CA Enterprise Log Manager

Notas de la versión

r12.1 SP1

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
- CA Security Command Center (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:

- Actualización mediante suscripción: este tema existente se ha modificado para agregar información específica para CA Enterprise Log Manager r12.1 SP1. Utilice la suscripción para obtener este Service Pack, y actualizar CA Enterprise Log Manager para que sea compatible con el estándar FIPS.
- Funciones nuevas y modificadas en r12.1 SP1: este capítulo describe la compatibilidad con FIPS para CA Enterprise Log Manager, el cifrado que se utiliza, las limitaciones y las modificaciones de configuración necesarias para acceder a la interfaz de usuario desde Microsoft Internet Explorer o desde Mozilla Firefox. También incluye información acerca de cómo utilizar la imagen ISO para nuevas implementaciones y de cómo agregar un nuevo servidor de CA Enterprise Log Manager a una implementación existente.
- Si se cambia la hora en el sistema en el servidor de CA EEM se produce un error de incompatibilidad del certificado: este tema existente se ha modificado para reflejar la nueva extensión de los archivos de certificado.
- Requisitos previos de configuración de energía para determinados equipos HP e IBM: este nuevo capítulo describe los cambios en los requisitos previos de configuración de energía predeterminada en los servidores HP Proliant DL 380G5 Series y IBM X3650 Series.
- Puesto que ya se han arreglado o ya no suponen un problema en esta actualización, se han eliminados los problemas conocidos siguientes:
  - Se produce un error al ejecutar los agentes con certificados personalizados.
  - El distribuidor de Syslog secundario no se puede ejecutar durante la carga
  - Los eventos del mismo host se pueden mostrar con nombres de host de destino diferentes
  - Limitación en las especificaciones del informe en PDF
  - No se puede iniciar sesión en CA Enterprise Log Manager después de una actualización
  - La actualización directa a r12.1 M10 causa la visualización incorrecta de la versión del sensor
  - El error Audit Policy Manager Not Installed es incorrecto
  - Actualización a CA Audit necesaria para la interacción con CA Enterprise Log Manager

Más información:

Actualización mediante suscripción (en la página 11)
Funciones nuevas y modificadas en r12.1 SP1 (en la página 35)
Descripción general del cumplimiento de FIPS 140-2 (en la página 35)
Modos operativos (en la página 36)
Bibliotecas de cifrado (en la página 36)
Algoritmos utilizados (en la página 37)
Acerca de los certificados y los archivos clave (en la página 38)
Limitaciones de la compatibilidad con FIPS (en la página 39)
Configuración de Microsoft Internet Explorer para acceder a CA Enterprise Log Manager en modo FIPS. (en la página 41)
Configuración de Mozilla Firefox para acceder a CA Enterprise Log Manager en modo FIPS (en la página 41)

Contenido

Capítulo 1: Introducción 11

Actualización mediante suscripción 11

Capítulo 2: Entorno operativo 13

Entornos de hardware y software 13
Requisitos previos de configuración de energía para determinados equipos HP e IBM 15
Resolución del monitor 15
CA EEM Referencias del servidor 16

Capítulo 3: Características 17

Recopilación de registros 17
Almacenamiento de registros 20
Presentación estandarizada de los registros 22
Generación de informes de cumplimiento 23
Generación de alertas de infracción de política 25
Acceso basado en roles 26
Gestión de suscripciones 27
Compatibilidad con direcciones IPv6 28

Capítulo 4: Funciones nuevas y modificadas en r12.1 31

Cómo abrir el acceso a las API 31
Alertas procesables: integración de CA IT PAM 32
Alertas procesables: integración de SNMP en los productos NSM 32
Acceso a ODBC y JDBC 33
Relevancia de identidades y activos: integración de CA IT PAM 33
Recopilación directa extendida de registros mediante el agente predeterminado 34
Programaciones de actualizaciones automatizadas para los clientes de la suscripción 34

Capítulo 5: Funciones nuevas y modificadas en r12.1 SP1 35

Descripción general del cumplimiento de FIPS 140-2 35
Modos operativos 36
Bibliotecas de cifrado 36
    Algoritmos utilizados 37
Acerca de los certificados y los archivos clave 38
Limitaciones de la compatibilidad con FIPS 39

Configuración de Microsoft Internet Explorer para acceder a CA Enterprise Log Manager en modo FIPS. 41
Configuración de Mozilla Firefox para acceder a CA Enterprise Log Manager en modo FIPS 41
Imagen ISO para nuevas instalaciones 43

Capítulo 6: Problemas conocidos 45

Agentes y adaptadores de CA 45
Dependencias de la instalación del agente en Red Hat Linux 4 45
La precisión del tiempo en el estado del agente depende de la configuración de servidor NTP 46
Espere un tiempo para la actualización tras la implementación de conector masivo 46
La implementación del conector masivo con la dirección IPv6 no es correcta 46
El nombre de montaje del DVD no puede contener espacios 47
Error en la configuración de origen de evento en el nivel de dominio 48
La activación de la comunicación SSL retrasa ODBC/JDBC 49
Las integraciones de File Log Sensor 4.0.0.0 no son compatibles con SUSE Linux 49
Limitación en la configuración del puerto 49
El rendimiento puede disminuir al seleccionar demasiadas integraciones 50
La eliminación de un servidor de la federación no elimina el agente predeterminado 50
Los informes de datos recopilados desde el recopilador de SAPI de CA no muestran los eventos correctamente 50
La entrega de syslog en UDP no está garantizada 51
Servicios de syslog un conflicto de UNIX 52
El sensor de registro de WMI genera varios eventos de privilegios de usuario 52
Detención de la recepción de eventos por parte del sensor de registro de archivos de texto que se ejecuta en un sistema de agente de Solaris 53
Capacidad de respuesta nula del agente a causa de un flujo de eventos demasiado elevado . . . 54
Dispositivo (no - interfaz de usuario) 54
No se puede iniciar sesión en el servidor de CA Enterprise Log Manager con el nombre de usuario EiamAdmin 55
Número excesivo de archivos de registro de ELMAdapter 56
Al importar manualmente archivos de análisis puede ser necesario modificar el valor del tiempo de espera 57
Refinamiento de eventos 58
El bloqueo de la asignación de cadenas y valores numéricos requiere operadores diferentes 58
La asignación de datos personalizada no puede asignar los eventos de epSIM (iTech) 59
Consultas e informes 59
Los resultados de consultas de alertas de acciones pueden estar incompletos 60
Limitación en las consultas con las búsquedas de varios términos 60
El filtro simple del asistente de consultas produce un error al usar caracteres especiales 61
Después de la actualización no se muestra el estado de la tarea programada 61

Algunos trabajos de alerta de acción dan error cuando se programan con demasiada frecuencia 62
No se pueden borrar las etiquetas que contengan caracteres especiales 63
Suscripción 63
Reiniciar automáticamente tras la actualización del SO durante la actualización del SP 63
Error de falta de memoria en equipos con poca memoria 63
Los cambios en las credenciales del proxy provocan el bloqueo de la cuenta del dominio 64
El autocontrol de eventos para reiniciar sólo aparece una vez 65
Reselección de los módulos de suscripción tras su actualización 66
El botón Probar proxy devuelve un falso positivo tras realizar el cambio de configuración 67
Dos reglas de supresión no se aplican correctamente 67
Es necesario reiniciar iGateway para actualizar a r12.1 68
La actualización a r12.1 SP1 requiere el reinicio de iGateway 69
El sensor de registros de syslog actualizado en r12.1 SP1 requiere la actualización a integraciones para los agentes para Windows 70
Gestión de usuarios y accesos 70
Limitaciones de acceso desde un explorador en Windows Vista 70
Limitación del uso del calendario con las políticas de acceso 71
Opciones varias 72
CA Enterprise Log Manager no responde a veces 72
Error de las llamadas de consulta o informe a API en ciertos exploradores 73
Fin de la compatibilidad de CAELM4Audit 73
Impacto del nombre de aplicación personalizado en las consultas de archivos 74
Monitor con configuración de alto contraste 74
iGateway está continuamente deteniéndose y reiniciándose 74
El espacio en disco máximo para CA Enterprise Log Manager virtual no es suficiente 75
Al actualizar el explorador se cierra la sesión de usuario de CA Enterprise Log Manager 76
Posible error en la interfaz del explorador o del servicio tras el reinicio de iGateway 76
Cargas e importaciones incorrectas con exploradores distintos al explorador de Internet Microsoft Internet Explorer 77
La interfaz de usuario no puede mostrarse inesperadamente al realizar la instalación con EEM remoto 78

Capítulo 7: Problemas arreglados 81

Problemas arreglados en la versión r12.1 SP1 81

Capítulo 8: Documentación 83

Biblioteca 83
Acceso a la biblioteca 84

Apéndice A: Agradecimientos a terceros 85

Adaptive Communication Environment (ACE) 86
Software bajo la Licencia de Apache 88
boost 1.35.0 92
JDOM 1.0 93
PCRE 6.3 95
Zlib 1.2.3 97
ZThread 2.3.2 97

Capítulo 1: Introducción

Bienvenido a CA Enterprise Log Manager. Este documento contiene información sobre la compatibilidad con sistemas operativos, mejoras, incidencias conocidas e información de contacto con el Soporte técnico de CA.

Actualización mediante suscripción

Actualice CA Enterprise Log Manager a la última versión o service pack descargando todos los módulos entregados por suscripción.

Importante: Actualice el servidor de CA Enterprise Log Manager de gestión antes de instalar cualquier servidor nuevo de CA Enterprise Log Manager en la red. Este método permite registrar los servidores correctamente.

Siga los siguientes pasos:

1. Revise la configuración de suscripción para verificar que se ha completado la configuración básica.
   a. Haga clic en la ficha Administración, subficha Servicios y seleccione el módulo suscripción.
   b. Seleccionar No en la opción Reiniciar automáticamente tras la actualización del SO.
   c. Desplace el módulo gestor de registros a la lista seleccionada en caso de que no aparezca seleccionado.
   d. Compruebe que todos los valores requeridos estén configurados en el nivel global.
   e. Compruebe cada servidor de CA Enterprise Log Manager tiene todos los valores requeridos configurados.

   Nota: En entornos federados, actualice los elementos principales antes de actualizar los elementos secundarios.

   Un evento autocontrolado manifestando que las actualizaciones de suscripción se han instalado indica que se ha completado.

2. Revise la configuración de suscripción para verificar que se ha completado la configuración básica.
   a. Haga clic en la ficha Administración, subficha Servicios y seleccione el módulo suscripción.
   b. Seleccionar No en la opción Reiniciar automáticamente tras la actualización del SO.
   c. Desplace el resto de módulos para descargar a la lista de selección.

   Nota: En entornos federados, actualice los elementos principales antes de actualizar los elementos secundarios.
3. Cuando el proceso de actualización de la suscripción finalice, reinicie todos los servidores de CA Enterprise Log Manager.

   Un evento autocontrolado manifestando que las actualizaciones de suscripción se han instalado indica que se ha completado.
4. Actualice los agentes y conectores de la manera siguiente:
   a. Haga clic en la ficha Administración, subficha Recopilación de registros, y seleccione el Explorador de agente.
   b. Determine si desea aplicar las actualizaciones de la suscripción a nivel del explorador de agente, a nivel del grupo de agentes o a nivel de agente.
   c. Seleccione el nivel deseado y haga clic en el botón Suscripción.
   d. Aplique las actualizaciones a los agentes si ha descargado el módulo Agentes.
   e. Haga clic en el botón Suscripción otra vez.
   f. Aplique actualizaciones a los conectores, cuando estén disponibles.
5. Vuelva a registrar los productos de terceros y otros productos de CA, como CA Access Control, que muestra los informes de CA Enterprise Log Manager en las interfaces nativas mediante las llamadas Open-API.

   Con este paso se actualizan los certificados que cambiaron en esta versión. Para obtener más información, consulte la *Guía de programación de la API de CA Enterprise Log Manager*.

Nota: Consulte las Notas de la versión para cualquier problema conocido relacionado con la actualización de suscripciones.

Más información:

Reiniciar automáticamente tras la actualización del SO durante la actualización del SP (en la página 63)
El sensor de registros de syslog actualizado en r12.1 SP1 requiere la actualización a integraciones para los agentes para Windows (en la página 70)

Capítulo 2: Entorno operativo

Esta sección contiene los siguientes temas:

Entornos de hardware y software (en la página 13)
Requisitos previos de configuración de energía para determinados equipos HP e IBM (en la página 15)
Resolución del monitor (en la página 15)
CA EEM Referencias del servidor (en la página 16)

Entornos de hardware y software

CA Enterprise Log Manager instala el sistema operativo Red Hat Enterprise Linux como parte de la configuración inicial.

