CA Enterprise Log Manager

Guía de descripción general

r12.1 SP2

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 Enterprise Log Manager.
- 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 Enterprise Log Manager.

Más información:

Descripción general del inicio rápido (en la página 15)
Generación de alertas de infracción de política (en la página 57)
Exploración de la Biblioteca de documentación (en la página 67)

Contenido

Capítulo 1: Introducción

Esta sección contiene los siguientes temas:

Acerca de esta guía

Esta *Guía de descripción general* presenta CA Enterprise Log Manager. 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 Enterprise Log Manager 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 Enterprise Log Manager	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 Enterprise Log Manager 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 Enterprise Log Manager, vea la Ayuda en línea.

Acerca de CA Enterprise Log Manager

CA Enterprise Log Manager 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.

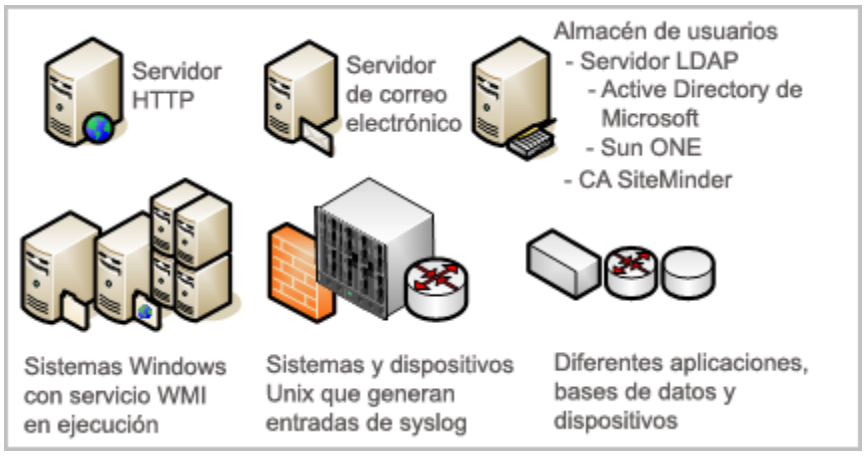
Su red--Antes de la instalación

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 Enterprise Log Manager ofrece estas ventajas y le permite enviar alertas a individuos y a sistemas cuando se producen eventos críticos.

Componentes de instalación

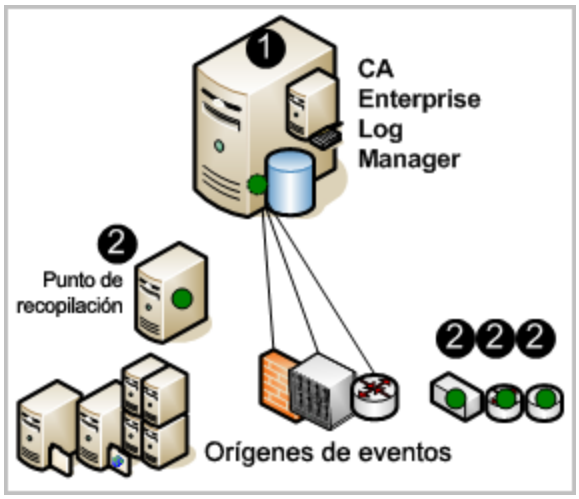
No le llevará mucho tiempo configurar una solución de servidor único y empezar a recopilar eventos.

El disco de instalación incluye estos componentes:

- Sistema operativo (Red Hat Enterprise Linux) para el dispositivo de software
- Servidor de CA Enterprise Log Manager
- Agente de CA Enterprise Log Manager (a partir de ahora llamado el agente)

En la ilustración siguiente, CA Enterprise Log Manager 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 Enterprise Log Manager. Tan pronto como configure los orígenes para enviar los syslogs a CA Enterprise Log Manager 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 39)

Capítulo 2: Implementación de inicio rápido

Esta sección contiene los siguientes temas:

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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager.

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 Enterprise Log Manager

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.

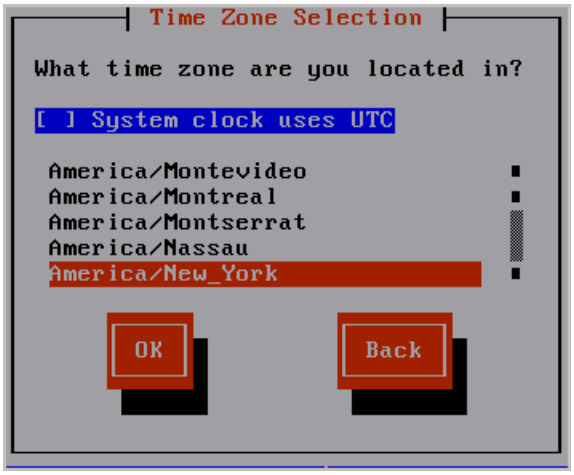
     Nota: Para que se complete la instalación, se debe registrar el dominio con los servidores DNS de la red.
   - La direcciones IP de los servidores DNS.
   - (Opcional) Dirección IP del servidor de NTP
   - Una contraseña para el nombre de superusuario predeterminado de la instalación, EiamAdmin.
   -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

     Este es el nombre predeterminado de la aplicación de CA Enterprise Log Manager.

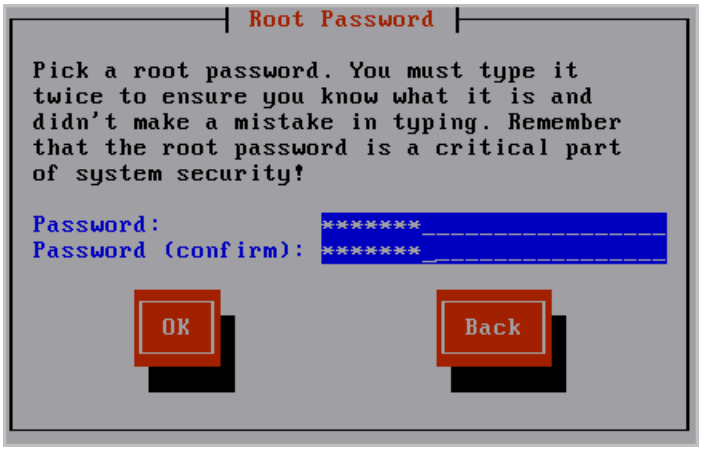
2. Instale el sistema operativo predeterminado preconfigurado mediante el uso de los medios que creó del paquete de descarga de CA Enterprise Log Manager. Durante la instalación del sistema operativo, realice las siguientes operaciones:

   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 Enterprise Log Manager. Pulse Intro.

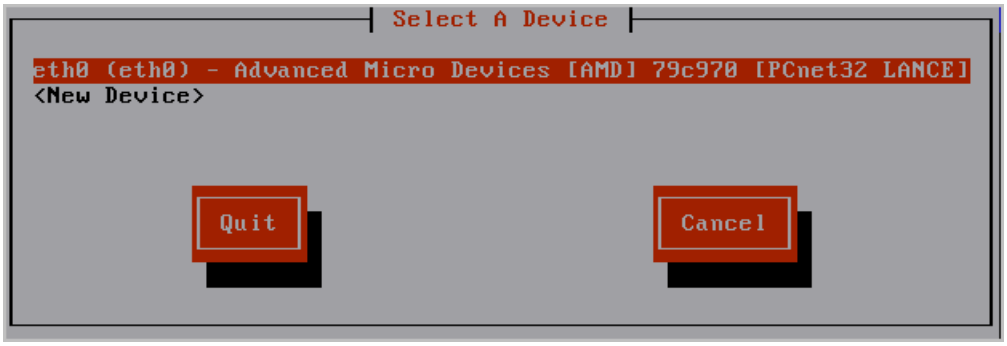
   Para un óptimo rendimiento, se revisará el sistema para comprobar que éste cumple con las especificaciones mínimas recomendadas. En el caso que no las cumpla, aparecerá un aviso para comprobar si quiere continuar con el proceso de instalación.

   Aparecerá el mensaje siguiente:

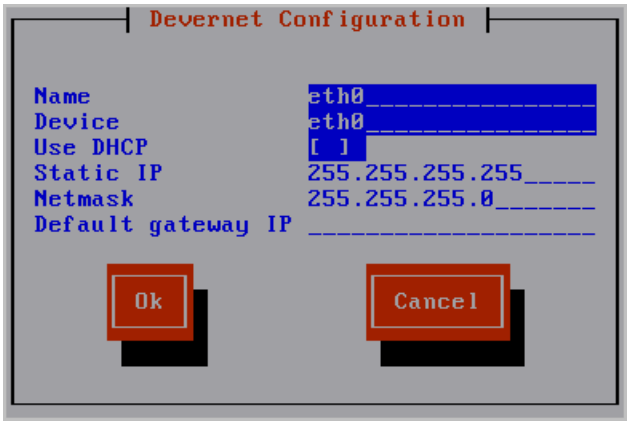
   ```
   Escriba un nombre de host nuevo.
   ```

4. Introduzca el nombre de host para la aplicación de software CA Enterprise Log Manager. 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 Enterprise Log Manager, 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.

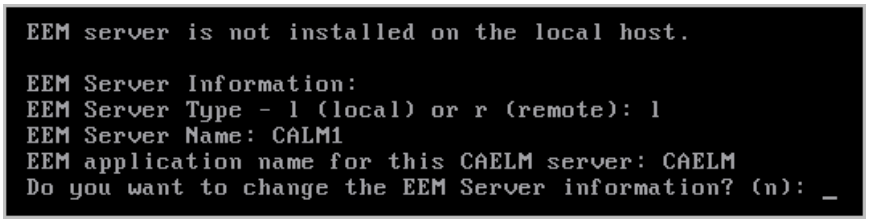
       ```
       Especifique la contraseña para el usuario EiamAdmin del servidor de EEM:
       Confirme la contraseña para el usuario EiamAdmin del servidor de EEM:
       ```

    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 Enterprise Log Manager.

   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 Enterprise Log Manager: 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 Enterprise Log Manager 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 Enterprise Log Manager. 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 Enterprise Log Manager, 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager único, se debe preparar la configuración mediante la búsqueda de la URL de CA Enterprise Log Manager 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 Enterprise Log Manager.

   `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 Enterprise Log Manager.

   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.

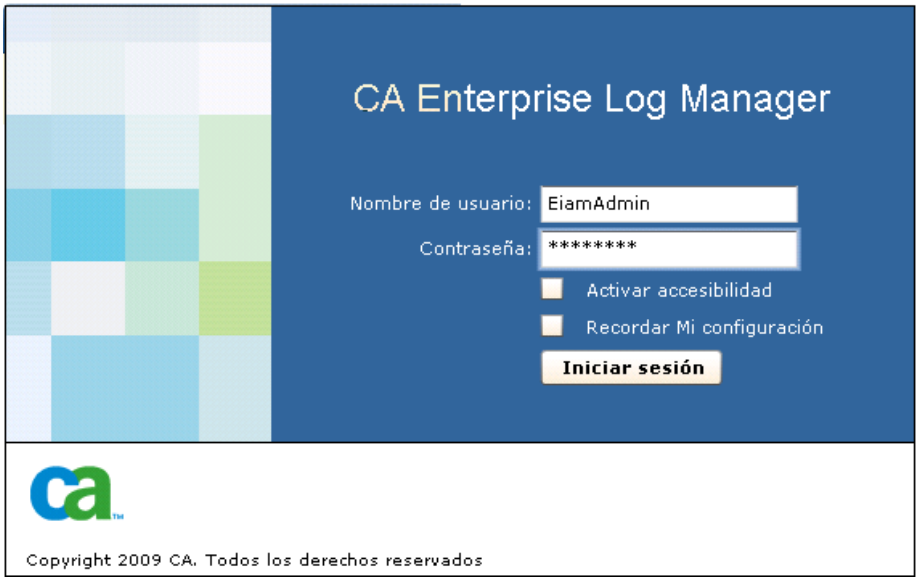
      Aparecerá el cuadro de diálogo Certificado de confianza.

   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.

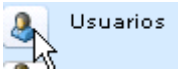
      Aparecerá la página de inicio de sesión.

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

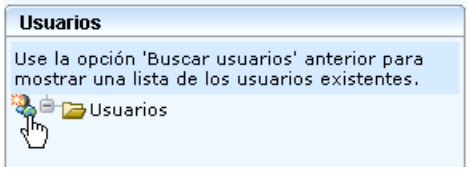


La aplicación se abrirá sólo con la ficha Administrator y la subficha Gestión de usuarios y accesos activas.

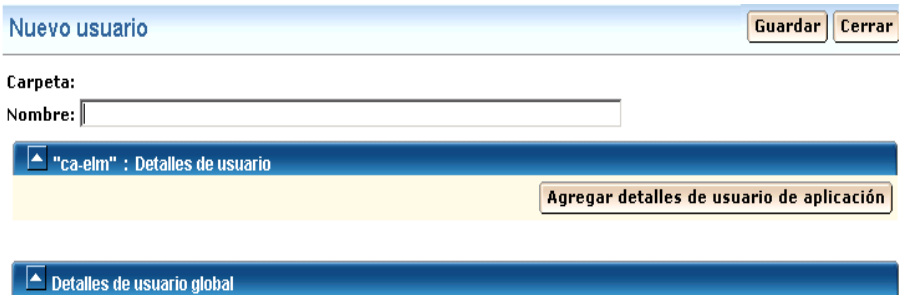
4. Haga clic en Usuarios.



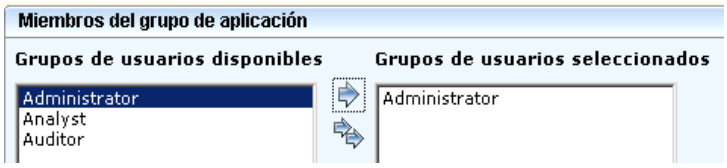
5. Haga clic en Agregar nuevo usuario.



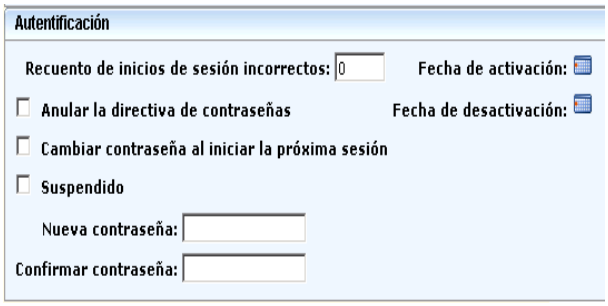
6. Introduzca su nombre en el campo Nombre y haga clic en Agregar detalles del usuario de la aplicación.



