CA User Activity Reporting Module

Guía de descripción general

r12.5.02

Referencias a productos de CA

En este documento se hace referencia a los siguientes productos de CA:

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- Centro de comandos de seguridad de CA (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Información de contacto del servicio de Asistencia técnica

Para obtener asistencia técnica en línea, una lista completa de direcciones y el horario de servicio principal, acceda a la sección de Asistencia técnica en la dirección http://www.ca.com/worldwide.

Cambios en la documentación

Desde la última versión de esta documentación, se han realizado estos cambios y actualizaciones:

- Información general de inicio rápido: este apartado se ha actualizado para hacer referencia a más tipos de eventos, aparte de los eventos de syslog, que puede recopilar el agente predeterminado en el servidor de CA User Activity Reporting Module.
- Alerta de infracción de políticas: este apartado se ha actualizado para hacer referencia a la capacidad de enviar alertas como traps de SNMP a sistemas de control de seguridad de red y para hacer que las alertas ejecuten un proceso de salida de eventos/alertas de IT PAM, como uno para generar partes del departamento de asistencia.
- Exploración de la documentación de la biblioteca: este apartado se ha actualizado para hacer referencia a la nueva Guía de programación de API, que ahora aparece en la biblioteca de CA User Activity Reporting Module.

Más información:

Descripción general del inicio rápido (en la página 13)
Generación de alertas de infracción de política (en la página 58)
Exploración de la Biblioteca de documentación (en la página 68)

Contenido

Capítulo 1: Introducción 7

Acerca de esta guía 7
Acerca de CA User Activity Reporting Module 8
Su red--Antes de la instalación 9
Componentes de instalación 10

Capítulo 2: Implementación de inicio rápido 13

Descripción general del inicio rápido 13
Instalación del sistema de servidor único 14
Actualización del archivo host de Windows 21
Configuración del primer Administrator 21
Configuración de los orígenes de eventos de syslog 25
Edición del conector de syslog 29
Visualización de eventos syslog 32

Capítulo 3: Implementación del agente para Windows 35

Creación de una cuenta de usuario para el agente 36
Configuración de la clave de autenticación del agente 38
Descarga del programa de instalación del agente 39
Instalación del agente 40
Creación de un conector basado en NTEventLog 43
Configuración de un origen de eventos de Windows 47
Visualización de registros de los orígenes de eventos de Windows 47

Capítulo 4: Funcionalidades clave 51

Recopilación de registros 51
Almacenamiento de registros 53
Presentación estandarizada de los registros 55
Generación de informes de cumplimiento 56
Generación de alertas de infracción de política 58
Gestión de la titularidad 59
Acceso basado en roles 60
Gestión de suscripciones 61
Contenido predeterminado 62

Capítulo 5: Más información acerca de CA User Activity Reporting Module 63

Visualización de la información sobre herramientas 63
Visualización de la Ayuda en línea 65
Exploración de la Biblioteca de documentación 68

Índice 71

Capítulo 1: Introducción

Esta sección contiene los siguientes temas:

Acerca de esta guía (en la página 7)
Acerca de CA User Activity Reporting Module (en la página 8)

Acerca de esta guía

Esta *Guía de descripción general* presenta CA User Activity Reporting Module. Empieza con tutoriales rápidos que le proporcionan experiencia práctica e inmediata del producto. El primer tutorial le guiará a través de los pasos necesarios para configurar y ejecutar un servidor único de CA Enterprise Log Manager y visualizar los syslog recopilados de los dispositivos UNIX en la proximidad de red cercana. El segundo tutorial le guiará a través de la instalación de un agente en un sistema operativo Windows, de la configuración de la recopilación de registros y de la visualización de los registros de eventos resultantes. A continuación, realizará una breve descripción de las funciones y características principales y le indicará dónde obtener más información. Esta guía está dirigida a todos los usuarios.

A continuación, presentamos una lista resumida del contenido de la guía:

Sección	Describe cómo
Acerca de CA Enterprise Log Manager	Integrar CA User Activity Reporting Module en el entorno de red actual
Implementación de inicio rápido	Instalar un sistema de servidores único, configurar los orígenes de los eventos de syslog, actualizar el conector de syslog para el agente predeterminado y visualizar los eventos refinados.
Implementación del agente para Windows	Preparar la instalación del agente, instalar un agente para el sistema operativo Windows, configurar un conector para la recopilación basada en el agente, actualizar el origen de los eventos y visualizar los eventos generados.
Funcionalidades clave	Beneficiarse de las funciones y características clave, incluyendo la recopilación de registros, el almacenamiento de registros, y la generación de informes y alertas de cumplimiento.

Sección	Describe cómo
Más información acerca de CA User Activity Reporting Module	Obtener la información que requiere a través de la información sobre herramientas, la ayuda en línea y la biblioteca de documentación.

Nota: Para obtener más información acerca de la compatibilidad del sistema operativo o acerca de los requisitos del sistema, consulte las *Notas de la versión*. Para más información acerca de los procedimientos a seguir paso a paso para la instalación de CA User Activity Reporting Module y la configuración inicial, consulte la *Guía de implementación.* Para información detallada sobre la instalación del agente, vea la *Guía de instalación del agente*. Para obtener más información sobre el uso y mantenimiento del producto, consulte la *Guía de administración.* Para obtener ayuda acerca del uso de cualquier página de CA User Activity Reporting Module, vea la Ayuda en línea.

Acerca de CA User Activity Reporting Module

CA User Activity Reporting Module se centra en la seguridad y cumplimiento de las TI Le permite recopilar, normalizar, agregar y generar informes de la actividad de las TI. Asimismo, puede generar alertas que requieran acción cuando ocurran posibles infracciones de cumplimiento. Puede recoger datos de dispositivos de seguridad y de no seguridad.

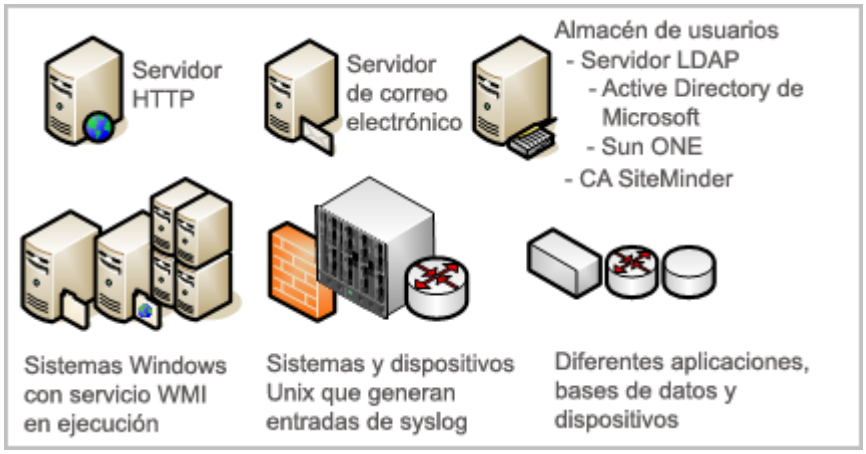
Su red--Antes de la instalación

Los mandatos y regulaciones federales exigen la gestión de registros. Para actuar en conformidad con ellos, debe:

- Hacer que los registros estén disponibles para las auditorías.
- Almacenar los registros durante varios años.
- Restaurar los registros si así se solicita.

La principal dificultad que surge de la gestión de registros es su gran cantidad, su ubicación y su naturaleza temporal. La actividad de los procesos y los usuarios en el software genera registros continuamente. El intervalo de generación se mide en eventos por segundo (EPS). Los eventos sin procesar se registran en todas las aplicaciones, bases de datos y sistemas que estén activos en la red. La creación de copias de seguridad de registros para su almacenamiento debe llevarse a cabo en cada origen de evento antes de que se sobrescriban. La restauración de registros de eventos cuando se almacenan por separado copias de seguridad de orígenes de evento diferentes.

El aspecto más fastidioso de la interpretación de eventos sin procesar es su formato de cadena, en el que no se destaca la severidad. Asimismo, los datos parecidos de diferentes sistemas pueden variar.



El nivel de eficacia operativa exige una solución que consolide todos los registros, facilite su lectura, automatice el archivado en el almacenamiento y simplifique la restauración de registros. CA User Activity Reporting Module ofrece estas ventajas y le permite enviar alertas a individuos y a sistemas cuando se producen eventos críticos.

Componentes de instalación

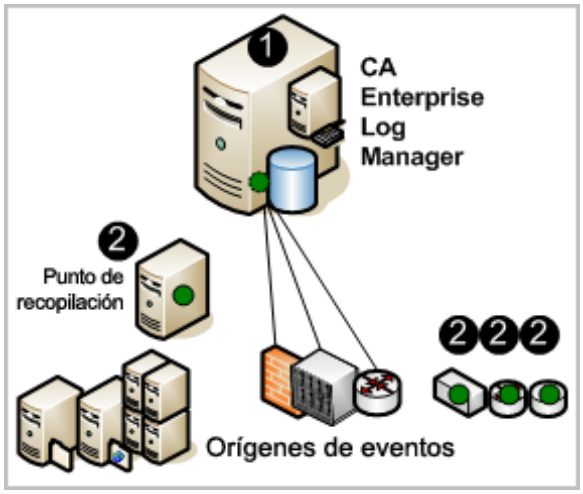
No le llevará mucho tiempo configurar una solución de servidor único y empezar a recopilar eventos.

El disco de instalación incluye estos componentes:

- Sistema operativo (Red Hat Enterprise Linux) para el dispositivo de software
- Servidor de CA User Activity Reporting Module
- Agente de CA User Activity Reporting Module (a partir de ahora llamado el agente)

En la ilustración siguiente, CA User Activity Reporting Module aparece como un servidor que contiene un servidor pequeño, un círculo oscuro (verde) y una base de datos. El servidor pequeño representa el repositorio local que almacena contenido a nivel de aplicación. El círculo oscuro representa el agente predeterminado y la base de datos representa el almacén de registro de eventos donde se procesan las registros de eventos entrantes y donde se hacen disponibles para las consultas y e informes.

Los círculos oscuros (verdes) en el punto de recopilación y los otros orígenes de eventos representan agentes instalados por separado. La instalación de agentes es opcional. Una vez completada la configuración necesaria, puede recopilar syslogs desde orígenes de eventos compatibles con UNIX con el agente predeterminado.



Los números de la ilustración se refieren a estos pasos:

1. Instale el sistema operativo para el dispositivo de software y después haga lo mismo con la aplicación de CA User Activity Reporting Module. Tan pronto como configure los orígenes para enviar los syslogs a CA User Activity Reporting Module e indicar los destinos de éstos en la configuración del conector para el agente predeterminado, se recopilarán y se refinarán los syslogs para una fácil interpretación.
2. (Opcional) Puede instalar un agente en un host que destine a ser el punto de recopilación o puede instalar agentes directamente en los host con orígenes que generan eventos que desea recopilar.

Nota: Vea la *Guía de implementación* para obtener más información acerca de la instalación del dispositivo de software. Vea la *Guía de instalación del Agente* para obtener más información acerca de la instalación de agentes.

Más información:

Instalación del agente (en la página 40)

Capítulo 2: Implementación de inicio rápido

Esta sección contiene los siguientes temas:

Descripción general del inicio rápido (en la página 13)
Instalación del sistema de servidor único (en la página 14)
Actualización del archivo host de Windows (en la página 21)
Configuración del primer Administrator (en la página 21)
Configuración de los orígenes de eventos de syslog (en la página 25)
Edición del conector de syslog (en la página 29)
Visualización de eventos syslog (en la página 32)

Descripción general del inicio rápido

Puede llevar a cabo una implementación simple y correcta con una sola aplicación de software. El conector de syslog predefinido hace posible que el agente predeterminado reciba los eventos de syslog generados. Sólo necesita configurar los orígenes de syslog para enviar los eventos de syslog a CA User Activity Reporting Module y editar la configuración del conector Syslog para identificar los destinos de syslog. El número de eventos de syslog recibidos variará, según el ancho de banda entre el servidor y los orígenes y latencia de syslog.

Los sensores de registro, incluidos WinRM y ODBC, admiten la recopilación de registros directa de más de 20 orígenes de eventos que no pertenecen a syslog. El sensor de registro WinRM permite recopilar eventos directamente de servidores que ejecutan sistemas operativos Windows, como Forefront Security for Exchange server, Forefront Security for SharePoint Server, Microsoft Office Communication Server y el servidor virtual Hyper-V, así como servicios como los servicios de certificados de Active Directory. El sensor de registro ODBC permite capturar eventos generados por las bases de datos Oracle9i o SQL Server 2005. Para obtener detalles, consulte la Matriz de integración de productos de CA Enterprise Log Manager.

Para poder instalar CA User Activity Reporting Module deberá estar provisto de las credenciales de EiamAdmin. Como superusuario EiamAdmin, debe configurar una cuenta de Administrator que utilizará para realizar la configuración. Si inicia sesión con credenciales de Administrator, podrá verificar que la configuración funciona correctamente al visualizar los eventos autocontrolados.

Instalación del sistema de servidor único

El sistema de servidor único es la implementación más sencilla para visualizar eventos consultados. Asegúrese de que selecciona una máquina que cumpla o exceda los requisitos mínimos de hardware para la aplicación de software de CA User Activity Reporting Module.

Nota: Consulte las *Notas de la versión*, si desea obtener la lista de hardware certificado e información sobre la compatibilidad del sistema operativo y sobre los requisitos del servicio y del software del sistema.

Para instalar el sistema de servidor único de CA User Activity Reporting Module

1. Tenga preparada la siguiente información:
   - Una contraseña para la contraseña root.
   - Un nombre de host para la aplicación.
   - La dirección IP, la máscara de subred y la puerta de enlace predeterminada para la aplicación, en el caso que no se utilice un servidor DHPC.
   - El dominio de la aplicación.

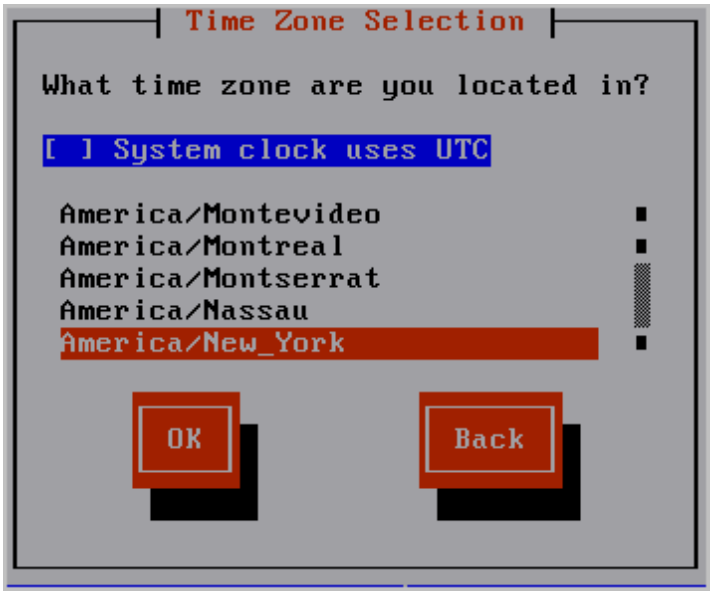
     Nota: Para que se complete la instalación, se debe registrar el dominio con los servidores DNS de la red.
   - La direcciones IP de los servidores DNS.
   - (Opcional) Dirección IP del servidor de NTP
   - Una contraseña para el nombre de superusuario predeterminado de la instalación, EiamAdmin.
   - CAELM.