El índice de matrices de certificación de CA Enterprise Log Manager muestra las lista de los vínculos para todas las matrices de certificación de CA Enterprise Log Manager, incluyendo las siguientes:

- Hardware y software del servidor

  Matriz de certificación de hardware y software del servidor de CA Enterprise Log Manager

- Hardware y software del agente

  Matriz de certificación de hardware y software del agente para CA Enterprise Log Manager

- Sensores de registro y compatibilidad del sistema operativo relacionado

  Matriz de certificación del sensor de registros de CA Enterprise Log Manager

- Integraciones del producto

  Matriz de certificación de la integración del producto CA Enterprise Log Manager

- Certificaciones con CA Audit iRecorders

  Matriz de certificación de CA Audit iRecorder para CA Enterprise Log Manager

Puede acceder a CA Enterprise Log Manager con los siguientes navegadores y Adobe Flash Player 9 o 10:

- Internet Explorer 6 SP2 (sólo modo no FIPS)
- Internet Explorer 7 o 8 (modos FIPS o no FIPS)
- Mozilla Firefox 2.0.x y 3.0.x (sólo modo no FIPS)
- Mozilla Firefox 3.5.8 o superior (modos FIPS y no FIPS)

Nota: Las exportaciones de archivo no funcionan cuando se accede a CA Enterprise Log Manager con un explorador Mozilla Firefox.

Requisitos previos de configuración de energía para determinados equipos HP e IBM

Cuando se instala CA Enterprise Log Manager en servidores HP Proliant DL 380G5 Series e IBM X3650 Series con la configuración predeterminada de consumo de energía, se pueden producir problemas con iGateway. Ello puede causar lentitud en el funcionamiento u otros problemas con la interfaz que podrían requerir un reinicio manual del servicio.

Para evitar este problema potencial, modifique la configuración predeterminada antes de instalar CA Enterprise Log Manager.

Nota: Si ya ha instalado CA Enterprise Log Manager, puede detener el equipo, modificar la configuración de la forma indicada a continuación y reiniciar el equipo.

Para modificar la configuración de consumo de energía de equipos HP Proliant DL 380G5

1. Acceda al menú de configuración de BIOS.
2. Acceda a la configuración de consumo de energía.
3. Seleccione OS Control Mode de entre las opciones disponibles.

   Nota: El valor de configuración predeterminado es HP Dynamic Power Settings Mode.

Para modificar la configuración de consumo de energía de equipos IBM X3650

1. Acceda al menú de configuración de BIOS.
2. Acceda a la configuración de consumo de energía.
3. Desactive los parámetros siguientes:
   - Active Energy Manager
   - Enhanced C1 Power State

Resolución del monitor

La resolución mínima del monitor es 1024 x 768 pixels. Se recomienda la resolución 1280 x 1024.

CA EEM Referencias del servidor

Para obtener información sobre la compatibilidad del sistema operativo con un servidor de CA EEM existente, consulte la *Guía de procedimientos iniciales de CA Embedded Entitlements Manager*. Esta guía está incluida en la biblioteca de CA Enterprise Log Manager.

También puede descargar esta biblioteca desde el sitio de Soporte técnico. Para obtener ayuda, póngase en contacto con el Soporte técnico en el sitio Web http://www.ca.com/worldwide/.

Capítulo 3: Características

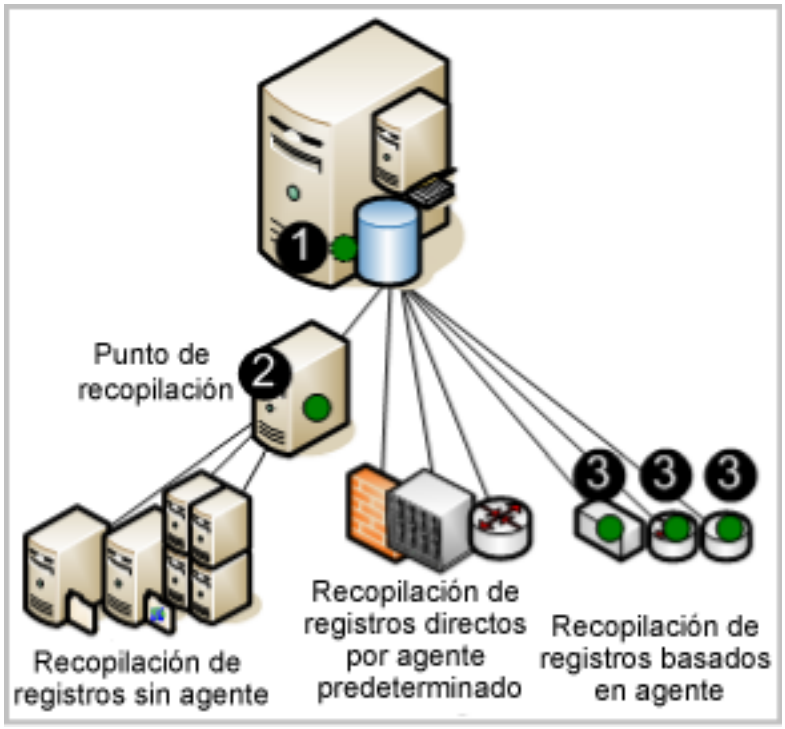
Esta sección contiene los siguientes temas:

Recopilación de registros (en la página 17)
Almacenamiento de registros (en la página 20)
Presentación estandarizada de los registros (en la página 22)
Generación de informes de cumplimiento (en la página 23)
Generación de alertas de infracción de política (en la página 25)
Acceso basado en roles (en la página 26)
Gestión de suscripciones (en la página 27)
Compatibilidad con direcciones IPv6 (en la página 28)

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

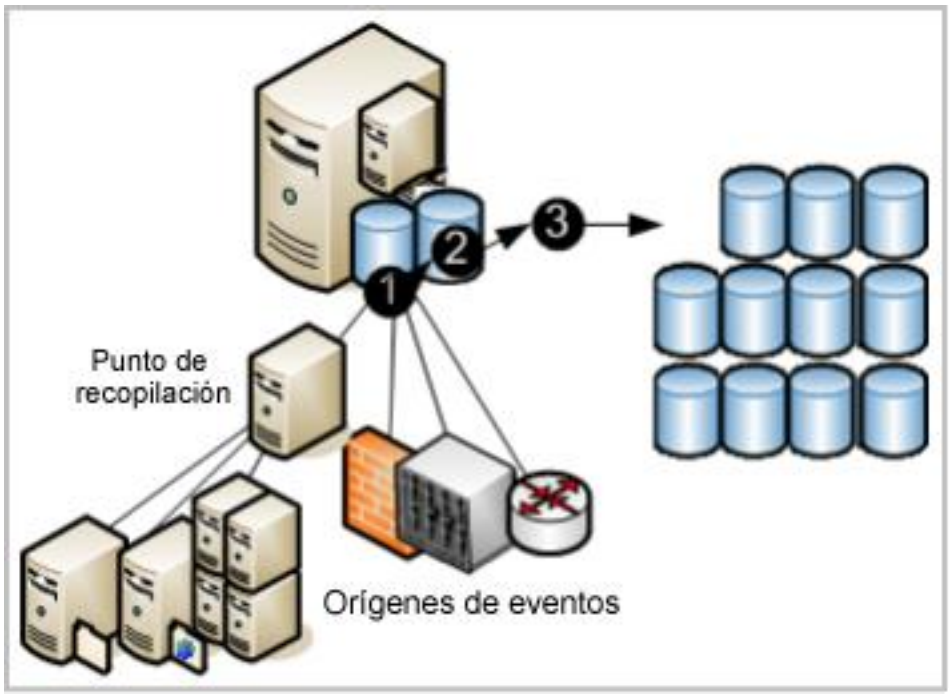
  Con la recopilación basada en el agente, se instala un agente donde un o más orígenes de eventos se ejecutan y donde se configura un conector para cada origen de evento.

  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.

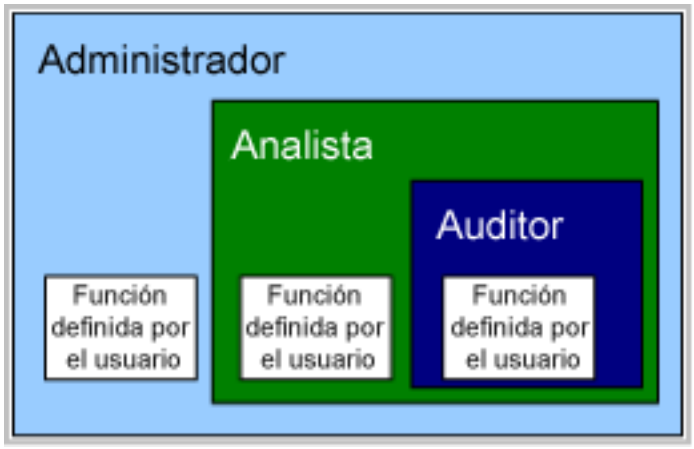
Nota: Consulte la *Guía de administración de CA Enterprise Log Manager* para obtener detalles sobre las alertas de acción.

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.



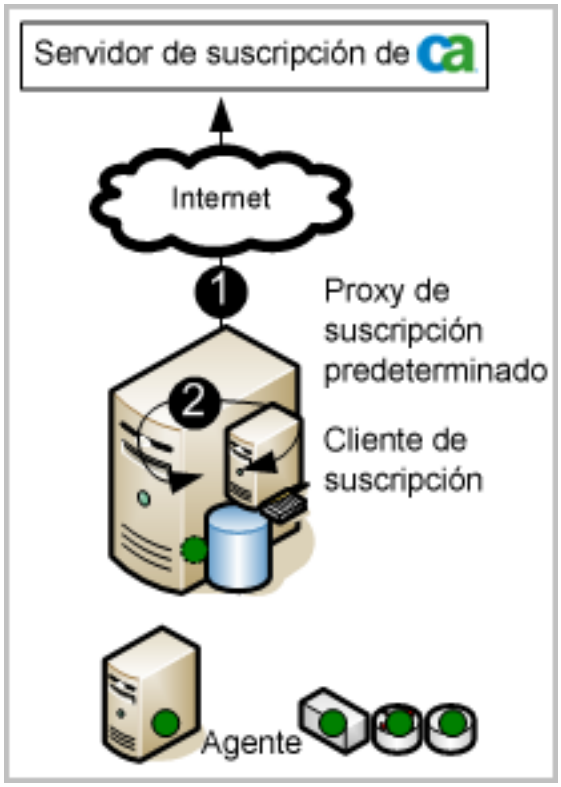
Los Administrators pueden personalizar el acceso a cualquier recurso mediante la creación de un grupo de aplicaciones personalizado con políticas asociadas y a través de la asignación de dicho grupo de aplicaciones, o rol, a las cuentas de usuario.

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.

Compatibilidad con direcciones IPv6

Anteriormente, la especificación de direcciones IP se limitaba a la notación decimal separada por puntos IPv4. Con la versión actual, se pueden especificar direcciones IPv6 en cualquier campo de IP. IPv6 utiliza direcciones IP de 128 bit en lugar de las direcciones de 32 bit utilizadas por IPv4. Todas las políticas basadas en la versión de dirección IP admiten IPv6 e IPv4.

Puede utilizar direcciones IPv6 con direcciones IPv4 asignadas o el formato IPv6 tradicional. El formato de dirección IPv6 asignada a IPv4 permite que la dirección IPv4 de un nodo IPv4 se represente como una dirección IPv6.

- El formato preferido de IPv6 se escribe como ocho grupos de cuatro dígitos hexadecimales (x:x:x:x:x:x:x:x). Cada x representa de uno a cuatro dígitos hexadecimales de las ocho partes de 16 bits de la dirección.
- La dirección IPv6 asignada a IPv4, que resulta muy cómoda en un entorno mixto de nodos IPv4 y IPv6 es 0:0:0:0:0:FFFF:d.d.d.d, donde cada d es un valor decimal de la dirección (notación decimal separada por puntos IPv4).

  Importante: Direcciones IPv6 compatibles con IPv4 en el formato 0:0:0:0:0:0:d.d.d.d ahora no están permitidas, de acuerdo con las recomendaciones del RFC 4291, porque los mecanismos de transición de IPv6 actuales no utilizan estas direcciones.

Dirección IPv6 válida escrita en formato tradicional:

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

Si uno o más grupos de cuatro dígitos es 0000, los ceros se pueden omitir y reemplazarse por dos puntos repetidos (::). Los ceros líderes de un grupo también se pueden omitir. Ejemplos de direcciones IP equivalentes:

- 2001:0db8:0000:0000:0000:0000:1428:57ab
- 2001:0db8::1428:57ab
- 2001:db8:0:0:0:0:1428:57ab
- 2001:db8::1428:57ab

Si reemplaza direcciones IPv4 con direcciones IPv4 asignadas, siga los siguientes ejemplos como modelo:

- 0:0:0:0:0:FFFF:192.168.2.128
- 0:0:0:0:0:FFFF:172.16.2.128

También puede utilizar las formas comprimidas:

- ::FFFF:192.168.2.128
- ::FFFF:172.16.2.128

Capítulo 4: Funciones nuevas y modificadas en r12.1

Esta sección contiene los siguientes temas:

Cómo abrir el acceso a las API (en la página 31)
Alertas procesables: integración de CA IT PAM (en la página 32)
Alertas procesables: integración de SNMP en los productos NSM (en la página 32)
Acceso a ODBC y JDBC (en la página 33)
Relevancia de identidades y activos: integración de CA IT PAM (en la página 33)
Recopilación directa extendida de registros mediante el agente predeterminado (en la página 34)
Programaciones de actualizaciones automatizadas para los clientes de la suscripción (en la página 34)

Cómo abrir el acceso a las API

CA Enterprise Log Manager permite utilizar llamadas a la API para acceder a los datos del repositorio de eventos mediante el uso del mecanismo de consulta e informe, y mostrarlos en un explorador Web. También puede usar la API para incrustar consultas o informes de CA Enterprise Log Manager en una interfaz de CA o de un producto de terceros.