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 Enterprise Log Manager con las credenciales de Administrator que acaba de definir.

    CA Enterprise Log Manager 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 Enterprise Log Manager, 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 Enterprise Log Manager para visualizar o generar informes de eventos que le interesan en un formato estándar. También podrá generar alertas durante la ocurrencia de eventos específicos.

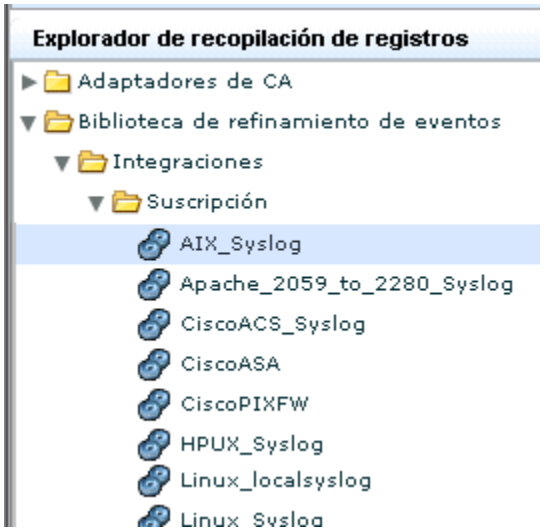
Cómo configurar un origen de evento de syslog seleccionado

1. Inicie sesión en el host con un origen de evento de syslog de destino.
2. Inicie CA Enterprise Log Manager 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 Enterprise Log Manager.

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 Enterprise Log Manager 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 Enterprise Log Manager contiene un agente predeterminado. Una vez configurado CA Enterprise Log Manager, 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 Enterprise Log Manager. Sin embargo, para que CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager que se deberá configurar.

3. Seleccione el nombre del servidor de CA Enterprise Log Manager.

   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.

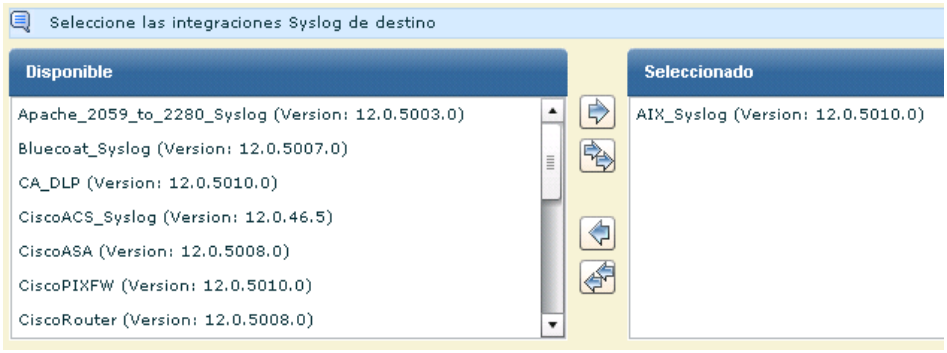
5. (Opcional) Haga clic en Aplicar reglas de supresión. Si existe algún tipo de evento de syslog que quiera suprimir , es decir, *no* recopilado, desplace el tipo de evento de la lista Disponible a la lista Seleccionado. Seleccione el evento para desplazarlo y haga clic en el botón Mover.

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 Enterprise Log Manager. 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.

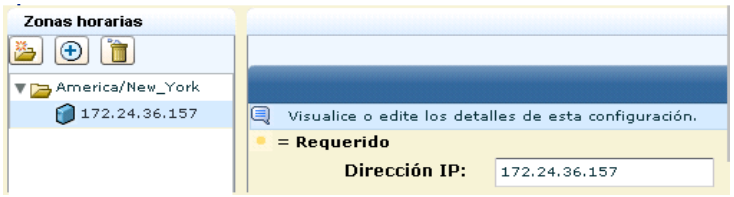
   Puede aceptar los puertos predeterminados UPD y TCP para el agente predeterminado.

   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.

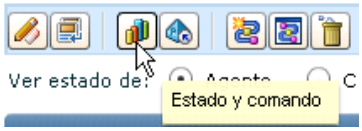
    b. Resalte la entrada en blanco bajo la carpeta. Introduzca la dirección IP de un host de confianza que haya configurado para este conector o de un servidor horario NTP que haya especificado durante la instalación de CA Enterprise Log Manager.



11. Haga clic en Guardar y cerrar.

12. Visualice el estado.

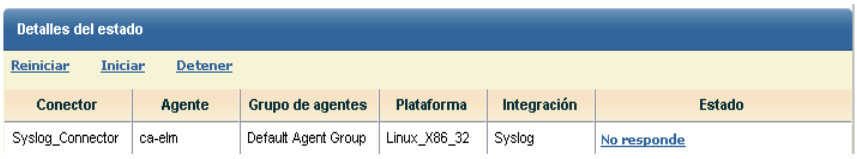
    a. Haga clic en Estado y comando



    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

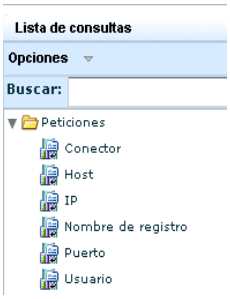
Una de la maneras más rápidas de visualizar los resultados de las consultas en los eventos recopilados por la escucha de syslog es la utilización de la Petición para el host.

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.

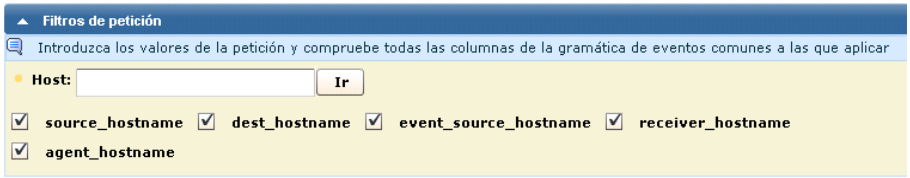


3. Envíe la consulta para los eventos recopilados por el agente predeterminado.

   a. Introduzca el nombre de host del agente predeterminado, que también es el nombre del CA Enterprise Log Manager 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 Enterprise Log Manager 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

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.

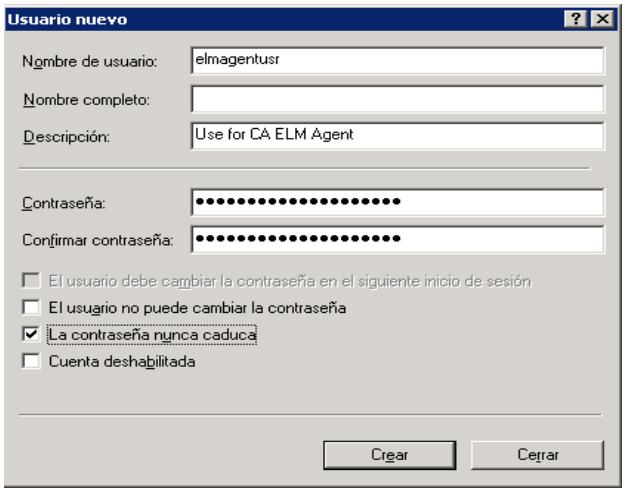
Nota: .Aunque no es recomendable, puede omitir este paso y especificar las credenciales de dominio de un Administrator para el agente durante la instalación.

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 39)

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 Enterprise Log Manager para este agente. A continuación, se muestra un ejemplo:

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

2. Inicie sesión en CA Enterprise Log Manager. 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.

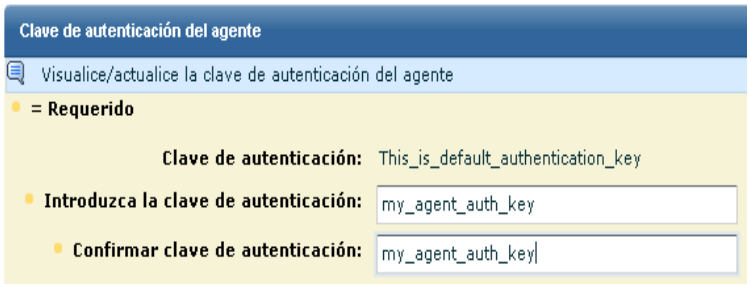
4. Seleccione la carpeta Explorador de agente.

   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.



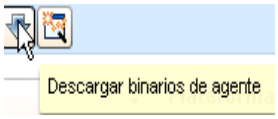
7. Haga clic en Guardar.
8. Continúe con el siguiente paso, Descarga del programa de instalación del agente.

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.

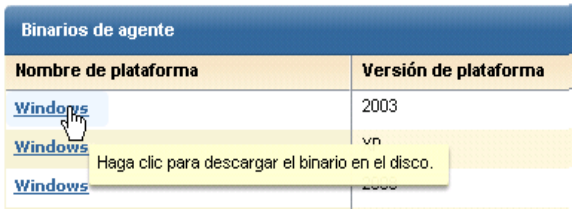
Para descargar el programa de instalación del agente

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.



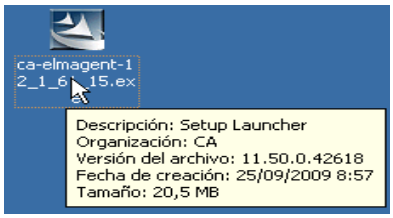
Aparecerá el cuadro de diálogo Seleccionar ubicación para la descarga por <dirección IP>.

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 Enterprise Log Manager 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.

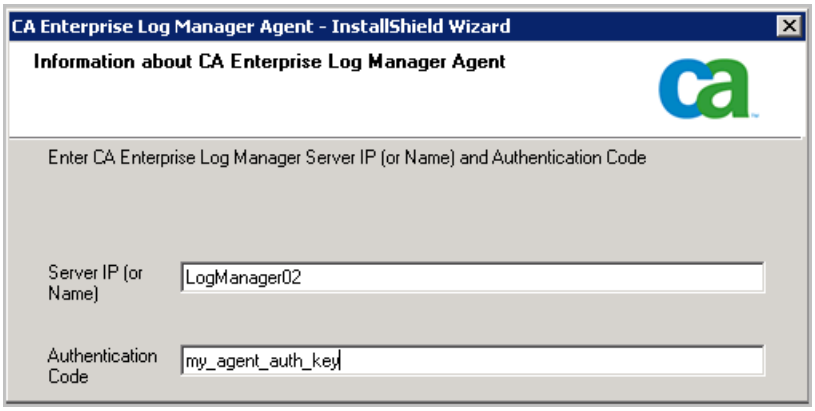
Se iniciará el asistente de instalación.

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 Enterprise Log Manager al que el agente enviará los registros que haya recopilado.

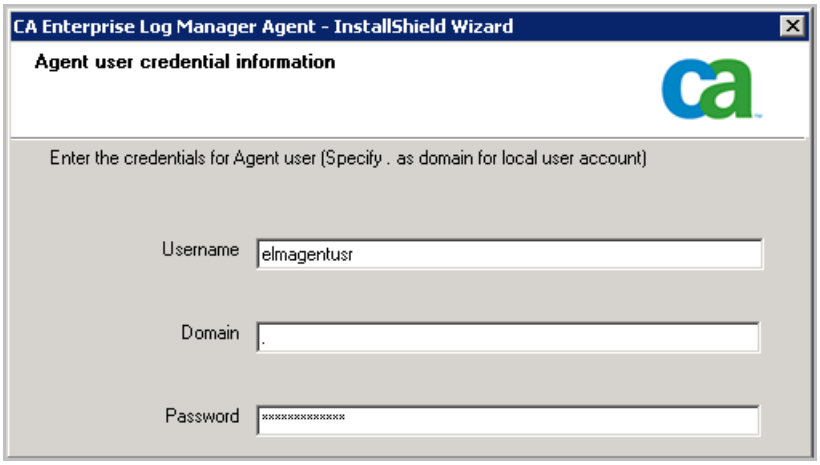
      Nota: Dado que en este ejemplo, CA Enterprise Log Manager utiliza DHCP para la asignación de la dirección IP, no deberá introducir la dirección IP aquí. Si lo hiciera, es posible que tuviera que volver a instalar el agente si se modificase la dirección IP del servidor.

   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 Enterprise Log Manager 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 38)
Creación de una cuenta de usuario para el agente (en la página 36)
Configuración de la clave de autenticación del agente (en la página 37)

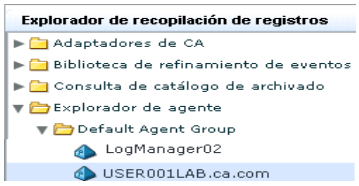
Creación de un conector basado en NTEventLog

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 Enterprise Log Manager.
2. Expanda primero el Explorador de agente, y, a continuación, el Grupo de agentes predeterminado.

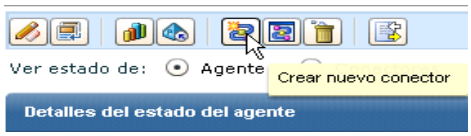
   Aparecerá el nombre del equipo donde instaló el agente.

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.

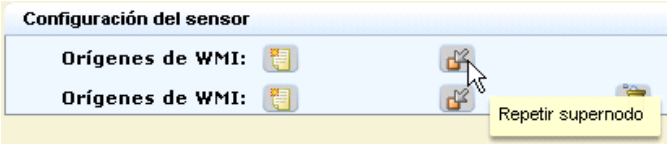
9. Configure los valores de configuración de WMILogSensor para el equipo local para la recopilación de registros basada en el agente. Para obtener más detalles, haga clic en el vínculo Ayuda.

   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 Enterprise Log Manager 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 Enterprise Log Manager.

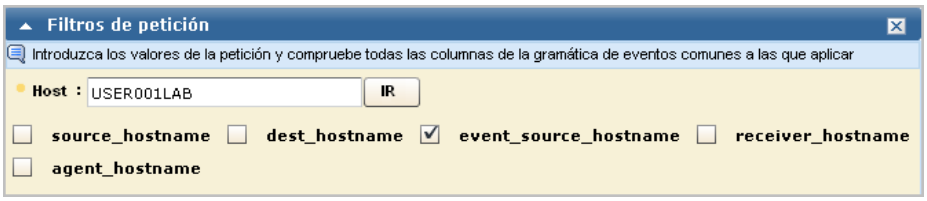
Visualización de registros de los orígenes de eventos de Windows

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.