     Este es el nombre predeterminado de la aplicación de CA User Activity Reporting Module.

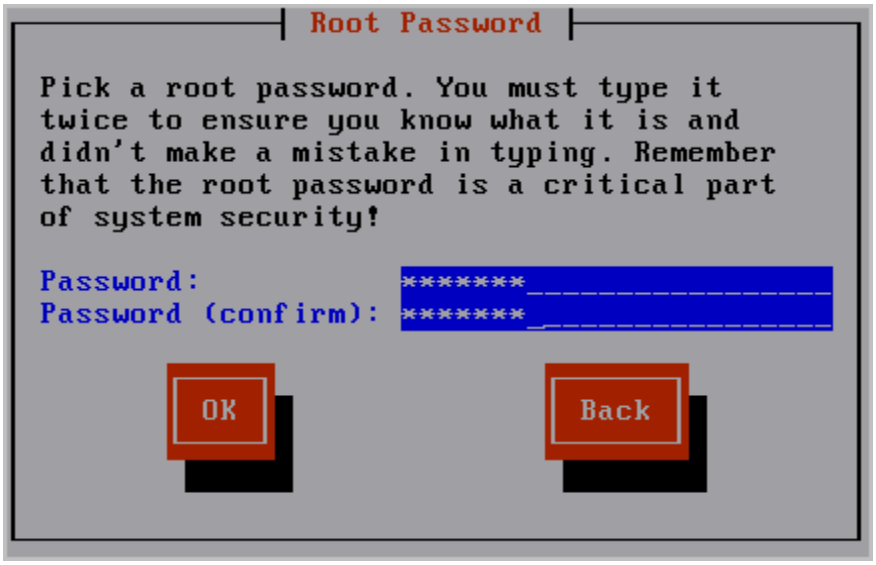
2. Instale el sistema operativo predeterminado preconfigurado mediante el uso de los medios que creó del paquete de descarga de CA User Activity Reporting Module. Durante la instalación del sistema operativo, realice las siguientes operaciones:

   a. Elija un tipo de teclado. El predeterminado es el estadounidense.

   b. Seleccione una zona horaria, por ejemplo America/Nueva York, y, a continuación, haga clic en Aceptar.



   c. Escriba la contraseña que utilizará como contraseña root, y después, vuelva a introducirla para confirmarla. Haga clic en Aceptar.



Aparecerá el cuadro de diálogo con información sobre el estado del proceso.

d. Elimine el disco de instalación del sistema operativo y pulse Intro para reiniciar el sistema.

El sistema se reiniciará en modo no interactivo. Éste mostrará mensajes informando acerca del progreso de la instalación. La información detallada acerca de la instalación se guardará en el archivo: /tmp/pre-install_ca-elm.log.

Aparecerá el mensaje siguiente:

```
Introduzca el disco Instalación de la aplicación CA Enterprise Log Manager r12 y pulse Intro.
```

3. Inserte el disco de la aplicación CA User Activity Reporting Module. Pulse Intro.

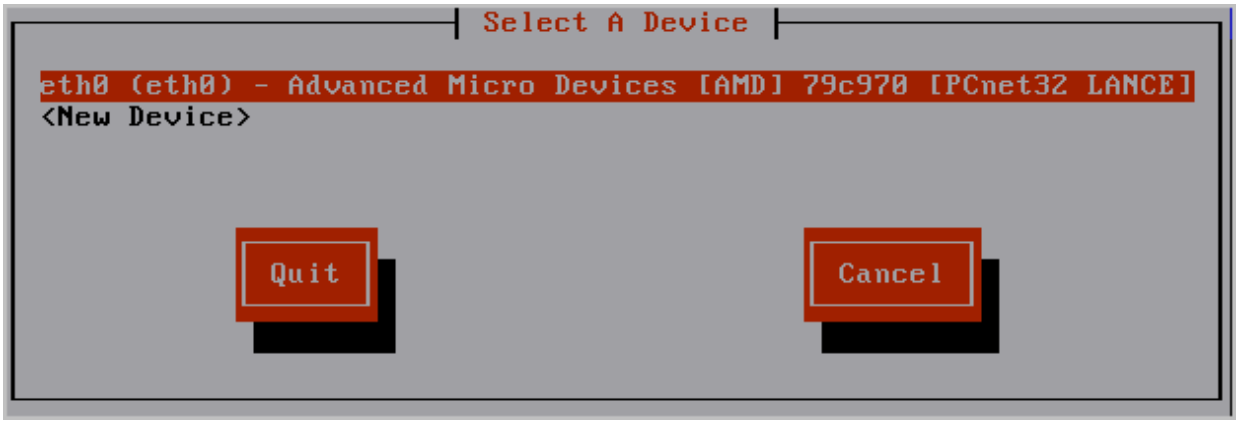
   Para un óptimo rendimiento, se revisará el sistema para comprobar que éste cumple con las especificaciones mínimas recomendadas. En el caso que no las cumpla, aparecerá un aviso para comprobar si quiere continuar con el proceso de instalación.

   Aparecerá el mensaje siguiente:

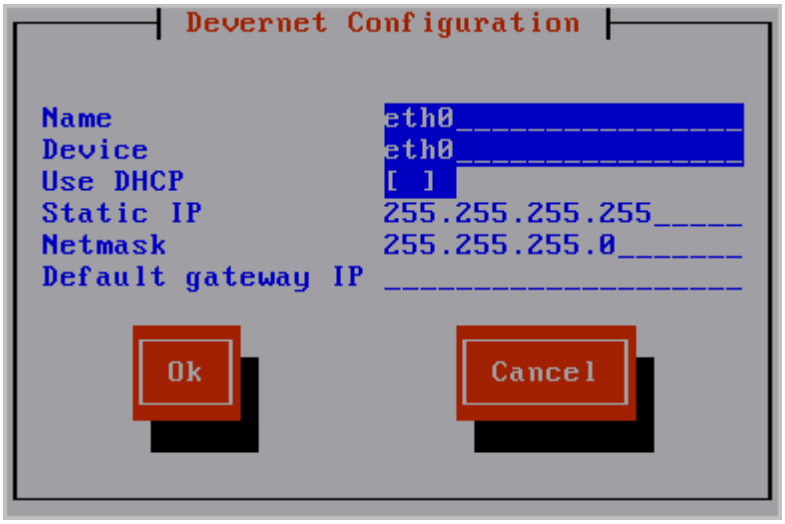
   ```
   Escriba un nombre de host nuevo.
   ```

4. Introduzca el nombre de host para la aplicación de software CA User Activity Reporting Module. Por ejemplo, introduzca CALM1.

5. Acepte el dispositivo predeterminado, eth0. Pulse Intro para ir a la pantalla siguiente.



6. Realice una de las acciones siguientes, que encontrará explicadas con detalle más abajo, y al final haga clic en Aceptar.
   - Seleccione Utilizar DHCP. Es una opción aceptable, sólo si se trata de un sistema de prueba independiente.
   - Introduzca la dirección IP estática, la máscara de subred y la dirección IP de la puerta de enlace predeterminada que se asociarán al nombre de host especificado.



Se reiniciarán los servicios de red con los nuevos valores de configuración mostrados.

Aparece el mensaje siguiente:

```
¿Desea cambiar la configuración de red? (n):
```

7. Revise la configuración de red. Si es correcta, escriba 'n', o pulse Intro, cuando aparezca el mensaje que le permita cambiar la configuración de red.

   Aparece el mensaje siguiente:

   ```
   Introduzca un nombre de dominio para este sistema:
   ```

8. Introduzca el nombre de dominio, como por ejemplo <yourcompany>.com.

   Aparece el mensaje siguiente:

   ```
   Introduzca una lista con los servidores DNS que va a utilizar separados por
   comas:
   ```

9. Introduzca las direcciones IP de los servidores DNS internos separadas por comas y sin espacios.

   Mediante el siguiente mensaje, se mostrará la fecha y hora del sistema:

   ```
   ¿Desea cambiar la fecha y hora del sistema? (n)
   ```

10. Revise la fecha y hora del sistema mostradas. Si son correctas, escriba 'n' o pulse Intro..

    Aparece el mensaje siguiente:

    ```
    ¿Desea configurar el sistema para actualizar la hora mediante NTP?
    ```

11. Si desea utilizar un servidor de Protocolo de tiempo de redes (NTP), realice las operaciones que le indicamos más abajo. Si no desea utilizarlo, especifique No y continúe con el paso siguiente.

    a. Responda Sí al mensaje.

       Si especifica Sí, aparecerá el mensaje siguiente:

       ```
       Introduzca el nombre del servidor NTP o la dirección IP.
       ```

    b. Defina el nombre de host o la dirección IP del servidor NTP.

       Aparecerá un mensaje de confirmación parecido al siguiente: "El sistema se ha configurado correctamente para actualizar la hora a media noche mediante el uso del servidor NTP ubicado en <yourntpserver>."

12. Lea detenidamente los Acuerdos de licencia de usuario final (EULAs) que aparezcan, y a continuación, responda:

    a. Lea el Acuerdo de licencia de usuario final para Sun Java Development Kit (JDK).

       Al final del acuerdo, aparecerá el mensaje siguiente:

       ```
       ¿Está de acuerdo con los términos y condiciones especificados más arriba? [sí o no]
       ```

    b. Escriba Sí, si está de acuerdo con los términos.

       Se mostrará la información de registro del producto junto con el mensaje siguiente:

       ```
       Pulse Intro para continuar...
       ```

    c. Pulse Intro.

       El mensaje informará acerca del estado de preparación de CA User Activity Reporting Module, en que la configuración del sistema se está realizando. Se mostrará el Acuerdo de licencia de usuario final de CA.

    d. Lea el Acuerdo de licencia de usuario final de CA.

       Al final del acuerdo, aparecerá el mensaje siguiente:

       ```
       ¿Está de acuerdo con los términos y condiciones especificados más arriba? [sí o no]
       ```

    e. Escriba Sí, si está de acuerdo con los términos del acuerdo de licencia.

       Aparecerá la información acerca del servidor de CA EEM.

13. Responda a los siguientes mensajes para configurar CA EEM.

    ```
    ¿Utiliza un servidor de EEM local o remoto?
    Introduzca l (local) o r (remoto)
    ```

    a. Para crear un sistema de prueba independiente, introduzca l para local.

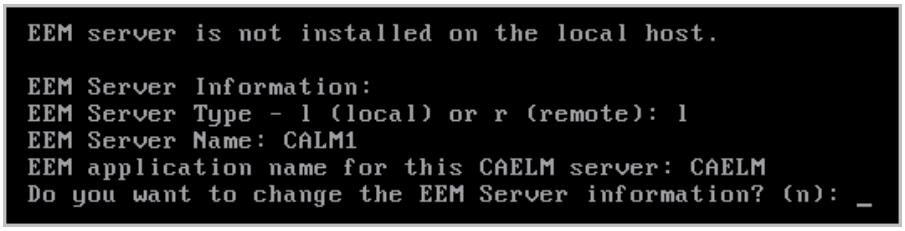
       ```
       Especifique la contraseña para el usuario EiamAdmin del servidor de EEM:
       Confirme la contraseña para el usuario EiamAdmin del servidor de EEM:
       ```

    b. Escriba la contraseña que quiera asignar al supe usuario predeterminado EiamAdmin. Vuelva a introducirla.

       ```
       Introduzca el nombre de la aplicación para el servidor de CAELM (CAELM):
       ```

c. Pulse Intro para aceptar CAELM, el nombre predeterminado de la aplicación para CA User Activity Reporting Module.

Aparecerá un mensaje con la información introducida hasta el momento y una pregunta sobre si quiere realizar cambios.



d. Pulse Intro o introduzca N para cancelar la información introducida para el servidor de CA EEM.

Comenzará el proceso de instalación. Aparecerá un mensaje mostrando la siguiente información de cada uno de los componentes de CA User Activity Reporting Module: instalación correctamente finalizada, registro completado, certificado adquirido, archivos importados y componentes configurados. Aparecerá el mensaje informando acerca de la instalación correcta de CA ELM. Una vez completada la instalación, el sistema mostrará la dirección de inicio de sesión de la consola.

14. Responda a la siguiente solicitud:

```
Do you want to run CAELM Server in FIPS mode?
Introduzca Yes o No.
```

Si introduce y, el servidor de CA User Activity Reporting Module se iniciará en modo FIPS. Si introduce n, el servidor no se iniciará en modo FIPS.

15. Anote la dirección. La deberá introducir en el explorador para acceder a este servidor de CA User Activity Reporting Module. Es https://<nombre de host>:5250/spin/calm

Aparecerá el mensaje de inicio de sesión del <nombre de host>. Puede ignorarlo.

Nota: Si por cualquier motivo, desea visualizar la indicación del sistema operativo desde el mensaje de inicio de sesión, deberá introducir caelmadmin y la contraseña predeterminada, es decir, la contraseña que asignó a la cuenta de usuario EiamAdmin. Para iniciar sesión en la aplicación, deberá utilizar la cuenta caelmadmin o el protocolo de Shell seguro (SSH).

16. Continúe como sigue:
    - Si ha configurado la dirección IP estática, asegúrese de registrar la dirección IP con los servidores DNS especificados en el paso 9.
    - Si ha configurado DHCP, actualice los archivos host en la máquina desde donde pretende buscar este servidor.
    - Busque la URL que anotó en el paso 14 y configure el primer Administrator.

Actualización del archivo host de Windows

Durante la instalación de CA User Activity Reporting Module, puede identificar uno o más servidores DNS o seleccionar Utilizar DHCP. Si selecciona la opción del servidor DHCP, debe actualizar el archivo host de Windows en el equipo en donde planea acceder a CA User Activity Reporting Module a través del explorador.

Para actualizar el archivo host en el host a través del explorador

1. Abra el Explorador de Windows y navegue hasta C:\WINDOWS\system32\drivers\etc.
2. Utilice un editor para abrir el archivos host, como por ejemplo Notepad.
3. Agregue una entrada en la dirección IP del servidor de CA User Activity Reporting Module y el nombre de host correspondiente.
4. Seleccione Guardar del menú Archivo, y, a continuación, cierre el archivo.

Configuración del primer Administrator

Tras la instalación de un servidor de CA User Activity Reporting Module único, se debe preparar la configuración mediante la búsqueda de la URL de CA User Activity Reporting Module desde una estación de trabajo remoto. A continuación, se deberá iniciar sesión y crear una cuenta Administrator que se pueda utilizar para realizar la configuración.

Nota: A fin de llevar a cabo una implementación de inicio rápido, se aceptarán el almacén de usuarios predeterminado, así como las políticas de contraseñas predeterminadas. Normalmente, estos se configuran antes de agregar el primer Administrator.

Para configurar el primer Administrator

1. Conéctese a la URL siguiente desde un explorador en el que el nombre de host pueda ser el propio nombre de host o la dirección IP del servidor donde instaló CA User Activity Reporting Module.

   `https://<hostname>:5250/spin/calm`

2. En el caso que apareciera una alerta de seguridad, realice lo siguiente:

   a. Haga clic en Ver certificado.

   b. Haga clic en Instalar certificado. A continuación, acepte los valores predeterminados y finalmente cierre el asistente de importación.

