CA Enterprise Log Manager

Guía de implementación

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:

- Consideraciones acerca de la instalación para un sistema con unidades de SAN: en esta sección nueva se detallan los enfoques alternativos para prevenir la instalación de CA Enterprise Log Manager en una unidad de SAN. Esto resulta en un error de instalación.
- Asignaciones de puertos predeterminados: se ha agregado una descripción del puerto 53, el puerto de TCP/UDP conocido para sistema de nombre de dominio (DNS), a este tema existente.
- Configuración de la autenticación no interactiva para el archivado automático: esta sección se ha ampliado para describir el escenario típico de archivado de varios servidores de recopilación a un único servidor de informes. Para el escenario con un servidor de recopilación, un servidor de informes y un servidor de almacenamiento remoto; los ejemplos muestran la relación entre la autenticación no interactiva y la configuración de archivado automático correspondiente.
- Funcionamiento de la suscripción con proxy sin conexión: este tema se ha actualizado para abordar un sitio de FTP nuevo que contiene un archivo tar para cada Service Pack y versión de CA Enterprise Log Manager. Es posible descargarse el archivo tar y descomprimirlo en un proxy de suscripción sin conexión.
- Diagrama de flujo de la implementación de suscripción: este nuevo tema se ha agregado para proporcionar una referencia cruzada a la información acerca de la obtención de actualizaciones en un entorno sin conexión e invocación de actualizaciones a petición.
- El apéndice Consideraciones de CA IT PAM: este apéndice se refiere a las rutas de instalación a las cuales se ha hecho referencia previamente y que no son aplicables en todos los escenarios. Este punto se ha corregido. Se han modificado diversos temas en esta sección con el fin de mostrar que compartir un servidor de CA EEM entre CA Enterprise Log Manager y CA IT PAM no es compatible en el modo FIPS.
- Actualización de los servidores y los agentes de CA Enterprise Log Manager existentes: esta nueva sección describe el proceso para la actualización de servidores y agentes para la compatibilidad con FIPS, la conversión al modo FIPS y la verificación del modo FIPS para agentes mediante el cuadro de mandos de agente.
- Cómo agregar servidores de CA Enterprise Log Manager nuevos en una federación existente en el modo FIPS: en esta sección nueva se describen los procesos que se utilizan para agregar servidores nuevos a una federación existente que está ejecutándose en el modo con servidores de CA EEM tanto locales como remotos.

- Implementación de certificados personalizados: el tema existente se ha modificado para que refleje la nueva extensión .cer para certificados.
- Adición del certificado de raíz de confianza al servidor de gestión de CA Enterprise Log Manager: el tema existente se ha modificado para que refleje la nueva extensión .cer para certificados.
- Adición del certificado de raíz de confianza a todos los demás servidores de CA Enterprise Log Manager: el tema existente se ha modificado para que refleje la nueva extensión .cer para certificados.
- Adición del nombre común del certificado a una política de acceso: el tema existente se ha modificado para que refleje la nueva extensión .cer para certificados.
- Implementación de certificados nuevos: el tema existente se ha modificado para que refleje la nueva extensión .cer para certificados.
- Certificado de agente y agentes: este tema existente se ha modificado para que refleje la nueva extensión .cer para certificados.
- Restauración de un servidor de CA EEM para utilizar con CA Enterprise Log Manager: este tema existente se ha modificado para que refleje la nueva extensión .cer para certificados.
- Realización de una copia de seguridad de un servidor de CA Enterprise Log Manager: el tema existente se ha modificado para que refleje la nueva extensión .cer para certificados.
- Integración con CA Audit r8 SP2: los temas de esta sección se han eliminado porque CAELM4Audit no es compatible con r12.1 SP1 y posteriores.

Más información:

Funcionamiento de la suscripción con proxy sin conexión (en la página 59)
Certificado de agente y agentes (en la página 66)
Actualización de los servidores y agentes de CA Enterprise Log Manager para el soporte de FIPS (en la página 87)
Requisitos previos para la actualización de la compatibilidad con FIPS (en la página 90)
Directrices de actualización (en la página 90)
Actualización de un servidor de CA EEM remoto (en la página 91)
Desactive el acceso a ODBC y a JDBC en el almacenamiento de registro de eventos. (en la página 91)
Activación de la operación en modo FIPS (en la página 92)
Visualización del cuadro de mandos de los agentes (en la página 94)
Consideraciones acerca de la instalación para un sistema con unidades de SAN (en la página 97)
Desactive las unidades de SAN para realizar la instalación. (en la página 98)
Desactive las unidades de SAN. (en la página 99)
Establezca una configuración de múltiples rutas para el almacenamiento de SAN. (en la página 99)
Cree un volumen lógico (en la página 101)
Prepare el volumen lógico para CA Enterprise Log Manager (en la página 102)
Recicle el servidor de CA Enterprise Log Manager. (en la página 104)
Active las unidades de SAN para realizar la instalación (en la página 104)
Asignaciones de puertos predeterminados (en la página 108)
Desplazamiento de la base de datos y copia de seguridad del diagrama de flujo de estrategia (en la página 155)
Configuración de la autenticación no interactiva para el archivado automático (en la página 156)
Ejemplo: Configuración de la autenticación no interactiva para concentrador y periferia (en la página 157)
Configuración de las claves para el primer par de informes de recopilación (en la página 158)
Configuración de las claves para los pares de informes de recopilación adicionales (en la página 159)
Creación de un único archivo de clave pública en el servidor de informes y configuración de la propiedad de archivo (en la página 160)
Cómo validar la autenticación no interactiva entre servidores de informes y de recopilación. (en la página 162)
Creación de una estructura de directorios con propiedades en el servidor de almacenamiento remoto (en la página 162)
Configure las claves para el par de almacenamiento remoto de informes (en la página 163)
Configuración de propiedad de archivo clave en el servidor de almacenamiento remoto (en la página 164)
Cómo validar la autenticación no interactiva entre los servidores de informes y de almacenamiento (en la página 165)
Ejemplo: Configuración de una autenticación no interactiva en tres servidores (en la página 166)

Contenido

Capítulo 3: Instalación de CA Enterprise Log Manager 73

Capítulo 1: Introducción

Esta sección contiene los siguientes temas:

Acerca de esta guía

Esta *Guía de implementación de CA Enterprise Log Manager* proporciona las instrucciones necesarias para realizar la planificación, instalación y configuración de CA Enterprise Log Manager para recibir registros de eventos de los orígenes de eventos de la red. Esta guía está organizada de forma que las tareas comienzan con una descripción del proceso y de los objetivos. Normalmente, después de los procesos se incluyen conceptos relevantes y uno o más procedimientos para cumplir el objetivo.

La *Guía de implementación de CA Enterprise Log Manager* se ha diseñado para los administradores de sistemas encargados de instalar, configurar y mantener una solución de recopilación de registros, crear usuarios y asignar o definir funciones y accesos así como para realizar copias de seguridad de datos.