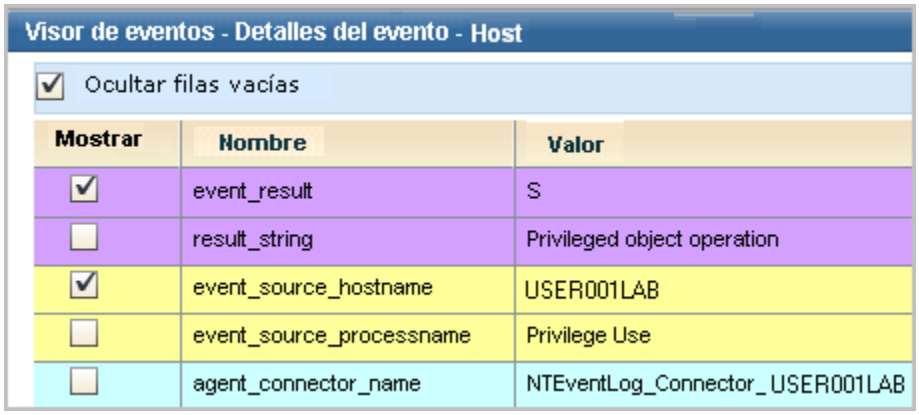


   Aparecerán los orígenes de los eventos del servidor WMI.
4. Haga clic en Severidad de CA y desplácese hasta encontrar una advertencia. A continuación, se muestra un ejemplo sin las columnas Fecha y Origen de eventos:

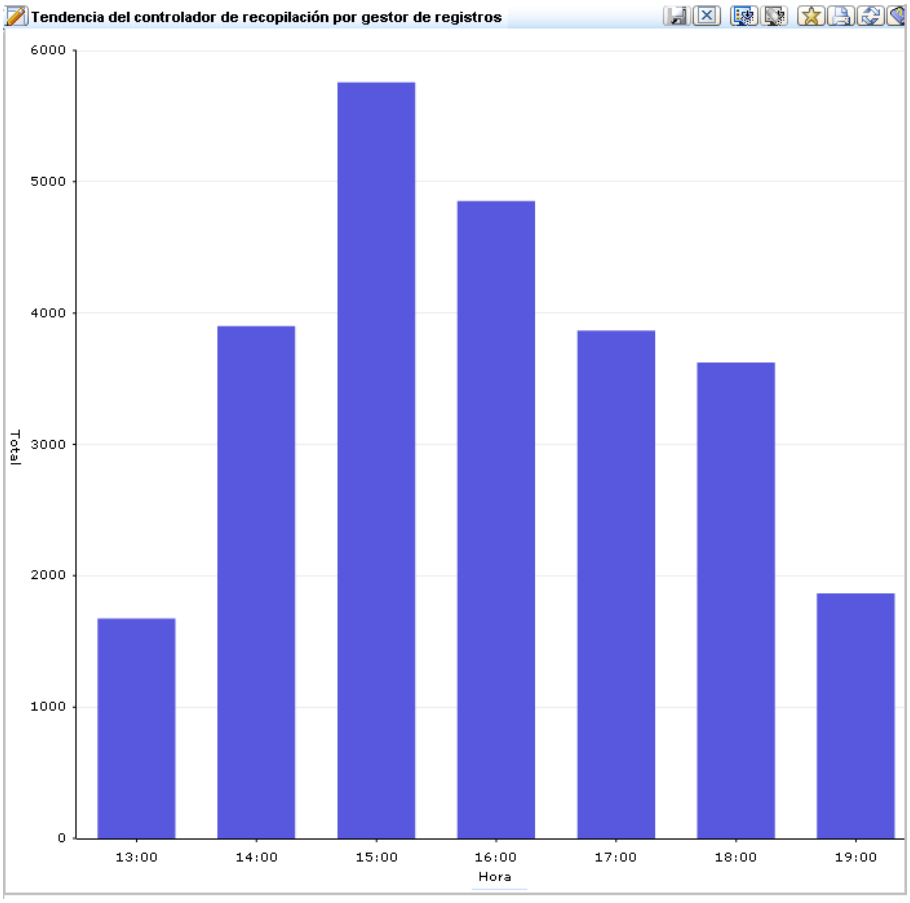
Severidad de CA	Usuario de origen	Resultado	Categoría	Acción	Nombre de registro
Advertencia	calm_agent	S	System Access	Privilege Use	NT-Security

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 Enterprise Log Manager.

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

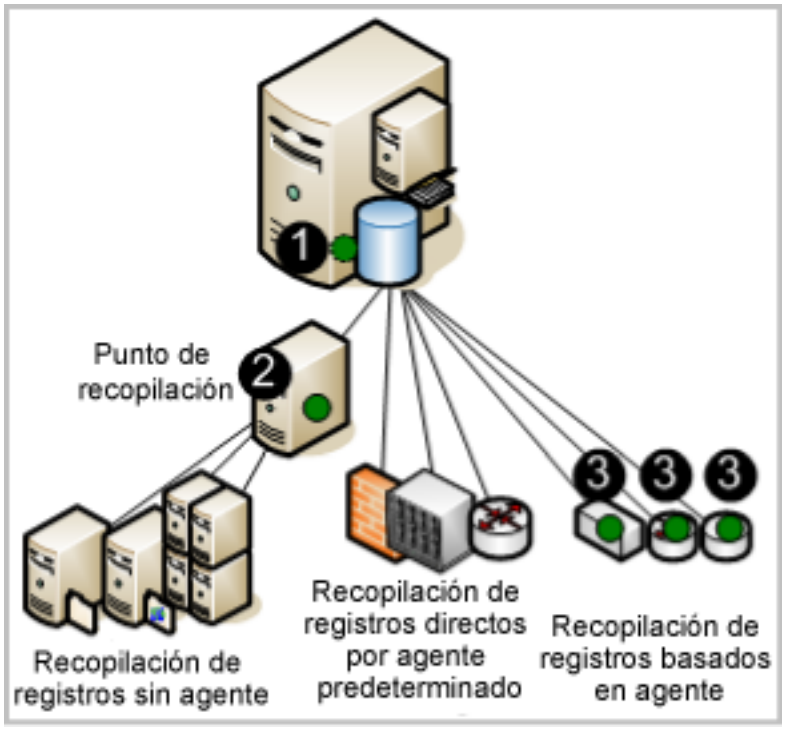
Capítulo 4: Funcionalidades clave

Esta sección contiene los siguientes temas:

Recopilación de registros

El servidor de CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager.
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 Enterprise Log Manager 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 Enterprise Log Manager.

- 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

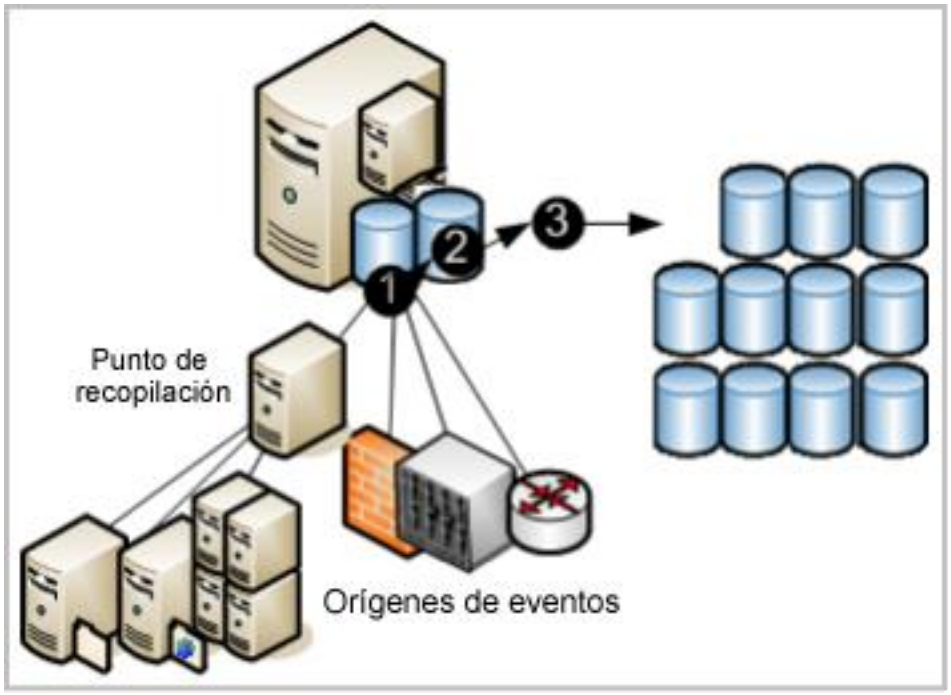
  Con la recopilación basada en el agente, se instala un agente donde un o más orígenes de eventos se ejecutan y donde se configura un conector para cada origen de evento.

  Ventaja: puede recopilar registros de un origen donde el ancho de banda de la red entre el dicho origen y CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager. 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 Enterprise Log Manager 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 Enterprise Log Manager* 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager.*

Generación de alertas de infracción de política

CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager* 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 Enterprise Log Manager 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 Enterprise Log Manager 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.

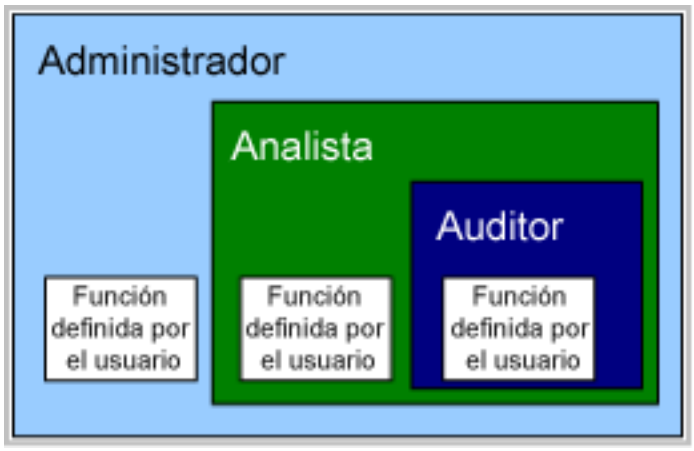
Nota: Consulte la *Guía de implementación de CA Enterprise Log Manager* para obtener más información acerca de la configuración del acceso de usuario básico. Consulte la *Guía de administración de CA Enterprise Log Manager* para obtener más información acerca de las políticas compatibles con roles predefinidos,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

Acceso basado en roles

CA Enterprise Log Manager 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 Enterprise Log Manager:

- 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 Enterprise Log Manager*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 Enterprise Log Manager. 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 Enterprise Log Manager 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 Enterprise Log Manager, 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 Enterprise Log Manager 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 Enterprise Log Manager.
2. El servidor de CA Enterprise Log Manager, 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 Enterprise Log Manager 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 Enterprise Log Manager

Esta sección contiene los siguientes temas:

Visualización de la información sobre herramientas

Puede identificar el propósito de los botones, casillas de verificación e informes en la página de CA Enterprise Log Manager en su vista actual.

Para mostrar información sobre herramientas y otra ayuda

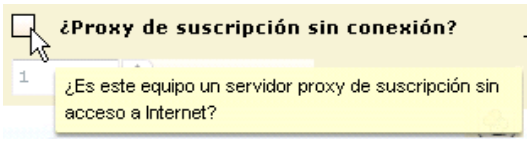
1. Mueva su cursor por encima de los botones para mostrar la descripción de la función del botón. Puede ver la función de cualquier botón de esta forma.

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

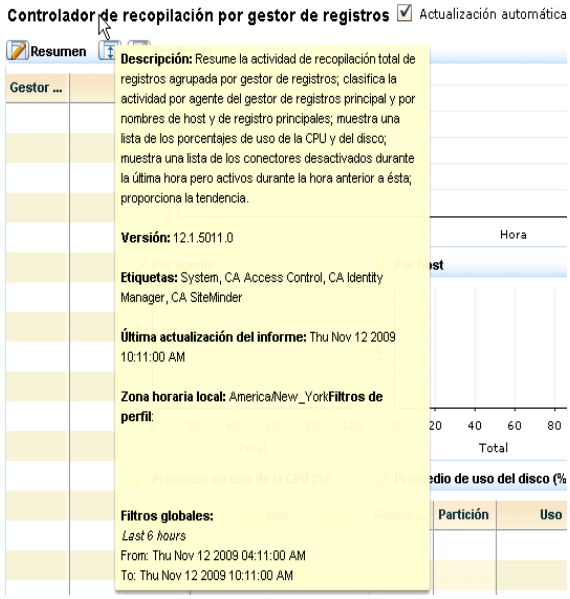
   Cuando están activados, los botones activos se muestran en color. Por ejemplo, los Administrators de la gestión de usuarios y accesos visualizarán el botón Lista de filtros de acceso en color.

   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.

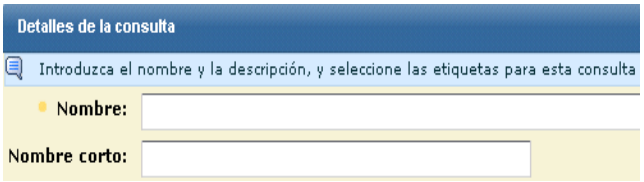
3. Visualice las descripciones de los campos de entrada o casillas de verificación moviendo el cursor por encima del nombre del campo.



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.



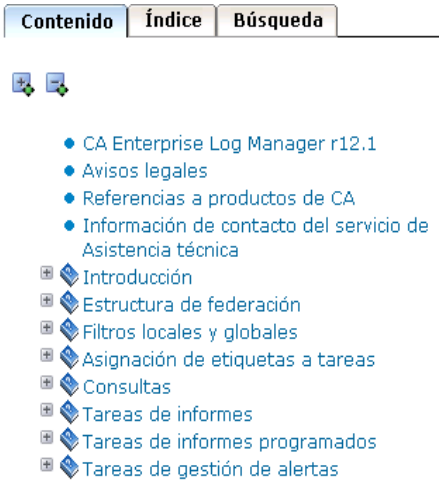
Visualización de la Ayuda en línea

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 Enterprise Log Manager.

Aparecerá el sistema de ayuda de CA Enterprise Log Manager. El contenido se mostrará en el panel izquierdo de la misma.