Entre las funciones de la API de CA Enterprise Log Manager se incluyen las siguientes:

- API autenticadas y seguras
- Registro de productos para inicio de sesión único (SSO
- Recuperación de listas de consultas o informes con opción de filtrado basada en etiquetas
- Visualización de consultas o informes en la interfaz interactiva de CA Enterprise Log Manager, lo que permite el filtrado y la inserción en una interfaz de usuario

Puede encontrar más información acerca de la API en la *Guía de programación de API* y en la ayuda en línea.

Alertas procesables: integración de CA IT PAM

A través de alertas programadas que consultan volúmenes de registros, CA Enterprise Log Manager detecta posibles infracciones de control y actividad sospechosa de TI. CA Enterprise Log Manager notifica al personal de seguridad de TI quien investiga cada alerta para determinar si se necesita alguna acción para solucionar el problema. Con frecuencia las actividades de investigación son rutinarias e idóneas para automatización. Gracias a una estrecha integración entre CA Enterprise Log Manager y CA IT PAM, estas acciones de respuesta rutinarias se pueden llevar a cabo automáticamente. El personal de seguridad de TI no tiene que realizar tareas repetitivas y se puede centrar exclusivamente en las incidencias más importantes.

La integración de CA IT PAM permite crear solicitudes en CA Service Desk mediante la ejecución de un proceso de salida de eventos/alertas predefinidos de CA IT PAM a partir de las alertas. También puede ejecutar procesos de salida de eventos/alertas personalizados de IT PAM a partir de CA Enterprise Log Manager para automatizar otras respuestas a los eventos sospechosos.

Para obtener detalles, consulte la sección "Working with CA IT PAM Event/Alert Processes" del capítulo Alertas de acción de la *Guía de administración* de CA Enterprise Log Manager.

Alertas procesables: integración de SNMP en los productos NSM

Cuando las consultas programadas recuperan eventos que indican una actividad sospechosa se generan alertas. El envío de estas alertas se puede automatizar como capturas SNMP a los productos de control de seguridad de la red (NSM), como CA Spectrum o CA NSM. Los productos de destino se preparan para recibir e interpretar las capturas SNMP de CA Enterprise Log Manager, se configuran las ubicaciones de destino y, a continuación, se especifica la información del evento que se va a enviar.

Para obtener detalles, consulte la sección "Trabajo con capturas SNMP" en el capítulo Alertas de accesión de la *Guía de administración* de CA Enterprise Log Manager.

Acceso a ODBC y JDBC

CA Enterprise Log Manager permite acceso de sólo lectura para recopilar información de registro de eventos mediante el uso de ODBC y JDBC. Puede utilizar este acceso para realizar operaciones como las siguientes:

- Crear informes de cliente con herramientas, como informes Crystal de Business Objects
- Recuperar información de registro seleccionada para utilizarla con un motor de correlación
- Examinar registros para intrusión o detección de software maligno

Las funciones de acceso a ODBC y JDBC utilizan un cliente que se instala en un servidor apropiado de la red. El servidor de CA Enterprise Log Manager instala automáticamente los componentes del servidor durante la actualización de la suscripción y el proceso de instalación.

En la *Guía de implementación* puede encontrar información de la instalación. En la *Guía de administración* puede encontrar información y ejemplos de la configuración.

Relevancia de identidades y activos: integración de CA IT PAM

La integración de CA IT PAM permite mantener valores actualizados para una clave determinada mediante la ejecución de un proceso de valores dinámicos de CA IT PAM. Un proceso de valores dinámicos es aquel que recupera los valores actuales de los repositorios en los que se almacenan los datos actuales. Si crea un proceso que recupere valores de los activos críticos de su archivo o base de datos de activos, podrá actualizar la clave Critical_Assets en las consultas y los informes predefinidos con sólo hacer clic en un botón.

Para obtener detalles, consulte la sección "Enabling Dynamic Values Import" del capítulo Consultas e informes de la *Guía de administración* de CA Enterprise Log Manager.

Recopilación directa extendida de registros mediante el agente predeterminado

Al instalar CA Enterprise Log Manager, la escucha de Syslog, denominada Syslog_Connector, se implementa en el agente predeterminado para activar la recopilación de eventos de syslog. La integración de Linux_localsyslog con el conector asociado, Linux_localsyslog_Connector, también está disponible para recopilar eventos de syslog.

Ahora, el agente predeterminado puede recopilar directamente algo más que eventos de syslog. Mediante el uso del conector WinRm, el agente predeterminado puede recopilar eventos de productos que se ejecuten en plataformas Microsoft Windows como, por ejemplo, Servicios de certificados de Active Directory y Microsoft Office Communication Server. Con el conector ODBC, el agente predeterminado recopila eventos de varias bases de datos como, por ejemplo, Oracle9i y SQL Server 2005, así como de las aplicaciones que almacenan sus eventos en estas bases de datos.

Programaciones de actualizaciones automatizadas para los clientes de la suscripción

Al instalar su primer servidor de CA Enterprise Log Manager, configure los valores globales para todos los servicios, incluida la suscripción. Para la suscripción, el primer servidor que se instala es el proxy de suscripción predeterminado. Configure la hora de inicio de la actualización y la frecuencia con la que el proxy comprueba si existen actualizaciones en el servidor de suscripción de CA. Al instalar más servidores, lo harán como clientes de suscripción de forma predeterminada. Si configura servidores adicionales, hágalo a nivel local. La configuración a nivel local se realiza mediante la selección del nombre del servidor para configurar y, a continuación, omitir las configuraciones globales seleccionadas.

De forma predeterminada, la hora de inicio de la actualización de los clientes de la suscripción se hereda de la configuración global. Cuando la configuración heredada no se omite manualmente para forzar un retraso, pueden producirse problemas. Para evitar este problema, se ha automatizado la programación de actualización para clientes ahora con un retraso de 15 minutos. Ya no es necesario llevar a cabo la configuración manual de la programación de actualización para los clientes de suscripción.

Capítulo 5: Funciones nuevas y modificadas en r12.1 SP1

Esta sección contiene los siguientes temas:

Descripción general del cumplimiento de FIPS 140-2 (en la página 35)
Modos operativos (en la página 36)
Bibliotecas de cifrado (en la página 36)
Acerca de los certificados y los archivos clave (en la página 38)
Limitaciones de la compatibilidad con FIPS (en la página 39)
Configuración de Microsoft Internet Explorer para acceder a CA Enterprise Log Manager en modo FIPS. (en la página 41)
Configuración de Mozilla Firefox para acceder a CA Enterprise Log Manager en modo FIPS (en la página 41)
Imagen ISO para nuevas instalaciones (en la página 43)

Descripción general del cumplimiento de FIPS 140-2

La publicación de los Estándares Federales de Procesamiento de la Información (FIPS) 140-2 es un estándar de seguridad para las bibliotecas criptográficas y los algoritmos que debería utilizar un producto para el cifrado. El cifrado FIPS 140-2 afecta la comunicación de todos los datos sensibles entre componentes de productos de CA, y entre productos de CA y productos de terceros. FIPS 140-2 especifica los requisitos para utilizar algoritmos criptográficos dentro de un sistema de seguridad que protege datos sensibles y sin clasificar.

CA Enterprise Log Manager ofrece compatibilidad con FIPS en el tráfico de eventos. Éste se asegura mediante algoritmos que cumplen con el estándar FIPS cuando operan en modo FIPS. CA Enterprise Log Manager también ofrece un modo no FIPS predeterminado en el que el tráfico de eventos *no* se asegura con algoritmos que cumplan con FIPS. Los servidores de CA Enterprise Log Manager en una red federada no pueden mezclar los dos modos operativos. Esto significa que un servidor que funciona en el modo no FIPS no puede compartir datos de consulta e informe con un servidor que está ejecutándose en modo FIPS.

En la sección sobre instalación de CA Enterprise Log Manager *Guía de implementación* encontrará información acerca de la activación y desactivación del modo FIPS.

Más información:

Modos operativos (en la página 36)
Bibliotecas de cifrado (en la página 36)
Algoritmos utilizados (en la página 37)
Acerca de los certificados y los archivos clave (en la página 38)
Limitaciones de la compatibilidad con FIPS (en la página 39)
Configuración de Microsoft Internet Explorer para acceder a CA Enterprise Log Manager en modo FIPS. (en la página 41)
Configuración de Mozilla Firefox para acceder a CA Enterprise Log Manager en modo FIPS (en la página 41)

Modos operativos

CA Enterprise Log Manager puede hacer operar en dos modos, modo FIPS o no FIPS. Los límites criptográficos son los mismos en los dos modos, pero los algoritmos difieren. De forma predeterminada, los servidores de CA Enterprise Log Manager operan en el modo no FIPS. Los usuarios con el rol Administrador pueden activar el modo operativo FIPS.

modo no FIPS

Este modo utiliza una mezcla de algoritmos de cifrado para el transporte de eventos y otras comunicaciones entre los servidores de CA Enterprise Log Manager y CA EEM que no necesariamente deben cumplir con los estándares FIPS 140-2.

modo FIPS

Este modo utiliza algoritmos de cifrado certificados por FIPS para el transporte de eventos y otras comunicaciones entre los servidores de CA Enterprise Log Manager y CA EEM.

Los usuarios de nivel Administrador pueden revisar los modos operativos del agente desde el nodo Explorador de agente que se encuentra en la subficha Recopilación de registros de la ficha Administración.

Para obtener más información acerca del cambio entre modo FIPS y no FIPS, consulte Tareas de estado del sistema en la Ayuda en línea, o la sección acerca de la configuración de servicios de la *Guía de implementación*.

Bibliotecas de cifrado

La publicación de los Estándares Federales de Procesamiento de la Información (FIPS) 140-2 especifica los requisitos para el uso de algoritmos criptográficos dentro de un sistema de seguridad que protege datos sensibles y sin clasificar.

CA Enterprise Log Manager también inserta la biblioteca criptográfica de Crypto-C Micro Edition (ME) v2.1.0.2 de RSA, que se ha comprobado que cumple con los *requisitos de seguridad para módulos de criptográficos de FIPS* 140-2. El número de certificado de validación para este módulo es 865.

Algoritmos utilizados

Los productos del equipo que utilizan módulos de criptográficos certificados por FIPS 140-2 en modo FIPS sólo pueden utilizar funciones de seguridad aprobadas por FIPS. Éstas incluyen AES (Estándar de cifrado avanzado), SHA-1 (Algoritmo hash seguro), y protocolos de niveles más altos como TLS v1.0, explícitamente permitido en los estándares FIPS 140-2 y guías de implementación.

En modo no FIPS, CA Enterprise Log Manager utiliza los algoritmos siguientes:

- AES 128
- Triple DES (3DES)
- SHA-1
- MD5
- SSL v3

En modo FIPS, CA Enterprise Log Manager utiliza los algoritmos siguientes:

- AES 128
- Triple DES (3DES)
- SHA-1
- TLS v1

CA Enterprise Log Manager utiliza SHA-1 como el algoritmo de certificación predeterminado para cifrar las contraseñas y firmar las solicitudes del servidor.

CA Enterprise Log Manager utiliza TLS v1.0 para comunicarse con directorios de LDAP externos siempre que la conexión de LDAP utilice TLS, las comunicaciones entre componentes de iTechnology, la comunicación del agente con el servicio de iGateway en modo FIPS, y el canal de eventos entre un agente y el servicio logDepot.

Acerca de los certificados y los archivos clave

A fin de cumplir con los estándares de FIPS 140-2, la actualización a CA Enterprise Log Manager r12.1 SP1 convierte los certificados en formato P12 existentes a certificados en formato PEM. Esta conversión da lugar a la generación de los archivos siguientes:

- Archivo de certificado con una extensión .cer
- Archivo clave con una extensión .key

Los archivos clave no se cifran, y asegurarlos contra accesos no autorizados tanto en el servidor como en los host de agente dependerá del usuario. La aplicación de software de CA Enterprise Log Manager utiliza diversas técnicas de protección del sistema operativo para proteger las claves y certificados guardados en el sistema de archivos. CA Enterprise Log Manager no es compatible con el uso de dispositivos de almacenamiento clave externos.

CA Enterprise Log Manager utiliza los certificados y los archivos clave siguientes:

Nombre de certificado/archivo clave	Ubicación	Descripción
CAELMCert	/opt/CA/SharedComponents/iTechnology (Se puede referir a este directorio mediante el nombre abreviado de la variable, $IGW_LOC.)	Todos los servicios de CA Enterprise Log Manager utilizan este certificado para comunicaciones entre servidores de CA Enterprise Log Manager, y entre servidores de CA Enterprise Log Manager y el servidor de CA EEM. El archivo de configuración principal, CALMA. cnf, contiene una entrada para este certificado y para el archivo clave correspondiente. Los pares de etiqueta empiezan por <Certificate> y <KeyFile> respectivamente.
CAELM_AgentCert	$IGW_LOC en el servidor host del agente	Los agentes usan este certificado para comunicarse con cualquier servidor de CA Enterprise Log Manager. El servidor de gestión de CA Enterprise Log Manager proporciona este certificado al agente. El certificado es válido para cualquier servidor de CA Enterprise Log Manager dentro de una instancia de aplicación proporcionada.