      Aparecerá una advertencia de seguridad informando acerca de la instalación de un certificado que afirma representar el nombre de host del servidor de CA User Activity Reporting Module.

   c. Haga clic en Sí.

      Una vez instalado el certificado root, aparecerá un mensaje informando acerca de la correcta importación.

   d. Haga clic en Aceptar.

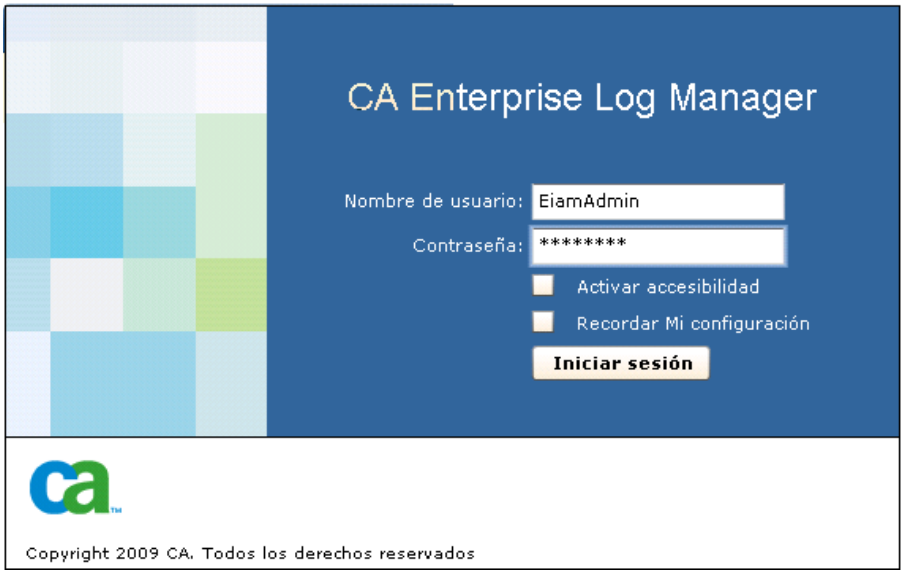
      Aparecerá el cuadro de diálogo Certificado de confianza.

   e. (Opcional) Haga clic en la Ruta de certificación y verifique que el estado del certificado sea correcto.

   f. Haga clic en Aceptar y, a continuación, en Sí.

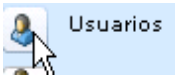
      Aparecerá la página de inicio de sesión.

3. Inicie sesión con el nombre de usuario EiamAdmin y la contraseña que creó al instalar el software. Haga clic en Iniciar sesión.

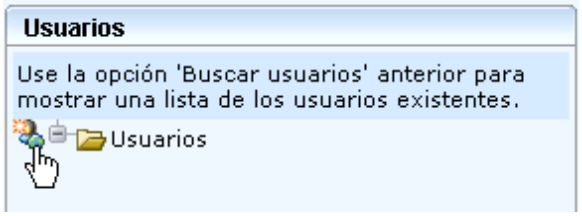


La aplicación se abrirá sólo con la ficha Administrator y la subficha Gestión de usuarios y accesos activas.

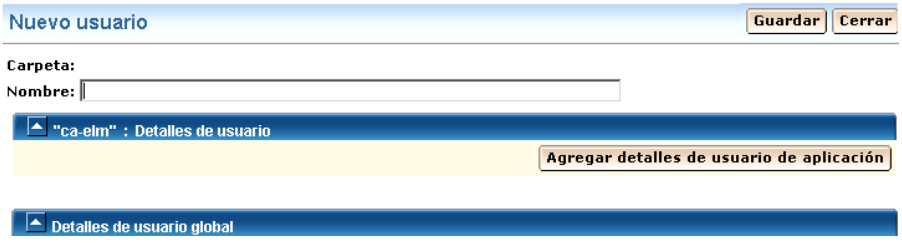
4. Haga clic en Usuarios.



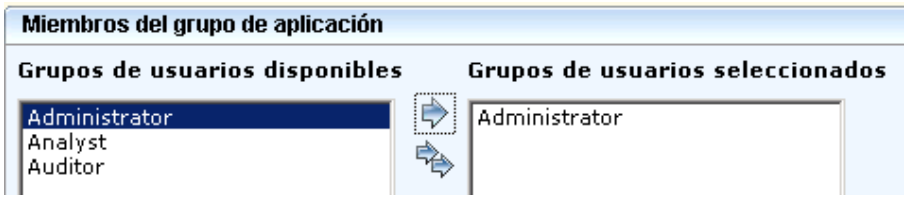
5. Haga clic en Agregar nuevo usuario.



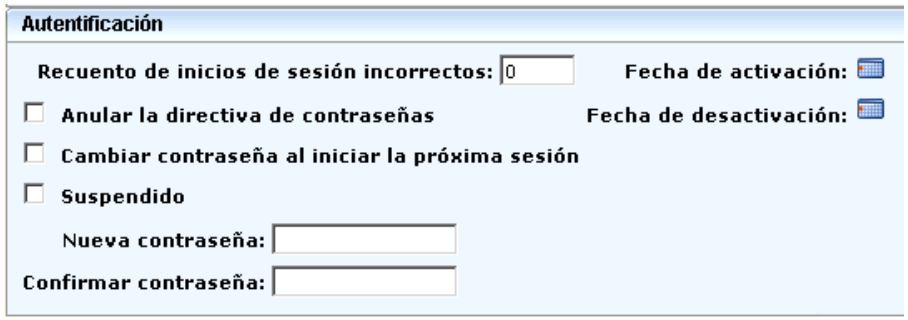
6. Introduzca su nombre en el campo Nombre y haga clic en Agregar detalles del usuario de la aplicación.



7. Seleccione Administrator y desplácelo a la lista Grupos de usuarios seleccionados.



8. En Autenticación, introduzca una contraseña para esta nueva cuenta en los dos campos, introducción y confirmación.



9. Haga clic en Guardar y, a continuación, en Cerrar. Haga clic en Cerrar.
10. Haga clic en el vínculo Cerrar sesión de la barra de herramientas.

    Aparecerá la página de inicio de sesión.
11. Vuelva a iniciar sesión en CA User Activity Reporting Module con las credenciales de Administrator que acaba de definir.

    CA User Activity Reporting Module se iniciará con todas las funcionalidades habilitadas. Se mostrarán la ficha Consultas e informes y la subficha Consultas.
12. (Opcional) Visualice los intentos de inicio de sesión de la manera siguiente:
    a. Seleccione el acceso al sistema de la lista de etiquetas de consulta.
    b. Seleccione Detalles del acceso al sistema de la lista de consultas.

    Los resultados de las consultas mostrarán dos intentos de inicio de sesión, el primero como EiamAdmin, y el segundo con su nombre de Administrator en donde los intentos de inicio de sesión se marcarán con una S en el caso que sean correctos.

Severidad de CA	Fecha	Cuenta	Ejecutor	Host	Nombr...	Categoría	Acción	Resultado
Información	Jueves, 05/11/09 19:59:24	EiamAdmin	EiamAdmin	ca-elm	CALM	System Access	Login Attempt	S
Información	Jueves, 05/11/09 20:00:22	EiamAdmin	EiamAdmin	ca-elm	CALM	System Access	Logoff	S
Información	Jueves, 05/11/09 20:44:32	admin	admin	ca-elm	CALM	System Access	Login Attempt	S
Información	Jueves, 05/11/09 21:07:47	admin	admin	ca-elm	CALM	System Access	Logoff	S

Configuración de los orígenes de eventos de syslog

Para activar la recopilación directa de eventos de syslog por el agente predeterminado que existe en cada uno de los servidores de CA User Activity Reporting Module, empiece por identificar los orígenes de los eventos de syslog desde donde desea recopilar eventos y determinar la integración asociada. A continuación, realice las dos operaciones siguientes en cualquier orden:

- Configure los orígenes de eventos de syslog. Inicie sesión en cada uno de los host donde se estén ejecutando los orígenes de los eventos de syslog. Configúrelos como documentados en la Guía de conectores para la integración de syslog.
- Configure el conector Syslog en el agente predeterminado para agregar las integraciones de syslog de destino asociadas con los orígenes de eventos configurados.

Tan pronto como se haya completado esta configuración de dos pasos, empezará la recopilación y refinamiento de eventos. En ese momento, ya se podrá utilizar CA User Activity Reporting Module para visualizar o generar informes de eventos que le interesan en un formato estándar. También podrá generar alertas durante la ocurrencia de eventos específicos.

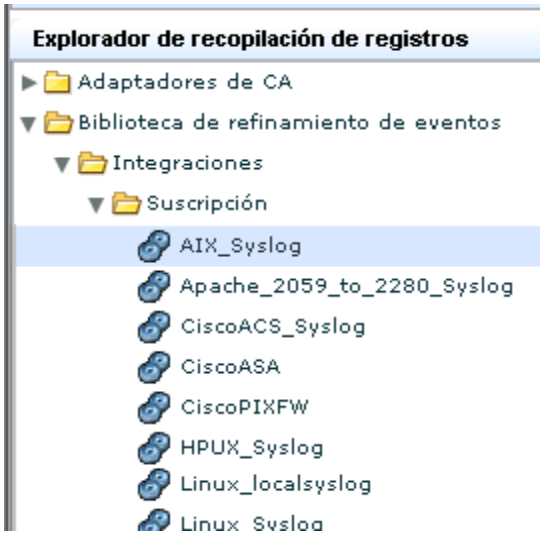
Cómo configurar un origen de evento de syslog seleccionado

1. Inicie sesión en el host con un origen de evento de syslog de destino.
2. Inicie CA User Activity Reporting Module desde un explorador del host.
3. Haga clic en la ficha Administración, y, después, en la subficha Recopilación de registros.

   Aparecerá el Explorador de recopilación de registros.

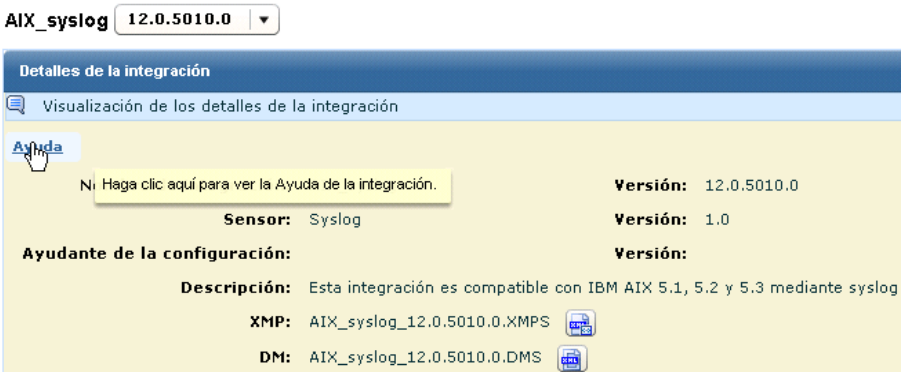
4. Expanda la Biblioteca de refinamiento de eventos> Integraciones> Suscripciones.

   Se mostrará la lista de integraciones predefinidas. A continuación, se muestra un ejemplo abreviado:



5. Seleccione la integración para el origen del evento que necesita configurar. Por ejemplo, si desea recopilar syslogs generados por un sistema operativo AIX, debería seleccionar AIX_Syslog.

   Se mostrarán los detalles de la integración.



6. Haga clic en el botón Ayuda, situado justo encima de Nombre de la integración en el panel derecho.

   Aparecerá la Guía de conectores para la integración seleccionada.

7. Haga clic en la sección en los requisitos de la configuración del origen del evento. En este ejemplo, la documentación describe cómo configurar e origen del evento del sistema operativo AIX para el envío de sus syslogs a CA User Activity Reporting Module.

1.0 Guía del conector para AIX

2.0 Requisitos previos

3.0 Configuración de AIX
3.1 Configuración de archivo de syslog
3.2 Escritura de un script PERL
3.3 Activación de auditoría
3.3.1 Cierre de auditoría
3.3.2 Configuración de archivos de directorio de auditoría
3.3.2.1 Configuración de archivo de objetos
3.3.2.2 Configuración del archivo de configuración
3.3.2.3 Configuración de archivo streamcmds
3.3.3 Modificación del archivo /etc/rc
3.3.4 Modificación del archivo /etc/shutdown
3.3.5 Inicio de auditoría

Ejemplo: origen alternativo para las Guías de conectores - soporte en línea.

Puede abrir una Guía de conectores seleccionada desde la interfaz de usuario de CA User Activity Reporting Module o desde Soporte de CA en línea. A continuación, se muestra un ejemplo que muestra cómo abrir una Guía de conectores desde este origen alternativo.

1. Inicie una sesión en el sitio de Soporte de CA en línea.
2. Seleccione CA Enterprise Log Manager de la lista desplegable de la página Seleccionar un producto.
3. Desplácese al Estado del producto y seleccione la Matriz de certificado de CA Enterprise Log Manager.
4. Seleccione la Matriz de integración del producto.
5. Busque la categoría para la integración asociada con el origen del evento que está configurando. Por ejemplo, si el origen del evento es el sistema operativo AIX, navegue hasta la categoría Sistemas operativos y haga clic en el vínculo AIX.

Producto	Versión	Sensor de
Sistemas operativos		
AIX	5.1 5.2 5.3	syslog

Edición del conector de syslog

Cada uno de los CA User Activity Reporting Module contiene un agente predeterminado. Una vez configurado CA User Activity Reporting Module, el agente predeterminado tendrá el conector Syslog_Connector, basado en la escucha Syslog, parcialmente configurado. La escucha recibe los eventos syslog sin formato en los puertos predeterminados tan pronto como se configuran los orígenes de los eventos y se envían los syslogs a CA User Activity Reporting Module. Sin embargo, para que CA User Activity Reporting Module refine estos eventos sin formato, deberá editar el Syslog_Connector. Algunas ediciones son obligatorias y otras opcionales.

- Debe especificar los destinos de syslog cuando edite este conector. Debe seleccionar como destinos de syslog cada una de las integraciones que correspondan a uno o más orígenes de eventos que configuró o planea configurar. La identificación de los destinos de syslog activará CA User Activity Reporting Module para poder refinar adecuadamente los eventos.
- Opcionalmente, puede aplicar las reglas de supresión, limitar la aceptación de syslogs en host de confianza, especificar los puertos de escucha en otros además del puerto 154 (el conocido puerto Syslog UDP) y del puerto 1468 (el puerto TCP predeterminado), y agregar una nueva zona horaria para el host de confianza.

Para configurar el conector Syslog para el agente predeterminado

1. Haga clic en la ficha Administración.

   Se mostrará la subficha Recopilación de registros.

2. Expanda el Explorador de agente y, a continuación, expanda el Grupo de agentes predeterminado o el grupo definido por el usuario con CA User Activity Reporting Module que se deberá configurar.

3. Seleccione el nombre del servidor de CA User Activity Reporting Module.

   Se mostrará el conector Syslog_Connector.

4. Haga clic en Editar.

   Aparecerá el asistente de edición del conector con el paso Detalles del conector seleccionado.