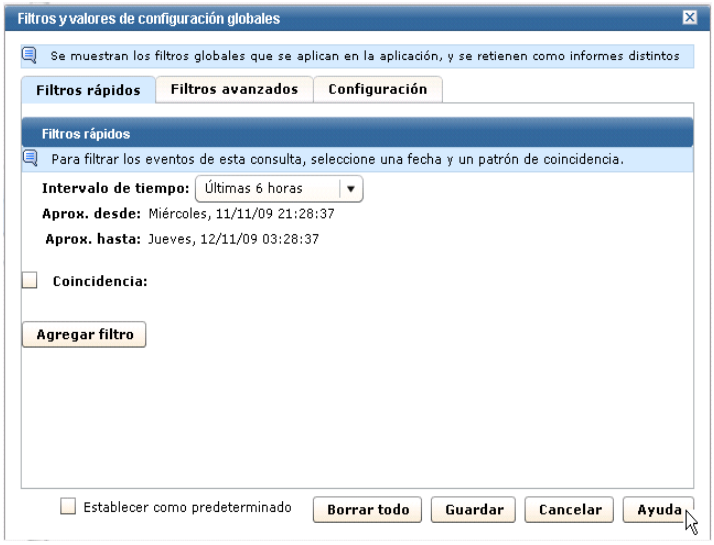


2. Acceda a la ayuda sensible al contexto desde el botón Ayuda como se muestra en el ejemplo siguiente:

   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 Enterprise Log Manager, 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.

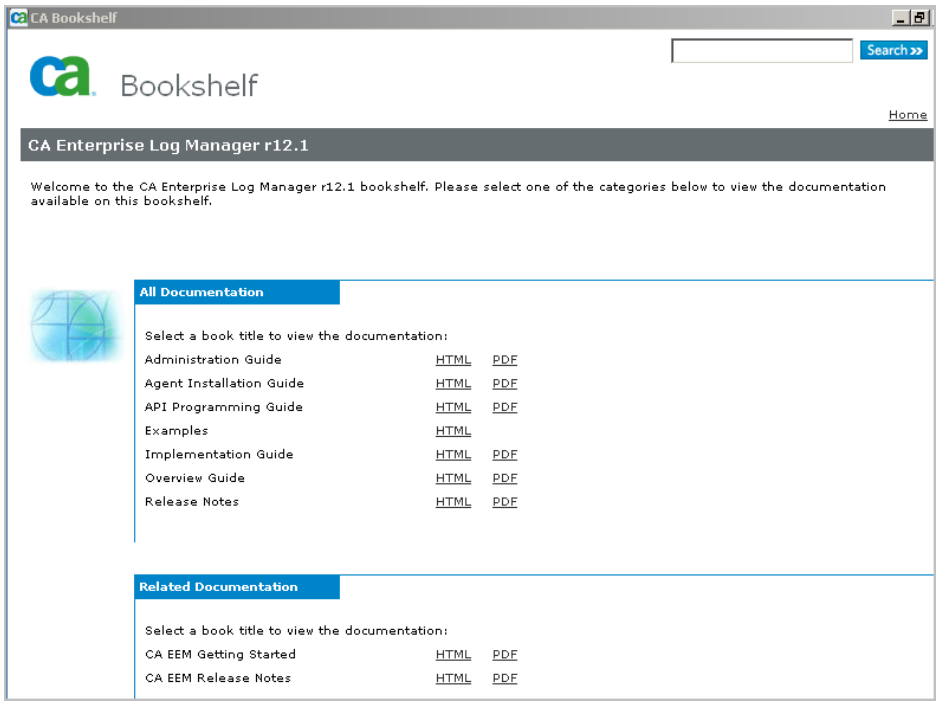
Exploración de la Biblioteca de documentación

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:

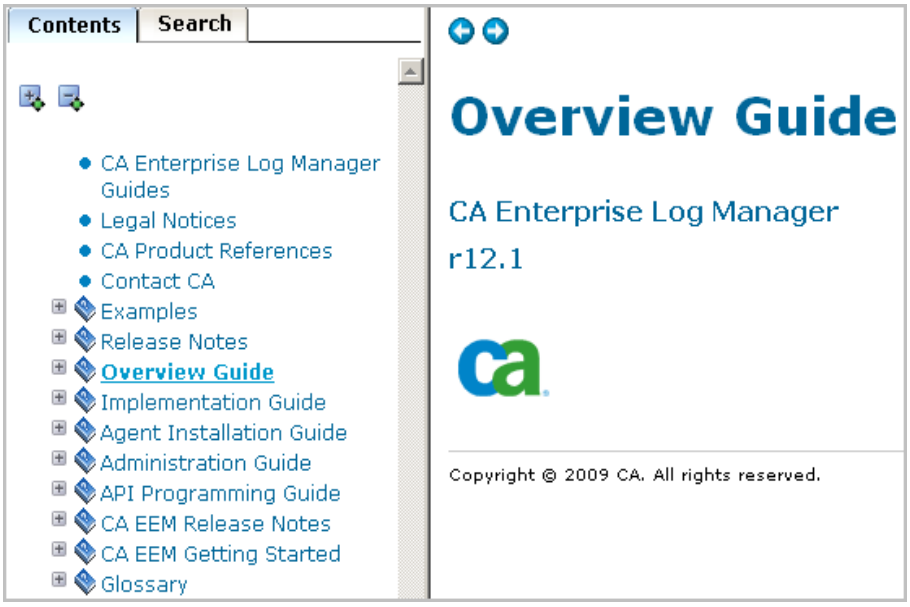


A continuación, encontrará una lista con el contenido de las guías principales así como los ejemplos correspondientes:

Guía	Describe cómo
Guía de instalación del agente	Instalar agentes
Guía de implementación	Instalar y configurar el sistema de CA Enterprise Log Manager.
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.



Capítulo 6: Glosario

acceso a datos

El *acceso a datos* es un tipo de autorización que se ofrece a todos los servidores de CA Enterprise Log Manager mediante la política de acceso a datos predeterminada del tipo de recurso de CALM. Los usuarios pueden acceder a todos los datos, excepto a aquellos restringidos por filtros de acceso a datos.

Acceso de ODBC y JDBC

El *acceso de ODBC y JDBC* a los almacenes de registro de eventos de CA Enterprise Log Manager admite el empleo de datos de eventos con diversos productos de terceros, incluida la generación de informes de eventos mediante herramientas de generación de informes de terceros, la correlación de eventos mediante motores de correlación y la evaluación de eventos mediante productos de detección de intrusiones o software maligno. Los equipos con sistemas operativos Windows emplean el acceso de ODBC; los equipos con sistemas operativos UNIX y Linux emplean en acceso de JDBC.

actualizaciones de contenido

Las *actualizaciones de contenido* son la parte no binaria de las actualizaciones de suscripción que se almacenan en el servidor de gestión de CA Enterprise Log Manager. Las actualizaciones de contenido incluyen contenido como archivos XMP, archivos de asignación de datos, actualizaciones de configuración para módulos de CA Enterprise Log Manager y actualizaciones de claves públicas.

actualizaciones de suscripción

Las *actualizaciones de suscripción* hacen referencia a archivos binarios y no binarios que están disponibles mediante el servidor de suscripción de CA. Los archivos binarios son actualizaciones de módulos de productos que se suelen instalar en CA Enterprise Log Manager. Los archivos no binarios, o actualizaciones de contenido, se guardan en el servidor de gestión.

acumulación de eventos

La *acumulación de eventos* es el proceso a través del cual las entradas de registro similares se consolidan en una única entrada que contiene un recuento del número de repeticiones del evento. Las reglas de resumen definen cómo se acumulan los eventos.

adaptadores de CA

Los *adaptadores de CA* son un grupo de escuchas que reciben eventos de componentes de CA Audit como clientes de CA Audit, iRecorders y SAPI recorders, así como orígenes que envían eventos de forma nativa en iTechnology.

agente

Un *agente* es un servicio genérico configurado mediante conectores, cada uno de los cuales recopila eventos sin formato de un único origen de eventos y, a continuación, los envía a CA Enterprise Log Manager para procesarlos. Cada CA Enterprise Log Manager cuenta con un agente incorporado. Además, puede instalar un agente en un punto de recopilación remoto y, de este modo, recopilar eventos en host en los que no se pueden instalar agentes. Puede instalar un agente en el host en el que se ejecutan los orígenes de eventos y aprovechar las ventajas de la posibilidad de aplicar reglas de supresión y cifrar la transmisión a CA Enterprise Log Manager.

agente predeterminado

El *agente predeterminado* es el agente integrado que se instala con el servidor de CA Enterprise Log Manager. Puede configurarse para la recopilación directa de eventos de syslog, así como de eventos de diversos orígenes de eventos que no son de syslog, como CA Access Control r12 SP1, el servicio de certificados de Microsoft Active Directory y las bases de datos de Oracle9i.

alerta de acción

Una *alerta de acción* es una tarea de consulta programada que se puede emplear para detectar infracciones de políticas, tendencias de uso, patrones de inicio de sesión y otras acciones que pueden requerir atención a corto plazo. De forma predeterminada, cuando las consultas de alerta devuelven resultados, éstos se muestran en la página de alertas de CA Enterprise Log Manager y también se añaden a una fuente RSS. Al programar una alerta, puede especificar más destinos, incluido el correo electrónico, un proceso de obtención de resultados de eventos/alertas de CA IT PAM y traps de SNMP.

almacén de usuarios

Un *almacén de usuarios* es el repositorio de las políticas de contraseña y la información de usuario global. El almacén de usuarios de CA Enterprise Log Manager es el repositorio local predeterminado, pero se puede configurar para hacer referencia a CA SiteMinder o a un directorio de LDAP compatible como Microsoft Active Directory, Sun One o Novell eDirectory. Independientemente de cómo se configure el almacén de usuarios, el repositorio local del servidor de gestión contiene información específica de la aplicación sobre usuarios, como su función y las políticas de acceso asociadas.

almacenamiento automático

El *almacenamiento automático* es un proceso configurable que automatiza el desplazamiento de bases de datos de archivo de un servidor a otro. En la primera fase del almacenamiento automático, el servidor de recopilación envía las bases de datos recién almacenadas al servidor de informes con la frecuencia establecida. En la segunda fase, el servidor de informes envía las bases de datos antiguas al servidor de almacenamiento remoto para su almacenamiento a largo plazo, evitando así la necesidad de realizar una copia de seguridad manual y un desplazamiento. El almacenamiento automático requiere que configure una autenticación sin contraseña del origen al servidor de destino.

almacenamiento de registro de eventos

El *almacenamiento de registro de eventos* es el resultado del proceso de almacenamiento, durante el que el usuario realiza una copia de seguridad de una base de datos tibia, notifica a CA Enterprise Log Manager mediante la ejecución de la utilidad LMArchive y desplaza la base de datos con copia de seguridad del almacenamiento de registro de eventos al almacenamiento a largo plazo.

almacenamiento de registro de eventos

El *almacenamiento de registro de eventos* es un componente del servidor de CA Enterprise Log Manager en el que los eventos entrantes se almacenan en bases de datos. Las bases de datos del sistema de almacenamiento de registro de eventos deben tener copias de seguridad hechas a mano y se deben trasladar a una ubicación de almacenamiento de registros remota antes de la fecha configurada para su eliminación. Las bases de datos almacenadas se pueden restaurar en un sistema de almacenamiento de registro de eventos.

almacenamiento de registros

El *almacenamiento de registros* es el proceso de lo que sucede cuando la base de datos caliente alcanza el tamaño máximo, momento en que se lleva a cabo la compresión de las filas y el estado pasa de caliente a tibio. Los administradores deben realizar copias de seguridad manuales de las bases de datos tibias antes de que se alcance el umbral de eliminación. También deben ejecutar la utilidad LMArchive para registrar el nombre de las copias de seguridad. Esta información se puede visualizar a través de la consulta de archivos.

análisis

El *análisis*, también denominado análisis de mensajes (MP), es el proceso de conversión de datos sin formato del dispositivo en pares clave-valor. El análisis se lleva a cabo mediante un archivo XMP. El análisis, que precede a la asignación de datos, es un paso del proceso de integración que convierte el evento sin formato recopilado de un origen de eventos en un evento refinado que se puede visualizar.

análisis de archivos XMP

El *análisis de archivos XMP* es el proceso que lleva a cabo la utilidad de análisis de mensajes para buscar todos los eventos que contienen cada una de las cadenas de coincidencia previa y, para cada evento coincidente, analizar el evento en tokens mediante el primer filtro detectado que emplee la misma cadena de coincidencia previa.

análisis de asignaciones

El *análisis de asignaciones* es un paso del asistente para el archivo de asignación que le permite comprobar y realizar cambios en un archivo de asignación de datos (DM). Los eventos de ejemplo se prueban con respecto al archivo de asignación de datos y los resultados se validan con la gramática de eventos comunes.

análisis de mensajes

El *análisis de mensajes* es el proceso de aplicación de reglas al análisis de un registro de eventos sin formato para obtener información relevante como la indicación de tiempo, la dirección IP y el nombre de usuario. Las reglas de análisis emplean la coincidencia de caracteres para ubicar determinado texto de eventos y vincularlo a los valores seleccionados.

análisis de registros

El *análisis de registros* es el estudio de las entradas de registro para identificar los eventos de interés. Si los registros no se analizan de forma periódica, su valor se reduce en gran medida.

análisis de registros

El *análisis de registros* es el proceso de extracción de datos de un registro de manera que los valores analizados se pueden emplear en una etapa posterior de la gestión de registros.

archivo de análisis de mensajes (XMP)

Un *archivo de análisis de mensajes (XMP)* es un archivo XML asociado a un tipo de origen de evento específico que aplica reglas de análisis. Las reglas de análisis dividen los datos relevantes de un evento sin formato recopilado en pares nombre-valor que se transfieren al archivo de asignación para continuar el procesamiento. Este tipo de archivo se emplea en todas las integraciones y en los conectores que se basan en integraciones. En el caso de los adaptadores de CA, los archivos XMP también se pueden aplicar en el servidor de CA Enterprise Log Manager.

archivos de asignación de datos (DM)

