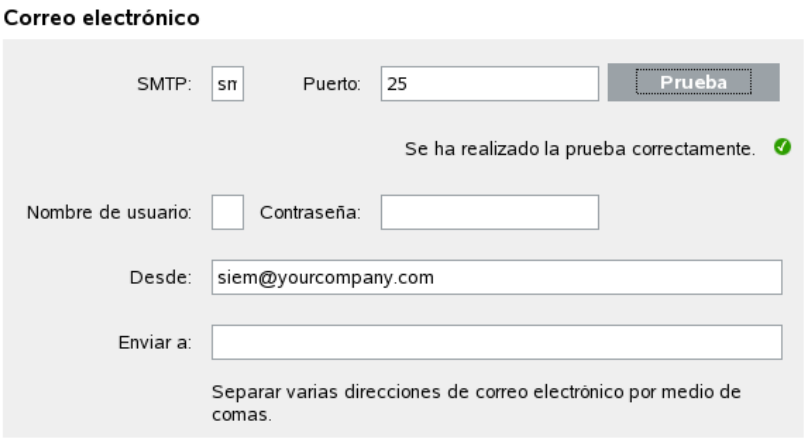
8.3.1 Enviar por correo electrónico

Para configurar la acción Enviar por correo electrónico, necesita la información de conexión de un relevo SMTP (direcciones IP y número de puerto) y las direcciones Para y De. Puede efectuar el envío a más de una dirección de correo electrónico mediante una lista de correos separados por comas.

Nota: A fin de evitar la sobrecarga del relevo SMTP o de los destinatarios de correo, esta acción sólo debería utilizarse con reglas que crean un volumen bajo de eventos.

La configuración de este relevo SMTP también se utiliza para ofrecer informes a los usuarios.

1. Entre en Identity Audit como administrador.
2. Haga clic en *Reglas* en la esquina superior derecha de la página.
3. Haga clic en *Configuración*.
4. En *correo electrónico*, introduzca el nombre y el puerto de un relé SMTP disponible. Si lo desea, haga clic en *Probar* para probar la conexión.



5. Introduzca el nombre y la contraseña en caso de que sea necesaria la autenticación para el relé SMTP.
6. Introduzca una dirección desde la que procederán los mensajes de correo electrónico.

7 Introduzca una o varias direcciones de correo electrónico separadas por comas.

8 Haga clic en *Guardar*.

Todos los eventos de Identity Audit que cumplan los criterios de filtro para los que se define una acción Enviar por correo electrónico se envían al mismo relevo SMTP y al mismo grupo de direcciones.

8.3.2 Enviar a Syslog

Para configurar la acción Enviar a Syslog, necesita la información de conexión para el servidor syslog (dirección IP y número de puerto).

1 Entre en Identity Audit como administrador.

2 Haga clic en *Reglas* en la esquina superior derecha de la página.

3 Haga clic en *Configuración*.

4 En *Syslog*, introduzca un nombre o una dirección IP y abra el puerto de un servidor syslog. Si lo desea, haga clic en *Probar* a fin de comprobar si existen el puerto y el servidor de destino.

5 Haga clic en *Guardar*.

Todos los eventos de Identity Audit que cumplen los criterios de filtro para los que se define una acción Enviar a Syslog se envían en el mismo servidor syslog.

8.3.3 Escritura en archivo

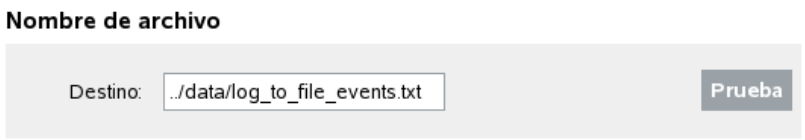
Para configurar la acción Escritura en archivo, se requieren el nombre y la ruta del archivo en el que se escribirán los eventos. Este directorio debe existir de antemano y el usuario de Novell debe tener permiso de escritura sobre él. Si el archivo aún no existe, Identity Audit lo creará.

1 Entre en Identity Audit como administrador.

2 Haga clic en *Reglas* en la esquina superior derecha de la página.

3 Haga clic en *Configuración*.

4 En *Nombre de archivo*, introduzca la vía del archivo en el que desea que se escriban los eventos. Si lo desea, haga clic en *Probar* para probar la conexión.



5 Haga clic en *Guardar*.

Todos los eventos de Identity Audit que cumplan los criterios de filtro para los que se define la acción Escritura en archivo se escriben en el mismo archivo.

Administración de usuario

9

Los administradores pueden añadir, editar y eliminar usuarios de Novell® Identity Audit y conceder derechos administrativos. Los usuarios pueden editar los detalles de su propio perfil de usuario.

9.1 Adición de un de usuario

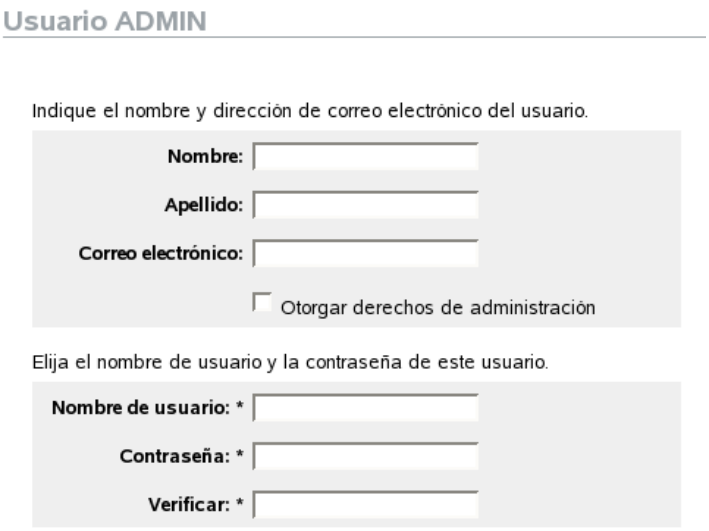
Al añadir un usuario en el sistema Identity Audit se crea un usuario de la aplicación que puede entrar en la aplicación Identity Audit.