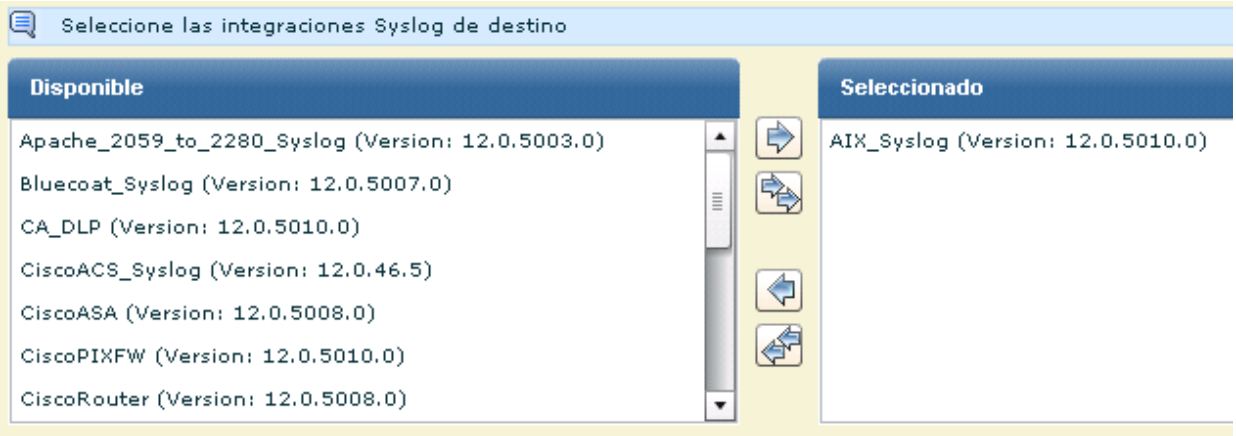
5. (Opcional) Haga clic en Aplicar reglas de supresión. Si existe algún tipo de evento de syslog que quiera suprimir , es decir, *no* recopilado, desplace el tipo de evento de la lista Disponible a la lista Seleccionado. Seleccione el evento para desplazarlo y haga clic en el botón Mover.

6. Seleccione el paso Configuración del conector.

   Se seleccionarán todas las integraciones de manera predeterminada.

7. Seleccione los destinos de syslog moviendo las integraciones de syslog al destino desde la lista Disponible a la lista Seleccionado.

   Por ejemplo, si ha configurado el sistema operativo AIX en un host de la red, debería mover el destino de syslog AIX_Syslog de la lista Disponible a la lista Seleccionado.



8. (Opcional) Identifique los host de confianza desde los cuales el conector Syslog aceptará los eventos entrantes. Introduzca la dirección IP en el campo de entrada y haga clic en Agregar. Repita la operación para cada uno de los host de confianza. De este modo, se rechazarán todos aquellos eventos que provengan de un host no configurado como de confianza.

   Nota: Se recomienda configurar los host de confianza. Normalmente, se configuran los host en los que se han configurado los orígenes de los eventos para que envíen los syslogs a CA User Activity Reporting Module. Si se especifican los orígenes de los host de confianza, se asegura de que el agente predeterminado no acepta eventos de sistemas rogue que un atacante ha configurado para enviar eventos a la escucha de syslog.

9. (Opcional) Agregue puertos.

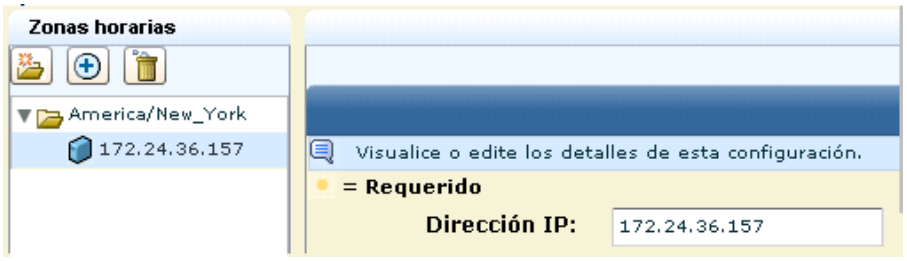
   Puede aceptar los puertos predeterminados UPD y TCP para el agente predeterminado.

   Nota: Para aumentar el rendimiento, defina un conector Syslog para diferentes tipos de eventos y especifique distintos puertos para cada uno de ellos. Asegúrese de que selecciona los puertos que no se utilizaron durante la asignación de nuevos puertos.

10. (Opcional) Agregue una zona horaria sólo si recopila syslogs de máquinas con zonas horarias distintas a las de soft-appliance.

    a. Haga clic en Crear carpeta y expándala.

    b. Resalte la entrada en blanco bajo la carpeta. Introduzca la dirección IP de un host de confianza que haya configurado para este conector o de un servidor horario NTP que haya especificado durante la instalación de CA User Activity Reporting Module.



11. Haga clic en Guardar y cerrar.

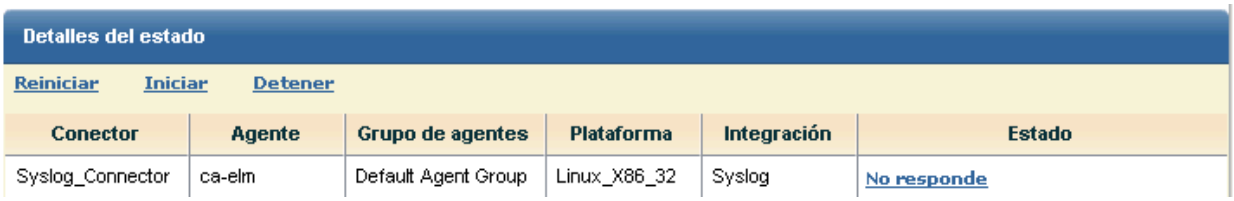
12. Visualice el estado.

    a. Haga clic en Estado y comando

Ver estado de los agentes está seleccionado. Dado que el agente predeterminado se encuentra en este servidor, en la columna Agente aparecerá el nombre de host del servidor que instaló. El estado se mostrará en ejecución.

b. Haga clic en el vínculo En ejecución para visualizar los detalles.

c. Haga clic en el botón Conectores para comprobar el estado de los conectores.



d. Haga clic en el vínculo En ejecución.

Aparecerá el porcentaje de la CPU, el uso de la memoria, el promedio de eventos por segundo (EPS) y el recuento de eventos filtrados.

Visualización de eventos syslog

Una de la maneras más rápidas de visualizar los resultados de las consultas en los eventos recopilados por la escucha de syslog es la utilización de la Petición para el host.

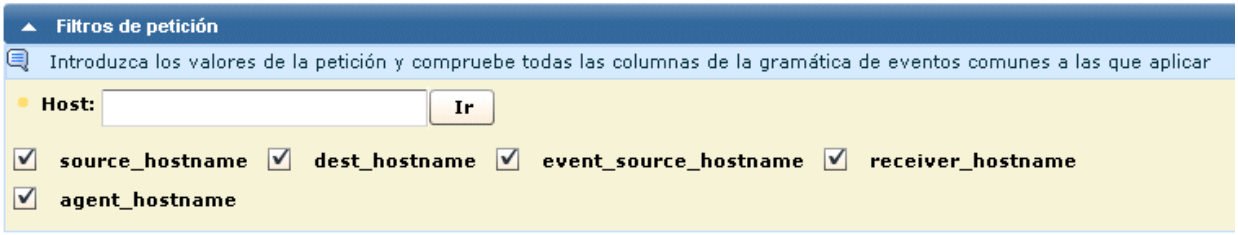
Cómo visualizar eventos de syslog

1. Seleccione la ficha Consultas e informes.

   Aparecerá la subficha Consultas.

2. Expanda las peticiones bajo la lista de consultas y seleccione Host.

3. Envíe la consulta para los eventos recopilados por el agente predeterminado.
   a. Introduzca el nombre de host del agente predeterminado, que también es el nombre del CA User Activity Reporting Module donde está ubicado, en el campo Host.
   b. Seleccione agent_hostname.
   c. Haga clic en Ir.



4. Visualice los resultados que quiera examinar.
   a. Haga clic en la columna Resultados para filtrar por resultado.
   b. Desplácese hasta el primer resultado F para error. Suponga que se trata de una advertencia de configuración en la categoría de gestión de la configuración.
   c. Haga doble clic para seleccionar la fila y así visualizar los detalles.

   Aparecerá el Visor de eventos.

5. Desplácese hasta el área donde se muestran los resultados. En el ejemplo se muestra un error de advertencia que indica la necesidad de configurar el módulo de suscripción. Ignore la advertencia hasta que haya terminado con la instalación de todos los servidores de CA User Activity Reporting Module que desea instalar.

Capítulo 3: Implementación del agente para Windows

Esta sección contiene los siguientes temas:

Creación de una cuenta de usuario para el agente (en la página 36)
Configuración de la clave de autenticación del agente (en la página 38)
Descarga del programa de instalación del agente (en la página 39)
Instalación del agente (en la página 40)
Creación de un conector basado en NTEventLog (en la página 43)
Configuración de un origen de eventos de Windows (en la página 47)
Visualización de registros de los orígenes de eventos de Windows (en la página 47)

Creación de una cuenta de usuario para el agente

Antes de instalar el agente en un sistema operativo Windows, puede crear una nueva cuenta de usuario para el agente en la carpeta Usuarios de Windows. El propósito de crear esta cuenta de usuario con privilegios bajos para el agente es la de permitir al agente ejecutarse con el menor número de privilegios posible. Proporcione el nombre de usuario y la contraseña que creó durante la instalación del agente.

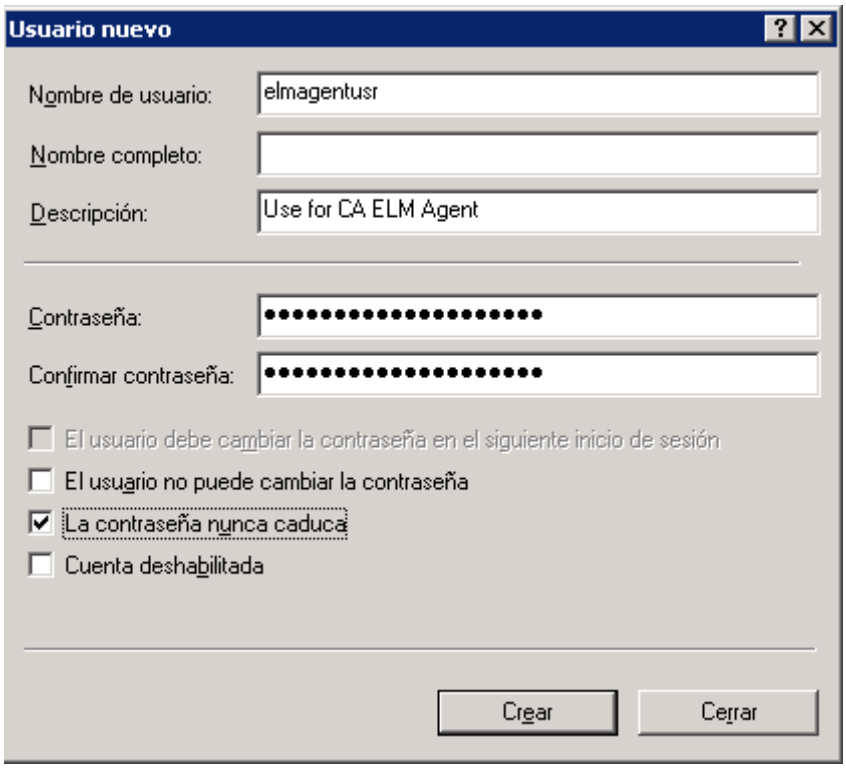
Nota: .Aunque no es recomendable, puede omitir este paso y especificar las credenciales de dominio de un Administrator para el agente durante la instalación.

Para crear una cuenta de usuario de Windows para el agente

1. Inicie sesión en el host donde pretende instalar el agente. Utilice credenciales administrativas.
2. Haga clic en Inicio> Archivos de programa> Herramientas administrativas> Gestión de equipos.
3. Expanda Grupos y usuarios locales.
4. Haga clic con el botón secundario en Usuarios y seleccione Nuevo usuario.

   Aparecerá el cuadro de diálogo de Windows Nuevo usuario.
5. Introduzca un nombre de usuario e introduzca la contraseña dos veces. Una contraseña segura es aquella que alterna caracteres alfa, numéricos y especiales. Por ejemplo, calmr12_agent. Opcionalmente, escriba una descripción.

   Importante: recuerde este nombre y contraseña o anótelos. Deberá introducirlos cuando instale el agente.



6. Haga clic en Crear. Haga clic en Cerrar.

Más información:

Instalación del agente (en la página 40)

Configuración de la clave de autenticación del agente

Antes de poder instalar el primer agente, debe conocer de antemano la clave de autenticación del agente. Si no se ha establecido ninguna clave con anterioridad, puede utilizar la clave predeterminada. En el caso que ya se haya configurado una clave, utilice la clave actual o configure una nueva. Durante la instalación de cada uno de los agentes, se deberá introducir la clave de autenticación del agente configurada. Está operación sólo la podrá realizar el Administrator.

Para configurar la clave de autenticación del agente.

1. Abra el explorador en el host donde planea instalar el agente e introduzca la URL del servidor de CA User Activity Reporting Module para este agente. A continuación, se muestra un ejemplo:

   `https://<dirección IP>:5250/spin/calm`

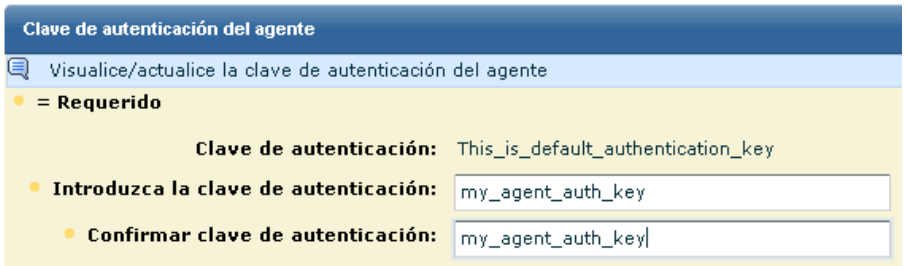
2. Inicie sesión en CA User Activity Reporting Module. Introduzca su nombre de usuario y contraseña y haga clic en Iniciar sesión.
3. Haga clic en la ficha Administración.

   En el panel izquierdo, se mostrará el Explorador de recopilación de registros.
4. Seleccione la carpeta Explorador de agente.

   Aparecerá una barra de herramientas en el panel principal.
5. Haga clic Clave de autenticación del agente.

6. Introduzca la clave de autenticación del agente que utilizará durante la instalación del agente o anote la entrada actual.

   Importante: recuerde o anote esta clave. La necesitará durante la instalación.



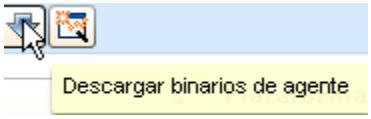
7. Haga clic en Guardar.
8. Continúe con el siguiente paso, Descarga del programa de instalación del agente.

Descarga del programa de instalación del agente

Una vez configurada la clave de autenticación del agente, podrá descargar el programa de instalación del agente en el escritorio.