Los *archivos de asignación de datos (DM)* son archivos XML que emplean la gramática de eventos comunes (CEG) de CA para transformar eventos del formato de origen a un formato compatible con la gramática de eventos comunes con el fin de poder almacenarlos para realizar informes y análisis en el sistema de almacenamiento de registro de eventos. Es necesario crear un archivo de asignación de datos para cada nombre de registro para poder almacenar datos de eventos. Los usuarios pueden modificar o copiar un archivo de asignación de datos y aplicarlo a un determinado conector.

asignación de datos (DM)

La *asignación de datos* es el proceso de asignación de los pares clave-valor en la gramática de eventos comunes. La asignación de datos se lleva a cabo mediante un archivo de asignación de datos.

asignaciones de función

Las *asignaciones de función* son una parte opcional del archivo de asignación de datos para una integración del producto. Las asignaciones de funciones se emplean para rellenar un campo de la gramática de eventos comunes cuando el valor requerido no se puede obtener directamente del evento de origen. Todas las asignaciones de función constan de un nombre de campo de gramática de eventos comunes, un valor de campo predefinido o de clase y la función empleada para obtener o calcular el valor.

asistente para el archivo de análisis

El *asistente para el archivo de análisis* es una función de CA Enterprise Log Manager que emplean los administradores para crear, editar y analizar archivos eXtensible Message Parsing (XMP) almacenados en el servidor de gestión de CA Enterprise Log Manager. La personalización del análisis de los datos de eventos entrantes incluye la edición de filtros y cadenas de coincidencias previas. Los archivos nuevos y los editados se muestran en el explorador de recopilaciones, en la biblioteca de refinamiento de eventos, en los archivos de análisis de la carpeta de usuarios.

base de datos en estado tibio

El *estado tibio de una base de datos* es el estado en el que se encuentra una base de datos de registros de eventos cuando se supera el tamaño (Número máximo de filas) de la base de datos caliente o cuando se lleva a cabo una recatalogación tras restaurar una base de datos fría en un sistema de almacenamiento de registro de eventos nuevo. Las bases de datos tibias se comprimen y se retienen en el sistema de almacenamiento de eventos hasta que su antigüedad en días supera el valor configurado para Número máximo de días de archivado. Puede realizar consultas en registros de eventos de bases de datos en estado caliente, tibio y descongelado.

bases de datos archivadas

Las *bases de datos archivadas* de un determinado servidor de CA Enterprise Log Manager incluyen todas las bases de datos tibias que están disponibles para realizar consultas pero que deben poseer copias de seguridad antes de caducar, todas las bases de datos frías que se han registrado como poseedoras de copias de seguridad, así como todas las bases de datos registradas como restauradas a partir de copias de seguridad.

biblioteca de análisis de mensajes

La *biblioteca de análisis de mensajes* es una biblioteca que acepta eventos de las colas de escucha y emplea expresiones regulares para convertir las cadenas de pares nombre/valor mediante tokens.

biblioteca de consultas

La *biblioteca de consultas* es la biblioteca que almacena todas las consultas predefinidas y definidas por el usuario, las etiquetas de consultas y los filtros de solicitudes.

biblioteca de informes

La *biblioteca de informes* es la biblioteca que almacena todos los informes predefinidos y definidos por el usuario, las etiquetas de informes y las tareas de informes programadas.

biblioteca de refinamiento de eventos

La *biblioteca de refinamiento de eventos* es el sistema de almacenamiento de integraciones predefinidas y definidas por el usuario, archivos de asignación y análisis, así como reglas de supresión y resumen.

CA Enterprise Log Manager

CA Enterprise Log Manager es una solución que le ayuda a recopilar registros de diversos tipos de orígenes de eventos dispersos, comprobar la conformidad con las consultas y los informes, así como guardar entradas de bases de datos de registros comprimidos que ha trasladado a sistemas de almacenamiento externos a largo plazo.

CA IT PAM

CA IT PAM es la forma abreviada de CA IT Process Automation Manager. Este producto de CA automatiza los productos que haya definido. CA Enterprise Log Manager emplea dos procesos: el proceso de creación de un proceso de obtención de eventos/alertas para un producto local, como CA Service Desk; y el proceso de generación dinámica de listas que pueden importarse como valores con clave. La integración requiere CA IT PAM r2.1.

CA Spectrum

CA Spectrum es un producto de gestión de errores de red que se puede integrar con CA Enterprise Log Manager para emplearlo como destino de las alertas enviadas en forma de traps de SNMP.

CAELM

CAELM es el nombre de la instancia de la aplicación que emplea CA EEM para CA Enterprise Log Manager. Para acceder a la funcionalidad de CA Enterprise Log Manager en CA Embedded Entitlements Manager, introduzca la URL: https://<ip_address>:5250/spin/eiam/eiam.csp, seleccione CAELM como nombre de la aplicación e introduzca la contraseña del usuario de EiamAdmin.

caelmadmin

El nombre de usuario y la contraseña de *caelmadmin* son las credenciales necesarias para acceder al sistema operativo del dispositivo de software. El ID de usuario de caelmadmin se crea durante la instalación de este sistema operativo. Durante la instalación del componente de software, el instalador debe especificar la contraseña de la cuenta del superusuario de CA EEM, EiamAdmin. La cuenta de caelmadmin tendrá la misma contraseña. Es recomendable que el administrador del servidor realice ssh como usuario de caelmadmin y cambie esta contraseña predeterminada. Aunque el administrador no puede realizar ssh como raíz, sí puede trasladar a los usuarios a la raíz (su root) si lo considera necesario.

caelmservice

caelmservice es una cuenta de servicio que permite a iGateway y a los servicios de CA EEM locales ejecutarse como un usuario no-root. La cuenta caelmservice se emplea para instalar actualizaciones del sistema operativo descargadas con actualizaciones de suscripción.

calendario

Un *calendario* es un sistema para limitar las veces que una política de acceso es efectiva. Una política permite que determinadas identidades lleven a cabo acciones especificadas con respecto a cierto recurso durante un tiempo determinado.

CALM

CALM es un tipo de recurso predefinido que incluye los recursos de CA Enterprise Log Manager siguientes: Alert, ArchiveQuery, calmTag, Data, EventGrouping, Integration y Report. Las acciones permitidas en este tipo de recurso son Anotar (Reports), Crear (Alert, calmTag, EventGrouping, Integration y Report), Acceso a datos (Data), Ejecutar (ArchiveQuery) y Programar (Alert, Report).

calmTag

calmTag es un atributo de Objeto aplicación que se emplea al crear políticas de ámbito para limitar a los usuarios a los informes y las consultas pertenecientes a determinadas etiquetas. Todos los informes y las consultas son Objetos aplicación y tienen calmTag como atributo. (Esto no debe confundirse con la etiqueta de recursos.)

Campos de la gramática de eventos comunes

Los *campos de la gramática de eventos comunes* son etiquetas empleadas para estandarizar la presentación de campos de eventos sin formato de diversos orígenes de eventos. Durante el refinamiento de eventos, CA Enterprise Log Manager analiza mensajes de eventos en una serie de pares de nombres y valores y, a continuación, asigna los nombres de eventos sin formato a campos de la gramática de eventos comunes estándar. Este refinamiento crea pares de nombres y valores que constan de campos de la gramática de eventos comunes y de valores del evento sin formato. Esto quiere decir que las diferentes etiquetas empleadas en eventos sin formato para el mismo objeto de datos o elemento de red se convierten con el mismo nombre de campo de la gramática de eventos comunes al refinar los eventos sin formato. Los campos de la gramática de eventos comunes se asignan al OID en la MIB empleada para traps de SNMP.

carpeta

Una *carpeta* es la ubicación de la ruta del directorio que emplea el servidor de gestión de CA Enterprise Log Manager para almacenar los tipos de objetos de CA Enterprise Log Manager. Se hace referencia a carpetas en las políticas de ámbito para otorgar o denegar a los usuarios el derecho a acceder a un tipo de objeto determinado.

catálogo

El *catálogo* es la base de datos de cada CA Enterprise Log Manager que mantiene el estado de las bases de datos guardadas, al tiempo que actúa como un índice de alto nivel en todas las bases de datos. La información sobre el estado (caliente, tibio o descongelado) se mantiene para todas las bases de datos presentes en algún momento en este servidor de CA Enterprise Log Manager y para cualquier base de datos que se haya restaurado en este servidor de CA Enterprise Log Manager como base de datos descongelada. La capacidad de indexación se extiende a todas las bases de datos calientes y tibias del sistema de almacenamiento de eventos de este servidor de CA Enterprise Log Manager.

catálogo de archivos

Consulte catálogo.

categorías de eventos

Las *categorías de eventos* son etiquetas empleadas por CA Enterprise Log Manager para clasificar eventos por su función antes de insertarlos en el almacén de eventos.

certificados

Los *certificados* que CA Enterprise Log Manager utiliza de modo predeterminado son CAELMCert.cer y CAELM_AgentCert.cer. Todos los servicios CA Enterprise Log Manager utilizan CAELMCert.cer para comunicar con el servidor de gestión. Todos los agentes utilizan CAELM_AgentCert.cer para comunicar con su servidor de recopilación.

cliente de suscripción

Un *cliente de suscripción* es un servidor de CA Enterprise Log Manager que obtiene contenido de otro servidor de CA Enterprise Log Manager denominado servidor proxy de suscripción. Los clientes de suscripción sondean el servidor proxy de suscripción configurado de manera regular y recuperan las actualizaciones nuevas cuando están disponibles. Tras recuperar las actualizaciones, el cliente instala los componentes descargados.

complemento de eventos iTech

El *complemento de eventos iTech* es un adaptador de CA que puede configurar un administrador con archivos de asignación seleccionados. Recibe eventos de forma remota de iRecorders, CA EEM, la propia iTechnology o cualquier producto que envía eventos mediante iTechnology.

componentes de visualización

Los *componentes de visualización* son opciones disponibles para mostrar datos de informes que incluyen una tabla, un gráfico (gráfico de escala, gráfico de barras, gráfico de columnas, gráfico circular) o un visor de eventos.

conector

Un *conector* es la integración de un determinado origen de evento que se configura en un agente determinado. Un agente puede cargar múltiples conectores de tipos similares o distintos en la memoria. El conector permite la recopilación de eventos sin formato de un origen de eventos, así como la transmisión basada en reglas de los eventos convertidos a un sistema de almacenamiento de registro de eventos, donde se introducen en la base de datos caliente. Las integraciones predeterminadas permiten realizar una recopilación optimizada de un amplio rango de orígenes de eventos, incluidos sistemas operativos, bases de datos, servidores Web, cortafuegos y muchos tipos de aplicaciones de seguridad. Puede definir un conector para un origen de evento propio desde el principio o puede emplear para ello una integración a modo de plantilla.

configuración global

La *configuración global* es una serie de ajustes que se aplica a todos los servidores de CA Enterprise Log Manager que emplean el mismo servidor de gestión.

configuración guardada

Una *configuración guardada* es una configuración almacenada con los valores de los atributos de acceso a los datos de una integración que se puede emplear como plantilla al crear una integración nueva.

consulta

Una *consulta* es un conjunto de criterios empleado para realizar búsquedas en los sistemas de almacenamiento de registro de eventos del servidor de CA Enterprise Log Manager activo y, si se especifica, de sus servidores federados. Una consulta se dirige a las bases de datos calientes, tibias o descongeladas especificadas en la cláusula de la consulta. Por ejemplo, si la cláusula Dónde limita la consulta a eventos con el origen source_username="myname" en un determinado intervalo de tiempo y sólo 10 de las 1.000 bases de datos contienen registros que cumplen los criterios basados en información contenida en la base de datos del catálogo, la consulta sólo se ejecutará en esas 10 bases de datos. Una consulta sólo puede devolver un máximo de 5.000 filas de datos. Cualquier usuario con una función predefinida puede ejecutar una consulta. Sólo los analistas y los administradores pueden programar una consulta para distribuir una alerta de acción, crear un informe mediante la selección de las consultas que se van a incluir o crear una consulta personalizada mediante el asistente de diseño de consulta. Consulte también consulta de archivo.

consulta de acción

Una *consulta de acción* es una consulta que admite una alerta de acción. Se ejecuta en una programación repetitiva para probar las condiciones indicadas por la alerta de acción a la que está vinculada.

consulta de archivos

Una *consulta de archivos* es una consulta del catálogo que se emplea para identificar las bases de datos frías que se deben restaurar y descongelar para realizar consultas. Una consulta de archivos se diferencia de una consulta normal en que se realiza en bases de datos frías, mientras que una consulta normal se realiza en bases de datos calientes, tibias y descongeladas. Los administradores pueden emitir una consulta de archivos desde la ficha Administración, subficha Recopilación de registros, opción Consulta de catálogo de archivos.

Contenido de los trap de SNMP

Un *trap de SNMP* consta de pares de nombres y valores, donde cada nombre es un OID (identificador de objeto) y cada valor se obtiene de la alerta programada. Los resultados de consultas obtenidos por una alerta de acción constan de campos de la gramática de eventos comunes y sus valores. El trap de SNMP se rellena sustituyendo un OID para cada campo de la gramática de eventos comunes empleado para el nombre del par de nombre y valor. La asignación de cada campo de la gramática de eventos comunes a un OID se almacena en la MIB. El trap de SNMP sólo incluye pares de nombres y valores para los campos seleccionados al configurar la alerta.

cuenta

Una *cuenta* es un usuario global que también es un usuario de la aplicación de CALM. Una persona puede tener más de una cuenta, cada una de ellas con una función definida por el usuario distinta.

descongelación

La *descongelación* es el proceso de modificación del estado de una base de datos de frío a descongelado. El proceso de descongelación se lleva a cabo mediante el servidor de CA Enterprise Log Manager cuando éste recibe una notificación de la utilidad LMArchive de que se ha restaurado una base de datos fría conocida. (Si la base de datos fría no se restaura en el servidor de CA Enterprise Log Manager original, no se empleará la utilidad LMArchive y no será necesario realizar la descongelación; la recatalogación añadirá la base de datos restaurada como base de datos tibia.)