Nombre de certificado/archivo clave	Ubicación	Descripción
itpamcert	Servidor de CA IT PAM	Este certificado se utiliza para comunicaciones con CA IT PAM. Para obtener más información, consulte la documentación de CA IT PAM.
rootcert	$IGW_LOC	Este certificado es un certificado raíz autofirmado por iGateway durante la instalación.
iPozDsa	$IGW_LOC	El servidor de CA EEM, tanto local como remoto, utiliza este certificado. Si desea obtener más información, consulte la documentación de CA EEM.
iPozRouterDsa	$IGW_LOC	El servidor de CA EEM, tanto local como remoto, utiliza este certificado. Si desea obtener más información, consulte la documentación de CA EEM.
iTechPoz-trusted	/opt/CA/Directory/dxserver/config/ssld	CA Directory utiliza este certificado.
iTechPoz-<hostname>-Router	/opt/CA/Directory/dxserver/config/ssld	CA Directory utiliza este certificado.

Limitaciones de la compatibilidad con FIPS

Las funciones de CA Enterprise Log Manager y las inter operaciones del producto siguientes no son compatibles con las operaciones en modo FIPS:

Acceso de los servicios de ODBC y JDBC al almacén de registro de eventos.

ODBC y JDBC en CA Enterprise Log Manager se basa en un SDK subyacente que no es compatible con las operaciones en modo FIPS. Los administradores de redes federadas que necesitan realizar operaciones en modo FIPS deben desactivar manualmente el servicio ODBC en cada servidor de CA Enterprise Log Manager. Consulte la sección acerca de la desactivación de los accesos de ODBC y JDBC al almacén de registro de eventos de la *Guía de implementación*.

Servidor de CA EEM compartido

CA Enterprise Log Manager r12.1 SP1 utiliza CA EEM r8.4 SP3, que es compatible con FIPS. La activación del modo FIPS en el servidor de CA Enterprise Log Manager desactiva la comunicación entre CA EEM compartido y cualquier producto que no sea compatible con CA EEM r8.4 SP3.

Por ejemplo, CA IT PAM no es compatible con FIPS. Si se actualiza el servidor de CA Enterprise Log Manager al modo FIPS, se producirá un error en la integración con CA IT PAM.

Sólo se puede compartir un servidor de CA EEM entre CA Enterprise Log Manager r12.1 SP1 y CA IT PAM r2.1 SP2 y r2.1 SP3 en modo no FIPS.

Si la instalación de CA IT PAM no comparte el mismo servidor de CA EEM, CA Enterprise Log Manager r12.1 SP1 puede ejecutarse en modo FIPS y puede comunicarse con CA IT PAM. Sin embargo, estos canales de comunicación no son compatibles con FIPS.

El vínculo LDAP necesita modos operativos coincidentes

La comunicación correcta con un almacén de usuarios externo depende de lo siguiente:

- Los servidores de CA Enterprise Log Manager y el servidor de gestión de CA EEM correspondiente deben estar en el mismo modo FIPS
- Cuando se utilice TLS v 1.0 para la conexión, el servidor de CA EEM debe estar ubicado en el mismo modo FIPS que un almacén de usuarios externo habilitado en modo FIPS.

  Nota: Cuando se utilizan comunicaciones no cifradas entre el servidor de CA EEM y el almacén de usuarios externo, o cuando el servidor de CA EEM y el almacén de usuarios se encuentran en modos FIPS diferentes, la compatibilidad con los estándares de FIPS no estará disponible.

Mensajes SNMP

Se pueden enviar eventos de SNMP mediante SNMP V2 o SNMP V3. Ambos son compatibles con el modo no FIPS.

Si el servidor de destino de mensajes SNMP está activado en modo FIPS, en la página Destino del Asistente de programación de alertas de acción se deberá seleccionar Seguridad de V3 y, a continuación, SHA como el protocolo de autenticación y AES como el protocolo de cifrado.

Configuración de Microsoft Internet Explorer para acceder a CA Enterprise Log Manager en modo FIPS.

Cuando se ejecuta el explorador Microsoft Internet Explorer en modo FIPS, es posible que requiera configuración adicional antes de poder mostrar la interfaz de usuario del servidor de CA Enterprise Log Manager. Utilice el procedimiento siguiente para configurar las opciones necesarias de acceso a CA Enterprise Log Manager en Microsoft Internet Explorer 7 o 8.

Nota: No puede utilizarse Microsoft Internet Explorer 6 para acceder a un servidor de CA Enterprise Log Manager que se ejecuta en modo FIPS.

Para configurar Microsoft Internet Explorer 7 o 8

1. Abra el explorador y seleccione las Herramientas, Opciones de internet.
2. Seleccione la ficha Opciones avanzadas y avance por la página hasta la sección Seguridad.
3. Seleccione las siguientes opciones:
   - Usar SSL 2.0
   - Usar SSL 3.0
   - Usar TLS 1.0
4. Haga clic en Aceptar.

Configuración de Mozilla Firefox para acceder a CA Enterprise Log Manager en modo FIPS

Cuando se ejecuta el explorador Mozilla Firefox en modo FIPS, es posible que requiera configuración adicional antes de poder mostrar la interfaz de usuario del servidor de CA Enterprise Log Manager. Utilice el procedimiento siguiente para configurar las opciones necesarias en la Mozilla Firefox 3.5.8 o el explorador posterior para acceder a un servidor de CA Enterprise Log Manager que entra corriendo modo.

Nota: El acceso a CA Enterprise Log Manager requiere la instalación del complemento de Mozilla Firefox para el Adobe Flash 9 o 10.

Para configurar Mozilla Firefox

1. Abra el explorador y seleccione Herramientas, Opciones.
2. Haga clic en la ficha Opciones avanzadas y, a continuación, en la subficha Cifrado.
3. Seleccione las siguientes opciones:
   - Usar SSL 3.0
   - Usar TLS 1.0
4. Seleccione la subficha Seguridad, y a continuación seleccione la opción para utilizar una contraseña maestra.
5. Haga clic en Cambiar contraseña maestra y proporcione una contraseña adecuada cuando aparezca la ventana. A continuación haga clic en Aceptar.
6. Seleccione la subficha Opciones avanzadas.
7. Haga clic en Dispositivos de seguridad.

   Aparecerá la ventana Administrador de dispositivos.
8. Seleccione el módulo interno PKCS #11 de NSS del panel de la izquierda.

   Tras la selección el panel derecho se rellenará automáticamente.
9. Seleccione la línea, módulo interno FIPS PKCS #11 de NSS, y haga clic en Habilitar FIPS.
10. Introduzca la contraseña maestra que creó en un paso anterior, y a continuación haga clic en Aceptar.
11. Haga clic en Aceptar en la ventana Administrador de dispositivos.
12. Haga clic en Aceptar en la ventana Opciones.
13. Reinicie el explorador.

Más información:

Actualización mediante suscripción (en la página 11)

Imagen ISO para nuevas instalaciones

En el Service Pack se proporciona una imagen ISO para ayudar a implementar CA Enterprise Log Manager de manera rápida o para agregar un nuevo servidor de CA Enterprise Log Manager a una implementación existente. La imagen ISO está disponible en el área de descargas de Soporte de CA en línea.

Se recomienda utilizar la imagen ISO más reciente en los casos siguientes:

- Implementación de CA Enterprise Log Manager. La instalación de la última imagen ISO minimiza el número de actualizaciones de suscripción necesarias y acelera su implementación.
- Agregación de un nuevo servidor de CA Enterprise Log Manager tras la actualización de los servidores en la implementación existente. Primero debe comprobarse que los servidores y los agentes de la implementación actual se han actualizado correctamente y que reciben los eventos. A continuación, deben instalarse los nuevos servidores mediante la imagen ISO para agregar más capacidad y minimizar el número de actualizaciones de suscripción para aplicar.

Nota: El procedimiento de instalación ha cambiado. A partir de ahora, se preguntará al usuario si desea proceder con la instalación con el modo FIPS activado. Al agregar un nuevo servidor de CA Enterprise Log Manager a una implementación de FIPS existente (el servidor de gestión de CA Enterprise Log Manager o el servidor de CA EEM remoto se encuentran en el modo FIPS), deberá activarse el modo FIPS durante la instalación. De lo contrario, el nuevo servidor no podrá registrarse y deberá instalarse de nuevo. Para obtener más información acerca del modo FIPS, consulte la *Guía de implementación* .

Capítulo 6: Problemas conocidos

Esta sección contiene los siguientes temas:

Agentes y adaptadores de CA (en la página 45)
Dispositivo (no - interfaz de usuario) (en la página 54)
Refinamiento de eventos (en la página 58)
Consultas e informes (en la página 59)
Suscripción (en la página 63)
Gestión de usuarios y accesos (en la página 70)
Opciones varias (en la página 72)

Agentes y adaptadores de CA

A continuación se presentan los problemas conocidos relacionados con los agentes y los adaptadores de CA.

Dependencias de la instalación del agente en Red Hat Linux 4

Síntoma:

Cuando se instala el agente de CA Enterprise Log Manager en sistemas Red Hat Enterprise Linux 4 se produce un error en la instalación y se muestra un mensaje de error sobre las dependencias requeridas.

Solución:

El agente de CA Enterprise Log Manager en Red Hat Enterprise Linux 4 necesita el paquete Legacy Software Development. Instale el paquete antes de instalar el agente.

La precisión del tiempo en el estado del agente depende de la configuración de servidor NTP

Síntoma:

Si varios servidores de CA Enterprise Log Manager que ejecutan la recopilación se configuran manualmente a distintos relojes, puede ocurrir una discrepancia en el tiempo de la actividad del agente.

Solución:

Cuando instale cada CA Enterprise Log Manager en la red, especifique un servidor NTP. La configuración de un servidor NTP para cada servidor sincroniza el tiempo para los agentes gestionados por distintos servidores.

Espere un tiempo para la actualización tras la implementación de conector masivo

Síntoma:

Los conectores nuevos no aparecen inmediatamente en el Explorador de agente al realizar una implementación de conector masivo.

Solución:

En función de la cantidad de conectores (y agentes que se implementen en éstos), deberá esperar unos minutos para que se actualicen todos los conectores en el Explorador de agente.

La implementación del conector masivo con la dirección IPv6 no es correcta

Síntoma:

La implementación de los conectores del asistente de implementación del conector masivo que proporciona la dirección del servidor en formato IPv6 no funciona de la forma esperada. Tras cierto tiempo, el estado del conector pasa a ser En ejecución. Al editar el conector, puede ver que en el nombre del servidor sólo se muestran los cuatro primeros dígitos de la dirección IPV6. Los campos de nombre de usuario, contraseña y dominio aparecen en blanco.

Solución:

La interfaz de usuario de CA Enterprise Log Manager envía el contenido del archivo de origen utilizando :: como el delimitador que separa cada origen. Ya que la dirección IPv6 contiene dos puntos dobles ::, se procesa como un delimitador. El registro del conector no se guarda correctamente.

No utilice las direcciones IPv6 para llevar a cabo la implementación del conector masivo. *Puede* utilizar los nombres de host a fin de configurar conectores para la implementación masiva. También puede configurar un conector IPv6 en el asistente de creación del nuevo conector siguiendo las instrucciones normales.

El nombre de montaje del DVD no puede contener espacios

Síntoma:

Al instalar un agente manualmente desde el DVD en un equipo con el sistema operativo Linux, aparece un mensaje de error de permiso denegado y el programa de instalación se cierra.

Solución:

Para instalar un agente desde un DVD, primero debe montar la unidad de DVD con un comando similar al siguiente:

```
$ mount /dev/cdrom <ruta local>
```

La unidad de DVD-ROM no se puede montar en un nombre de ruta local (directorio) cuyo nombre contenga espacios. Monte el DVD-ROM en un nombre de directorio que no contenga espacios y entonces instale el agente.

Error en la configuración de origen de evento en el nivel de dominio

Síntoma:

La configuración de cualquier conector para que acceda a un origen de evento y lea sus registros implica la creación de una cuenta de usuario con privilegios bajos y su asignación a los permisos necesarios. Cuando el origen de evento es un host de Windows Server 2003 SP1, uno de los pasos es el establecimiento de la política de seguridad local, *Suplantar a un cliente tras la autenticación*. Cuando el derecho de usuario se establece localmente, no se produce ningún problema. No obstante, si esta configuración se aplica como política de dominio a todos los servidores, la aplicación global elimina las asignaciones locales existentes para otros usuarios: administradores y servicio.

En un artículo de soporte técnico de Microsoft, se indica que "... problemas se producen cuando se vincula una configuración de política de grupo que define el derecho de usuario Suplantar a un cliente tras la autenticación al dominio. Este derecho de usuario debe vincularse únicamente a un sitio o a una unidad organizativa (OU)".