Esta guía también es útil para el personal que requiere información sobre alguno de los siguientes temas:

- Configuración de un conector o adaptador para recopilar datos de eventos
- Configuración de servicios para controlar la generación de informes, la retención de datos, las copias de seguridad y el archivado
- Configuración de una federación de servidores de CA Enterprise Log Manager
- Configuración de una suscripción para obtener contenidos, configuraciones y actualizaciones del sistema operativo

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

Sección	Descripción
Planificación del entorno	Describe las actividades de planificación para áreas como, por ejemplo, la recopilación de registros, agentes, federación, gestión de accesos y usuarios, actualizaciones de suscripción y recuperación de desastres.
Instalación de CA Enterprise Log Manager	Proporciona hojas de trabajo para recopilar la información necesaria y para obtener instrucciones detalladas sobre cómo instalar CA Enterprise Log Manager y sobre cómo realizar una

Sección	Descripción
	instalación correcta.
Configuración de accesos y usuarios básicos	Proporciona instrucciones para identificar un almacén de usuarios y para crear el usuario administrativo inicial para realizar la configuración de otros detalles de acceso y usuarios.
Configuración de servicios	Proporciona instrucciones para configurar servicios, incluidos los filtros locales y globales, el almacenamiento del registro de eventos, el servidor de informes y las opciones de suscripción.
Configuración de la recopilación de eventos	Proporciona conceptos e instrucciones sobre la utilización o configuración de los componentes de la biblioteca de refinamiento de eventos, incluidos los archivos de asignación y análisis y los adaptadores de CA.
Creación de federaciones	Describe distintos tipos de federaciones y proporciona instrucciones para crear relaciones federadas entre los servidores de CA Enterprise Log Manager y ver gráficos de federaciones.
Empleo de la biblioteca de refinamiento de eventos	Proporciona información muy útil sobre los archivos de asignación de datos y de análisis de mensajes.
Consideraciones sobre los usuarios de CA Audit	Describe las interacciones que puede implementar entre CA Enterprise Log Manager y CA Audit, cómo configurar iRecorders y políticas y cómo importar datos desde la base de datos del recopilador de CA Audit.
Consideraciones sobre los usuarios de CA Access Control	Describe cómo realizar la integración con CA Access Control, cómo modificar las políticas de CA Audit para enviar eventos a CA Enterprise Log Manager, cómo configurar CA Access Control iRecorder para enviar eventos a CA Enterprise Log Manager y cómo importar eventos de CA Access Control desde una base de datos de CA Audit Collector.
Consideraciones de CA IT PAM	Describe el proceso de instalación de CA IT PAM de forma que el componente de EEM en la gestión de CA Enterprise Log Manager se encarga de la autenticación.
Recuperación de desastres	Describe los procedimientos para realizar copias de seguridad, restauraciones y reemplazos para garantizar la recuperación de la solución de gestión de registros en caso de que se produzca un desastre.
CA Enterprise Log Manager y virtualización	Describe el proceso para utilizar, crear y configurar una máquina virtual para que contenga un servidor de CA Enterprise Log Manager.

Nota: Para obtener más información acerca de la compatibilidad del sistema operativo o acerca de los requisitos del sistema, consulte las *Notas de la versión*. Para obtener una descripción general de CA Enterprise Log Manager y su escenario de uso, consulte la *Guía de descripción de problemas*. Para obtener más información sobre el uso y mantenimiento del producto, consulte la *Guía de administración.* Para obtener ayuda acerca del uso de cualquier página de CA Enterprise Log Manager, vea la Ayuda en línea.

Capítulo 2: Planificación del entorno

Esta sección contiene los siguientes temas:

Planificación de servidores

El primer paso en la planificación de su entorno es determinar el número de servidores de CA Enterprise Log Manager que necesita y la función que realizará cada servidor. Entre las funciones, se incluyen las siguientes:

- Gestión

  Almacena las configuraciones y el contenido definido por el usuario. También autentica a los usuarios y autoriza el acceso a funciones.

- Recopilación

  Recibe registros de eventos de su agente; refina eventos.

- Generación de informes

  Procesa consultas en eventos recopilados, consultas e informes a petición así como alertas e informes programados.

- Punto de restauración

  Recibe bases de datos de registros de eventos restaurados para la investigación de eventos antiguos

El primer servidor que instala es el servidor de gestión; este servidor también puede realizar otras funciones. Puede tener un solo servidor de gestión en una única red de CA Enterprise Log Manager. Cada red de CA Enterprise Log Manager debe tener un servidor de gestión.

Entre las posibles arquitecturas, se incluyen las siguientes:

- Sistema con un solo servidor, donde el servidor de gestión realiza el resto de funciones.
- Sistema con dos servidores, donde el servidor de gestión realiza todas las funciones salvo la recopilación. La recopilación la realiza un servidor dedicado para esta función.
- Sistema con varios servidores, donde cada servidor tiene una determinada función.

A continuación, se muestran más detalles sobre las funciones y las arquitecturas de servidores.

Funciones de servidor

Un sistema de CA Enterprise Log Manager puede tener uno o varios servidores. La asignación de distintos servidores a distintas funciones optimiza el rendimiento. Sin embargo, puede utilizar cualquier servidor para realizar diversas funciones o todas las funciones, según lo desee. Tenga en cuenta la carga de procesamiento asociada a cada función de servidor respecto a otros factores relevantes de su entorno a la hora de determinar las asignaciones a cada servidor que instala.

- Servidor de gestión

  La función de servidor de gestión la realiza, de forma predeterminada, el primer servidor de CA Enterprise Log Manager que instala. Las funciones más importantes que realiza el servidor de gestión son las siguientes:

  - Actúa como repositorio habitual de todos los servidores que se registran con este servidor. En concreto, almacena usuarios de aplicaciones, grupos de aplicaciones (funciones), políticas, calendarios y AppObjects.
  - Si configura el almacén de usuarios como almacén interno, se almacenarán usuarios globales, grupos globales y políticas de contraseñas. Si el almacén de usuarios configurado hace referencia a un almacén de usuarios externo, cargará los detalles de la cuenta del usuario global y los detalles del grupo global desde el almacén de usuarios al que se hace referencia.
  - Gestiona titularidades de usuario con un archivo asignado a la memoria de alta velocidad. Autentica a los usuarios en el inicio de sesión en función de la configuración de usuarios o grupos. Permite que los usuarios accedan a diversas partes de la interfaz de usuario en función de las políticas y los calendarios.
  - Recibe todas las actualizaciones de contenido y configuración descargadas a través de la suscripción.

  En una red de servidores de CA Enterprise Log Manager, sólo puede haber un servidor de gestión activo, pero puede tener un servidor de gestión de conmutación por error (inactivo). Si crea más de una red de CA Enterprise Log Manager, cada una debe contar con su propio servidor de gestión activo.

- Servidor de recopilación

  En un sistema con un solo servidor, el servidor de gestión realiza la función de un servidor de recopilación. En un sistema con dos o más servidores, baraje la posibilidad de instalar un servidor de recopilación dedicado. Un servidor de recopilación realiza las siguientes funciones:

  - Admite la configuración de conectores.
  - Acepta los registros de eventos entrantes de los conectores en sus agentes.
  - Refina los registros de eventos entrantes, lo que implica el análisis de cada mensaje y la asignación de sus datos en formato CEG que permite la presentación uniforme de datos de eventos de distintos orígenes de eventos.
  - Inserta los registros de eventos en la base de datos caliente y comprime la base de datos caliente en una base de datos tibia cuando alcanza el tamaño configurado.
  - Autoarchiva la base de datos tibia en el servidor de informes relacionado según la programación configurada.

    Importante: Si define los servidores independientes en la recopilación y en los informes, deberá configurar la autenticación no interactiva y el archivado automático cada hora desde el servidor de recopilación hasta el servidor de informes.

  Tenga en cuenta el volumen de eventos generado por los orígenes de eventos a la hora de determinar si desea dedicar servidores para el refinamiento y la recopilación de eventos. También piense en el número de servidores de recopilación que van a autoarchivar sus datos en un único servidor de informes.