Destinos de traps de SNMP

Se pueden agregar uno o varios *destinos de traps de SNMP* al realizar la programación de una alerta de acción. Cada destino de trap de SNMP se configura mediante un puerto y una dirección IP. El destino suele ser un NOC o un servidor de gestión como CA Spectrum o CA NSM. Se envía un trap de SNMP a los destinos configurados cuando las consultas de una tarea de alerta programada devuelven resultados.

dispositivo de software

El *dispositivo de software* incluye el componente de un sistema operativo y el componente del software de CA Enterprise Log Manager.

elementos de integración

Los *elementos de integración* incluyen un sensor, un ayudante de la configuración, un archivo de acceso a datos, uno o varios archivos de análisis de mensajes (XMP) y uno o varios archivos de asignación de datos.

enrutador de SAPI

El *enrutador de SAPI* es un adaptador de CA que recibe eventos de integraciones, como la unidad central, y los envía a un enrutador de CA Audit.

entrada de registro

Una *entrada de registro* es un registro de auditoría individual.

entrada de registro

Una *entrada de registro* es la entrada de un registro que contiene información sobre un determinado evento que se ha producido en un sistema o en una red.

estado caliente de base de datos

Un *estado caliente de base de datos* es el estado de la base de datos del sistema de almacenamiento de registro de eventos en la que se insertan los eventos nuevos. Cuando la base de datos caliente alcanza el tamaño configurable en el servidor de recopilación, dicha base de datos se comprime, se cataloga y se traslada al almacenamiento tibio del servidor de informes. Además, todos los servidores almacenan eventos autocontrolados nuevos en una base de datos caliente.

estado descongelado de base de datos

El *estado descongelado de base de datos* es el estado aplicado a una base de datos que se ha restaurado en el directorio de archivo después de que el administrador haya ejecutado la utilidad LMArchive para notificar a CA Enterprise Log Manager de que se ha restaurado. Las bases de datos descongeladas se retienen durante el número de horas configurado en la política de exportación. Puede realizar consultas en registros de eventos de bases de datos en estado caliente, tibio y descongelado.

estado frío de base de datos

El *estado frío de base de datos* se aplica a una base de datos tibia cuando un administrador ejecuta la utilidad LMArchive para notificar al servidor de CA Enterprise Log Manager de que la base de datos tiene una copia de seguridad. Los administradores deben realizar copias de seguridad de las bases de datos tibias y ejecutar esta utilidad antes de que se eliminen. Una base de datos tibia se elimina automáticamente cuando su antigüedad supera el número máximo de días de archivado o cuando se alcanza el umbral de espacio en disco para archivo, lo que suceda en primer lugar. Puede realizar consultas en la base de datos de archivo para identificar las bases de datos en estado tibio o frío.

estados de la base de datos

Los *estados de la base de datos* son los siguientes: caliente para las bases de datos con eventos nuevos no comprimidas; tibio para las bases de datos de eventos no comprimidos; frío para bases de datos con copia de seguridad; y descongelado para las bases de datos restauradas en el sistema de almacenamiento de registro de eventos desde el que se copiaron. Puede realizar consultas en bases de datos calientes, tibias y descongeladas. Una consulta de archivos muestra información de las bases de datos frías.

etiqueta

Una *etiqueta* es una frase clave o un término empleado para identificar consultas o informes pertenecientes al mismo grupo relevante para el negocio. Las etiquetas permiten realizar búsquedas basadas en grupos relevantes para el negocio. Etiqueta también es el nombre del recurso empleado en todas las políticas para permitir a los usuarios crear etiquetas.

event_action

El campo *event_action* es el campo específico del evento de cuarto nivel de la normalización de eventos empleado por la gramática de eventos comunes. Describe acciones comunes. Entre los ejemplos de tipos de acciones de eventos se incluyen los de inicio de proceso, detención de proceso y error de aplicación.

event_category

El campo *event_category* es el campo específico del evento de segundo nivel de la normalización de eventos empleado por la gramática de eventos comunes. Ofrece una mayor clasificación de eventos mediante un campo ideal_model específico. Los tipos de categorías de eventos incluyen seguridad operativa, gestión de identidades, gestión de la configuración, acceso a recursos y acceso al sistema.

event_class

El campo *event_class* es el campo específico del evento de tercer nivel de la normalización de eventos empleado por la gramática de eventos comunes. Ofrece una mayor clasificación de eventos mediante un campo event_category específico.

evento autocontrolado

Un *evento autocontrolado* es un evento que se registra mediante CA Enterprise Log Manager. Estos eventos se generan de forma automática mediante acciones llevadas a cabo por usuarios registrados y mediante funciones llevadas a cabo por varios módulos, como servicios y escuchas. El informe de detalles de eventos autocontrolados de SIM se puede visualizar seleccionando un servidor de informes y abriendo la ficha Eventos autocontrolados.

evento local

Un *evento local* es un evento que afecta a una sola entidad, mientras que el origen y el destino del evento están en el mismo equipo de host. Un evento local es el tipo 1 de los cuatro tipos de eventos empleados en la gramática de eventos comunes (CEG).

evento nativo

Un *evento nativo* es el estado o la acción que desencadena un evento sin formato. Los eventos nativos se reciben y se analizan/asignan según corresponda y, a continuación, se transmiten como eventos sin formato o refinados. Una autenticación errónea es un evento nativo.

evento observado

Un *evento observado* es un evento que afecta al origen, al destino y al agente. Un agente de recopilación de eventos observa y registra dicho evento.

evento refinado

Un *evento refinado* consta de la información de un evento asignado o analizado derivada de eventos sin formato o resumidos. CA Enterprise Log Manager lleva a cabo la asignación y el análisis de manera que se puedan realizar búsquedas en la información almacenada.

evento registrado

Un *evento registrado* consta de la información de un evento sin formato o refinado tras su inserción en la base de datos. Los eventos sin formato siempre se registran, a no ser que se supriman o se resuman, ya que son eventos refinados. Esta información se almacena y se pueden realizar búsquedas en ella.

evento remoto

Un *evento remoto* es un evento que afecta a dos equipos de host diferentes: el de origen y el de destino. Un evento remoto es el tipo 2 de los cuatro tipos de eventos empleados en la gramática de eventos comunes (CEG).

evento RSS

Un *evento RSS* (del inglés Rich Site Summary) es un evento generado por CA Enterprise Log Manager para transmitir una alerta de acción a usuarios y productos de terceros. El evento consta de un resumen del resultado de cada alerta de acción, así como de un vínculo al archivo de resultados. Se puede configurar la duración de un determinado elemento de fuente RSS.

evento sin formato

Un *evento sin formato* es la información activada por un evento nativo que se envía a través de un agente de control al recopilador del gestor de registros. El evento sin formato se formatea a menudo como cadena de syslog o par de nombre y valor. Se puede revisar un evento en su estado sin formato en CA Enterprise Log Manager.

eventos

Los *eventos* de CA Enterprise Log Manager son las entradas de registro generadas por cada origen de eventos especificado.

explorador de agentes

El *explorador de agentes* es el almacén de los ajustes de la configuración de agentes. (Es posible instalar agentes en un punto de recopilación o en los puntos finales en los que existen orígenes de eventos.)

federación en malla

Una *federación en malla* de servidores de CA Enterprise Log Manager es una topología que establece una relación entre los servidores al mismo nivel. En su estructura más sencilla, el servidor 2 es el servidor secundario del servidor 1, y el servidor 1 es el servidor secundario del servidor 2. Un par de servidores en malla tiene una relación bidireccional. Una federación en malla puede definirse de manera que muchos servidores sean equivalentes entre sí. Una consulta federada arroja resultados del servidor seleccionado y sus equivalentes.

federación jerárquica

Una *federación jerárquica* de servidores de CA Enterprise Log Manager es una topología que establece una relación jerárquica entre los servidores. En su estructura más sencilla, el servidor 2 es el servidor secundario del servidor 1, pero el servidor 1 no es el servidor secundario del servidor 2, es decir, que la relación es unidireccional. Una federación jerárquica puede tener múltiples niveles de relaciones principal-secundario y un solo servidor principal puede tener numerosos servidores secundarios. Una consulta federada arroja resultados del servidor seleccionado y sus servidores secundarios.

filtrado de eventos

El *filtrado de eventos* es el proceso de interrupción de eventos en función de los filtros de la gramática de eventos comunes.

filtro

Un *filtro* es un método que puede emplear para restringir una consulta del sistema de almacenamiento de registro de eventos.

filtro de acceso

Un *filtro de acceso* es un filtro que el administrador puede emplear para controlar qué datos de eventos pueden visualizar los grupos o los usuarios que no son administradores. Por ejemplo, un filtro de acceso puede restringir los datos que pueden ver en un informe las identidades especificadas. Los filtros de acceso se convierten de forma automática en políticas de obligación.

filtro global

Un *filtro global* es un conjunto de criterios que puede especificar y que limita lo que se muestra en todos los informes. Por ejemplo, un filtro global de los eventos de informes de los últimos 7 días generado durante los últimos siete días.

filtro local

Un *filtro local* es un conjunto de criterios que puede establecer mientras visualiza un informe para limitar los datos mostrados en dicho informe.

función Administrator

La *función Administrator* ofrece a los usuarios la posibilidad de llevar a cabo todas las acciones válidas en todos los recursos de CA Enterprise Log Manager. Los administradores son los únicos que pueden configurar los servicios y la recopilación de registros, así como gestionar usuarios, políticas de acceso y filtros de acceso.

función Analyst

La *función Analyst* ofrece a los usuarios la posibilidad de crear y editar consultas e informes personalizados, editar y anotar informes, crear etiquetas, así como programar informes y alertas de acción. Los analistas también pueden llevar a cabo las tareas de los auditores.

función Auditor

La *función Auditor* ofrece a los usuarios acceso a informes y a los datos que contienen. Los auditores puede visualizar informes, la lista de plantillas de informes, la lista de trabajos de informes programados y la lista de informes generados. Los auditores pueden programar y anotar informes. Los auditores no tienen acceso a las fuentes RSS a no ser que la configuración se establezca para no solicitar ninguna autenticación para visualizar alertas de acción.

función del usuario

Una *función del usuario* puede ser un grupo de usuarios de la aplicación predeterminado o un grupo de aplicaciones definido por el usuario. Es necesario contar con funciones de usuarios personalizadas cuando los grupos de la aplicación predeterminados (Administrator, Analyst y Auditor) no están lo suficientemente depurados como para reflejar las asignaciones de trabajo. Las funciones de usuarios personalizadas requieren el empleo de políticas de acceso personalizado y la modificación de las políticas predefinidas para incluir la función nueva.

gestión de agentes

La *gestión de agentes* es el proceso de software que controla todos los agentes asociados a los servidores de CA Enterprise Log Manager federados. Autentica los agentes que se comunican con este proceso.

gestión de la titularidad

La *gestión de la titularidad* es el método para controlar lo que los usuarios pueden hacer una vez que se autentican e inician sesión en la interfaz de CA Enterprise Log Manager. Esto se logra mediante políticas de acceso asociadas a funciones asignadas a usuarios. Las funciones o grupos de usuarios de la aplicación, así como las políticas de acceso pueden estar predefinidos o definidos por el usuario. El almacén de usuarios interno de CA Enterprise Log Manager es el que realiza la gestión de la titularidad.

gestión de los registros de seguridad de equipos

La *gestión de los registros de seguridad de equipos (Computer Security Log Management)* se define, según el NIST, como "el proceso de generar, transmitir, almacenar, analizar y eliminar datos de registros de seguridad de los equipos".

gramática de eventos comunes (CEG)

La *gramática de eventos comunes (CEG)* es el esquema que ofrece un formato estándar al que CA Enterprise Log Manager convierte los eventos mediante archivos de análisis y asignación antes de almacenarlos en el sistema de almacenamiento de registro de eventos. La gramática de eventos comunes emplea campos comunes y normalizados para definir los eventos de seguridad desde diferentes plataformas y productos. Los eventos que no se pueden analizar o asignar se almacenan como eventos sin formato.

grupo de agentes

Un *grupo de agentes* es una etiqueta que pueden aplicar los usuarios a agentes seleccionados que permite a los usuarios aplicar la configuración de un agente a múltiples agentes a la vez, así como recuperar informes basados en los grupos. Un agente determinado sólo puede pertenecer a un grupo a la vez. Los grupos de agentes se basan en criterios definidos por el usuario, como la región geográfica o la importancia.

grupo de aplicaciones

Un *grupo de aplicaciones* es un grupo específico del producto que se puede asignar a un usuario global. Los grupos de aplicaciones predefinidos para CA Enterprise Log Manager, o funciones, son Administrator, Analyst y Auditor. Estos grupos de aplicaciones sólo están disponibles para usuarios de CA Enterprise Log Manager; no se pueden asignar a usuarios de otros productos registrados en el mismo servidor de CA EEM. Los grupos de aplicaciones definidos por el usuario debe añadirse a la política predeterminada de acceso a la aplicación de CALM para que los usuarios de dichos grupos puedan acceder a CA Enterprise Log Manager.

grupo de usuarios

Un *grupo de usuarios* puede ser un grupo de aplicaciones, un grupo global o un grupo dinámico. Los grupos de aplicaciones de CA Enterprise Log Manager predefinidos son Administrator, Analyst y Auditor. Los usuarios de CA Enterprise Log Manager pueden formar parte de grupos globales a través de pertenencias independientes de CA Enterprise Log Manager. Los grupos dinámicos son grupos definidos por el usuario y creados mediante una política de grupos dinámicos.

grupo dinámico de usuarios

Los *grupos dinámicos de usuarios* constan de usuarios globales que comparten uno o varios atributos. Los grupos dinámicos de usuarios se crean mediante una política de grupo dinámico de usuarios en la que el nombre del grupo dinámico de usuarios y la pertenencia se basan en un conjunto de filtros configurados en los atributos de los usuarios y del grupo.

grupo global

Un *grupo global* es un grupo compartido en las instancias de la aplicación registradas en el mismo servidor de gestión de CA Enterprise Log Manager. Un usuario puede estar asignado a uno o varios grupos globales. Las políticas de acceso se pueden definir en los grupos globales como identidades que pueden o no llevar a cabo acciones seleccionadas en determinados recursos.

ideal_model

ideal_model representa la tecnología que expresa el evento. Este es el primer campo de la gramática de eventos comunes en una jerarquía de campos empleados para la clasificación y la normalización de eventos. Los ejemplos de un modelo ideal incluyen antivirus, DBMS, cortafuegos, sistema operativo y servidor Web. Los productos de cortafuegos Check Point, Cisco PIX y Netscreen/Juniper podrían normalizarse mediante la introducción del valor "Cortafuegos" en el campo ideal_model.

identidad

Una *identidad* de CA Enterprise Log Manager es un usuario o un grupo que puede acceder a la instancia de la aplicación de CAELM y a sus recursos. La identidad de los productos de CA puede ser un usuario global, un usuario de la aplicación, un grupo global, un grupo de aplicaciones o un grupo dinámico.

informe

Un *informe* es una pantalla gráfica o en forma de tabla de datos de registro de eventos generada mediante la ejecución de consultas predefinidas o personalizadas con filtros. Los datos pueden proceder de bases de datos calientes, tibias y descongeladas del sistema de almacenamiento de registro de eventos del servidor seleccionado y, si se solicita, de sus servidores federados.