Solución:

Consulte el artículo de Microsoft Knowledge Base con ID 930220 si desea consultar las recomendaciones para la restauración de la conectividad TCP/IP no segura completa mediante la desactivación de los servicios IPSec y el reinicio del equipo, así como los pasos para volver a agregar los grupos Administradores y SERVICIO como configuración de política de grupo. Visite el vínculo que aparece a continuación:

http://support.microsoft.com/kb/930220

Microsoft también recomienda los siguientes métodos para la resolución de problemas generados al aplicar la configuración Suplantar a un cliente tras la autenticación como política de grupo:

- Método 1: modificación de la configuración de la política de grupo
- Método 2: modificación del registro

Consulte el artículo de Microsoft Knowledge Base con ID 911801 para obtener información acerca de los pasos necesarios para implementar las dos soluciones recomendadas. Visite el vínculo que aparece a continuación:

http://support.microsoft.com/kb/911801

La activación de la comunicación SSL retrasa ODBC/JDBC

Síntoma:

Cuando la comunicación del servidor del agente de CA Enterprise Log Manager se encuentra en el modo no FIPS, la activación de la comunicación SSL causa una breve interrupción en la comunicación de ODBC/JDBC.

Solución:

Si está utilizando ODBC o JDBC, cuando activa SSL el servidor de CA Enterprise Log Manager puede producir un error al comunicarse de forma inmediata. La comunicación se restablece pasados cinco minutos.

Las integraciones de File Log Sensor 4.0.0.0 no son compatibles con SUSE Linux

Síntoma:

Una vez actualizado desde CA Enterprise Log Manager 12.1 directamente a 12.1 SP1, aparece una declaración de compatibilidad de la plataforma incorrecta en el Asistente de integración. Si selecciona la versión 4.0.0.0 del sensor de registro de archivos en el primer paso del asistente, en la lista de plataformas disponibles aparecerá Linux_X86_32 SLES11.

Solución:

Esta información es incorrecta. SUSE Linux no es compatible con el FileLogSensor 4.0.0.0. Ignore la declaración. Por lo tanto, no puede crearse una integración personalizada mediante este sensor de registro.

Limitación en la configuración del puerto

Síntoma:

Cuando se configura la escucha de syslog con el puerto UDP predeterminado en un agente que funciona como un usuario no root en un host Linux, el puerto UDP 514 (predeterminado para syslog) no se abre y en ese puerto se recopilan los eventos que no son de syslog.

Solución:

Si el agente está funcionando como un usuario no raíz en un sistema UNIX, deberá cambiar los puertos de escucha de syslog a números de puerto superiores a 1024 o cambiar el servicio para que se ejecute como raíz.

El rendimiento puede disminuir al seleccionar demasiadas integraciones

Síntoma:

El rendimiento del agente predeterminado disminuye al especificar demasiadas integraciones predeterminadas de syslog para un conector. En este caso, el rendimiento hace referencia al número de eventos por segundo (EPS) gestionado.

Solución:

Para cada integración, CA Enterprise Log Manager carga los archivos de análisis de mensajes (XMP) y de asignación de archivos (DM). Durante las operaciones, CA Enterprise Log Manager comprueba los eventos entrantes con las listas de expresiones regulares. Cuanto mayor sea el número de archivos, mayor será el tiempo de procesamiento.

Para evitar un rendimiento lento, elimine las integraciones que no sean necesarias al crear un conector de syslog. Tras la instalación, revise las integraciones configuradas para el conector de syslog predeterminado y elimine las que no sean necesarias.

La eliminación de un servidor de la federación no elimina el agente predeterminado

Síntoma:

Cuando se elimina un servidor de CA Enterprise Log Manager de un grupo de servidores federados, el agente predeterminado del servidor eliminado no se elimina del grupo de agentes relacionado.

Solución:

Elimine manualmente el agente de este grupo en la subficha Explorador de agente.

Los informes de datos recopilados desde el recopilador de SAPI de CA no muestran los eventos correctamente

Síntoma:

Los eventos recopilados mediante el recopilador de SAPI de CA Audit no presentan todos los campos de evento rellenados correctamente. Por ello la mayoría de los informes no muestran los datos correctamente.

Solución:

Utilice el enrutador de SAPI de CA Audit para recopilar eventos de su infraestructura de CA Audit.

Para obtener más información acerca de la configuración del enrutador de SAPI, consulte la sección Considerations for CA Audit Users Router de la *Guía de implementación*.

La entrega de syslog en UDP no está garantizada

Síntoma:

Garantizar la entrega puede ser un problema para la recopilación directa de syslogs mediante el protocolo UDP de la escucha syslog.

Solución:

Una posible solución es utilizar un mecanismo de recopilación local de syslog para los problemas potenciales relacionados con entregas garantizadas. Es decir, en el caso de una escucha de syslog configurada en un agente instalado con el origen de evento de syslog.

Nota: Utilice el puerto conocido por syslog, puerto 514, solamente si el agente se ejecuta como root. Si el agente se ejecuta como un usuario de privilegios bajos, tal y como se recomienda, asígnele un puerto privado. Los puertos privados son los que van desde 49152 a 65535.

Servicios de syslog un conflicto de UNIX

Síntoma:

En el siguiente escenario, CA Enterprise Log Manager no recibe ningún evento de syslog:

Equipo 1

Una escucha del servidor de CA Enterprise Log Manager para eventos de syslog en el equipo 2.

Equipo 2

Un equipo RHEL 4.0 con un agente local que contiene un conector de syslog y enviando sus eventos al equipo 1 mediante la escucha de syslog.

Equipo 3

Un equipo UNIX enviando eventos al equipo 2 mediante el conector instalado en el mismo.

En este caso, el equipo del agente no puede capturar los eventos del equipo 3 puesto que el servicio de syslog del SO y el conector de syslog se están ejecutando en el mismo sistema.

Solución:

Detenga el servicio de syslog en el equipo 2 para recibir eventos del equipo 3 (el equipo UNIX). También puede volver a configurar el entorno para evitar conflictos entre los servicios de syslog en el mismo equipo.

El sensor de registro de WMI genera varios eventos de privilegios de usuario

Síntoma:

Al utilizar un conector, el sensor de registro de WMI para recopilar eventos, puede observar varios eventos relacionados con el "uso de privilegios".

Solución:

Estos eventos aparecen si la política de auditoría de Windows que registra las acciones correctas de uso de privilegios está activada en el sistema de destino. Se trata de una consecuencia del proceso de recopilación de eventos y no indica la existencia de ningún problema. Puede crear una regla de supresión para evitar que CA Enterprise Log Manager los reciba si no desea que aparezcan.

Detención de la recepción de eventos por parte del sensor de registro de archivos de texto que se ejecuta en un sistema de agente de Solaris

Síntoma:

El sensor de registro de archivos de texto que se ejecuta en un sistema de agente de Solaris deja de recibir eventos

El archivo de registro del conector contiene un error que indica que se ha producido un error al abrir el archivo de la biblioteca libssl.so.0.9.7:

```
[4] 20/07/10 18:55:50 ERROR :: [ProcessingThread::DllLoad] :Error is: ld.so.1:
caelmconnector: fatal: libssl.so.0.9.7: open failed: No such file or directory
[4] 20/07/10 18:55:50 ERROR :: [ProcessingThread::run] Dll Load and Initialize
failed, stopping the connector ...
[3] 20/07/10 18:55:50 NOTIFY :: [CommandThread::run] Cmd_Buff received is START
```

Solución:

Identifique la ubicación de la biblioteca para permitir que el agente reciba eventos.

Para solucionar el error en el sistema de agente de Solaris

1. Vaya a la carpeta /etc. Por ejemplo:

   ```
   cd /etc
   ```

2. Abra el archivo de perfil en la carpeta etc. Por ejemplo:

   ```
   vi /etc/profile
   ```

3. Agregue las dos líneas siguientes al final del archivo de perfil:

   ```
   LD_LIBRARY_PATH=/usr/sfw/lib:$LD_LIBRARY_PATH
   ```

   ```
   export LD_LIBRARY_PATH
   ```

4. Cierre la sesión actual del sistema del agente de Solaris.
5. Abra una nueva sesión en el sistema del agente de Solaris.
6. Detenga el agente de CA Enterprise Log Manager en el sistema Solaris. Por ejemplo:

   ```
   /opt/CA/ELMAgent/bin/S99elmagent stop
   ```

7. Inicie el agente de CA Enterprise Log Manager en el sistema Solaris. Por ejemplo:

   ```
   /opt/CA/ELMAgent/bin/S99elmagent start
   ```

   El sensor de registro de archivos de texto empezará a recibir eventos y ya no aparecerá ningún error en el archivo de registro.

Capacidad de respuesta nula del agente a causa de un flujo de eventos demasiado elevado

Síntoma:

El agente de CA Enterprise Log Manager deja de responder y no acepta eventos. Aparece el siguiente mensaje de error en el archivo caelmdispatcher.log:

```
[275] 12/07/10 14:32:05 ERROR :: FileQueue::PutEvents Unable to write to new event file
[275] 12/07/10 14:32:05 ERROR :: WriterThread::run Unable to push events to FileQueue, Retrying
[275] 12/07/10 14:32:10 NOTIFY :: FileQueue::UpdateCurrentWriterFile Reached Max files configured limit=10, Not creating any new files for now
```

Solución:

Estos mensajes indican que hay una tasa muy elevada de eventos entrantes para el hardware del entorno. Para solucionar este problema vuelva a configurar el agente siguiendo el procedimiento siguiente:

1. Haga clic en Administración, seleccione la subficha Recopilación de registros y amplíe la carpeta Explorador de agente.
2. Seleccione el agente que desea volver a configurar, haga clic en Editar y ajuste los parámetros siguientes:

   Número máx. de archivos

   Establece el número máximo de archivos que se pueden crear en la cola de archivos de recepción de eventos. El número máximo de archivos es 1.000. El valor predeterminado es 10.

   Tamaño máx. por archivo

   Establece el tamaño máximo, en MB, para cada archivo de la cola de archivos de recepción de eventos. Cuando un archivo alcanza el tamaño máximo, CA Enterprise Log Manager crea un archivo nuevo. El tamaño máximo es 2.048 MB. El valor predeterminado es 100 MB.

   Estos parámetros se pueden incrementar según la necesidad del entorno y según la tasa de eventos por segundo.

Dispositivo (no - interfaz de usuario)

Problemas relacionados con el dispositivo de software (no relacionados con la interfaz de usuario de CA Enterprise Log Manager)

No se puede iniciar sesión en el servidor de CA Enterprise Log Manager con el nombre de usuario EiamAdmin

Síntoma:

El nombre de usuario EiamAdmin y la contraseña no se reconocen cuando se intenta iniciar sesión en el servidor de CA Enterprise Log Manager (no a través de la interfaz de usuario).

Solución:

Para realizar tareas de mantenimiento, como configurar el archivado, el programa de instalación crea otro nombre de usuario, caelmadmin, y le asigna la misma contraseña que el instalador ha proporcionado para EiamAdmin. Utilice el nombre de usuario y la contraseña caelmadmin para iniciar sesión en el servidor de CA Enterprise Log Manager.

Si desea obtener más información, consulte la sección Cuentas de usuario predeterminadas en la *Guía de implementación*.

Número excesivo de archivos de registro de ELMAdapter

Síntoma:

Se puede acumular una gran cantidad de archivos de registro del adaptador en el servidor de CA Enterprise Log Manager. Esto no es frecuente, ya que lo normal es agregar mensajes de registro en un único archivo de registro. El problema puede producirse al activar el seguimiento.

Para determinar si el problema existe

1. Programe informes y alertas, y ejecute consultas de ODBC, como la siguiente:

   ```
   select event_logname,count(*) from view_event where event_time_gmt >=
   timestampadd(hh,-1,now()) AND event_time_gmt <= now() group by event_logname;
   ```

2. Inicie sesión en el servidor CA Enterprise Log Manager mediante SSH e indique el nombre de usuario y la contraseña caelmadmin.
3. Utilice su para root e indique la contraseña del usuario root.
4. Vaya a la carpeta de iTechnology:

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ```

5. Determine si se ha creado un número excesivo de archivos de registro a causa de la creación de consultas a través de los controladores de ODBC. Estos archivos se denominan ELMAdapter_<oaserverpid>_-IP.log.

Solución:

Si se detecta este problema, asegúrese de que el seguimiento de errores está desactivado del siguiente modo:

1. Inicie sesión en el servidor de gestión de CA Enterprise Log Manager mediante SSH e indique el nombre de usuario y la contraseña caelmadmin.
2. Utilice su para root e indique la contraseña del usuario root.
3. Vaya a la carpeta de iTechnology:

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ```

4. Abra oaserver-dm.ini para editarlo.
5. Desplácese a [Service_0] asegúrese de que el seguimiento está desactivado. De lo contrario, cámbielo para que coincida con el siguiente ejemplo:

   ```
   ServiceDebugLogLevel=0
   ServiceIPLogOption=Disable All Tracing
   ```

6. Reinicie el servicio ODBC del siguiente modo:
   a. Seleccione la ficha Administración y, a continuación, la subficha Servicios.

b. Haga clic en Servidor ODBC.

c. A continuación, realice una de las siguientes acciones:

- Si la opción Activar servicio está seleccionada, seleccione Activar servicio y haga clic en Guardar.
- Si la opción Activar servicio está activada, desactive la casilla de verificación Activar servicio, haga clic en Guardar, seleccione Activar servicio y vuelva a hacer clic en Guardar.