- Servidor de informes

  En un sistema con uno o dos servidores, el servidor de gestión realiza la función de un servidor de informes. En un sistema con varios servidores, baraje la posibilidad de dedicar uno o más servidores para la generación de informes. Un servidor de informes realiza las siguientes funciones:

  - Si la autenticación no interactiva y el archivado automático están configurados, recibirá nuevas bases de datos de eventos refinados desde los servidores de recopilación.
  - Procesa a petición informes, consultas y mensajes.
  - Procesa alertas e informes programados.
  - Admite asistentes para la creación de consultas e informes personalizados.
  - Si la autenticación no interactiva y el archivado automático se configuran desde el servidor de informes a un servidor de almacenamiento remoto, se moverán las bases de datos antiguas a un servidor de almacenamiento remoto.

  Si va a generar un gran número de informes y alertas complejos en un servidor con una gran actividad a petición, baraje la posibilidad de dedicar un servidor para la generación de informes.

- Servidor de almacenamiento remoto

  Un servidor de almacenamiento remoto, que no es un servidor de CA Enterprise Log Manager, realizar esta función:

  - Recibe, a intervalos configurados, bases de datos autoarchivadas muy comprimidas de servidores de informes antes de que estas bases de datos se eliminen debido a su antigüedad o a la falta de espacio libre en disco. El archivado automático evita la acción de mover manualmente las bases de datos.
  - Almacena bases de datos frías de forma local. También puede mover o copiar estas bases de datos a una ubicación externa para el almacenamiento a largo plazo. Normalmente, las bases de datos frías se retienen durante el número de años establecido por los organismos reguladores.

  Los servidores de almacenamiento remoto nunca forman parte de una federación de CA Enterprise Log Manager. No obstante, es importante tenerlos en cuenta cuando planifica una arquitectura.

- Servidor de punto de restauración

  Normalmente, los servidores de informes actúan como servidores de punto de restauración de las bases de datos que retuvieron en algún momento. Si su red es grande, baraje la posibilidad de dedicar un servidor de CA Enterprise Log Manager para esta función. Un servidor de punto de restauración realiza las siguientes funciones:

  - Se utiliza para investigar los registros de eventos antiguos.
  - Recibe las bases de datos restauradas desde un servidor de almacenamiento remoto que retiene todas las bases de datos frías. Se puede utilizar la utilidad restore-ca-elm.sh para mover las bases de datos al punto de restauración si configura primero la autenticación no interactiva desde el servidor de almacenamiento al punto de restauración.
  - Recataloga el catálogo de archivos para agregar las bases de datos restauradas a sus registros.
  - Retiene registros de distintos períodos de tiempo en función del método de restauración.

  La ventaja de contar con un punto de restauración dedicado es que puede excluir este servidor de la federación para que ningún informe federado contenga datos restaurados antiguos. Todos los informes generados en el servidor de punto de restauración sólo reflejan los datos de eventos de las bases de datos restauradas.

La dedicación de un servidor a una determinada función no implica que pueda realizar funciones desde éste relacionadas con otras funciones. Piense en un entorno con servidores de recopilación dedicados y con un servidor de informes. Si desea programar una alerta para comprobar una condición en un servidor de recopilación porque es crucial que sea notificado lo antes posible, cuenta con esta flexibilidad.

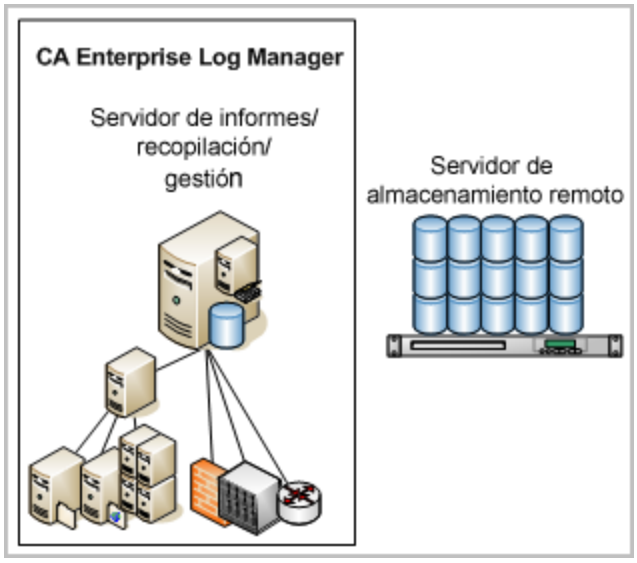
Ejemplo: arquitecturas de red

La arquitectura de CA Enterprise Log Manager más sencilla es un sistema con un solo servidor, donde un servidor de CA Enterprise Log Manager realiza todas las funciones:

- El servidor de CA Enterprise Log Manager de gestión, recopilación e informes realiza la gestión de configuración/contenido y recopilación/refinamiento de eventos, además de gestionar las consultas e informes.

  Nota: Un servidor remoto que no es de CA Enterprise Log Manager almacena las bases de datos de registros de eventos almacenados.

Esta configuración es adecuada para el procesamiento de un volumen de eventos pequeño y de pocos informes programados, como en un sistema de prueba.

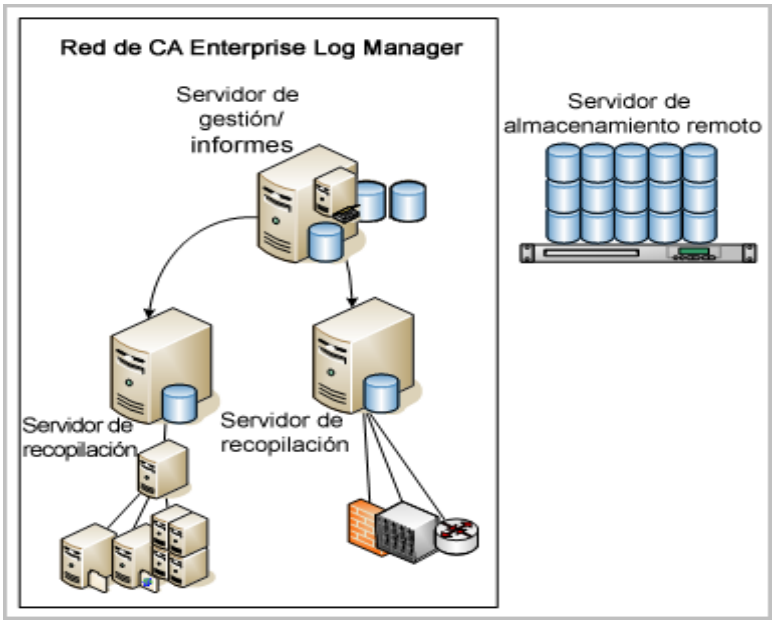


La siguiente arquitectura más sencilla es un sistema de varios servidores donde el primer servidor de CA Enterprise Log Manager instalado realiza la mayor parte de las funciones:

- El servidor de CA Enterprise Log Manager de gestión e informes realiza la gestión de la configuración/contenido y gestiona las consultas y los informes.
- El servidor de recopilación de CA Enterprise Log Manager gestiona la recopilación y el refinamiento de eventos.

Nota: Un servidor remoto que no es de CA Enterprise Log Manager está configurado para almacenar bases de datos almacenadas de registros de eventos.

Esta arquitectura es adecuada para una red con un volumen moderado de eventos. Las flechas muestran que la funcionalidad de gestión del servidor de gestión/informes conserva la configuración global que se aplica a todos los servidores. Cuando hay muchos servidores de recopilación, esta arquitectura se denomina "concentrador y periferia".