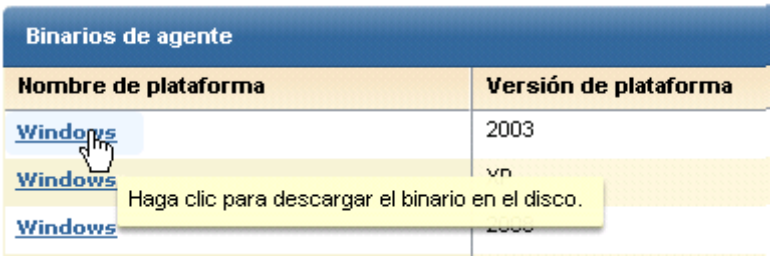
Para descargar el programa de instalación del agente

1. Haga clic en Descargar binarios de agente en la barra de herramientas que se muestra en el Explorador de agente.



   En el panel principal se mostrarán una serie vínculos disponibles para los binarios del agente.

2. Haga clic en el vínculo de Windows para instalar el agente en un servidor con un sistema operativo Windows Server 2003.



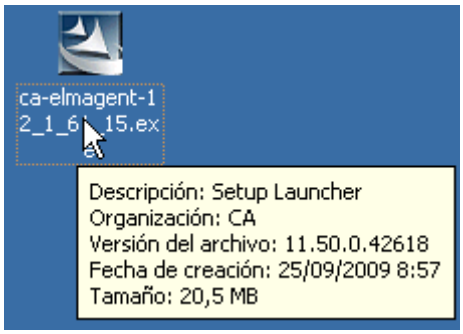
   Aparecerá el cuadro de diálogo Seleccionar ubicación para la descarga por <dirección IP>.

3. Seleccione el escritorio y haga clic en Guardar.

Aparecerá un mensaje informando acerca del progreso de la descarga del binario del agente, seguido de un mensaje de confirmación.

4. Haga clic en Aceptar.
5. Minimice el explorador pero mantenga la conexión abierta de modo que, una vez completada, pueda verificar de manera rápida la instalación.

   En el escritorio aparecerá el programa de inicio de la instalación para el programa de instalación del agente.



Instalación del agente

Antes de empezar con la instalación, prepare la siguiente información:

- Dirección IP del servidor de CA User Activity Reporting Module desde donde descargó el programa del agente
- El nombre de usuario y contraseña de la cuenta de usuario que creó para el agente
- La clave de autenticación del agente que configuró

Para instalar el agente en un host de Windows

1. Haga doble clic en el iniciador de la instalación del agente.

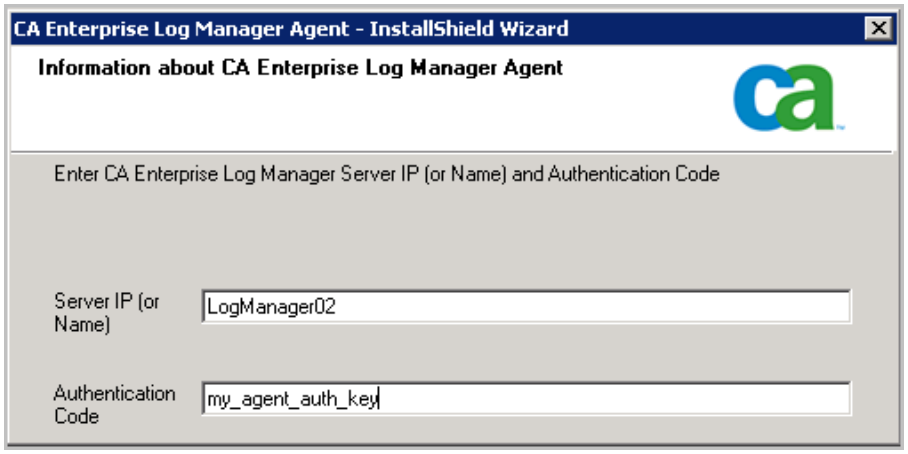
Se iniciará el asistente de instalación.

2. Haga clic en Siguiente. A continuación, lea detenidamente la licencia y haga clic en Acepto los términos de los acuerdos de licencia. Para continuar, haga clic en Siguiente.
3. Acepte o modifique la ruta de instalación y, a continuación, haga clic en Siguiente.
4. Introduzca la información solicitada de la manera siguiente:
   a. Introduzca el nombre de host para CA User Activity Reporting Module al que el agente enviará los registros que haya recopilado.

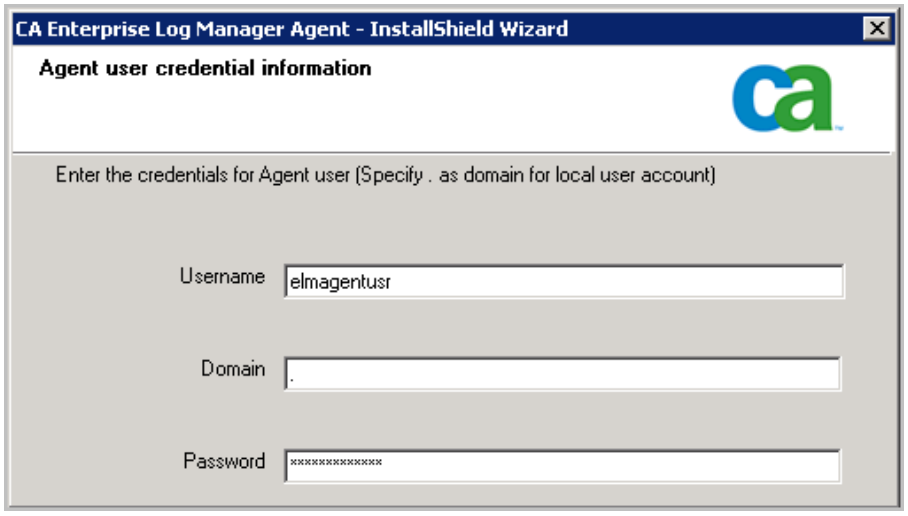
      Nota: Dado que en este ejemplo, CA User Activity Reporting Module utiliza DHCP para la asignación de la dirección IP, no deberá introducir la dirección IP aquí. Si lo hiciera, es posible que tuviera que volver a instalar el agente si se modificase la dirección IP del servidor.

   b. Introduzca la clave de autenticación del agente.

   A continuación, se muestra un ejemplo:



5. Introduzca el nombre y contraseña definidos en la cuenta de usuario que configuró para el agente y, a continuación, haga clic en Siguiente.



6. Haga clic en Siguiente. Opcionalmente, podrá especificar un archivo Connector exportado.

   Aparecerá la página Iniciar copia de archivos.

7. Haga clic en Siguiente.

   Se completará el proceso de instalación.

8. Haga clic en Finalizar.

9. Continúe con la configuración de conectores para este agente.

   Una vez configurados los conectores, se enviarán los eventos recopilados al almacén de registro de eventos de CA User Activity Reporting Module a través del puerto 17001.

   Importante: si no permite el tráfico saliente del host en el que instaló el agente y utiliza el cortafuegos de Windows, deberá abrir este puerto en el cortafuegos de Windows.

Más información:

Descarga del programa de instalación del agente (en la página 39)
Creación de una cuenta de usuario para el agente (en la página 36)
Configuración de la clave de autenticación del agente (en la página 38)

Creación de un conector basado en NTEventLog

Una vez instalado el agente, se creará un conector para especificar los orígenes del evento para eventos que quiera recopilar. Dado que instaló un agente en un servidor que trabaja con un sistema operativo Windows, deberá crear un conector basado en una integración de NTEventLog y especificar los valores de configuración para WMILogSensor tal y como se describe en la Guía del conector que abrió desde el asistente de creación del nuevo conector. Especifique el nombre de host en el que se instaló el agente para la recopilación de registros basada en el agente. De manera opcional, podrá agregar otro sensor de registro WMI para este conector y especificar un host, a parte del host donde instaló el agente. Con ello activará la conexión de registros sin agentes. Los host adicionales deben encontrarse en el mismo dominio y estar bajo el mismo Administrator de Windows que el primer host que se agregó.

Para configurar el conector basado en NTEventLog

1. Maximice el explorador de modo que se muestre el Explorador de agente de CA User Activity Reporting Module.
2. Expanda primero el Explorador de agente, y, a continuación, el Grupo de agentes predeterminado.

   Aparecerá el nombre del equipo donde instaló el agente.

3. Seleccione este agente.

   Aparecerá el panel Conectores de agente.

4. Haga clic en Crear nuevo conector

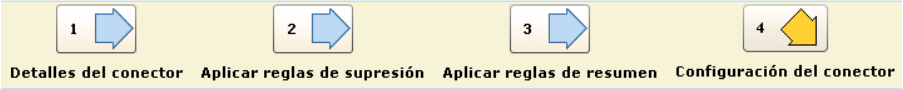
Aparecerá el asistente de creación del nuevo conector con el paso Detalles del conector seleccionado.

5. Mantenga la integración seleccionada, y seleccione NTEventLog de la lista desplegable de la integración.

   Se rellenarán los campos Nombre de conector y Descripción del conector según la integración seleccionada.

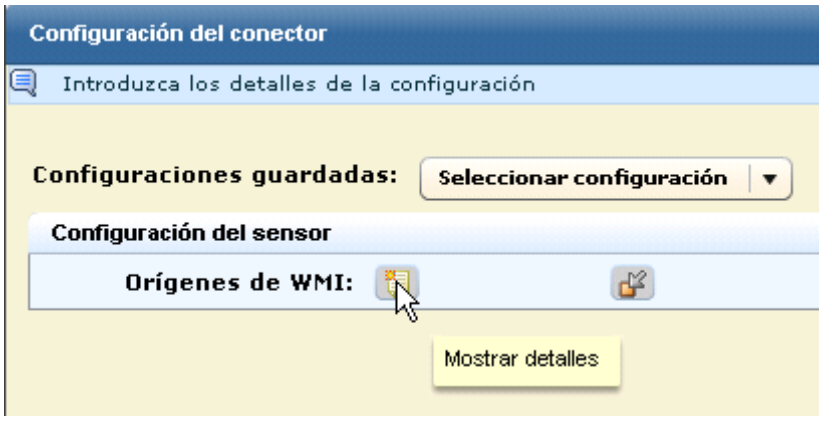
6. Edite el nombre del conector para hacerlo único. Considere la extensión del nombre con el nombre del servidor de destino. Por ejemplo: NTEventLog_Connector_USER001LAB.

7. Seleccione el paso Configuración del conector.



Aparecerá el panel Configuración del sensor con un botón de ayuda para la Guía del conector para NTEventLog, que proporciona ayuda en los campos de la configuración del agente.

8. Haga clic en el botón Mostrar detalles para los orígenes de WMI.



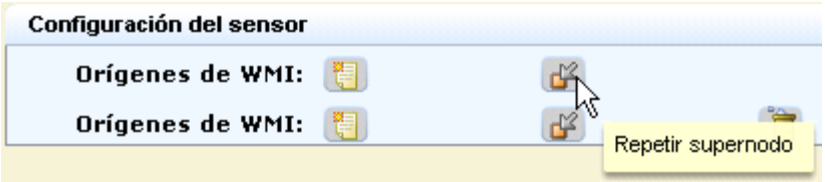
9. Configure los valores de configuración de WMILogSensor para el equipo local para la recopilación de registros basada en el agente. Para obtener más detalles, haga clic en el vínculo Ayuda.

   El ejemplo siguiente muestra una configuración en la que el usuario del servidor WMI especificado es el Administrator de Windows. El dominio será para el servidor de WMI.

10. (Opcional) Configure un sensor WMI para un equipo diferente para la recopilación de registros sin agentes mediante el mismo conector.

    a. Haga clic en el botón Repetir supernodo.

       El dibujo siguiente muestra una configuración con dos orígenes de WMI.



b. Configure los valores de configuración de WMILogSensor para otro equipo.

El ejemplo siguiente muestra una configuración para un segundo sensor de registro WMI en el mismo dominio y con las mismas credenciales de Administrator.

11. Haga clic en Guardar y cerrar.
12. Para visualizar el estado del conector que ha configurado, realice los pasos siguientes:
    a. Seleccione el agente del panel izquierdo.
    b. Haga clic en Estado y comando.
    c. Seleccione Ver estado de los conectores.

    Aparecerá el panel Detalles del estado.

13. Haga clic en el vínculo En ejecución.

    El estado que se muestra del destino configurado en el conector incluye información acerca del porcentaje de la CPU, el uso de la memoria y el promedio de eventos por segundo (EPS).

Configuración de un origen de eventos de Windows

Una vez configurado el conector mediante la utilización de la integración de NTEventLog en el agente, debe ser capaz de visualizar los eventos a través del Visor de eventos. Si los eventos no se envían al Visor de eventos, debe cambiar la configuración de Windows para las políticas locales en el origen del evento.

Cómo configurar las políticas locales en el origen del evento para un conector NTEventLog.

1. Si no se muestra el Explorador de recopilación de eventos, haga clic en la ficha Administración.
2. Expanda la Biblioteca de refinamiento de eventos> Integraciones> Suscripción y seleccione NTEventLog. Por último, haga clic en el vínculo Ayuda, ubicado justo encima de Nombre de la integración en el panel Visualización de los detalles de la integración.

   Aparecerá la Guía de conectores para el registro de eventos de NT (seguridad, aplicación, sistema).
3. Minimice la interfaz de usuario de CA User Activity Reporting Module y siga las instrucciones de la Guía de conectores para la edición de políticas locales en un origen de evento que se ejecuta en un sistema operativo Windows.

   Nota: .Si trabaja con Windows Server 2003, seleccione el Panel de control> Herramientas administrativas> Política de seguridad local, y a continuación, expanda Políticas locales.
4. (Opcional) Si configuró un sensor WMI para un segundo sensor WMI, edite las políticas locales en ese servidor.
5. Maximice CA User Activity Reporting Module.

Visualización de registros de los orígenes de eventos de Windows

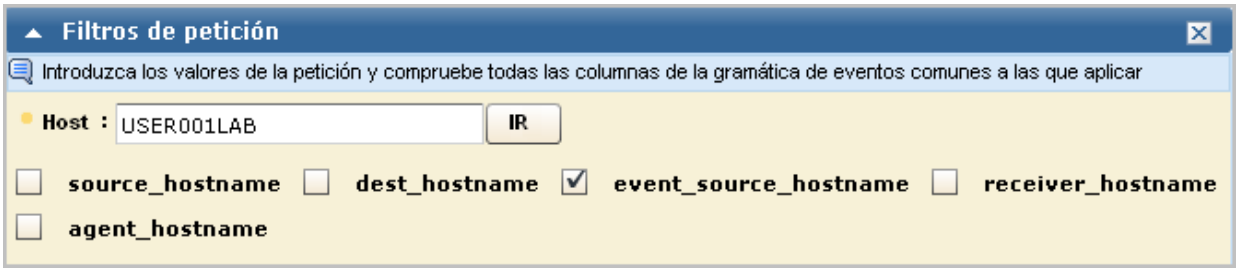
Una de las maneras más rápidas de visualizar los resultados de una consulta en eventos entrantes es el uso de Petición para el host. También se pueden utilizar consultas e informes.

Para visualizar registros de eventos entrantes

1. Seleccione la ficha Consultas e informes.

   Aparecerá la subficha Consultas.
2. Expanda las peticiones bajo la lista de consultas y seleccione Host.

3. Introduzca el nombre de servidor WMI configurado para el sensor en el campo Host. Deseleccione el resto y haga clic en Ir.