Al importar manualmente archivos de análisis puede ser necesario modificar el valor del tiempo de espera

En ocasiones, se produce un problema durante la importación de archivos de análisis (.XMP) al instalar CA Enterprise Log Manager. Este problema se produce con más frecuencia al instalar CA Enterprise Log Manager en servidores que no cumplen los requisitos de hardware mínimos o en redes lentas.

Síntoma:

Durante la instalación, se produce un error durante la importación o el análisis de archivos. Puede corregir este problema una vez que finalice la instalación. Ejecute el script proporcionado, *EEM/content/ImportCALMXMP.sh*, para importar los archivos de forma manual. (Hay disponible más información acerca de este script en la *Guía de implementación*). Esta acción suele solucionar el error.

No obstante, en ocasiones el archivo XMP del enrutador de Cisco no puede realizar la importación correctamente mientras se ejecutan las secuencias de comandos de importación manual. La instalación del servidor de CA Enterprise Log Manager se llevó a cabo correctamente. No obstante, el error al importar XMP hace que los conectores predeterminados no se instalen correctamente en el agente local. No se pueden implementar los conectores hasta que se realice correctamente la importación manual de los archivos XMP .

Solución:

Al superar un valor de tiempo de espera predeterminado en el script *EEMImportUtility.sh*, se genera el problema de importación del archivo XMP de Cisco. El script *ImportCALMXMP.sh* llama al script *EEMImportUtility.sh*. El valor de tiempo de espera predeterminado es 4 minutos. Establezca el tiempo de espera predeterminado en 6 minutos con el fin de permitir tiempo suficiente para llevar a cabo una importación manual en servidores más lentos.

Para cambiar el valor de tiempo de espera predeterminado

1. Desplácese al directorio EEM/content.
2. Edite el archivo de configuración ImportCALMXMP.sh.
3. Busque la siguiente línea y cambie el valor de tiempo de espera como se muestra a continuación:

   ```
   ./EEMImportUtility.sh -h simdemo01 -u EiamAdmin -m FgAMCQQJAllf -a CAELM -type xmp -l XMP" to "./EEMImportUtility.sh -timeout 360000 -h simdemo01 -u EiamAdmin -m FgAMCQQJAllf -a CAELM -type xmp -l XMP
   ```

   Nota: El valor de tiempo de espera se expresa en milisegundos.
4. Guarde y cierre el archivo.
5. Vuelva a ejecutar el script.
6. Implemente manualmente conectores para syslog y Linux_LocalSyslog en el agente predeterminado.

Refinamiento de eventos

A continuación se presentan los problemas conocidos relacionados con el refinamiento de eventos.

El bloqueo de la asignación de cadenas y valores numéricos requiere operadores diferentes

Síntoma:

Cuando utilice el asistente de asignación, es posible que los valores de asignación de bloqueo para las columnas de cadenas de texto o numéricas no funcionen correctamente.

Solución:

Al crear asignaciones de bloqueo, el operador Equal solamente puede utilizarse con columnas numéricas. Utilice el operador 'Match' para todas las columnas de cadena de texto.

La asignación de datos personalizada no puede asignar los eventos de epSIM (iTech)

Síntoma:

El archivo de la asignación de datos (DM) personalizada creado para los eventos de epSIM (iTechnology) no puede asignar los eventos después de haber sido aplicados al complemento de eventos de iTechnology bajo el Adaptador de CA en el Explorador de recopilación de registros.

Cuando examina la consulta Todos los eventos del sistema para determinar si se asignan eventos de iTech según el archivo de DM personalizado, encuentra que no se están asignando eventos de iTech y, por lo tanto, no se devuelven como resultados de consulta. Se muestra el mensaje 'No se han asignado eventos. No se pueden asignar eventos.'.

Solución:

Abra el archivo de DM personalizado y reemplace $EventLog por $Log.

Cambie la línea: <DM_Field name="event_logname" type="string" value="$EventLog" mapping="direct"/>

a: <DM_Field name="event_logname" type="string" value="$Log" mapping="direct"/>

Este cambio asegura la asignación de los eventos. Ignore cualquier mensaje siguiente durante el análisis de la asignación que afirme 'No se han asignado eventos'.

Consultas e informes

A continuación se presentan los problemas conocidos relacionados con las consultas y los informes.

Los resultados de consultas de alertas de acciones pueden estar incompletos

Síntoma:

Cuando se genera una alerta de acción, puede ver el resultado de la consulta de inmediato en CA Enterprise Log Manager. Para ver los resultados en CA Enterprise Log Manager, haga clic en la ficha Gestión de alertas y en la subficha Alertas de acción, y, a continuación, seleccione el nombre de la alerta. Los resultados aparecen en una vista de gráfico. Cuando la alerta de acción ejecuta un proceso de salida de alerta/evento de CA IT PAM que abre un parte del departamento de asistencia técnica en CA Service Desk (aparece una URL en el problema del servicio de asistencia). Cuando se desplaza a esta URL e inicia sesión, los resultados de la consulta aparecen en una sola página. Si compara estos resultados con los resultados que aparecen en la subficha Alertas de acción, puede observar que los resultados de la consulta no coinciden. Por ejemplo, si se muestran los resultados de Total, los números de la vista en la URL pueden ser superiores a las cifras que se muestran en CA Enterprise Log Manager. Este problema puede observarse en sistemas que soporten demasiada carga cuando el tiempo de finalización dinámico establecido para las condiciones de resultado es inadecuado. Una configuración inadecuada es aquélla que no permite suficiente tiempo para que se lleve a cabo la actualización de la base de datos antes de realizar la lectura de la base de datos. Las probabilidades de que esto ocurra se han reducido mediante el establecimiento del valor predeterminado del tiempo de finalización dinámico en 'ahora', '-2 minutos' para el intervalo predefinido Últimos 5 minutos.

Solución:

Modifique el tiempo de finalización dinámico en el paso Condiciones de resultado de la alerta de acción de 'ahora', '-2 minutos' a un valor que permita más tiempo, por ejemplo, 'ahora', '-10 minutos'.

Limitación en las consultas con las búsquedas de varios términos

Síntoma:

Una consulta en una columna de búsqueda sólo realizar una búsqueda sin distinción entre mayúsculas y minúsculas, tal y como se espera. Sin embargo, una consulta en varias columnas de búsqueda realiza una búsqueda que distingue entre mayúsculas y minúsculas en la que los asteriscos (*), que se deberían interpretar como comodines, se interpretan literalmente. Este problema se produce cuando el código SQL generado internamente contiene el operador OR en la cláusula WHERE.

Solución:

Limite sus consultas a búsquedas en una columna solamente cada vez cuando utilice peticiones. Si crea su propia columna con varias expresiones, puede conectar varias expresiones comodín LIKE con el operador lógico AND.

El filtro simple del asistente de consultas produce un error al usar caracteres especiales

Síntoma:

El filtro simple del asistente de consultas produce un error al escribir caracteres especiales como parte de un valor de campo de filtro simple. Puede guardar y ejecutar la consulta con los siguientes caracteres especiales:

```
( ) & * > < ? : } {
```

No obstante, la consulta se ejecuta sin usar dicho campo como filtro y se muestran los datos aunque la condición de coincidencia no se cumpla.

Solución:

No utilice los caracteres especiales que se enumeran como parte de los valores de campo de filtro simple.

Después de la actualización no se muestra el estado de la tarea programada

Síntoma:

En la ficha Informes programados, la subficha Programación de informes, puede ver todas las tareas programadas con su estado. En la columna Estado aparece Generando durante el proceso de generación de informes y Programado cuando la tarea está programada. Tras una actualización desde la versión r12.0 GA base, la columna Estado de los informes se borra sin tener en cuenta el estado. Cuando se vuelve a generar un informe programado, el estado se muestra de nuevo.

Solución:

La omisión de un valor en la columna Estado de una tarea programada es un problema de visualización temporal. No es necesario tomar ninguna medida Cuando se vuelva a generar el informe se mostrará el estado correcto.

Algunos trabajos de alerta de acción dan error cuando se programan con demasiada frecuencia

Síntoma:

Cuando una alerta de acción que consulta eventos generados durante un intervalo de tiempo determinado se programa para ejecutarse más frecuentemente que ese intervalo de tiempo, los trabajos solapados pueden producir un error. Se muestra el siguiente mensaje Failed to generate the alert as the previous query is in progress. Por ejemplo, si quisiera consultar eventos específicos que se generaron durante las últimas tres horas, pero se configuró la consulta para ejecutarse a cada hora, el primer trabajo no tendría tiempo de completarse antes de que empezase el segundo trabajo. En este caso, CA Enterprise Log Manager continúa procesando el primer trabajo programado y envía mensajes de error a los dos trabajos programados siguientes. En cuanto transcurre el intervalo de 3 horas, se envía una alerta si existen eventos que coincidan con los criterios de la consulta, y se ejecuta el proceso de la alerta siguiente.

Solución:

Si especifica solamente la Selección de intervalo de fechas en el paso de Condiciones de resultado, seleccione un intervalo de recurrencia *igual al* intervalo que se configuró para la Selección de intervalo de fechas. Por ejemplo, si quisiera consultar eventos que coincidan con los criterios específicos que se generaron durante las últimas tres horas, configurare la Selección de intervalo de fechas en el paso de Condiciones de resultado como sigue:

Tiempo de finalización dinámico: 'ahora' '-2 minutos'

Tiempo de finalización dinámico: 'ahora' '-182 minutos'

Cuando defina la programación, configure el Intervalo de recurrencia en el paso Programar tareas con un valor igual a 3 horas (180 minutos) como sigue:

Intervalo de recurrencia: 3 horas

La configuración del mismo intervalo de consulta y de recurrencia asegura que cada evento coincidente con los criterios de la consulta se registre en una alerta generada. Esta recomendación no se aplica si se especifica un intervalo de tiempo para eventos agrupados.

No se pueden borrar las etiquetas que contengan caracteres especiales

Síntoma:

No se pueden eliminar etiquetas de informes o consultas que contengan los caracteres especiales ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ? .

Solución:

No utilice los caracteres especiales mencionados al crear etiquetas de informes o consultas.

Suscripción

A continuación se presentan los problemas conocidos relacionados con la suscripción.

Reiniciar automáticamente tras la actualización del SO durante la actualización del SP

Síntoma:

Si la opción de suscripción Reiniciar automáticamente tras la actualización del SO está seleccionada, cuando se aplique la actualización del service pack, el sistema operativo se reinicia antes de que la actualización del archivo binario de CA Enterprise Log Manager se complete. Si no se completa la actualización, se actualizan los scripts de cierre de iGateway. Esta actualización debe aplicarse para que iGateway se puede cerrar correctamente cuando se reinicie el sistema operativo.

Solución:

Antes de aplicar la actualización del módulo del gestor de registros del service pack, establezca la opción de Reiniciar automáticamente tras la actualización del SO en No.

Error de falta de memoria en equipos con poca memoria

Síntoma:

Si descarga una actualización de suscripción en un equipo que no disponga de la memoria recomendada de 8 GB se puede producir un error de Java de falta de memoria. Los paquetes de gran tamaño se descargan mediante el uso de iGateway cuando no existe ningún valor del tamaño de la memoria dinámica de Java Virtual Machine (JVM).

Solución:

Si instala CA Enterprise Log Manager en un equipo con menos de la memoria recomendada de 8 GB, modifique la configuración del tamaño de la memoria dinámica de JVM mediante la edición del archivo caelm-java.group.

Para modificar el valor del tamaño de la memoria dinámica de JVM.

1. Inicie sesión en el servidor de CA Enterprise Log Manager como caelmadmin.
2. Vaya a la carpeta de iGateway.
3. Abra el archivo caelm-java.group y ubique la sección de configuración de JVM.
4. Agregue la nueva línea, como se muestra en la ilustración siguiente en negrita:

```
<JVMSettings>
        <loadjvm>true</loadjvm>
        <javahome>/usr/java/latest/jre</javahome>
        <Properties
name="java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed">
            <system-
properties>java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed</
system-properties>
        </Properties>
    <Properties name="maxmemory"><jvm-property>-Xmx1250M</jvm-
property></Properties>
    </JVMSettings>
```

5. Guarde y cierre el archivo caelm-java.group

Importante: la configuración del valor del y tamaño de la memoria dinámica de JVM puede causar problemas al utilizar la opción Exportar a PDF con conjuntos grandes de datos. Es decir, es mejor utilizar esta opción solamente en equipos pequeños.

Los cambios en las credenciales del proxy provocan el bloqueo de la cuenta del dominio

Síntoma:

En un entorno con un servidor de CA Enterprise Log Manager sus credenciales de dominio no funcionan y su cuenta está bloqueada.