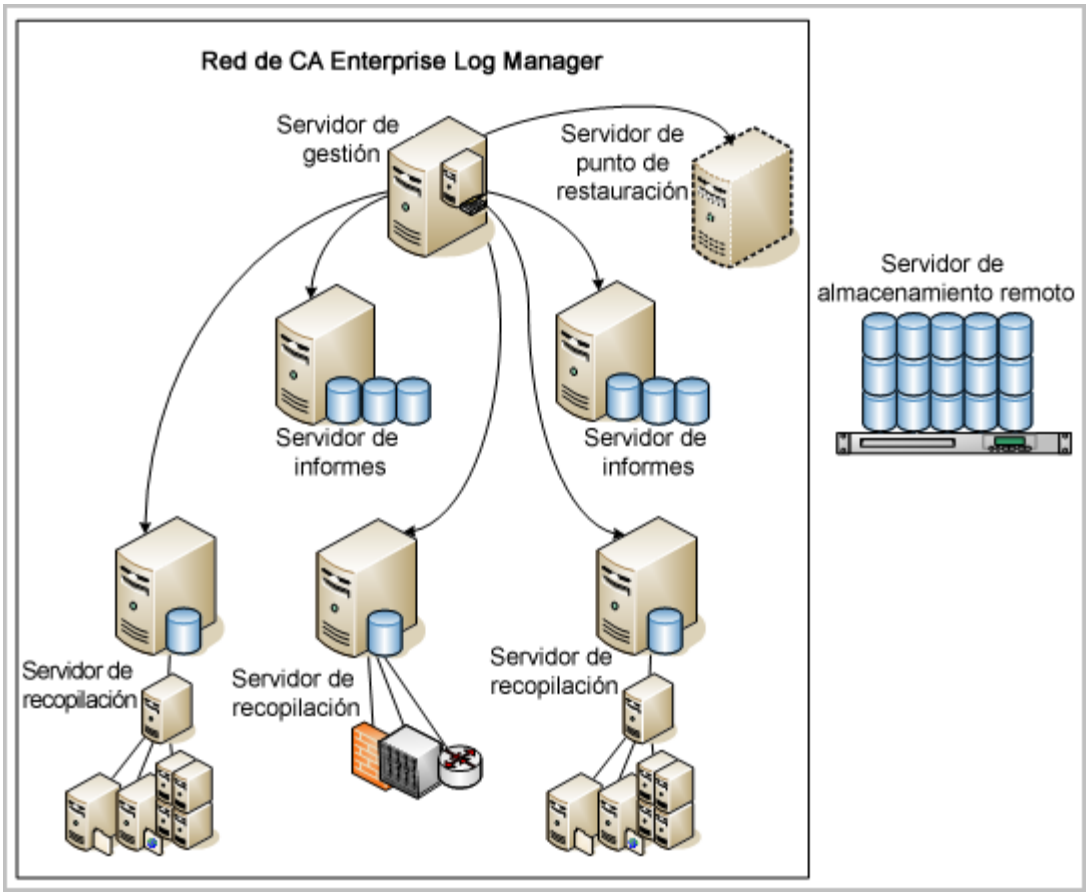


En una red con un gran volumen de eventos, un gran número de informes y alertas complejos programados y una personalización continua, puede asignarle a uno o varios servidores de CA Enterprise Log Manager diversas funciones específicas:

- El servidor de CA Enterprise Log Manager de gestión realiza la gestión de la configuración/contenido.
- El servidor de informes de CA Enterprise Log Manager gestiona las consultas y los informes.
- El servidor de recopilación de CA Enterprise Log Manager gestiona la recopilación y el refinamiento de eventos.
- De forma opcional, un servidor de punto de restauración de CA Enterprise Log Manager gestiona la investigación de eventos de las bases de datos de almacenamiento restauradas.

Nota: Un servidor remoto que no es de CA Enterprise Log Manager está configurado para almacenar bases de datos almacenadas de registros de eventos.

Esta configuración es ideal para redes de gran tamaño. Las flechas muestran que el servidor de gestión conserva la configuración global que se aplica a todos los servidores.



Planificación de la recopilación de registros

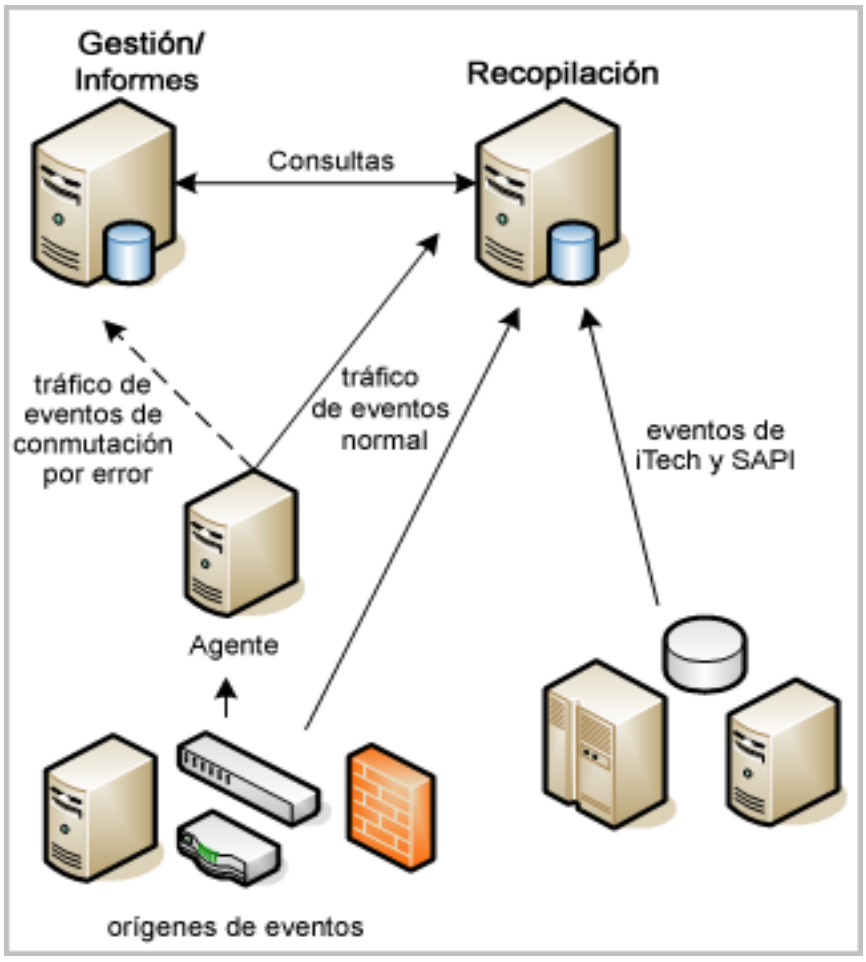
La planificación de recopilación de registros se basa en una serie de eventos por segundo (EPS) que necesita procesar para realizar el almacenamiento y en el tiempo necesario para que los datos se mantengan en línea (en este sentido, *en línea* se refiere a un estado de búsqueda inmediato). Normalmente, los datos en línea sólo son válidos unos 30-90 días.

Cada red cuenta con sus propios volúmenes de eventos según el número de dispositivos, los tipos de dispositivos y el nivel de ajuste de las aplicaciones y de los dispositivos de red, como los cortafuegos, para cumplir las necesidades de información de eventos de la empresa. Por ejemplo, algunos cortafuegos pueden generar volúmenes enormes de eventos innecesarios en función de su configuración.

Le recomendamos que planifique la recopilación de eventos de modo que el volumen total de eventos se expanda uniformemente por los servidores de CA Enterprise Log Manager sin forzar ninguno de ellos y sin que se supere el índice constante normal. Para mantener un rendimiento máximo en los volúmenes de eventos de la empresa, le recomendamos que instale al menos dos servidores de CA Enterprise Log Manager federados:

- Un servidor de informes de CA Enterprise Log Manager se encarga de las consultas e informes, alertas y gestión de alertas, actualizaciones de suscripciones y autorización y autenticación de usuario.
- Uno o más servidores de recopilación de CA Enterprise Log Manager se configuran específicamente para maximizar las inserciones en la base de datos.