Al seleccionar la opción *Conceder derechos administrativos*, el usuario obtiene derechos administrativos en el sistema Identity Audit. Los derechos administrativos incluyen la capacidad de gestionar las siguientes funciones:

- Administración de usuario
- Recopilación de datos
- Almacenamiento de datos

Para añadir un usuario:

1. Entre en Identity Audit como administrador.
2. Haga clic en *Administración de usuario* en la esquina superior derecha de la página.
3. Haga clic en *Añadir un usuario*.
4. Escriba la información del usuario.



Los campos marcados con asterisco (*) son obligatorios y el nombre de usuario debe ser único.

Nota: Se valida el formato de la dirección de correo electrónico, pero los campos del número de teléfono aceptan cualquier formato. Asegúrese de introducir un número de teléfono válido.

5 Si lo desea, seleccione *Conceder derechos administrativos*.

6 Haga clic en *Guardar*.

9.2 Edición de los detalles de usuario

Los administradores pueden editar la información de usuario de cualquier usuario del sistema. Cualquier usuario tiene la capacidad de editar cualquier campo en su propio perfil, excepto para su nombre de usuario y estado del administrador. Los usuarios también pueden cambiar las contraseñas.

- Sección 9.2.1, “Para editar su propio perfil”, en la página 64
- Sección 9.2.2, “Cambiar su contraseña”, en la página 65
- Sección 9.2.3, “Editar otro perfil del usuario (sólo para el administrador)”, en la página 65
- Sección 9.2.4, “Restaurar otra contraseña del usuario (sólo para el administrador)”, en la página 66

9.2.1 Para editar su propio perfil

1 Haga clic en *perfil* en la esquina superior derecha.

2 Editar cualquier campo disponible.

3 Haga clic en *Guardar*.

9.2.2 Cambiar su contraseña

Los usuario pueden cambiar su contraseña si saben cuál es la contraseña actual. De lo contrario, el administrador debe restaurar la contraseña.

1 Haga clic en *perfil* en la esquina superior derecha.

2 Escriba la contraseña actual.

3 Escriba la contraseña nueva.

4 Confirme la contraseña nueva.

5 Haga clic en *Guardar*.

9.2.3 Editar otro perfil del usuario (sólo para el administrador)

1 Entre en Identity Audit como administrador.

2 Haga clic en *Administración de usuario* en la esquina superior derecha de la página.

3 Haga clic en la opción *Editar* que se encuentra bajo el nombre que desea editar.

4 Editar todos los campos (excepto el nombre de usuario).

5 Haga clic en *Guardar*.

Los cambios realizados en *Conceder derechos administrativos* surtirán efecto la próxima vez que el usuario acceda.

9.2.4 Restaurar otra contraseña del usuario (sólo para el administrador)

Para restaurar la contraseña de otro usuario, consulte Sección 9.2.3, “Editar otro perfil del usuario (sólo para el administrador)”, en la página 65.

9.3 Suprimir un usuario

Los administradores pueden eliminar a un usuario del sistema.

1 Entre en Identity Audit como administrador.

2 Haga clic en *Administración de usuario* en la esquina superior derecha de la página.

3 Haga clic en la opción *Editar* que se encuentra bajo el usuario que desea suprimir.

4 Haga clic en *Suprimir este usuario* en la esquina superior derecha de la página.

5 Haga clic en *Suprimir* para confirmar.

Archivo truststore

A

Al usar la autenticación estricta para la conexión entre Identity Audit y las aplicaciones de Novell de la que colecciona datos, se puede mejorar la seguridad de los datos.

A.1 Crear un almacén de claves

Se puede crear un almacén de claves mediante el ejecutable "keytool", que se incluye con cualquier instalación de jre. Este almacén de claves contiene un par de claves público y privado que se puede utilizar para sustituir el certificado por defecto que se incluye con Identity Audit. A continuación, se muestran instrucciones básicas, pero si desea obtener información adicional sobre la herramienta de claves, consulte el sitio Web de Sun (http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html).

1. Vaya al directorio /bin para Java (por ejemplo, `$JAVA_HOME/bin`).
2. Ejecute el comando siguiente:

   ```
   keytool -genkey -alias alias -keystore .keystore
   ```

3. Introduzca una contraseña para el almacén de claves. Esta contraseña se utilizará para importar el archivo truststore.
4. Introduzca la siguiente información: nombre y apellido.
   - Nombre y Apellido
   - Unidad administrativa
   - Organización
   - Ciudad y localidad
   - Estado/Provincia
   - Código de país de dos dígitos
5. Verificar la información.
6. Pulse Intro para usar la misma contraseña como contraseña de almacén de claves.

   Se crea un archivo .keystore con una clave privada y su correspondiente clave pública (certificado).