Solución:

El servidor de CA Enterprise Log Manager contacta regularmente con el servidor de suscripción de CA para comprobar las actualizaciones del producto. Si las credenciales del proxy (como ID de usuario y contraseña) han caducado o se han modificado, CA Enterprise Log Manager no podrá ponerse en contacto con el servidor de suscripción y generará un evento autocontrolado para el error de inicio de sesión. El evento autocontrolado mostrará un mensaje similar al siguiente:

```
No se puede conectar con el servidor de contenido de suscripción. Puede ser que el servidor está desconectado o se produce un error en la conexión o que los valores del servidor proxy sean incorrectos. Valide los valores de configuración del servidor proxy.
```

Si se permite que continúen los inicios de sesión erróneos, la cuenta de dominio se puede bloquear dependiendo de las políticas locales. Verifique que las credenciales de proxy no se hayan modificado ni caducado.

Es recomendable que la cuenta de servicio utilizada para contactar el servidor de suscripción no tenga una política de caducidad de contraseña.

El autocontrol de eventos para reiniciar sólo aparece una vez

Síntoma:

Cuando se selecciona un módulo de sistema operativo para descargar mediante una suscripción y se especifica que se va a instalar con la opción de no reiniciar, se genera el siguiente evento autocontrolado solamente una vez: Las actualizaciones del SO se han instalado en este host...Reinicie el equipo para que las actualizaciones tengan efecto.

Solución:

La suscripción genera un evento que le recuerda que reinicie el sistema operativo sólo una vez cuando se necesite un reinicio manual. Es recomendable crear una alerta para este evento.

Reselección de los módulos de suscripción tras su actualización

Síntoma:

Cuando se actualiza CA Enterprise Log Manager a la versión r12.1, los módulos de suscripción previamente seleccionados se mueven de la lista Seleccionado de la interfaz a la lista Disponible. Esta acción evita actualizaciones futuras de suscripción de los módulos.

Solución:

Tras la actualización, el usuario deberá volver a seleccionar los módulos que desee utilizar. A continuación, se explican los pasos a seguir.

Para volver a seleccionar los módulos de suscripción

1. Inicie sesión con CA Enterprise Log Manager y haga clic en la ficha Administración. A continuación, haga clic en la subficha Servicios.
2. Abra el módulo Suscripción para cada uno de los servidores que desee actualizar.
3. Utilice el control de cambio de etiquetas para mover, de la lista Seleccionado a la lista Disponible, aquellos módulos que desee que estén disponibles para su actualización.
4. Haga clic en Guardar.

El botón Probar proxy devuelve un falso positivo tras realizar el cambio de configuración

Síntoma:

Cuando cambia la configuración del servidor proxy de CA Enterprise Log Manager tras realizar una prueba correcta y vuelve a realizar la prueba con el botón Probar proxy, aparece un mensaje de confirmación con independencia de si la nueva configuración es correcta o no.

Solución:

El botón Probar proxy utiliza la configuración de proxy especificada para acceder a una URL a través de dicho proxy. Los servidores proxy suelen almacenar en caché la autenticación de cliente cuando son válidos e ignoran las credenciales posteriores hasta que haya transcurrido un tiempo de inactividad.

Esto quiere decir que una vez que el botón Probar proxy haya indicado correctamente que la configuración es válida, es posible que, en comprobaciones posteriores, se muestren configuraciones incorrectas como válidas durante un período de tiempo.

Dos reglas de supresión no se aplican correctamente

Síntoma:

Las dos siguientes reglas de supresión, que son parte de r12.0, no se aplican correctamente:

- TMCM: Mensajes de actualización correcta del motor de virus & de las firmas de virus
- Mensajes de actualización del motor de virus & de la firma de virus de McAfee correcta

Solución:

Las reglas no pueden aplicarse correctamente, a causa del signo & que aparece en el título. La actualización de r12.1 contiene las dos siguientes reglas de sustitución:

- TMCM: Mensajes de actualización correcta del motor de virus y de las firmas de virus
- Mensajes de actualización del motor de virus y de la firma de virus de McAfee correcta

Utilice estas reglas en lugar de las versiones anteriores que contienen el signo &.

Es necesario reiniciar iGateway para actualizar a r12.1

Síntoma:

En un entorno federado, la actualización de r12.0 a r12.1 no se puede llevar a cabo sin reiniciar iGateway.

Solución:

Los archivos binarios de actualización se copian y se extraen, pero el cliente de suscripción no los instala. Permanecen en el directorio "/tmp/downloads". Esto indica que el proceso de actualización de la suscripción no se ha completado. En este punto, debe reiniciar iGateway de forma manual mediante el siguiente proceso:

Para reiniciar el servicio o el daemon de iGateway

1. Inicie sesión como usuario caelmadmin del servidor de CA Enterprise Log Manager.
2. Cambie los usuarios a la cuenta root con el siguiente comando:

   ```
   su -
   ```

3. Detenga el proceso de iGateway con el siguiente comando:

   ```
   $IGW_LOC/S99igateway stop
   ```

4. Inicie el proceso de iGateway con el siguiente comando:

   ```
   $IGW_LOC/S99igateway start
   ```

De esta forma, se podrá finalizar la actualización.

La actualización a r12.1 SP1 requiere el reinicio de iGateway

Síntoma:

La actualización de r12.1 a r12.1 SP1 puede que no se complete a tiempo. Si el proceso de suscripción se ejecuta sin completarse durante una hora y media o más, será preciso reiniciar iGateway.

Solución:

Se recomienda que utilice el procedimiento siguiente para identificar este problema:

1. Complete el contenido de la suscripción: Informes e integraciones desde 12.1 GA.
2. Complete la suscripción binaria: Servidor, agente y módulos de SO a SP1.

Con ello se podrá distinguir el tiempo transcurrido para descargar cada módulo, ya que el tiempo de descarga variará según el tamaño del módulo. Si la parte de suscripción se ejecuta durante mucho tiempo sin llegar a completarse, reanude iGateway desde la interfaz de usuario de CA Enterprise Log Manager.

Para reiniciar el servicio de iGateway

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda la entrada Estado del sistema.
3. Seleccione un servidor específico de CA Enterprise Log Manager.
4. Haga clic en la ficha Administración del servicio.
5. Haga clic en Reiniciar iGateway.

El sensor de registros de syslog actualizado en r12.1 SP1 requiere la actualización a integraciones para los agentes para Windows

Síntoma:

Si durante la actualización a la versión r12.1 SP1 no se aplica la actualización del módulo de integraciones, los conectores que utilizan el sensor de registros de syslog dejarán de ejecutarse. Por lo que se muestra el siguiente error en el archivo de registro del agente:

```
[6072] 9/03/10 17:22:51 ERROR :: MySAX2Handler::fatalError: at line1
[6072] 9/03/10 17:22:51 ERROR :: XMLTree::ParseUsingSAX2:error parsing
stringintruvert/jsp/admin/Login.jsp
[6072] 9/03/10 17:22:51 ERROR :: XMLTree::Parse Exit ParseUsingSAX2 FAILURE
[6072] 9/03/10 17:22:51 ERROR :: HTTP_Processor::ParseRequestXML: Unknown request
format:intruvert/jsp/admin/Login.jsp
```

Además, verifica la versión de la integración. Si es anterior a la versión 12.1.5104.0, debe aplicarse la actualización.

Solución:

Aplique la actualización del módulo de integraciones y, a continuación, actualice cada integración que utilice el sensor de registros de syslog a la versión 12.1.5104.0 o posterior. También puede seguir los pasos que se describen en la sección Actualización de varias configuraciones de conectores en la *Guía de administración*.

Para obtener una lista de integraciones que utilizan el sensor de registros de syslog, consulte la Matriz de integración del producto CA Enterprise Log Manager en: https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8238/8238_integration_certmatrix.htm.

Gestión de usuarios y accesos

A continuación se presentan los problemas conocidos relacionados con la gestión de usuarios y de accesos

Limitaciones de acceso desde un explorador en Windows Vista

Síntoma:

Cuando inicie sesión en CA Enterprise Log Manager desde un equipo con el sistema operativo Windows Vista SP1, con IPv6 activado desde cualquier explorador, no podrá acceder a la funcionalidad a través de los botones de la subficha Gestión de usuarios y accesos de la ficha Administración.

Los usuarios que inician sesión con las credenciales de EiamAdmin o credenciales de una cuenta de usuario de CA Enterprise Log Manager asignada a un rol de Administrator deberían tener acceso a esta funcionalidad. La limitación no aplica a los usuarios que exploran en CA Enterprise Log Manager desde cualquier otro sistema operativo de Windows. Ocurre solamente cuando se explora CA Enterprise Log Manager a través de una URL con el formato siguiente desde un equipo con Windows Vista https://[*ipv6-address*]:5250/spin/calm. La siguiente URL es un ejemplo:

`https://[::FFFF:192.168.00.00]:5250/spin/eiam`

Solución:

La solución para este problema consiste en acceder a la función Gestión de usuarios y accesos a través de una URL diferente.

1. Introduzca la siguiente URL en su explorador cuando la dirección la dirección IPv6 es la URL del servidor de gestión de CA Enterprise Log Manager.

   `https://[ipv6-address]:5250/spin/eiam`

2. Seleccione CAELM en la lista desplegable Aplicación.
3. En los campos Nombre de usuario y Contraseña introduzca EiamAdmin con la contraseña de esta cuenta o las credenciales de un usuario de CA Enterprise Log Manager con la función Administrator.
4. Haga clic en la ficha Gestionar identidades para configurar usuarios y grupos.
5. Haga clic en la ficha Gestionar directivas de acceso para configurar o probar los calendarios.
6. Haga clic en la ficha Configurar, servidor EEM, para configurar usuarios globales, grupos globales o políticas de contraseña.

Limitación del uso del calendario con las políticas de acceso

Síntoma:

Durante las horas y los días especificados en un calendario con una política que conceda acceso, tiene acceso de usuario o de grupo limitado a CA Enterprise Log Manager. No obstante, este calendario no funciona correctamente con una política que rechace el acceso de forma explícita.

Solución:

Utilice el tipo de política que concede acceso explícito para limitar el número de veces que desee conceder acceso a un grupo en lugar de utilizar una política de rechazo explícita.

Opciones varias

A continuación se presentan los problemas conocidos.

CA Enterprise Log Manager no responde a veces

Síntoma:

A veces CA Enterprise Log Manager no responde. Es decir, la interfaz de usuario no responde ni a las solicitudes del usuario ni a las internas realizadas desde el agente para que el gestor del agente se detenga. Sin embargo, la recopilación de registros continua.

Solución:

Utilice el siguiente procedimiento para detener el proceso de iGateway y reiniciarlo:

1. Inicie sesión en el servidor de CA Enterprise Log Manager que no responde mediante ssh como usuario caelmadmin.
2. Cambie los usuarios a la cuenta raíz con el siguiente comando y proporcione la contraseña root:

   ```
   su -
   ```

3. Desplácese hasta el directorio $IGW_LOC.

   De manera predeterminada, iGateway se encuentra en el directorio /opt/CA/SharedComponents/iTechnology.

4. Detenga el proceso de iGateway con el siguiente comando:

   ```
   ./S99igateway stop
   ```

5. Inicie el proceso de iGateway con el siguiente comando:

   ```
   ./S99igateway start
   ```

Error de las llamadas de consulta o informe a API en ciertos exploradores

Síntoma:

Cuando se utilizan las llamadas abiertas de API getQueryViewer o getReportViewer en Microsoft Internet Explorer 7 o 8, o en Mozilla Firefox,no se obtiene ningún resultado.

Solución:

En los exploradores especificados, la API de CA Enterprise Log Manager produce un error al reconocer el parámetro del servidor en la dirección URL de la llamada API. Para evitar este problema, no especifique ningún parámetro del servidor en las llamadas de getQueryViewer o getReportViewer. Cuando aparezca la interfaz de CA Enterprise Log Manager, seleccione el servidor que desee de la lista desplegable Servidor del gestor de registros ubicada en la parte superior de la página principal.

Para obtener más información acerca de las direcciones URL de las llamadas API, consulte la *Guía de programación de la API de CA Enterprise Log Manager*.

Fin de la compatibilidad de CAELM4Audit

CA Enterprise Log Manager r12.1 SP1 utiliza CA EEM r8.4 SP3, el cual no está certificado para el uso con CA Audit. Puesto que la integración entre CA Enterprise Log Manager y CA Audit comparte un servidor de CA EEM, CA Audit se ejecuta en una configuración no compatible.

Además, CA Audit no es compatible con FIPS, por lo que la conmutación de CA Enterprise Log Manager a modo FIPS provoca la interrupción de la ejecución de la interfaz de usuario de administración de CA Audit.

Impacto del nombre de aplicación personalizado en las consultas de archivos

Síntoma:

En un entorno con varios servidores de CA Enterprise Log Manager que utilicen el mismo servidor de gestión, las consultas de archivos suelen devolver resultados de los directorios de archivos de todos los servidores. No obstante, si establece un nombre de aplicación personalizado al instalar la gestión de CA Enterprise Log Manager en lugar de aceptar la predeterminada, CAELM, la consulta de archivo no funciona de la forma esperada. En lugar de eso, la consulta de archivo devuelve resultados sólo para el servidor en que se ejecuta la consulta. Los resultados de los demás servidores aparecen como *<host>User CERT-custom: Access is denied*.