La siguiente ilustración muestra un ejemplo simple de este tipo de red de CA Enterprise Log Manager federada. Los dos servidores de CA Enterprise Log Manager, uno de informes y otro de recopilación, controlan el tráfico de eventos de diversos orígenes de eventos. Ambos servidores pueden compartir datos entre ellos para procesar consultas e informes y gestionar alertas.



El servidor *de recopilación* controla principalmente el tráfico de registro de eventos entrantes y se centra en las inserciones en la base de datos. Utiliza una política de retención de datos corta de 24 horas o menos. Un script automatizado mueve los registros de eventos almacenados a un servidor de informes diariamente o con mayor frecuencia en función del volumen de eventos. La federación y la utilización de consultas federadas entre los dos servidores le garantiza que reciba informes precisos de los registros de eventos en *ambos* servidores.

El servidor *de informes* realiza varias funciones:

- Procesa consultas e informes
- Programa y gestiona alertas
- Mueve archivos almacenados a un servidor de almacenamiento remoto
- Proporciona una recopilación de conmutación por error de los eventos recopilados por el conector para el servidor de recopilación

Un script de copia de seguridad automatizado mueve los datos del servidor de informes a un servidor remoto (almacenamiento en frío). Si decide restaurar los datos desde el almacenamiento en frío, normalmente lo hará en el servidor de informes. Si el espacio en el servidor de informes es limitado, también podrá realizar la restauración en el servidor de recopilación. Dado que el servidor de recopilación no almacena grandes cantidades de datos y está federado, los resultados del informe son idénticos.

Además, el servidor de informes puede funcionar como un receptor de conmutación por error de los eventos recopilados por un conector en un agente remoto si el servidor de recopilación deja de recibir eventos por algún motivo. Puede configurar la conmutación por error al nivel de agente. El procesamiento de conmutación por error envía eventos a uno o más servidores de CA Enterprise Log Manager alternativos. La recopilación de eventos de conmutación por error no está disponible para los eventos de orígenes de eventos heredados recopilados a través de las escuchas de SAPI e iTech.

Más información:

CA Enterprise Log Manager y virtualización (en la página 293)

Planificación del espacio en disco

Cuando planifique su entorno, compruebe que dispone de suficiente espacio en disco para admitir grandes volúmenes de eventos. En el servidor de recopilación, es necesario disponer de suficiente espacio en disco en cada servidor de recopilación para poder dar cabida a las cargas compartidas y a las cargas más altas así como a los volúmenes de eventos estándar. En un servidor de informes, el espacio en disco se calcula en función del volumen de eventos y del período de retención en línea requerido.

Las bases de datos calientes no se comprimen. Las bases de datos tibias sí se comprimen. Se considera que las bases de datos calientes y tibias están en línea. Puede realizar búsquedas o generar informes sobre sus datos. Normalmente, los datos estarán listos entre 30 y 90 días y podrá generar informes y realizar búsquedas inmediatas en cualquier momento. Los registros más antiguos se almacenan en un servidor remoto. Puede restaurarlos para realizar búsquedas y generar informes.

Los servidores de recopilación admiten bases de datos calientes y tibias. Dado que el período de retención de un servidor de recopilación es muy breve, de una a 23 horas, el almacenamiento a largo plazo no es un factor a tener en cuenta.

En un servidor de gestión, hay una base de datos caliente para la inserción de mensajes de eventos autocontrolados.

Los servidores de informes admiten bases de datos calientes más pequeñas y un gran número de bases de datos tibias. Los servidores de informes también deben disponer de espacio adicional suficiente para admitir archivos restaurados durante un determinado período de tiempo. Cuando utiliza el almacenamiento conectado directo, las particiones se amplían automáticamente para permitir una mayor capacidad de almacenamiento.

Acerca del servidor de CA EEM

CA Enterprise Log Manager utiliza el servidor de CA Embedded Entitlements Manager (CA EEM) internamente para gestionar configuraciones, autorizar y autenticar usuarios, coordinar actualizaciones de suscripción de contenido y binarios y realizar otras funciones de gestión. En el entorno básico de CA Enterprise Log Manager, usted instala CA EEM cuando instala el servidor de gestión de CA Enterprise Log Manager. Desde ahí, CA EEM gestiona las configuraciones de todos los servidores de recopilación de CA Enterprise Log Manager así como sus agentes y conectores.

También puede instalar el servidor de CA EEM en un servidor remoto utilizando los paquetes de instalación proporcionados en el disco de instalación de la aplicación, o utilizar un servidor de CA EEM existente si está utilizando uno con otros productos de CA.

El servidor de CA EEM proporciona su propia interfaz Web. No obstante, casi todas las actividades de configuración y mantenimiento se desarrollan en la interfaz de usuario de CA Enterprise Log Manager. No debería ser necesario interactuar directamente con las funciones incrustadas del servidor de CA EEM excepto con las configuraciones de conmutación por error y con las funciones de copia de seguridad y restauración que forman parte de la recuperación de desastres.

Nota: La instalación del servidor de CA Enterprise Log Manager requiere que utilice la contraseña de la cuenta de administración predeterminada de CA EEM, EiamAdmin, para registrar correctamente un servidor de CA Enterprise Log Manager. Cuando instala el primer servidor de gestión de CA Enterprise Log Manager, crea esta nueva contraseña como parte de la instalación. Cuando instala otros servidores de CA Enterprise Log Manager utilizando el mismo nombre de instancia de aplicación, creará automáticamente un entorno de red en el que, posteriormente, podrá configurar relaciones de federación entre los servidores de CA Enterprise Log Manager.

Directrices de la recopilación de registros

Tenga en cuenta las siguientes directrices de la recopilación de registros durante la fase de planificación:

- El tráfico desde el agente al servidor de CA Enterprise Log Manager siempre está cifrado, ya se utilice una recopilación de registros sin agentes o basada en agentes.
- Considere la opción de emplear un mecanismo de recopilación local de syslog como solución alternativa ante los posibles problemas de la entrega garantizada.

A la hora de determinar si desea utilizar la recopilación directa mediante el agente predeterminado, la recopilación basada en agente donde el agente se instala en el host con el origen de eventos, o la recopilación sin agente donde el agente se instala en un punto de recopilación alejado de los orígenes de eventos, considere estos factores:

- Compatibilidad con la plataforma

  Por ejemplo, WMI sólo admite Windows con el sensor de registro.
- Compatibilidad del controlador con determinados sensores de registros

  Por ejemplo, es necesario un controlador ODBC para que ODBC funcione.
- Si se puede acceder al origen de registros de forma remota

  Por ejemplo, con los registros basados en archivos, necesita una unidad compartida para los que funcionen de forma remota.

Planificación de federación

En CA Enterprise Log Manager, una *federación* es una red de servidores que almacena datos de eventos, genera informes sobre datos de eventos y archiva estos datos. Una federación le permite controlar el modo en que se agrupan y se revisan los datos de una red. Puede configurar el modo en que sus servidores se relacionan con otros y, además, el modo en que se envían las consultas de un servidor a otro. Por otro lado, puede activar y desactivar consultas federadas para consultas específicas según sea necesario.

La decisión de utilizar una federación se basa en el volumen de eventos requerido y en sus necesidades empresariales para separar y generar informes sobre datos de registro. CA Enterprise Log Manager admite federaciones jerárquicas y en malla así como configuraciones que combinan los dos tipos. Todos los servidores de CA Enterprise Log Manager que desee federar deben utilizar el mismo nombre de instancia de aplicación de CA EEM. Cada instalación del servidor de CA Enterprise Log Manager se registra automáticamente con el servidor de CA EEM utilizando un nombre de instancia de aplicación.