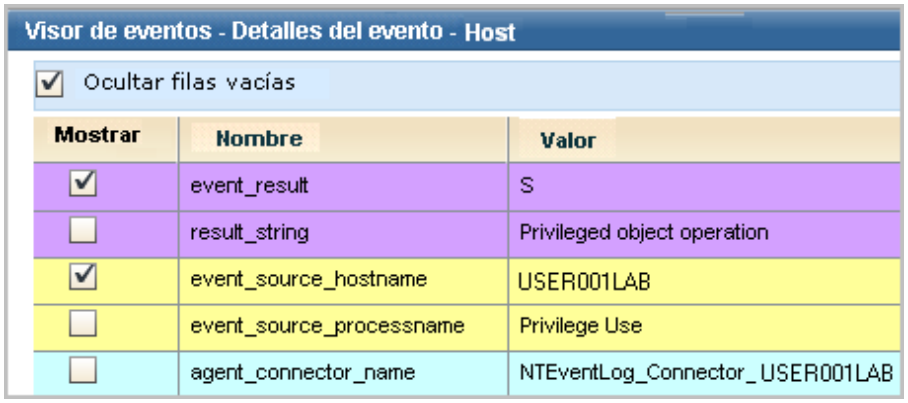
Aparecerán los orígenes de los eventos del servidor WMI.

4. Haga clic en Severidad de CA y desplácese hasta encontrar una advertencia. A continuación, se muestra un ejemplo sin las columnas Fecha y Origen de eventos:

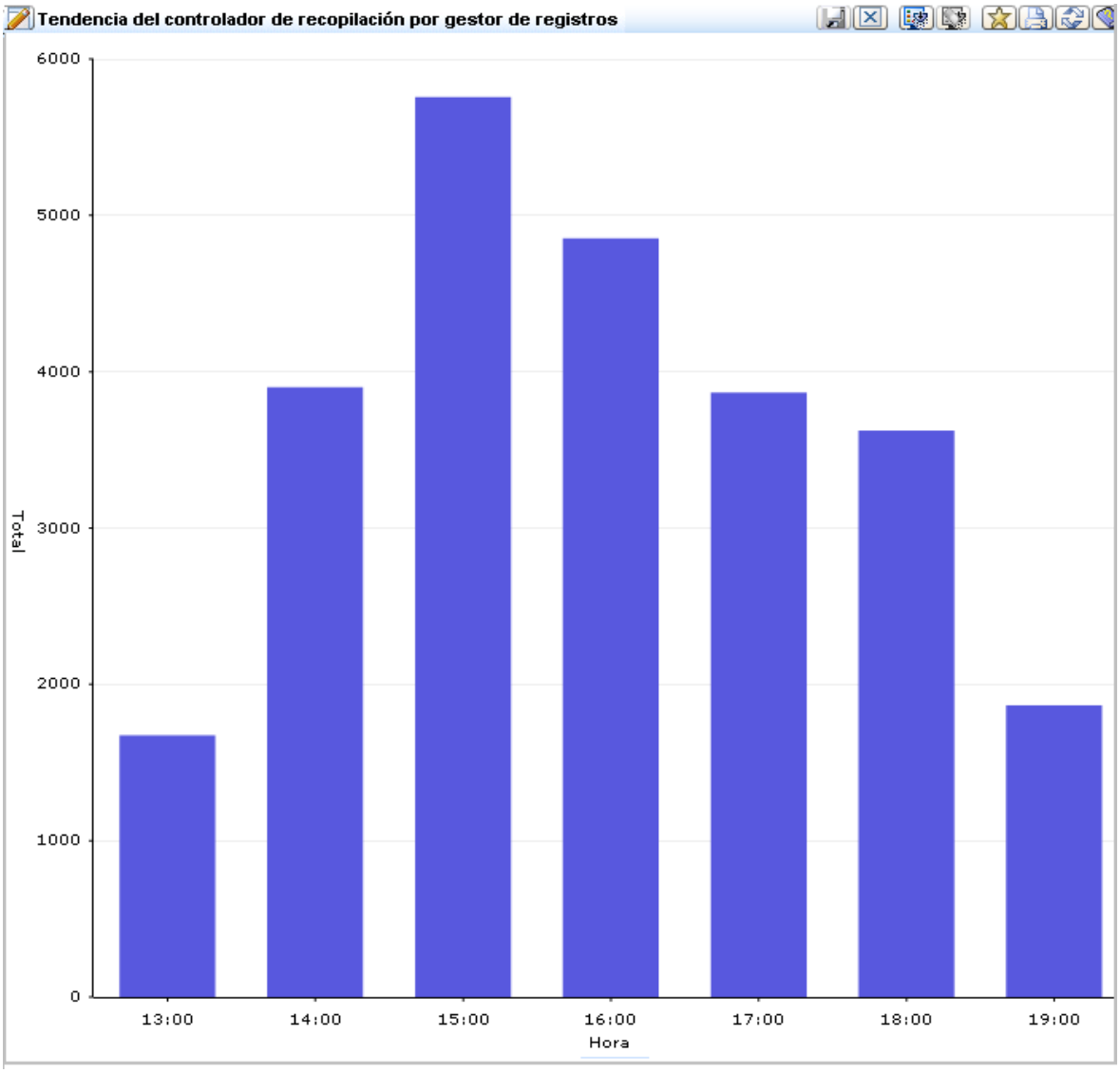
Severidad de CA	Usuario de origen	Resultado	Categoría	Acción	Nombre de registro
Advertencia	calm_agent	S	System Access	Privilege Use	NT-Security

5. Haga clic en Mostrar evento sin formato para mostrar los eventos sin formato de la advertencia.

6. Haga doble clic en la advertencia para mostrar el Visor de eventos con los datos ampliados. A continuación, se muestra una pequeña selección de filas de datos:



7. Haga clic en la ficha Consultas e informes. A continuación, haga clic en una consulta de la lista de consultas , como por ejemplo, Tendencia del controlador de recopilación por gestor de registros. Se mostrará el gráfico de barras resultante.



8. Haga clic en Informes. En la Lista de informes, utilice el campo Buscar para visualizar el nombre de informe Eventos autocontrolados del sistema. Seleccione el informe para que éste muestre una lista de los eventos que ha generado el servidor de CA User Activity Reporting Module.

Nota: Para obtener información detallada y de análisis sobre la programación de informes, consulte la Ayuda en línea o la *Guía de administración*.

Capítulo 4: Funcionalidades clave

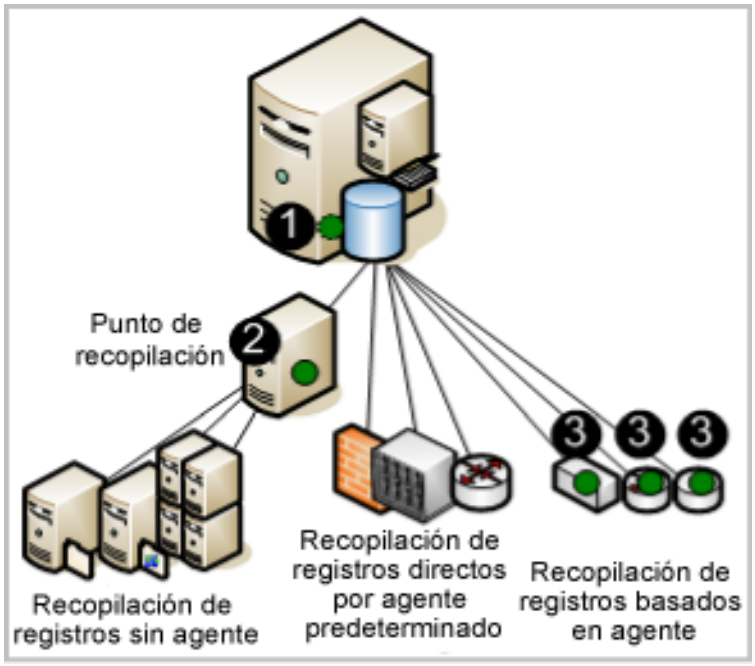
Esta sección contiene los siguientes temas:

Recopilación de registros (en la página 51)
Almacenamiento de registros (en la página 53)
Presentación estandarizada de los registros (en la página 55)
Generación de informes de cumplimiento (en la página 56)
Generación de alertas de infracción de política (en la página 58)
Gestión de la titularidad (en la página 59)
Acceso basado en roles (en la página 60)
Gestión de suscripciones (en la página 61)
Contenido predeterminado (en la página 62)

Recopilación de registros

El servidor de CA User Activity Reporting Module puede configurarse para recopilar registros utilizando una o más técnicas compatibles. Las técnicas difieren en el tipo y ubicación del componente que escucha y recopila los registros. Estos componentes se configuran en los agentes.

La ilustración siguiente muestra un sistema de servidor único, donde las ubicaciones del agente están indicadas con un círculo oscuro (verde).



Los números de la ilustración se refieren a los pasos siguientes:

1. Configure el agente predeterminado en CA User Activity Reporting Module para buscar eventos directamente desde los orígenes de syslog que especifique.
2. Configure el agente instalado en un punto de recopilación de Windows para recopilar eventos desde los servidores de Windows que especifique y transmítalos a CA User Activity Reporting Module.
3. Configure los agentes instalados en host donde los orígenes de los eventos se ejecutan para recopilar el tipo de eventos configurado y realizar la supresión.

Nota: El tráfico desde el agente al servidor de destino de CA User Activity Reporting Module está siempre cifrado.

Considere las ventajas siguientes de cada una de las técnicas de recopilación de registros:

- Recopilación de registros directa

  Con la recopilación de registros directa, se configura la escucha de syslog en el agente predeterminado para recibir eventos de los orígenes de confianza que usted especifique. También puede configurar otros conectores para recopilar eventos desde cualquier origen de evento que sea compatible con el entorno operativo del dispositivo de software.

  Ventaja: no necesita instalar un agente para recopilar registros desde los orígenes de los eventos que se encuentran en una proximidad de red cercana al servidor de CA User Activity Reporting Module.

- Recopilación sin agentes

  Con la recopilación sin agentes, en los orígenes del evento no se encuentra ningún agente. En cambio, el agente se instala en un punto de recopilación dedicado. Los conectores para cada origen de evento de destino se configuran en dicho agente.

  Ventaja: puede recopilar registros de recopilación en orígenes de eventos que se ejecutan en servidores en los que no puede instalar agentes, como, por ejemplo, servidores donde los agentes están prohibidos por la política corporativa. Se garantiza la entrega, por ejemplo, si la recopilación de registros de ODBC está configurada de manera correcta.

- Recopilación basada en el agente

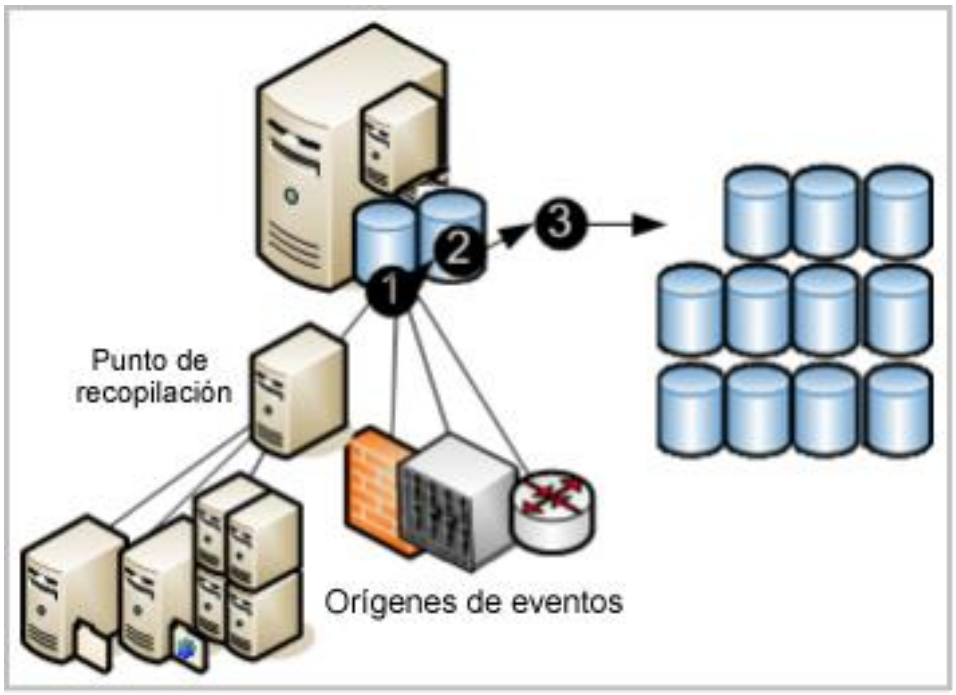
  Con la recopilación basada en el agente, se instala un agente donde un o más orígenes de eventos se ejecutan y donde se configura un conector para cada origen de evento.

  Ventaja: puede recopilar registros de un origen donde el ancho de banda de la red entre el dicho origen y
  CA User Activity Reporting Module no es suficientemente bueno contemplar la recopilación directa de registros. Puede utilizar el agente para filtrar los eventos y reducir el tráfico enviado a través de la red. Se garantiza la entrega de eventos.

Nota: Consulte la *Guía de administración* para obtener más información acerca de la configuración del agente.

Almacenamiento de registros

CA User Activity Reporting Module proporciona almacenamiento de registros incrustados gestionado para bases de datos archivadas recientemente. Los eventos recopilados por agentes en orígenes de eventos pasan por un ciclo de vida de almacenamiento, tal y como muestra el diagrama siguiente.



Los números de la ilustración se refieren a los pasos siguientes:

1. Los nuevos eventos recopilados por cualquier técnica se envían a CA User Activity Reporting Module. El estado de eventos entrantes depende de la técnica utilizada para recopilarlos. Los eventos entrantes deben refinarse antes de insertarse en la base de datos.
2. Cuando la base de datos de las entradas refinadas alcanza el tamaño configurado, todas las entradas se comprimen en una base de datos y se guardan con un nombre único. La compresión de datos de registros reduce el coste de su reubicación y del almacenamiento. La base de datos comprimida puede moverse automáticamente según la configuración del Autoarchivar o se puede realizar una copia de seguridad y moverla manualmente antes de que alcance la antigüedad configurada para su supresión. (Las bases de datos autoarchivadas se eliminan del origen en cuanto se mueven.)
3. Si configura Autoarchivar para mover diariamente las bases de datos comprimidas a un servidor remoto, puede mover esta copia a un almacén de registros a largo plazo y fuera del sitio cuando lo desee. La retención de copias de seguridad de registros le permite cumplir con las regulaciones que enuncian que los registros deben recopilarse de manera segura, almacenarse de forma central durante cierto número de años y deben estar disponibles para su revisión. (Puede restaurar una base de datos a partir de un almacenamiento de largo plazo en cualquier momento.)

Nota: Puede consultar la *Guía de implementación* para obtener más información acerca de la configuración del almacén de registro de eventos, incluyendo cómo configurar la autoarchivación. Consulte la *Guía de administración* para obtener más información acerca de la restauración de copias de seguridad para la investigación y la generación de informes.

Presentación estandarizada de los registros

Los registros generados por aplicaciones, sistemas operativos y dispositivos utilizan sus propios formatos. CA User Activity Reporting Module refina los registros recopilados para estandarizar la manera cómo se registran los datos. El formato estándar facilita a Auditors y a altos cargos la comparación de datos recopilados de distintos orígenes. Técnicamente, la gramática de eventos comunes (CEG) de CA ayuda a implementar la normalización y la clasificación de eventos.