Informes relacionados con EPHI

Los *informes relacionados con EPHI* son informes que se centran en la seguridad de HIPAA; EPHI hace referencia a la información médica protegida electrónicamente. Estos informes pueden ayudarle a demostrar que toda la información sanitaria identificable de forma individual y relacionada con los pacientes que se crea, se mantiene o se transmite electrónicamente está protegida.

Instalador

El *instalador* es la persona que instala el dispositivo de software y los agentes. Durante el proceso de instalación, se crean los nombres de usuario de caelmadmin y EiamAdmin y se asigna a caelmadmin la contraseña especificada para EiamAdmin. Estas credenciales de caelmadmin son necesarias para el primer acceso al sistema operativo; las credenciales de EiamAdmin son necesarias para el primer acceso al software de CA Enterprise Log Manager y para la instalación de agentes.

instancia de la aplicación

Una *instancia de la aplicación* es un espacio común en el repositorio de CA EEM donde se almacenan todas las configuraciones, usuarios, grupos, contenido y políticas de autorización. Normalmente, todos los servidores de CA Enterprise Log Manager de una empresa emplean la misma instancia de la aplicación (CAELM de forma predeterminada). Puede instalar servidores de CA Enterprise Log Manager con diferentes instancias de la aplicación, pero sólo se pueden federar los servidores que compartan la misma instancia de la aplicación. Los servidores configurados para emplear el mismo servidor de CA EEM, pero que tengan instancias de la aplicación diferentes, sólo compartirán el almacén de usuarios, las políticas de contraseñas y los grupos globales. Distintos productos de CA poseen instancias de la aplicación diferentes.

integración

La *integración* es el método a través del cual se procesan los eventos no clasificados para convertirlos en eventos refinados, de manera que se puedan visualizar en consultas e informes. La integración se lleva a cabo a través de un conjunto de elementos que permite a un agente y a un conector determinados recopilar eventos de uno o varios tipos de orígenes de eventos y enviarlos a CA Enterprise Log Manager. El conjunto de elementos incluye el sensor de registro y archivos XMP y de asignación de datos que están diseñados para leer un producto específico. Los ejemplos de integraciones predefinidas incluyen aquellos para el procesamiento de eventos de syslog y eventos WMI. Puede crear integraciones personalizadas para permitir el procesamiento de eventos no clasificados.

lista de control de acceso de identidades

Una *lista de control de acceso de identidades* le permite especificar las diferentes acciones que puede llevar a cabo cada identidad seleccionada en los recursos determinados. Por ejemplo, mediante una lista de control de acceso de identidades, puede especificar que una identidad pueda crear informes y que otra pueda programar y anotar informes. Una lista de control de acceso de identidades se diferencia de una lista de control de acceso en que la primera se centra en las identidades en lugar de centrarse en los recursos.

MIB (base de información gestionada)

La *MIB (base de información gestionada)* de CA Enterprise Log Manager, CA-ELM.MIB, debe importarse y compilarse por parte de cada producto que vaya a recibir alertas en forma de traps de SNMP de CA Enterprise Log Manager. La MIB muestra el origen de cada identificador de objeto (OID) empleado en un mensaje de trap de SNMP con una descripción de dicho objeto de datos o elemento de red. En la MIB de los traps de SNMP enviados por CA Enterprise Log Manager, la descripción textual de cada objeto de datos es para el campo de la gramática de eventos comunes asociada. La MIB permite asegurarse de que todos los pares de nombre/valor enviados en un trap de SNMP se interpretan correctamente en el destino.

módulo (para descargar)

Un *módulo* es un grupo lógico de actualizaciones de componentes disponible para su descarga a través de una suscripción. Un módulo puede contener actualizaciones de archivos binarios, actualizaciones de contenido o ambas. Por ejemplo, todos los informes forman un módulo; todas las actualizaciones de archivos binarios del patrocinador forman otro módulo. CA define los elementos que componen cada módulo.

módulo de suscripción

El *módulo de suscripción* es el servicio que permite que las actualizaciones de suscripción del servidor de suscripciones de CA se descarguen y se distribuyan de forma automática a todos los servidores de CA Enterprise Log Manager y a todos los agentes. La configuración global se aplica a los servidores de CA Enterprise Log Manager locales; la configuración local incluye si el servidor es un proxy sin conexión, un proxy en línea o un cliente de suscripción.

NIST

El *instituto nacional de normas y tecnología (NIST por sus siglas en inglés)* es una agencia estadounidense que ofrece recomendaciones en su publicación especial 800-92, *Guide to Computer Security Log Management* (Guía para la gestión de registros de seguridad de equipos), empleadas como base para CA Enterprise Log Manager.

nombre del usuario EiamAdmin

EiamAdmin es el nombre de superusuario predeterminado asignado al instalador de los servidores de CA Enterprise Log Manager. Al instalar el primer software de CA Enterprise Log Manager, el instalador crea una contraseña para esta cuenta de superusuario, a no ser que ya exista un servidor CA EEM remoto. En ese caso, el instalador debe introducir la contraseña existente. Tras instalar el dispositivo de software, el instalador abre un explorador desde una estación de trabajo, introduce la URL de CA Enterprise Log Manager e inicia sesión como EiamAdmin con la contraseña correspondiente. Este primer usuario define el almacén de usuarios, crea las políticas de contraseñas y crea la primera cuenta de usuario con la función Administrator. El usuario EiamAdmin también puede llevar a cabo cualquier operación controlada por CA EEM.

Objeto seguro

Objeto seguro es un tipo de recurso predefinido de CA EEM. Es la clase de recursos a la que pertenece Objetos aplicación, almacenado en la aplicación. Los usuarios que definen políticas y filtros para permitir el acceso a Objetos aplicación hacen referencia a este tipo de recurso.

Objetos aplicación

Objetos aplicación son recursos específicos del producto almacenados en CA EEM en la instancia de la aplicación de un producto determinado. En el caso de la instancia de la aplicación de CAELM, estos recursos incluyen contenido de consultas e informes, tareas programadas para informes y alertas, configuraciones y contenido de agentes, configuraciones de servicios, adaptadores e integración, archivos de asignación de datos y análisis de mensajes, así como reglas de supresión y resumen.

OID (identificador de objeto)

Un *OID (identificador de objeto)* es un identificador numérico exclusivo para un objeto de datos que se empareja con un valor en un mensaje de trap de SNMP. Cada OID empleado en un trap de SNMP enviado por CA Enterprise Log Manager se asigna a un campo de la gramática de eventos comunes de la MIB. Cada OID asignado a un campo de la gramática de eventos comunes tiene esta sintaxis: 1.3.6.1.4.1.791.9845.x.x.x, donde 791 es el número de empresa de CA y 9845 es el identificador de producto de CA Enterprise Log Manager.

origen de evento

Un *origen de evento* es el host desde el que un conector recopila eventos sin procesar. Un origen de evento puede incluir varios almacenes de registro. A cada uno de ellos se accede mediante un conector independiente. Al implementar un conector nuevo, suele ser necesario configurar el origen de evento, de forma que el agente pueda acceder a éste y leer los eventos sin procesar desde uno de sus almacenes de registro. Los eventos sin procesar del sistema operativo, diferentes bases de datos y varias aplicaciones de seguridad se almacenan por separado en el origen de evento.

perfil

Un *perfil* es un conjunto de filtros de datos y etiquetas opcional y configurable que puede ser específico del producto, específico de la tecnología o aplicado a una categoría seleccionada. Por ejemplo, un filtro de etiquetas para un producto limita las etiquetas listadas a la etiqueta del producto seleccionado. Los filtros de datos de un producto sólo muestran datos del producto especificado en los informes generados, las alertas programadas y los resultados de consultas que visualice. Después de crear el perfil necesario, puede definir que dicho perfil se active siempre que inicie sesión. Si crea varios perfiles, puede aplicar diferentes perfiles (de uno en uno) a las actividades durante una sesión. Los filtros predefinidos se envían con actualizaciones de suscripción.

Petición

Una *petición* es un tipo especial de consulta que muestra los resultados basados en el valor que ha especificado y los campos de la gramática de eventos comunes seleccionados. Sólo se devuelven filas para los eventos en los que el valor especificado aparece en uno o varios campos de la gramática de eventos comunes seleccionados.

política de acceso

Una *política de acceso* es una regla que otorga o deniega a una identidad (usuario o grupo de usuarios) los derechos de acceso a un recurso de la aplicación. CA Enterprise Log Manager determina si las políticas se aplican a un usuario determinado comparando identidades, recursos, clases de recursos, así como evaluando los filtros.

política de acceso a la aplicación de CALM

La *política de acceso a la aplicación de CALM* es un tipo de lista de control de acceso de política de ámbito que define quién puede iniciar sesión en CA Enterprise Log Manager. De forma predeterminada, el administrador [del grupo], el analista [del grupo] y el auditor [del grupo] pueden iniciar sesión.

política de ámbito

Una *política de ámbito* es un tipo de política de acceso que otorga o deniega el acceso a los recursos almacenados en el servidor de gestión, como Objetos aplicación, usuarios, grupos, carpetas y políticas. Una política de ámbito define las identidades que pueden acceder a los recursos especificados.

política de delegación

Una *política de delegación* es una política de acceso que permite a un usuario delegar su autoridad en otro usuario, grupo de aplicaciones, grupo global o grupo dinámico. Debe eliminar de forma explícita las políticas de delegación creadas por el usuario eliminado o desactivado.

política de obligación

Una *política de obligación* es una política creada automáticamente cuando crea un filtro de acceso. No intente crear, editar o eliminar una política de obligación de forma directa. En lugar de ello, cree, edite o elimine el filtro de acceso.

pozFolder

pozFolder es un atributo de Objeto aplicación cuyo valor es la ruta principal de Objeto aplicación. El valor y el atributo pozFolder se emplea en los filtros de las políticas de acceso que restringen el acceso a recursos como informes, consultas y configuraciones.

proceso de obtención de resultados de eventos/alertas

El *proceso de obtención de resultados de eventos/alertas* es el proceso de CA IT PAM que solicita a un producto de terceros una respuesta ante datos de alerta configurados en CA Enterprise Log Manager. Puede seleccionar un proceso de CA IT PAM como destino al programar una tarea de alerta. Cuando una alerta ejecuta el proceso de CA IT PAM, CA Enterprise Log Manager envía los datos de alerta de CA IT PAM y CA IT PAM los reenvía con sus propios parámetros de procesamiento al producto de terceros como parte del proceso de obtención de resultados de eventos/alertas.

proceso de valores dinámicos

Un *proceso de valores dinámicos* es un proceso de CA IT PAM que puede activar para rellenar o actualizar la lista de valores de una clave seleccionada empleada en informes o alertas. Ofrezca la ruta al proceso de valores dinámicos como parte de la configuración de IT PAM en la lista de servicios del servidor de informes en la ficha Administración. Haga clic en Importar lista de valores dinámicos en la sección de valores asociada a los valores clave de esa misma página de la IU. La activación del proceso de valores dinámicos es uno de los tres métodos que puede emplear para agregar valores a las claves.

proxy de suscripción (en línea)

Un *proxy de suscripción en línea* es un servidor de CA Enterprise Log Manager con acceso a Internet que obtiene actualizaciones de suscripción del servidor de suscripciones de CA de forma repetitiva. Se puede incluir un determinado proxy de suscripción en línea en la lista de proxys para uno o más clientes, que se ponen en contacto con los proxys de la lista por turnos para solicitar las actualizaciones de archivos binarios. Un determinado proxy en línea, si se configura de este modo, envía contenido nuevo y actualizaciones de configuraciones al servidor de gestión, a no ser que ya los haya enviado otro proxy. El directorio de actualizaciones de suscripción de un proxy en línea seleccionado se emplea como origen para copiar actualizaciones en proxys de suscripción sin conexión.

proxy de suscripción (predeterminado)

El *proxy de suscripción predeterminado* suele ser el servidor de CA Enterprise Log Manager que se ha instalado en primer lugar y también puede ser el servidor de CA Enterprise Log Manager principal. El proxy de suscripción predeterminado también es un proxy de suscripción en línea y, por lo tanto, debe tener acceso a Internet. Si no se define ningún otro proxy de suscripción en línea, este servidor obtiene las actualizaciones de suscripción del servidor de suscripciones de CA, descarga las actualizaciones de archivos binarios para todos los clientes y envía las actualizaciones de contenido a CA EEM. Si se definen otros servidores proxy, este servidor sigue obteniendo actualizaciones de suscripción, pero los clientes sólo se ponen en contacto con él para recibir actualizaciones cuando no se haya configurado ninguna lista de servidores proxy de suscripciones o cuando la lista configurada se haya agotado.

proxy de suscripción (sin conexión)

Un *proxy de suscripción sin conexión* es un servidor de CA Enterprise Log Manager que obtiene actualizaciones de suscripción a través de una copia de directorios manual (mediante scp) de un proxy de suscripción en línea. Los proxys de suscripción sin conexión se pueden configurar para descargar actualizaciones de archivos binarios para clientes que las soliciten y para enviar la versión más reciente de las actualizaciones de contenido al servidor de gestión si aún no las ha recibido. Los servidores proxy de suscripciones sin conexión no necesitan tener acceso a Internet.

proxys de suscripción (para actualizaciones de contenido)

Los *proxys de suscripción para actualizaciones de contenido* son los proxys de suscripción seleccionados para actualizar el servidor de gestión de CA Enterprise Log Manager con actualizaciones de contenido que se descargan desde el servidor de suscripciones de CA. Se recomienda configurar múltiples proxys para disponer de una alternativa en caso de error.

proxys de suscripción (para el cliente)