Puede configurar una federación en cualquier momento después de instalar el primer servidor de CA Enterprise Log Manager y, al menos, otro servidor más. No obstante, los mejores resultados se derivan de llevar a cabo una planificación *antes de* la instalación. Con la creación de un mapa de federación detallado, podrá completar las tareas de configuración de forma rápida y precisa.

En el nivel de *red*, si dispone de varios servidores de CA Enterprise Log Manager, puede gestionar volúmenes de eventos mayores. Desde la perspectiva de *generación de informes*, la utilización de una federación le permite controlar quién puede acceder a los datos de eventos y qué cantidad de datos pueden ver.

En un entorno básico de dos servidores, el servidor de gestión adopta la función de servidor de informes. El servidor de CA EEM interno del servidor de gestión de CA Enterprise Log Manager gestiona las configuraciones de la federación central y globalmente (puede cambiar las opciones de configuración desde cualquier servidor de CA Enterprise Log Manager de la red). Configure el servidor de recopilación de CA Enterprise Log Manager como servidor de informes secundario de modo que las consultas y los informes incluyan los datos más recientes.

Nota: Si cuenta con un servidor de CA EEM que va a utilizar con CA Enterprise Log Manager, configure los servidores de CA Enterprise Log Manager del mismo modo. El servidor de CA EEM remoto y dedicado almacena estas configuraciones.

También puede configurar las opciones de configuración local para que sobrescriban la configuración global de modo que los servidores de CA Enterprise Log Manager seleccionados funcionen de un modo distinto al resto. Por ejemplo, el envío de alertas e informes de correo electrónico a través de un servidor de correo diferente o la programación de informes de una rama de la red a distintas horas.

Más información:

Federaciones jerárquicas (en la página 212)
Federaciones en malla (en la página 214)
Consultas e informes en un entorno federado (en la página 211)
Configuración de una federación de CA Enterprise Log Manager (en la página 215)

Creación de un mapa de federación

La creación de un mapa de federación es un paso útil en la planificación y en la implementación de la configuración de la federación. Cuanto mayor sea la red, más útil será este mapa durante las tareas reales de configuración. Puede utilizar cualquier programa de diseño gráfico o puede esbozar el mapa a mano. Cuantos más detalles añada al mapa, con mayor rapidez realizará la configuración.

Para crear un mapa de federación

1. Inicie el mapa con dos servidores básico de CA Enterprise Log Manager, de gestión y recopilación, e incluya los detalles de cada uno.
2. Decida si necesita más servidores de recopilación y si representan la parte superior de una jerarquía o de una unidad en una federación en malla.
3. Decida el tipo de federación que mejor se ajuste a sus necesidades: jerárquica o en malla.
4. Identifique las oportunidades de las jerarquías, ramas o interconexiones en función de las necesidades de informes empresariales, de los requisitos de conformidad y del rendimiento de eventos.

   Por ejemplo, si su empresa cuenta con oficinas en tres continentes, es posible que decida crear tres federaciones jerárquicas. También puede decidir combinar las jerarquías a un nivel superior de modo que los ejecutivos que tienen mayor responsabilidad y la gestión de seguridad puedan generar informes que alcancen toda la red. Debe federar como mínimo los servidores de inserción y consultas de CA Enterprise Log Manager del entorno básico.
5. Decida cuántos servidores de CA Enterprise Log Manager totales necesita implementar.

   Este valor se basa en el número de dispositivos de la red y en el volumen de eventos que generan.
6. Decida el número de capas de servidores federados que necesita.

   Este número se basa en las decisiones tomadas en los pasos dos y tres.
7. Identifique los tipos de eventos que recibe cada uno de los servidores de CA Enterprise Log Manager en la federación.

   Si su red cuenta con un amplio número de dispositivos basados en syslog y sólo con unos pocos servidores de Windows, es posible que decida asignar expresamente un servidor de CA Enterprise Log Manager para la recopilación de eventos de Windows. Además, es posible que necesite varios servidores para que gestionen el tráfico de eventos syslog. La planificación con antelación de los tipos de eventos que reciben los servidores de CA Enterprise Log Manager facilita la configuración de los servicios y las escuchas locales.

8. Esboce un mapa de esta red para utilizar durante la configuración de los servidores de CA Enterprise Log Manager federados (secundarios).

   Incluya los nombres DNS y las direcciones IP en el mapa, si los sabe. Utilizará los nombres DNS de los servidores de CA Enterprise Log Manager para configurar las relaciones de federación entre ellos.

Ejemplo: Mapa de federación para una gran empresa

Cuando cree un mapa de federación, tenga en cuenta los distintos tipos de informes para los que desea diversos conjuntos de datos consolidados. Por ejemplo, piense en un escenario donde desea que los datos consolidados utilicen tres tipos de agrupaciones de servidores:

- Todos los servidores

  Para los informes del sistema en eventos autocontrolados, incluidos todos los servidores. Le permite evaluar el estado de toda su red de servidores de CA Enterprise Log Manager al mismo tiempo.

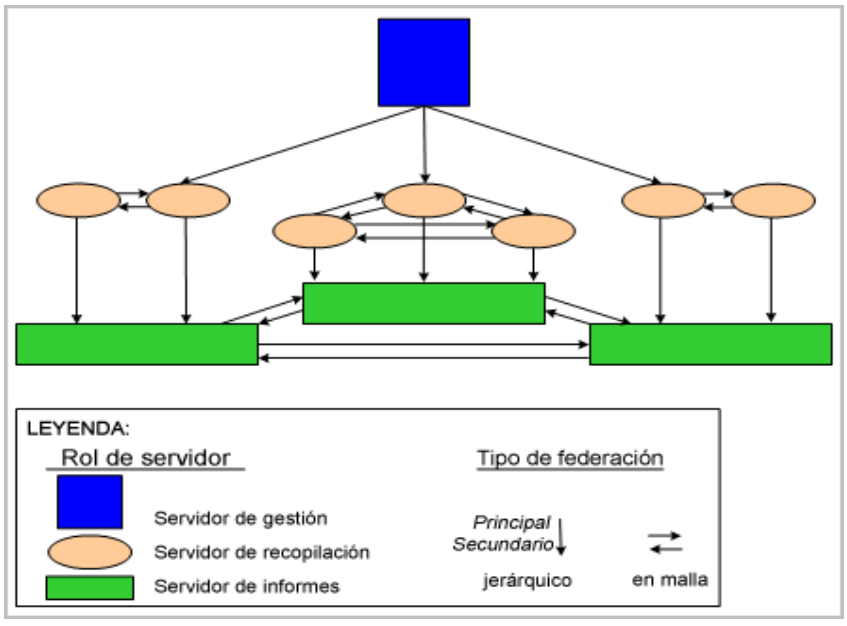
- Todos los servidores de informes

  Para los informes de resumen y de tendencias en los que desee examinar los datos recopilados por todos los agentes que envían datos a todos los servidores de recopilación al tiempo que los servidores de recopilación procesan consultas en nuevos eventos calientes, es necesario que ejecute informes federados que sólo incluyan servidores de informes.

- Un conjunto de servidores de recopilación con su servidor de informes

  Para los informes en los que desee limitar los datos a una configuración regional con un servidor de informes, pero desea que el informe incluya los eventos que todavía no han sido enviados a ese servidor por sus servidores de recopilación, es necesario que ejecute informes federados en este subconjunto de servidores.

A continuación, se muestra una mapa de federación que le permite cumplir estos objetivos:



Para implementar el diseño de este mapa de federación, deber seguir estos pasos:

- Cree una federación jerárquica desde el servidor de gestión con un servidor de recopilación relacionado con cada servidor de informes, donde el servidor de gestión es el principal y, cada servidor de recopilación, el secundario.
- Cree una federación en malla entre los servidores de recopilación para cada servidor de informes.
- Cree una federación jerárquica desde cada servidor de recopilación con su servidor de informes, donde el servidor de recopilación es el principal y, el servidor de informes, el secundario.
- Cree una federación en malla entre los servidores de informes.