La CEG proporciona distintos campos utilizados para la normalización de varios aspectos del evento, incluyendo lo siguiente:

- Modelo ideal (clase de tecnología como antivirus, DBMS y cortafuegos)
- Categoría (incluye ejemplos sobre gestión de identidades y seguridad de red)
- Clase (incluye ejemplos sobre gestión de cuentas y de grupos)
- Acción (incluye ejemplos sobre creación de cuentas y de grupos)
- Resultados (incluye ejemplos sobre acciones con éxito y erróneas)

Nota: Consulte la *Guía de administración de CA User Activity Reporting Module* para obtener más detalles acerca de las reglas y archivos usados en el refinamiento de eventos. Consulte la sección que trata acerca de la gramática de eventos comunes en la ayuda en línea para obtener información acerca de la normalización y la categorización de eventos.

Generación de informes de cumplimiento

CA User Activity Reporting Module permite recopilar y procesar datos relevantes para la seguridad y convertirlos en informes adecuados para Auditors internos y externos. Permite, además, interactuar con consultas e informes para llevar a cabo investigaciones. Se puede automatizar el proceso de generación de informes mediante la programación de tareas de informes.

El sistema proporciona:

- Funcionalidad de consulta con etiquetas de fácil uso
- Generación de informes casi a tiempo real
- Archivos de registros críticos distribuidos de modo que permiten búsquedas centralizadas

Se centra en la generación de informes de cumplimiento antes que en la correlación de eventos y alertas en tiempo real. La reglamentación exige la generación de informes que demuestren la conformidad con los controles en el campo de la industria. Para una fácil y rápida identificación,
CA User Activity Reporting Module proporciona informes con las etiquetas siguientes:

- Basel II
- COBIT
- COSO
- Directiva de la UE relativa a la protección de datos
- FISMA
- GLBA
- HIPAA
- ISO\IEC 27001\2
- JPIPA
- JSOX
- NERC
- NISPOM
- PCI
- SAS 70
- SOX

Se pueden revisar los informes de registros predefinidos o realizar búsquedas basadas en criterios específicos. Los nuevos informes se proporcionarán con actualizaciones de suscripción.

Las funcionalidades de visualización de registros son compatibles con:

- La capacidad de consulta a petición con consultas predefinidas o definidas por el usuario con hasta 5.000 registros por resultado
- La búsqueda rápida, mediante peticiones, de un nombre de host, dirección IP, número de puerto o nombre de usuario determinado
- La generación de informes a petición y de forma programada con contenido de generación de informes predefinido
- Las consultas y generación de alertas programadas
- Los informes básicos con información acerca de la tendencia
- Los visualizadores de eventos gráficos e interactivos
- La generación automática de informes con adjunto de correo electrónico
- Las políticas de retención automática de informes

Nota: Para la obtención de más detalles acerca del uso de consultas e informes predefinidos o de la generación de consultas e informes propios, consulte la *Guía de administración de CA User Activity Reporting Module.*

Generación de alertas de infracción de política

CA User Activity Reporting Module permite automatizar el envío de una alerta cuando se produce un evento que requiere una atención a corto plazo. También se pueden controlar las alertas de acción de CA User Activity Reporting Module a cualquier hora del día mediante la especificación de un intervalo de tiempo (por ejemplo, desde los últimos cinco minutos a los últimos 30 días). Las alertas también se envían automáticamente a una fuente RSS a la que se pueda acceder desde una explorador Web. Opcionalmente, puede especificar otros destinos, incluidas direcciones de correo electrónico, un proceso CA IT PAM como uno que genera partes del departamento de asistencia, y una o varias direcciones IP de destino de trap de SNMP.

Para ayudarle a comenzar, hay múltiples consultas predefinidas disponibles para su programación como alertas de acción directamente. Los ejemplos incluyen:

- Actividad de usuario excesiva
- Promedio de uso de la CPU alto
- Espacio en disco disponible bajo
- Registro de eventos de seguridad eliminado en las últimas 24 horas
- Se ha modificado la política de auditoría de Windows durante las últimas 24 horas

Algunas consultas utilizan listas con clave en las que se proporcionan los valores utilizados en la consulta. Existen algunas listas con clave que incluyen valores predefinidos que puede complementar. Los ejemplos incluyen cuentas predeterminadas y grupos con privilegios. Otras listas con clave, como las de recursos críticos para el negocio, no contienen valores predeterminados. Una vez configuradas, se pueden programas las alertas para consultas predeterminadas como:

- Adición o eliminación de pertenencia a grupo por grupo de privilegios
- Inicio de sesión correcto por cuenta predeterminada
- No se han recibido eventos de las fuentes críticas del negocio

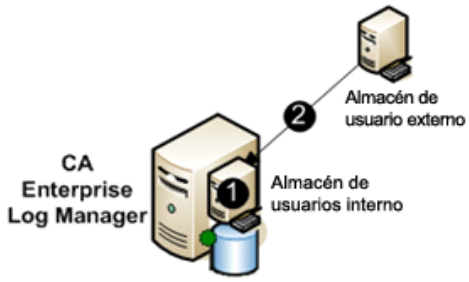
Las listas con clave se pueden actualizar de forma manual, importando un archivo o ejecutando un proceso de valores dinámicos de CA IT PAM.

Nota: Consulte la *Guía de administración de CA User Activity Reporting Module* para obtener detalles sobre las alertas de acción.

Gestión de la titularidad

Cuando configura el almacén de usuarios, debe elegir si desea utilizar el almacén predeterminado de usuarios en CA User Activity Reporting Module para configurar cuentas de usuario o utilizar un almacén de usuario externo donde las cuentas de usuario ya están definidas. La base de datos subyacente es exclusiva de CA User Activity Reporting Module y no utiliza un DBMS comercial.

Los almacenes de usuario externos compatibles incluyen CA SiteMinder y directorios LDAP, como Microsoft Active Directory, Sun One y Novell eDirectory. Si utiliza un almacén de usuario externo, la información de cuenta de usuario se carga de manera automática en formato de sólo lectura, como muestra la flecha del siguiente diagrama. Usted define sólo información específica de la aplicación en las cuentas seleccionadas. No se transfieren datos del almacén de usuario interno al almacén de usuario externo utilizado.



Los números de la ilustración hacen referencia a los tres pasos siguientes:

1. El almacén de usuarios interno realiza la gestión de titularidad mediante la autenticación de las credenciales introducidas por los usuarios en el inicio de sesión y la autorización a los usuarios para que accedan a las diferentes funcionalidades de la interfaz de usuario basadas en las políticas asociadas con los roles asignados a sus cuentas de usuario. Si el nombre y contraseña de usuario con los que se intenta iniciar sesión los ha cargado un almacén de usuarios externo, las credenciales introducidas deberán coincidir con las credenciales cargadas.
2. El almacén de usuario externo tiene la única función de cargar las cuentas de sus usuarios en el almacén de usuarios interno. Éstas se cargan de manera automática cuando se guarda la remisión al almacén de usuarios.

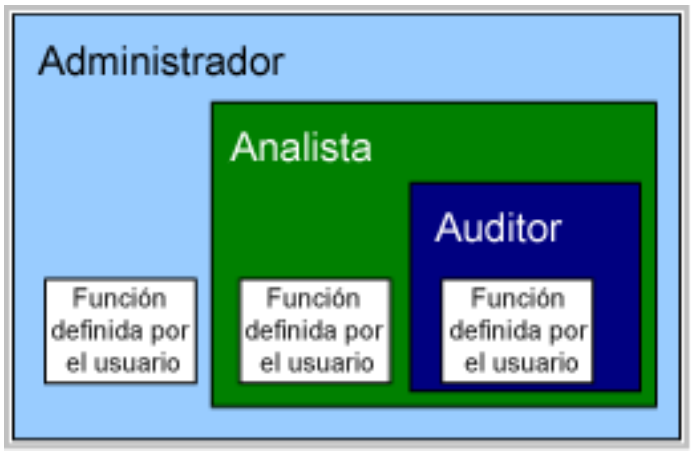
Nota: Consulte la *Guía de implementación de CA User Activity Reporting Module* para obtener más información acerca de la configuración del acceso de usuario básico. Consulte la *Guía de administración de CA User Activity Reporting Module* para obtener más información acerca de las políticas compatibles con roles predefinidos, la creación de cuentas de usuario y la asignación de roles.

Acceso basado en roles

CA User Activity Reporting Module proporciona tres grupos de aplicaciones o roles predefinidos. Los Administrators asignan los roles siguientes a los usuarios a fin de especificar sus derechos de acceso a las funciones de CA User Activity Reporting Module:

- Administrator
- Analyst
- Auditor

El Auditor tiene acceso a algunas funciones. El Analyst tiene acceso a otras funciones además de las funciones propias del Auditor. El Administrator tiene acceso a todas las funciones. Se puede definir un rol personalizado con políticas asociadas que limiten el acceso de un usuario a los recursos según sus necesidades del negocio.



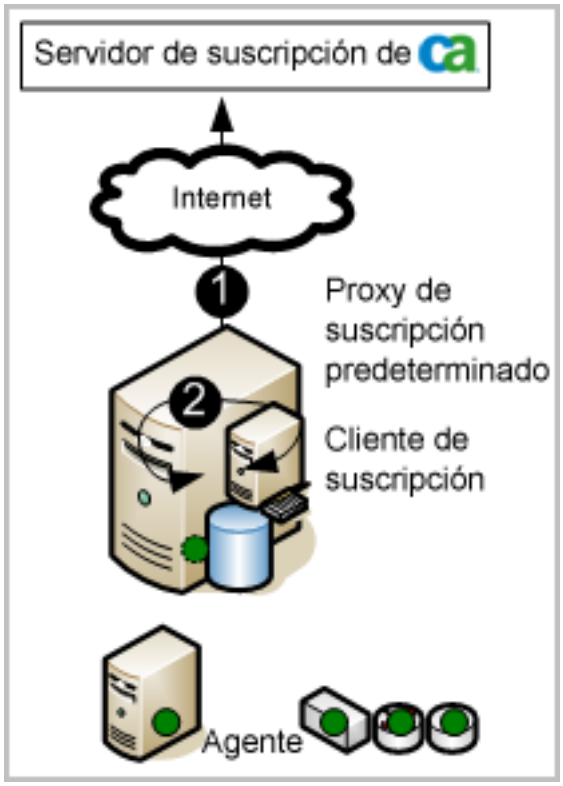
Los Administrators pueden personalizar el acceso a cualquier recurso mediante la creación de un grupo de aplicaciones personalizado con políticas asociadas y a través de la asignación de dicho grupo de aplicaciones, o rol, a las cuentas de usuario.

Nota: Consulte la *Guía de administración de CA User Activity Reporting Module*para obtener más detalles acerca de la planificación y creación de roles y políticas personalizadas, y filtros de acceso.

Gestión de suscripciones

El módulo de suscripción es el servicio que activa actualizaciones de suscripción desde el servidor de suscripción de CA para que se descarguen de manera automática con una frecuencia programada y distribuidas a los servidores de CA User Activity Reporting Module. Cuando una actualización de suscripción incluye el módulo para agentes, los usuarios inician la implementación de estas actualizaciones a los agentes. Las *actualizaciones de suscripciones* son actualizaciones de los componentes de software de CA User Activity Reporting Module y actualizaciones del sistema operativo, parches y actualizaciones de contenido, como informes.

La ilustración siguiente muestra el escenario más sencillo de una conexión directa a Internet:



Los números de la ilustración se refieren a los pasos siguientes:

1. El servidor de CA User Activity Reporting Module, como servidor de suscripción predeterminado, se pone en contacto con el servidor de suscripción de CA para detectar actualizaciones y descarga las actualizaciones nuevas disponibles. El servidor de CA User Activity Reporting Module crea una copia de seguridad y, a continuación, envía actualizaciones de contenido al componente incrustado del servidor de gestión que almacena las actualizaciones de contenido de todos los demás servidores de CA User Activity Reporting Module.
2. El servidor de CA User Activity Reporting Module, como cliente de suscripción, autoinstala el producto y el sistema operativo actualiza sus necesidades.

Nota: Consulte la *Guía de implementación* para obtener más información acerca de la planificación y configuración de la suscripción. Consulte la *Guía de administración* para obtener detalles acerca de la refinación y la modificación de la configuración de la suscripción y para aplicar actualizaciones a los agentes.

Contenido predeterminado

CA User Activity Reporting Module incluye contenido predefinido que puede comenzar a utilizar en cuanto instale y configure el producto. El proceso de suscripción actualiza el contenido existente y añade contenido nuevo de forma regular.

Las categorías de contenido predefinido incluyen las siguientes:

- Informes con etiquetas
- Consultas con etiquetas
- Integraciones con sensores asociados, archivos de análisis (XMP), archivos de asignación (DM) y, en algunos casos, reglas de supresión
- Reglas de resumen y supresión

Capítulo 5: Más información acerca de CA User Activity Reporting Module

Esta sección contiene los siguientes temas:

Visualización de la información sobre herramientas (en la página 63)
Visualización de la Ayuda en línea (en la página 65)
Exploración de la Biblioteca de documentación (en la página 68)

Visualización de la información sobre herramientas

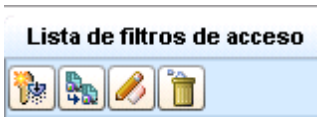
Puede identificar el propósito de los botones, casillas de verificación e informes en la página de CA User Activity Reporting Module en su vista actual.

Para mostrar información sobre herramientas y otra ayuda

1. Mueva su cursor por encima de los botones para mostrar la descripción de la función del botón. Puede ver la función de cualquier botón de esta forma.

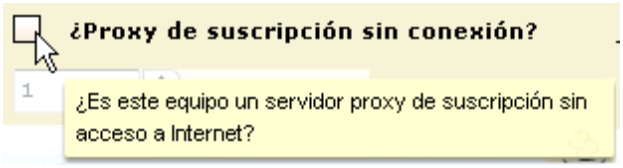
2. Vea la diferencia entre los botones activos e inactivos.

   Cuando están activados, los botones activos se muestran en color. Por ejemplo, los Administrators de la gestión de usuarios y accesos visualizarán el botón Lista de filtros de acceso en color.