Los *proxys de suscripción para el cliente* forman la lista de proxys de suscripción con la que se pone en contacto el cliente por turnos para obtener actualizaciones del sistema operativo y del software de CA Enterprise Log Manager. Si un proxy está ocupado, se contacta con el siguiente de la lista. Si no hay ninguno disponible y el cliente está en línea, se emplea el proxy de suscripción predeterminado.

punto de recopilación

Un *punto de recopilación* es un servidor en el que se ha instalado un agente y que tiene una proximidad de red con todos los servidores con orígenes de eventos asociados a los conectores de su agente.

recatalogación

Una *recatalogación* es una reconstrucción forzada del catálogo. La recatalogación sólo es necesaria al restaurar datos en un sistema de almacenamiento de registro de eventos situado en un servidor distinto de aquél en el que se han generado. Por ejemplo, si ha destinado un servidor de CA Enterprise Log Manager para que actúe como punto de restauración para investigaciones en datos fríos, tendrá que forzar una recatalogación de la base de datos tras restaurarla en el punto de restauración designado. La recatalogación se lleva a cabo de manera automática al reiniciar iGateway si es necesario. La recatalogación de un único archivo de la base de datos puede llevar varias horas.

recopilación de eventos

La *recopilación de eventos* es el proceso de lectura de la cadena de eventos sin formato en un origen de eventos y su envío al servidor CA Enterprise Log Manager configurado. La recopilación de eventos va seguida de un refinamiento de eventos.

recopilación directa de registros

La *recopilación directa de registros* es la técnica de recopilación de registros en la que no existe un agente intermedio entre el origen de evento y el software de CA Enterprise Log Manager.

recopilador de SAPI

El *recopilador de SAPI* es un adaptador de CA que recibe eventos de clientes de CA Audit. Los clientes de CA Audit envían con el recopilador una acción que permite una conmutación por error integrada. Los administradores configuran el recopilador de SAPI de CA Audit con, por ejemplo, archivos de asignación de datos y cifrados seleccionados.

recurso de la aplicación

Un *recurso de la aplicación* es cualquiera de los recursos específicos de CA Enterprise Log Manager en los que las políticas de acceso de CALM otorgan o deniegan a determinadas identidades la posibilidad de llevar a cabo acciones específicas de la aplicación como la creación, la programación y la edición. Los ejemplos incluyen los informes, las alertas y las integraciones. Consulte también recurso global.

recurso global

Un *recurso global* del producto de CA Enterprise Log Manager es un recurso compartido con otras aplicaciones de CA. Puede crear políticas de ámbito con recursos globales. Los ejemplos incluyen usuarios, políticas y calendarios. Consulte también recurso de la aplicación.

refinamiento de eventos

El *refinamiento de eventos* es el proceso mediante el cual una cadena de eventos sin formato recopilada se analiza en campos de eventos constitutivos y se asigna a campos de la gramática de eventos comunes. Los usuarios pueden ejecutar consultas para visualizar los datos de eventos refinados resultantes. El refinamiento de eventos es posterior a la recopilación de eventos y anterior al almacenamiento de eventos.

registro

Un *registro* es un registro de auditoría, o un mensaje registrado, correspondiente a un evento o a una recopilación de eventos. El registro puede ser un registro de auditoría, un registro de transacción, un registro de intrusos, un registro de conexión, un registro de rendimiento del sistema, un registro de actividad del usuario o una alerta.

registros de auditoría

Los *registros de auditoría* contienen eventos de seguridad como intentos de autenticación, accesos a archivos y cambios en las políticas de seguridad, las cuentas de usuario o los privilegios. Los administradores especifican qué tipos de eventos deberían auditarse y cuáles se deberían registrar.

reglas de resumen

Las *reglas de resumen* son reglas que combinan determinados eventos nativos del mismo tipo en un evento refinado. Por ejemplo, se puede configurar una regla de resumen para sustituir hasta 1.000 eventos duplicados con los mismos puertos y direcciones IP de origen y destino con un único evento de resumen. Estas reglas simplifican el análisis de eventos y reducen el tráfico de registro.

reglas de supresión

Las *reglas de supresión* son reglas que se configuran para evitar que aparezcan determinados eventos refinados en los informes. Puede crear reglas de supresión permanentes para eliminar eventos de rutina que no supongan problemas de seguridad y puede crear reglas temporales para suprimir el inicio de sesión de eventos planificados como la creación de múltiples usuarios nuevos.

reglas de transferencia de eventos

Las reglas de *transferencia de eventos* indican que los eventos seleccionados deben transferirse a productos de terceros, como aquellos que correlacionan eventos, tras guardarse en el almacén de registro de eventos.

SAPI recorder

Un *SAPI recorder* era la tecnología empleada para enviar información a CA Audit antes de iTechnology. SAPI significa Submit API (interfaz de programación de envío de aplicaciones). Los registradores de CA Audit para CA ACF2, CA Top Secret, RACF, Oracle, Sybase y DB2 son ejemplos de SAPI recorders.

sensor de registro

Un *sensor de registro* es un componente de integración diseñado para leer un tipo de registro específico, como una base de datos, syslog, un archivo o SNMP. Los sensores de registro se reutilizan. Normalmente, los usuarios no crean sensores de registro personalizados.

servicios

Los *servicios* de CA Enterprise Log Manager son el del sistema de almacenamiento de registro de eventos, el del servidor de informes y el de la suscripción. Los administradores configuran estos servicios en un nivel global en el que todos los ajustes se aplican a todos los servidores de CA Enterprise Log Manager de forma predeterminada. La mayor parte de las configuraciones globales de servicios se pueden anular en el nivel local, es decir, para cada servidor de CA Enterprise Log Manager especificado.

servidor de alertas

El *servidor de alertas* es el sistema de almacenamiento de alertas de acción y tareas de alertas de acción.

servidor de almacenamiento remoto

Un *servidor de almacenamiento remoto* es una función asignada a un servidor que recibe bases de datos almacenadas de forma automática de uno o varios servidores de informes. Un servidor de almacenamiento remoto almacena bases de datos frías durante la cantidad de años necesaria. El host remoto empleado para el almacenamiento no suele tener instalado ningún servidor de CA Enterprise Log Manager ni otros productos. Para el almacenamiento automático, configure la autenticación no interactiva.

servidor de gestión

El *servidor de gestión* es una función asignada al primer servidor de CA Enterprise Log Manager instalado. Dicho servidor de CA Enterprise Log Manager contiene el repositorio que almacena el contenido compartido, como las políticas, de todos los servidores de CA Enterprise Log Manager. Este servidor suele ser el proxy de suscripción predeterminado. Aunque no es recomendable para la mayoría de los entornos de producción, el servidor de gestión puede llevar a cabo todas las funciones.

servidor de informes

Un *servidor de informes* es una función desempeñada por un servidor de CA Enterprise Log Manager. Un servidor de informes recibe bases de datos tibias almacenadas de forma automática de uno o varios servidores de recopilación. Un servidor de informes gestiona consultas, informes, alertas programadas e informes programados.

servidor de informes

El *servidor de informes* es el servicio que almacena información de la configuración, como el servidor de correo electrónico que se debe emplear al enviar alertas por correo electrónico, el aspecto de los informes guardados en formato PDF y la retención de políticas para informes guardadas en el servidor de informes y para alertas enviadas a la fuente RSS.

Servidor de ODBC

El *servidor de ODBC* es el servicio configurado que define el puerto empleado para las comunicaciones entre el cliente de ODBC o JDBC y el servidor de CA Enterprise Log Manager, al tiempo que indica si se debe emplear el cifrado SSL.

servidor de punto de restauración

Un *servidor de punto de restauración* es una función desempeñada por un servidor de CA Enterprise Log Manager. Para investigar eventos "fríos", puede desplazar bases de datos del servidor de almacenamiento remoto al servidor de punto de restauración con una utilidad, agregar las bases de datos al catálogo y, a continuación, realizar las consultas. El desplazamiento de bases de datos frías a un punto de restauración dedicado es una alternativa a su desplazamiento al servidor de informes original para su investigación.

servidor de recopilación

Un *servidor de recopilación* es una función desempeñada por un servidor de CA Enterprise Log Manager. Un servidor de recopilación refina los registros de eventos entrantes, los introduce en la base de datos caliente, comprime la base de datos caliente y la copia o la guarda de forma automática en el servidor de informes correspondiente. El servidor de recopilación comprime la base de datos caliente cuando ésta alcanza el tamaño configurado y la almacena de forma automática según la programación configurada.

servidor de suscripciones de CA

El *servidor de suscripciones de CA* es el origen de las actualizaciones de suscripción de CA.

servidor proxy HTTP

Un *servidor proxy HTTP* es un servidor proxy que actúa como cortafuegos y evita que entre o salga tráfico de Internet de la empresa, salvo el que lo hace a través del proxy. El tráfico de salida puede especificar un ID y una contraseña para omitir el servidor proxy. Se puede configurar el empleo de un servidor proxy HTTP local en la gestión de suscripciones.

servidores de federación

Los *servidores de federación* son servidores de CA Enterprise Log Manager conectados entre sí en una red con el objetivo de distribuir la recopilación de los datos de registro, al tiempo que acumulan los datos recopilados para generar informes. Los servidores de federación se pueden conectar en una topología jerárquica o en malla. Los informes de datos federados incluyen los del servidor de destino, así como los de los secundarios o equivalentes, si los hay, de dicho servidor.

SNMP

SNMP es el acrónimo de protocolo simple de administración de redes (Simple Network Management Protocol), un estándar abierto para el envío de mensajes de alerta en forma de traps de SNMP desde un sistema de agente a uno o varios sistemas de gestión.

supresión

La *supresión* es el proceso de interrupción de eventos en función de los filtros de la gramática de eventos comunes. La supresión se lleva a cabo mediante archivos de supresión.

token de análisis de mensajes (ELM)

Un *token de análisis de mensajes* es una plantilla reutilizable para crear la sintaxis de expresión regular empleada en el análisis de mensajes de CA Enterprise Log Manager. El token tiene un nombre, un tipo y una cadena de expresión regular correspondiente.

URL de fuente RSS para alertas de acción

La *URL de fuente RSS para alertas de acción* es: https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp. En esta URL, puede visualizar alertas de acción sujetas a la configuración de cantidad y antigüedad máximas.

URL de fuente RSS para suscripción

La *URL de fuente RSS para suscripción* es un vínculo preconfigurado empleado por los servidores proxy de suscripción en línea durante el proceso de recuperación de actualizaciones de suscripción. Esta URL es para el servidor de suscripciones de CA.

URL para CA Embedded Entitlements Manager

La *URL para CA Embedded Entitlements Manager* (CA EEM) es: https://<ip_address>:5250/spin/eiam. Para iniciar sesión, seleccione CAELM como aplicación e introduzca la contraseña asociada al nombre de usuario de EiamAdmin.

URL para CA Enterprise Log Manager

La *URL para CA Enterprise Log Manager* es: https://<ip_address>:5250/spin/calm. Para iniciar sesión, introduzca el nombre de usuario definido en su cuenta por el administrador y la contraseña correspondiente. También puede introducir EiamAdmin, el nombre de superusuario predefinido, con la contraseña correspondiente.

usuario de EEM

El *usuario de EEM*, configurado en la sección de almacenamiento automático del sistema de almacenamiento de registro de eventos, especifica el usuario que puede realizar una consulta de archivo, recatalogar la base de datos de archivo, ejecutar la utilidad LMArchive y ejecutar el script shell restore-ca-elm para restaurar bases de datos almacenadas para su examen. A este usuario se le debe asignar la función predeterminada de administrador o una función personalizada asociada a una política personalizada que permita la acción de edición en un recurso de la base de datos.

usuario de la aplicación

Un *usuario de la aplicación* es un usuario global al que se han asignado detalles en el ámbito de la aplicación. Los detalles del usuario de la aplicación de CA Enterprise Log Manager incluyen el grupo de usuarios y cualquier restricción del acceso. Si el almacén de usuarios es el repositorio local, los detalles del usuario de la aplicación también incluyen las credenciales de inicio de sesión y las políticas de contraseñas.

usuario global

Un *usuario global* es la información de cuenta de usuario que excluye los detalles específicos de la aplicación. Los detalles de usuarios globales y las pertenencias a grupos globales se comparten en todas las aplicaciones de CA que se integran en el almacén de usuarios predeterminado. Los detalles de usuarios globales se pueden almacenar en el repositorio o en un directorio externo.

utilidad LMArchive

La *utilidad LMArchive* es la utilidad de línea de comandos que realiza el seguimiento de la copia de seguridad y la restauración de bases de datos de archivo en el sistema de almacenamiento de registro de eventos de un servidor de CA Enterprise Log Manager. Utilice LMArchive para realizar consultas de la lista de archivos de bases de datos tibias que están listos para su almacenamiento. Tras realizar una copia de seguridad de la base de datos listada y trasladarla al almacenamiento a largo plazo (frío), utilice LMArchive para crear un registro en el servidor de CA Enterprise Log Manager en el que se realizó la copia de seguridad de dicha base de datos. Tras restaurar la base de datos fría en su servidor de CA Enterprise Log Manager original, utilice LMArchive para notificar a CA Enterprise Log Manager, quien, a su vez, cambia el estado de los archivos de la base de datos a estado descongelado para que se puedan emplear en las consultas.

utilidad LMSEOSImport

La utilidad *LMSEOSImport* es una utilidad de línea de comandos empleada para importar SEOSDATA, o eventos existentes, en el servidor de CA Enterprise Log Manager como parte de la migración de Audit Reporter, Viewer o Audit Collector. Esta utilidad sólo es compatible con Microsoft Windows y Sun Solaris Sparc.

utilidad scp

La copia segura *scp* (programa de copia de archivos remota) es una utilidad de UNIX que transfiere archivos entre equipos de UNIX de una red. Esta utilidad está disponible al realizar la instalación de CA Enterprise Log Manager con el objetivo de emplearla para transferir archivos de actualización del proxy de suscripción en línea al proxy de suscripción sin conexión.

valores de clave

Los *valores de clave* son valores definidos por el usuario y asignados a una lista definida por el usuario (grupo de claves). Cuando una consulta emplea un grupo de claves, los resultados de la búsqueda incluyen las coincidencias con cualquiera de los valores de clave del grupo de claves. Existen varios grupos de claves predefinidos; algunos de ellos incluyen valores de clave predefinidos que se emplean en las consultas y los informes predefinidos.

Índice