Para cumplir un determinado objetivo de informes, es importante ejecutar el informe desde un servidor representado por una ubicación específica en el mapa de federación. A continuación, se muestran algunos ejemplos:

- Para generar un informe del sistema sobre los eventos autocontrolados que se generan en cada servidor de CA Enterprise Log Manager de la red, ejecute el informe desde el servidor de gestión.
- Para generar informes de resumen y de tendencias desde todos los servidores de informes de la red, ejecute el informe desde cualquier servidor de informes.
- Para generar un informe sobre los datos que residen en un servidor de informes y en sus servidores de recopilación, ejecute el informe desde uno de estos servidores de recopilación.

Ejemplo: Mapa de federación para una empresa mediana

Antes de crear un mapa de federación, determine el número de servidores que pretende dedicar a cada rol de servidor. En el ejemplo siguiente, un servidor está dedicado a la gestión y la generación de informes, mientras que los demás servidores están dedicados a la recopilación. Esta configuración es recomendable para un entorno de tamaño medio. Puede imaginar la arquitectura del servidor de gestión/informes y los servidores de recopilación como de concentrador y periferia, donde el servidor de gestión/informes es el concentrador. El diagrama del mapa de federación no refleja esta configuración; en su lugar, muestra los niveles para que puede distinguir fácilmente los pares federados de forma jerárquica de los pares en malla.

Cuando cree un mapa de federación, tenga en cuenta los informes y las alertas para los que desea diversos conjuntos de datos consolidados. Por ejemplo, piense en un escenario donde desea que los datos consolidados utilicen dos tipos de agrupaciones de servidores:

- Sólo el servidor de gestión/informes

  Para la mayoría de los informes, en los que desea examinar los eventos recientemente archivados (tibios) mientras evita que los servidores de recopilación procesen consultas de eventos nuevos (calientes)

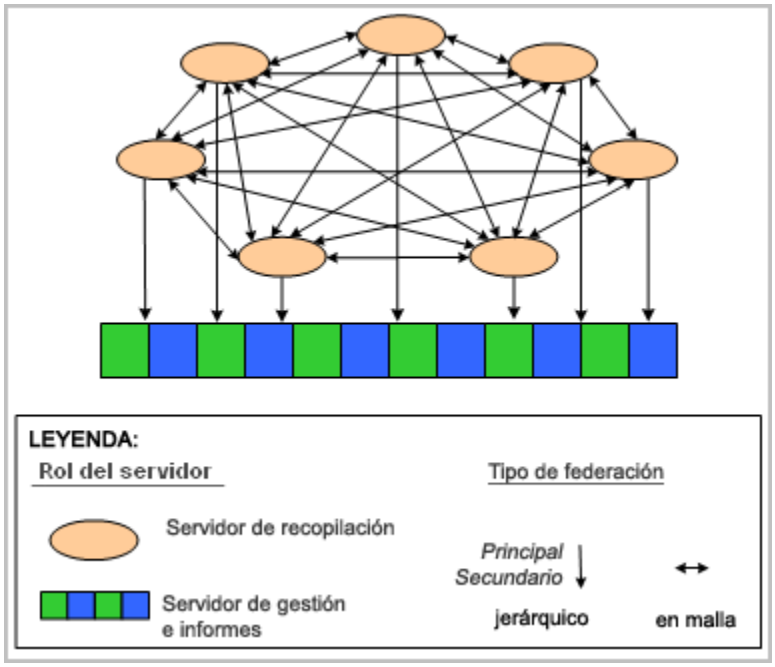
  Nota: Los eventos se suelen guardar desde servidores de recopilación (periferias) en el servidor de informes (concentrador) cada hora.

- Todos los servidores

  Para informes del sistema sobre eventos autocontrolados, en los que desea evaluar el estado de todos los servidores de CA Enterprise Log Manager a la vez

  Para alertas, en las que es importante realizar consultas de eventos nuevos de todos los servidores de recopilación

A continuación, se muestra una mapa de federación que le permite cumplir estos objetivos:



Para implementar el diseño de este mapa de federación, deber seguir estos pasos:

- Cree una federación en malla entre los servidores de recopilación. (Cada servidor de recopilación es tanto principal como secundario para los demás servidores de recopilación.)
- Cree una federación jerárquica de cada servidor de recopilación al servidor de gestión/informes, donde el servidor de recopilación es el principal y, el servidor de gestión/informes, el secundario.

Para cumplir con un objetivo determinado, es importante ejecutar el informe o la alerta desde un servidor representado por una ubicación determinada en el mapa de federación y especificar correctamente si es necesaria la federación. A continuación, se muestran algunos ejemplos:

- Para programar un informe del sistema sobre los eventos autocontrolados que se generan en cada servidor de CA Enterprise Log Manager de la red, ejecute el informe desde el servidor de gestión/informes y especifique la federación.
- Para programar un informe sobre eventos recientes (tibios), ejecute el informe desde el servidor de gestión/informes y elimine la consulta de federación. Estos informes incluyen datos recientemente archivados recopilados por todos los servidores de recopilación. No es necesaria la federación.
- Para programar una alerta que incluya eventos nuevos (calientes) de cada servidor de recopilación y eventos archivados (tibios) en el servidor de gestión/informes, ejecute la alerta desde cualquier servidor de recopilación y especifique la federación. Puede limitar los resultados obtenidos en los servidores de recopilación mediante la especificación del intervalo predefinido, que define los resultados de la última hora.

Más información:

Configuración de un servidor de CA Enterprise Log Manager como servidor secundario (en la página 216)
Funciones de servidor (en la página 23)
Ejemplo: Almacenamiento automático en tres servidores (en la página 167)

Planificación de acceso y usuarios

Después de instalar el primer servidor de CA Enterprise Log Manager y acceder a él como usuario de EiamAdmin, podrá configurar el almacén de usuarios, configurar un usuario como administrador y establecer políticas de contraseñas.

La planificación de acceso y usuarios se limita a lo siguiente:

- Determinar si desea aceptar el almacén de usuarios predeterminado en este servidor de CA Enterprise Log Manager o configurar un almacén de usuarios externo. Si es necesaria la configuración, registre los valores requeridos en las hojas de trabajo suministradas.
- Identificar al usuario que actuará como primer administrador. Sólo un administrador puede configurar los parámetros de CA Enterprise Log Manager.
- Definir las políticas de contraseñas para que los usuarios de CA Enterprise Log Manager utilicen contraseñas seguras.

  Nota: Sólo puede configurar políticas de contraseñas cuando configura el almacén de usuarios como el almacén de usuarios en este CA Enterprise Log Manager.

Más información:

Hoja de trabajo del directorio de LDAP (en la página 45)
Hoja de trabajo de CA SiteMinder (en la página 46)

Planificación del almacén de usuarios

Una vez instalado el primer servidor de CA Enterprise Log Manager, inicie sesión en CA Enterprise Log Manager y configure el almacén de usuarios. El almacén de usuarios configurado es donde se almacenan nombres y contraseñas de usuario, utilizados para realizar la autenticación, y otros detalles globales.

Junto con todas las opciones del almacén de usuarios, los detalles de usuarios de aplicaciones se almacenan en el almacén de usuarios de CA Enterprise Log Manager. Entre esta información, se incluyen las funciones, los favoritos del usuario y la hora del último inicio de sesión.