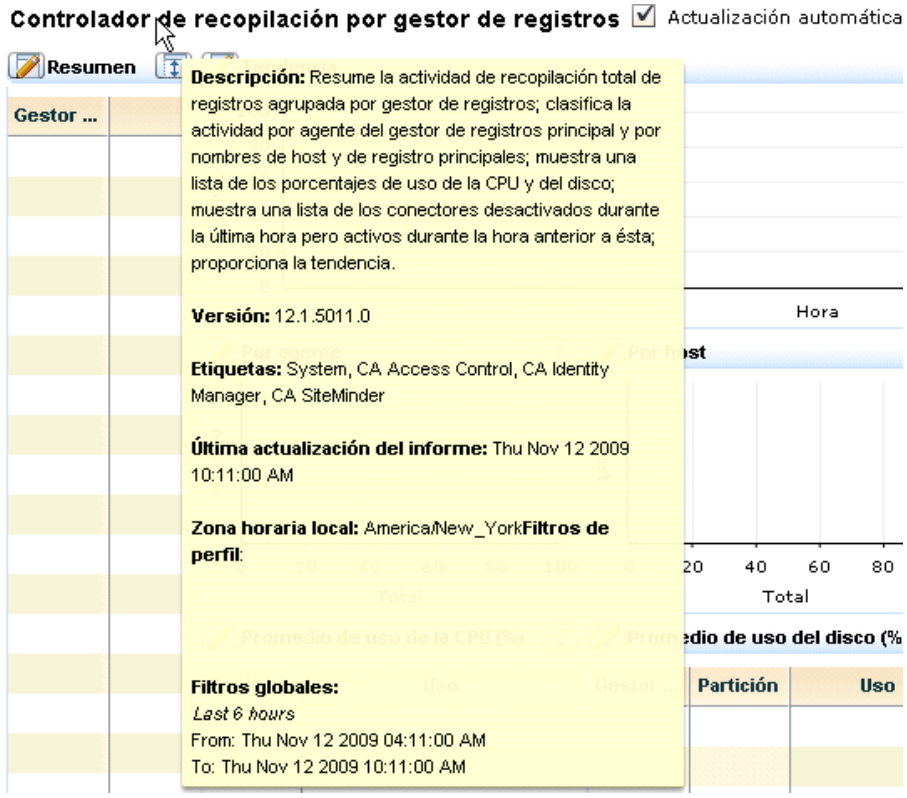


   Cuando están desactivados, los botones activos se muestran en blanco y negro. Por ejemplo, los Auditors verán los botones de la Lista de filtros de acceso en blanco y negro.

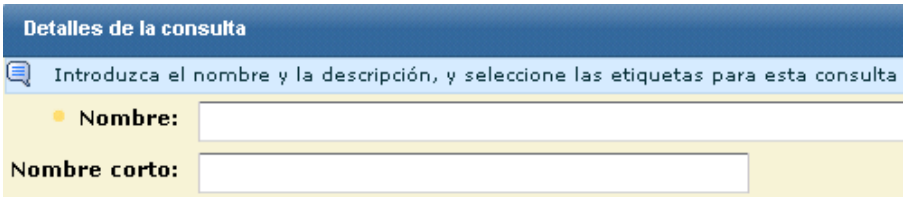
3. Visualice las descripciones de los campos de entrada o casillas de verificación moviendo el cursor por encima del nombre del campo.



4. Visualice las descripciones de los informes moviendo el cursor por encima del nombre del informe.



5. Vea que aparece un punto naranja a la izquierda de algunos campos. Este punto indica que el campo es obligatorio. Para las configuraciones que puede guardar, no se permite guardar hasta que haya introducido datos en todos los campos requeridos.



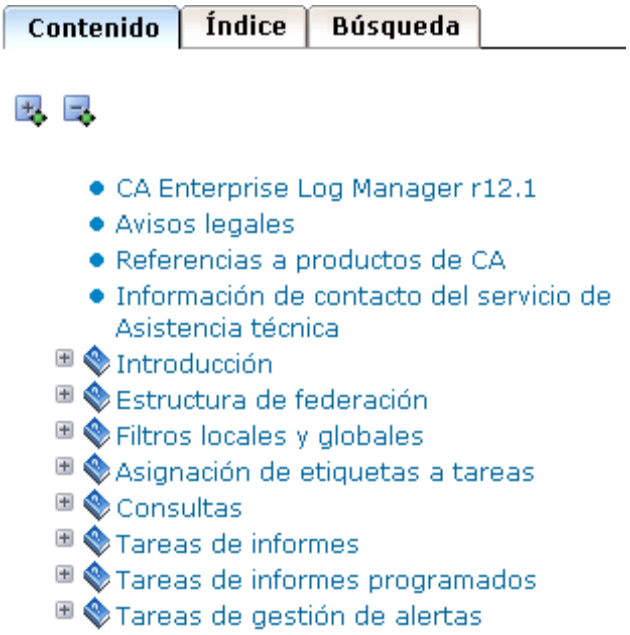
Visualización de la Ayuda en línea

Puede visualizar la ayuda en línea para la página que está utilizando en ese momento o para cualquier otra tarea que pretenda realizar más adelante.

Para visualizar la Ayuda en línea

1. Haga clic en el vínculo Ayuda de la barra de herramientas para mostrar el sistema de ayuda en línea para CA User Activity Reporting Module.

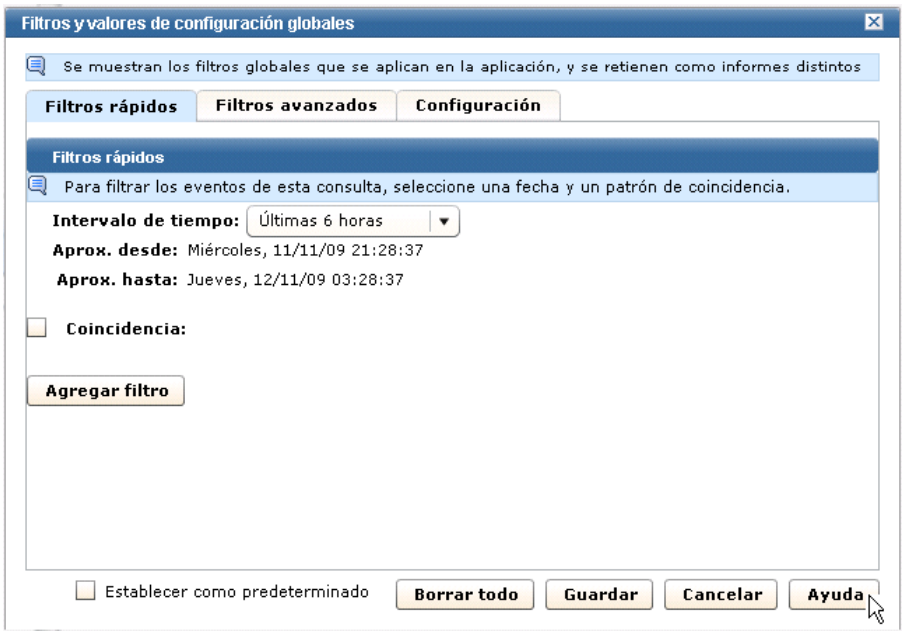
Aparecerá el sistema de ayuda de CA User Activity Reporting Module. El contenido se mostrará en el panel izquierdo de la misma.



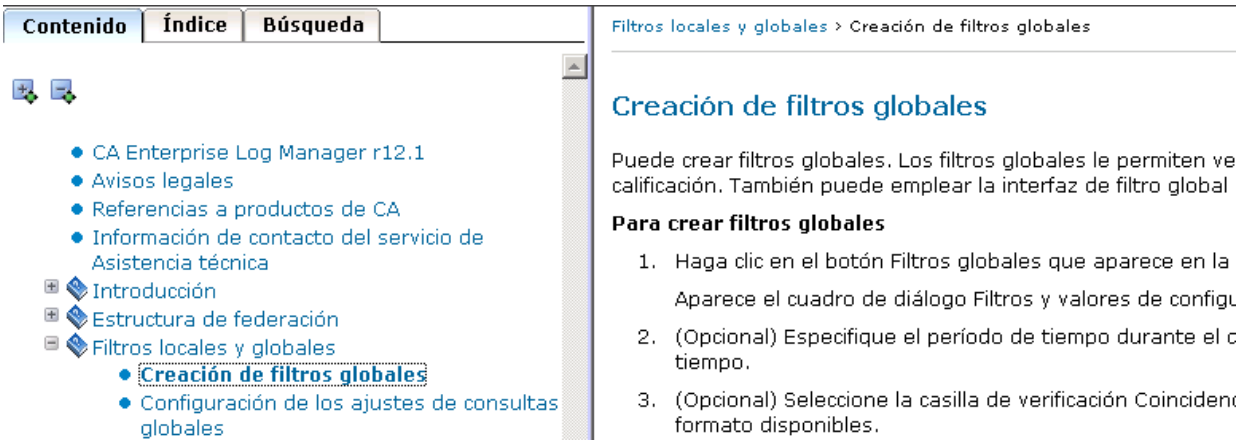
2. Acceda a la ayuda sensible al contexto desde el botón Ayuda como se muestra en el ejemplo siguiente:

   a. Haga clic en el botón Mostrar/editar filtros globales

   Aparecerá la ventana Filtros y valores de configuración globales con un botón de ayuda.



b. Haga clic en el botón Ayuda. En una ventana secundaria se mostrará la Ayuda en línea para los procedimientos que quiera llevar a cabo en la página, panel o cuadro de diálogo actuales.



c. Si conoce la tarea que quiere realizar, pero no sabe cómo acceder a la página correspondiente en CA User Activity Reporting Module, consulte la tarea en la Tabla de contenido. Al hacer clic en el título de la tarea, éste mostrará la página.

Nota: Si no encuentra la tarea que necesita en la Tabla de contenido, consulte la biblioteca de la documentación.

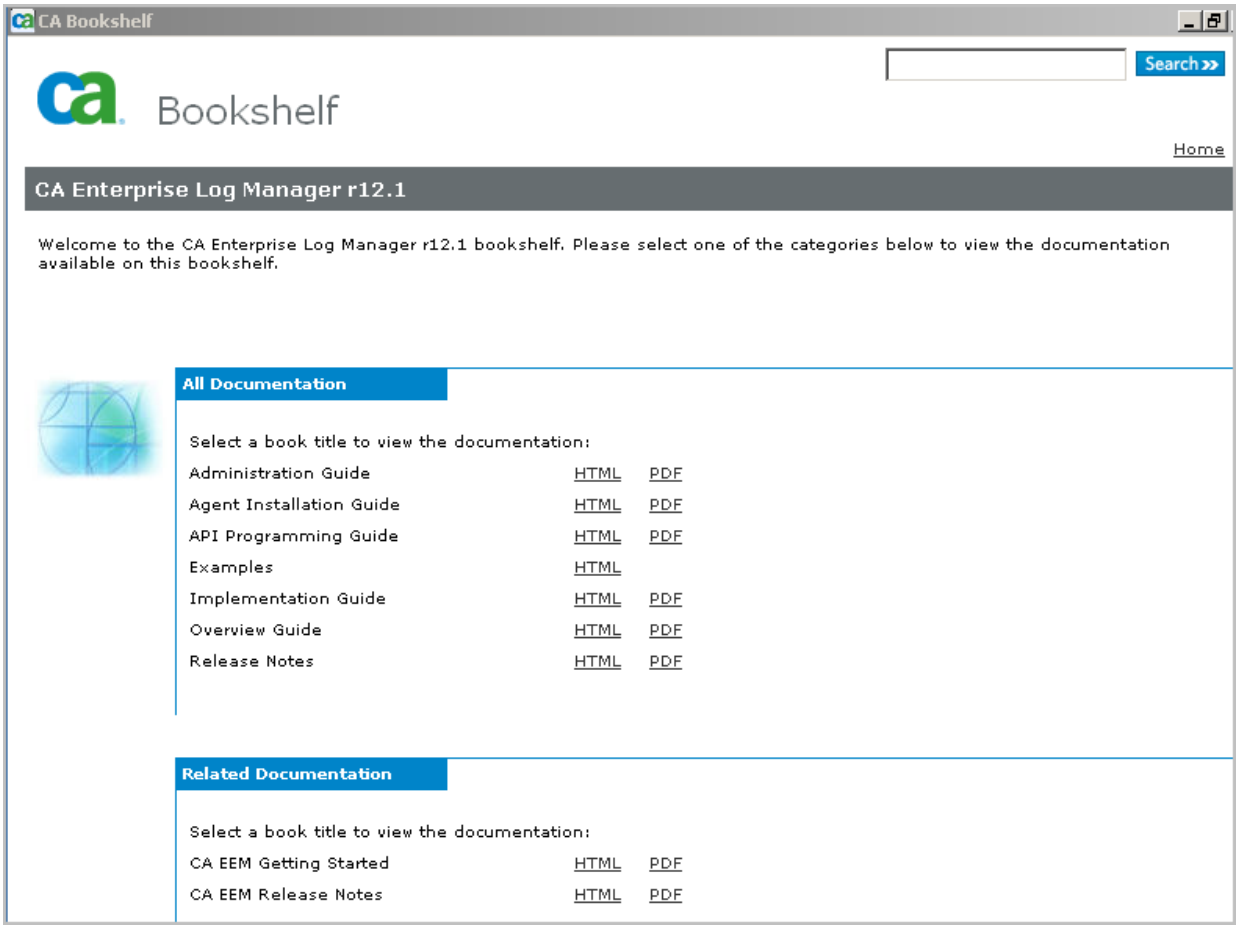
Exploración de la Biblioteca de documentación

Puede copiar la biblioteca en la unidad local y abrir cualquier libro en formato HTML o PDF. Los libros en formato HTML contienen libros y referencias cruzadas.

Para usar la biblioteca

1. Copie la Biblioteca en la unidad local desde el DVD de instalación de la aplicación o descárguela del sitio Web de Atención al cliente de CA. Haga doble clic en Bookshelf.hta o Bookshelf.html para abrir la biblioteca.

   Aparecerá una ventana parecida a la siguiente:



A continuación, encontrará una lista con el contenido de las guías principales así como los ejemplos correspondientes:

Guía	Describe cómo
Guía de instalación del agente	Instalar agentes
Guía de implementación	Instalar y configurar el sistema de CA User Activity Reporting Module.
Guía de administración	Personalizar la configuración, realizar tareas de administración rutinarias y trabajar con consultas, informes y alertas.
Guía de programación de API	Utilice API para mostrar datos de eventos en un explorador Web o para incrustar informes en otro producto de CA o de terceros.
Ejemplos	Solucionar problemas comunes de los negocios, con vínculos a los temas de la documentación.

2. Para mostrar todas las ocurrencias en la documentación de una entrada, introduzca un valor en el campo de entrada de la búsqueda y haga clic en el botón Buscar.
3. Haga clic en el vínculo Imprimir para abrir el PDF de la guía seleccionada.

4. Haga clic en el vínculo HTML para abrir el conjunto integrado de la documentación. El conjunto integrado incluye todas las guías en formato HTML. Si selecciona el vínculo HTML para la Guía de descripción general, se mostrará esa misma guía.

Índice

A

agente predeterminado
    configuración del conector Syslog para, - 29
almacenamiento de registros
    definido - 53
análisis de mensajes
    definido - 55
archivo
    definido - 53
asignación de datos
    definido - 55

B

binarios del agente
    descarga para sistemas Windows - 39

C

CA Embedded Entitlements Manager
    definido - 59
CA Enterprise Log Manager
    ayuda en línea - 65
    componentes - 10
    información sobre herramientas - 63
    instalación - 10
    roles de usuario - 60
clave de autenticación del agente
    actualizar - 38
conectores
    configurar - 43
cuenta de usuario del agente
    establecido para Windows - 36

E

entorno de prueba
    componentes de instalación - 10

G

gestión de suscripciones
    definido - 61
    descripción del proceso - 61
gramática de eventos comunes (CEG)
    definido - 55

I

información sobre herramientas
    uso - 63
instalación del agente
    manual, para Windows - 40

P

peticiones
    cómo visualizar de registros de los orígenes de eventos de Windows - 47
    cómo visualizar eventos de syslog - 32

R

recopilación de registros
    definido - 51
roles de usuario
    definido - 60

S

syslog
    visualización de eventos - 32