Solución:

Ejecute la consulta en el catálogo de archivado de cada CA Enterprise Log Manager por separado.

Monitor con configuración de alto contraste

Síntoma:

En Windows, el único contraste alto admitido es el negro en alto contraste; las otras tres opciones de alto contraste no se admiten. Las opciones de alto contraste son alto contraste núm. 1, alto contraste núm. 2, negro en alto contraste y blanco en alto contraste.

Solución:

Seleccionar la opción negro de alto contraste cuando sea necesario un alto contraste. Para establecer esta opción, vaya a Panel de control, Pantalla. La opción aparece en el cuadro de diálogo Propiedades de la pantalla, ficha Apariencia, lista desplegable Esquema de color.

iGateway está continuamente deteniéndose y reiniciándose

Síntoma:

La interfaz de CA Enterprise Log Manager deja de responder a veces durante las operaciones. La comprobación del servidor de CA Enterprise Log Manager muestra que el proceso de iGateway se detiene y se reinicia pero no se mantiene activo. Utilice el siguiente procedimiento para comprobar el proceso de iGateway:

1. Acceda al símbolo del sistema en el servidor de CA Enterprise Log Manager.
2. Inicie sesión con las credenciales de cuenta de caelmadmin.

3. Cambie los usuarios a la cuenta root con el siguiente comando:

   ```
   su - root
   ```

4. Utilice el siguiente comando para verificar que el proceso de iGateway se está ejecutando:

   ```
   ps -ef | grep igateway
   ```

   El sistema operativo devuelve información del proceso de iGateway y una lista de los procesos que se ejecutan en el mismo.

Solución:

Intente realizar las siguientes acciones para resolver el problema:

1. Vaya a $IGW_LOC (/opt/CA/SharedComponents/iTechnology), y busque el siguiente archivo:

   ```
   saf_epSIM.*
   ```

   Existen varias versiones, numeradas de manera secuencial, por ejemplo: saf_epSIM.1, saf_epSIM.2, saf_epSIM.3, etc.

2. Cambie el nombre del archivo con el número menor y guárdelo en otra ubicación para enviarlo a Soporte de CA.
3. Si iGateway no se reinicia automáticamente, reinícielo:
   a. Inicie sesión como usuario root.
   b. Abra una ventana de símbolo del sistema e introduzca el siguiente comando:

      ```
      /opt/CA/SharedComponents/iTechnology/S99igateway start
      ```

El espacio en disco máximo para CA Enterprise Log Manager virtual no es suficiente

Síntoma:

No se puede crear un equipo virtual con un espacio en disco asignado de 512 GB en el servidor de VMware ESX v3.5. Mi servidor virtual de CA Enterprise Log Manager necesita más de 256 GB para poder gestionar el volumen de eventos.

Solución:

El servidor de VMWare ESX utiliza un tamaño de bloque predeterminado de 1 MB, y calcula el espacio en disco máximo utilizando este valor. Cuando se establece el tamaño del bloque en 1MB, el espacio en disco máximo predeterminado es de 256 GB. Si desea configurar más de 256 GB de espacio en disco virtual, puede incrementar el tamaño del bloque predeterminado.

Para crear un disco virtual más grande

1. Acceda a la consola del servicio del servidor de VMware ESX.
2. Incremente el tamaño del bloque a 2MB con el siguiente comando:

   ```
   vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   En este comando, el valor 2M quiere decir 512 GB (2 x 256).
3. Reinicie el servidor de VMware ESX.
4. Crear un nuevo equipo virtual con espacio en disco de 512 GB.

Si desea más información sobre este comando y otros puede consultar la documentación del servidor de VMware ESX.

Al actualizar el explorador se cierra la sesión de usuario de CA Enterprise Log Manager

Síntoma:

Si actualiza el explorador cuando mientras está conectado a CA Enterprise Log Manager se cierra la sesión.

Solución:

CA Enterprise Log Manager no admite la actualización del explorador debido a limitaciones del Flex. Evite actualizar el explorador.

Posible error en la interfaz del explorador o del servicio tras el reinicio de iGateway

Síntoma:

Si hace clic en un objeto de los servicios o de los árboles del explorador de la interfaz de CA Enterprise Log Manager inmediatamente después de un reinicio de iGateway, aparece el mensaje de error Network error on receive.

Solución:

Este error se produce cuando se intenta acceder a uno de los objetos especificados mientras todavía se están recargando tras el reinicio de iGateway. Espere cinco minutos hasta que termine la carga y, a continuación, seleccione el objeto del explorador o de los servicios que desee.

Cargas e importaciones incorrectas con exploradores distintos al explorador de Internet Microsoft Internet Explorer

Síntoma:

Cuando el usuario explora CA Enterprise Log Manager con Mozilla Firefox, Safari o Chrome, puede realizar la mayoría de las tareas sin complicaciones. Sin embargo, estos exploradores dan error al realizar las tareas de carga o importación de archivos. A continuación, se muestran algunos ejemplos:

- El mensaje "Error de E/S: Error de solicitud" indica que la importación de una definición de consulta no se ha realizado correctamente.
- La carga de archivos CSV con el asistente de implementación de conector masivo no se realiza correctamente, aún cuando aparece el mensaje "Cargando archivo".

Solución:

Se recomienda la utilización del explorador Microsoft Internet Explorer en el caso de que el usuario desee realizar tareas de importación o carga de archivos.

La interfaz de usuario no puede mostrarse inesperadamente al realizar la instalación con EEM remoto

Síntoma:

Al instalar CA Enterprise Log Manager con un servidor EEM remoto, a veces la interfaz de usuario no es capaz de mostrarse correctamente cuando se inicia sesión por primera vez. Cuando se revisan los archivos de registro de iGateway, se descubre que no se han iniciado los servicios agentmanager, calmreporter, subscclient y subscproxy.

La sintaxis del archivo de registro puede ser parecida a la siguiente:

```
[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087527824] 23/09/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-msgbroker ] didn't respond OK for the termination
call

[1087527824] 09/23/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-oaserver ] didn't reaspond OK for the termination
call

[1087527824] 09/23/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-sapicollector ] didn't reaspond OK for the
termination call

[1087527824] 09/23/09 17:07:46 ERROR :: OutProcessSponsorManager::start :
SponsorGroup [ caelm-java ] failed to start ]

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
agentmanager ] failed to load

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
calmreporter ] failed to load

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscclient ] failed to load

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscproxy ] failed to load
```

Solución:

Para solucionar este problema, reinicie iGateway y vuelva a iniciar sesión en la interfaz.

Para reiniciar el servicio de iGateway

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
2. Expanda la entrada Estado del sistema.
3. Seleccione un servidor específico de CA Enterprise Log Manager.
4. Haga clic en la ficha Administración del servicio.
5. Haga clic en Reiniciar iGateway.

Capítulo 7: Problemas arreglados

Esta sección contiene los siguientes temas:

Problemas arreglados en la versión r12.1 SP1 (en la página 81)

Problemas arreglados en la versión r12.1 SP1

En CA Enterprise Log Manager r12.1 SP1, se han arreglado los problemas informados por los usuarios siguientes:

- 18789166-1
- 18790979-1
- 18955095-1
- 18973282-1
- 18982868-1
- 18988854-1
- 19005999-1
- 19066155-1
- 19077668-1
- 19087827-1
- 19127553-1
- 19176852-1
- 19182913-1
- 19188433-2

Capítulo 8: Documentación

Esta sección contiene los siguientes temas:

Biblioteca (en la página 83)
Acceso a la biblioteca (en la página 84)

Biblioteca

La biblioteca permite acceder a toda la documentación de CA Enterprise Log Manager desde una ubicación central. La biblioteca incluye lo siguiente:

- Una única lista ampliable de contenido para todas las guías en formato HTML
- Búsqueda de texto completo en todas las guías con los términos de la búsqueda resaltados en el contenido y los resultados de la búsqueda clasificados

  Nota: Al buscar términos puramente numéricos, preceda el valor de búsqueda con un asterisco.
- Rutas de navegación que enlazan con temas de nivel más alto.
- Un único índice para todas las guías
- Vínculos a las versiones en PDF de las guías para imprimirlas.

Acceso a la biblioteca

Las bibliotecas de documentación de los productos de CA están disponibles para su descarga en un archivo ZIP que incluye todas las guías y el índice de búsqueda.

Para acceder a la biblioteca de CA Enterprise Log Manager

1. Vaya a Search Documentation / Guides.
2. Introduzca CA Enterprise Log Manager para el producto, seleccione la versión y el idioma, y haga clic en Go.
3. Descargue el archivo ZIP en el escritorio u otra ubicación.
4. Abra el archivo ZIP y arrastre la carpeta de la biblioteca al escritorio o extráigalo a otra ubicación.
5. Abra la carpeta de la biblioteca.
6. Abra la biblioteca:
   - Si la biblioteca se encuentra en el sistema local y está utilizando Internet Explorer, abra el archivo Bookshelf.hta.
   - Si la biblioteca se encuentra en un sistema remoto o si está utilizando Mozilla Firefox, abra el archivo Bookshelf.html.

   Se abre la biblioteca.

Apéndice A: Agradecimientos a terceros

Esta sección contiene los siguientes temas:

Adaptive Communication Environment (ACE) (en la página 86)
Software bajo la Licencia de Apache (en la página 88)
boost 1.35.0 (en la página 92)
JDOM 1.0 (en la página 93)
PCRE 6.3 (en la página 95)
Zlib 1.2.3 (en la página 97)
ZThread 2.3.2 (en la página 97)

Adaptive Communication Environment (ACE)

Copyright and Licensing Information for ACE(TM), TAO(TM), and CIAO(TM).

ACE(TM), TAO(TM) and CIAO(TM) are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University Copyright (c) 1993-2003, all rights reserved. Since ACE TAO CIAO are open-source, free software, you are free to use, modify, copy, and distribute--perpetually and irrevocably--the ACE TAO CIAO source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using ACE TAO CIAO.

You can use ACE TAO CIAO in proprietary software and are under no obligation to redistribute any of your source code that is built using ACE TAO CIAO. Note, however, that you may not do anything to the ACE TAO CIAO code, such as copyrighting it yourself or claiming authorship of the ACE TAO CIAO code, that will prevent ACE TAO CIAO from being distributed freely using an open-source development model. You needn't inform anyone that you're using ACE TAO CIAO in your software, though we encourage you to let us know so we can promote your project in the ACE TAO CIAO success stories.

ACE TAO CIAO are provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, ACE TAO CIAO are provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies provide commercial support for ACE and TAO, however. ACE, TAO and CIAO are Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by ACE TAO CIAO or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE, TAO and CIAO web sites are maintained by the Center for Distributed Object Computing of Washington University for the development of open-source software as part of the open-source software community. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the ACE, TAO and CIAO software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source ACE TAO CIAO projects or their designees.

The names ACE(TM), TAO(TM), CIAO(TM), Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE(TM), TAO(TM), or CIAO(TM) nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Software bajo la Licencia de Apache

Este producto hace uso del software Apache siguiente:

- Apache Ant 1.6.5
- Apache Formatting Objects Processor (FOP) 0.95
- Apache Jakarta POI 3.0
- Apache Log4cplus 1.0.2
- Apache Log4j 1.2.15
- Apache Quartz 1.5.1
- Apache Xerces-C 2.6.0

Algunas partes de este producto incluyen software desarrollado por Apache Software Foundation. El software de Apache se distribuye de acuerdo con el siguiente acuerdo de licencia:

Licencia de Apache

Versión 2.0, enero de 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

'License' shall mean the terms and conditions for use, reproduction,and distribution as defined by Sections 1 through 9 of this document.

'Licensor' shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

'Legal Entity' shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, 'control' means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

'You' (or 'Your') shall mean an individual or Legal Entity exercising permissions granted by this License.

'Source' form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

'Work' shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work(an example is provided in the Appendix below).

'Derivative Works' shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

'Contribution' shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, 'submitted' means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as 'Not a Contribution.'

'Contributor' shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s)with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a 'NOTICE' text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an 'AS IS' BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

boost 1.35.0

Este producto incluye software distribuido bajo el siguiente Acuerdo de licencia:

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

JDOM 1.0

Este producto incluye software desarrollado por JDOM Project (http://www.jdom.org/). El software de JDOM se distribuye de acuerdo con el siguiente acuerdo de licencia.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact .

4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management .

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)." Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter and Brett McLaughlin . For more information on the JDOM Project, please see http://www.jdom.org.

PCRE 6.3

Algunas partes de este producto incluyen software desarrollado por Philip Hazel. El software de University of Cambridge Computing Service se distribuye de acuerdo con el siguiente acuerdo de licencia:

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

The "BSD" Licence

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"

AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Fin

Zlib 1.2.3

Este producto incluye zlib desarrollado por Jean-loup Gailly y Mark Adler.

ZThread 2.3.2

Algunas partes de este producto incluyen software desarrollado por Eric Crahen. El software de ZThread se distribuye de acuerdo con el siguiente acuerdo de licencia.