Tenga en cuenta lo que se indica a continuación a la hora de planificar la configuración del almacén de usuarios:

- Utilice el almacén de usuarios de CA Enterprise Log Manager (predeterminado)

  Los usuarios están autenticados con nombres y contraseñas de usuario creados en CA Enterprise Log Manager. Puede configurar las políticas de contraseñas. Los usuarios pueden cambiar sus propias contraseñas y desbloquear las cuentas de otros usuarios.

- Referencia desde CA SiteMinder

  Los nombres de usuario, contraseñas y grupos globales se cargan desde CA SiteMinder en el almacén de usuarios de CA Enterprise Log Manager. Los usuarios se autentican con los nombres y contraseñas de usuario utilizados. Puede asignar el grupo global a una política nueva o existente. No puede crear nuevos usuarios, cambiar contraseñas ni configurar políticas de contraseñas.

- Referencia desde el directorio de LDAP (protocolo ligero de acceso a directorios)

  Los nombres y contraseñas de usuario se cargan desde el directorio de LDAP en el almacén de usuarios de CA Enterprise Log Manager. Los usuarios se autentican con los nombres y contraseñas de usuario utilizados. La información de cuenta del usuario cargado pasa a formar parte de las cuentas de usuarios globales. Puede asignar a los usuarios globales una función de usuario que se corresponda con el acceso que desee que tengan en CA Enterprise Log Manager. No puede crear nuevos usuarios ni configurar políticas de contraseñas.

Importante: Le recomendamos que realice copias de seguridad de las políticas de acceso predefinidas proporcionadas con CA Enterprise Log Manager antes de que usted o cualquier otro administrador comience a trabajar con ellas. Para obtener más información, consulte la *Guía de administración de CA Enterprise Log Manager*.

Más información:

Aceptación del almacén de usuarios predeterminado (en la página 136)
Utilización de un directorio de LDAP (en la página 137)
Utilización de CA SiteMinder como almacén de usuarios (en la página 138)

Hoja de trabajo del directorio de LDAP

Antes de consultar un directorio de LDAP externo, recopile la información de configuración que se muestra a continuación:

Información obligatoria	Valor	Comentarios
Tipo		Observe el tipo de directorio que esté utilizando. CA Enterprise Log Manager admite diversos directorios entre los que se incluyen Microsoft Active Directory y Sun ONE Directory.º Consulte la interfaz de usuario para obtener una lista completa de directorios admitidos.
Host		Registre el nombre de host del servidor del directorio o del almacén de usuarios externo.
Puerto		Registre el nombre de puerto en el que el almacén de usuarios externo o el servidor del directorio realiza la escucha. El puerto 389 es el puerto conocido de LDAP (protocolo ligero de acceso a directorios). Si su servidor de registro no utiliza el puerto 389, registre el número de puerto correcto.
DN de base		Registre el nombre completo de LDAP (DN) que se utiliza como base. El DN es un identificador único de una entrada de una estructura de árbol del directorio de LDAP. En este DN de base no se admiten espacios. Sólo los grupos y los usuarios globales detectados debajo de este DN se asignan y se pueden asignar a una función o a un grupo de aplicación de CA Enterprise Log Manager.
Contraseña		Introduzca y confirme la contraseña del usuario enumerado en la fila DN de usuario.
DN de usuario		Introduzca las credenciales válidas de cualquier usuario válido del registro de usuarios cuyo registro se puede buscar. Introduzca el nombre completo (DN) del usuario. Puede iniciar sesión con cualquier ID de usuario con las funciones de administrador. El DN de usuario y la contraseña asociada son las credenciales utilizadas que hay que adjuntar al host del directorio externo.

Información obligatoria	Valor	Comentarios
Utilización de Transport Layer Security (TLS)		Especifica si el almacén de usuarios va a utilizar el marco de trabajo de TSL para proteger las transmisiones de texto sin formato. Cuando se selecciona, TLS se utiliza cuando se realiza la conexión de LDAP con el directorio externo.
Inclusión de atributos sin asignar		Especifica si desea incluir campos no sincronizados desde el directorio de LDAP. Los atributos externos no asignados se pueden utilizar para realizar búsquedas y como filtros.
Usuarios globales en caché		Especifica si desea almacenar usuarios globales en la memoria para lograr un acceso rápido. Esto acelera las búsquedas, a expensas de la escalabilidad. En un entorno de pruebas pequeño, se recomienda la selección.
Tiempo de actualización de caché		Si ha seleccionado Usuarios globales en caché, especifique la frecuencia, en minutos, para realizar la actualización de los usuarios y de los grupos globales en caché e incluir los registros nuevos y cambiados.
Recuperación de grupos de intercambio como grupos de usuarios globales		Si el tipo de directorio externo es Microsoft Active Directory, esta opción especifica que desea crear grupos globales desde la información del grupo de Microsoft Exchange Si se selecciona, podrá escribir políticas para los miembros de las listas de distribución.

Hoja de trabajo de CA SiteMinder

Antes de utilizar CA SiteMinder como almacén de usuarios, recopile la siguiente información de configuración:

Información obligatoria	Valor	Comentarios
Host		Especifica el nombre de host o la dirección IP del sistema CA SiteMinder utilizado. Puede utilizar direcciones IP IPv4 o IPv6.
Nombre de administrador		El nombre de usuario del superusuario de CA SiteMinder que realiza el mantenimiento del sistema y de los objetos de dominio.
Contraseña de administrador		La contraseña del nombre de usuario asociado.
Agent Name		El nombre del agente proporcionado por el servidor de políticas. El nombre no distingue

Información obligatoria	Valor	Comentarios
		mayúsculas de minúsculas.
Agent Secret		El secreto compartido distingue mayúsculas de minúsculas tal y como se define en CA SiteMinder. Agent Secret distingue mayúsculas de minúsculas.
Usuarios globales en caché		Especifica si los usuarios globales se almacenan en memoria caché de modo que se puedan realizar búsquedas más rápidas a expensas de la escalabilidad. **Nota:** Los *grupos* de usuarios globales siempre se almacenan en caché.
Tiempo de actualización de caché		Intervalo en minutos tras el que la caché del usuario se actualiza automáticamente.
Inclusión de atributos sin asignar		Especifica si se incluyen atributos externos que no están asignados para utilizarse como filtros o en búsquedas.
Recuperar los grupos de intercambio como grupos de usuarios globales		Si el tipo de directorio externo es Microsoft Active Directory, esta opción especifica que desea crear grupos globales desde la información del grupo de Microsoft Exchange. Si se selecciona, podrá escribir políticas para los miembros de las listas de distribución.
Tipo del almacén de autorizaciones		Define el tipo de almacén de usuarios en uso.
Nombre del almacén de autorizaciones		Especifica el nombre asignado del almacén de usuarios utilizado en el campo Tipo de almacén de autorizaciones.

Usuarios con función de administrador

Sólo los usuarios a los que se les ha asignado la función de administrador pueden configurar componentes de CA Enterprise Log Manager.

Una vez instalado el primer CA Enterprise Log Manager, podrá acceder al servidor de CA Enterprise Log Manager a través de un explorador, iniciar sesión con las credenciales de EiamAdmin y configurar el almacén de usuarios.

El siguiente paso es asignar el grupo de aplicaciones del administrador a la cuenta del usuario que va a realizar la configuración. Si configura el almacén de usuarios predeterminado como el almacén de usuarios de CA Enterprise Log Manager, cree una nueva cuenta de usuario y asígnele la función de administrador. Si ha utilizado un almacén de usuarios externo, no podrá crear un nuevo usuario. En este caso, busque el registro de usuario de la persona que va a ser el administrador y agregue el grupo de aplicaciones del administrador a la cuenta de este usuario.

Planificación de políticas de contraseñas

Si acepta el almacén de usuarios predeterminado, definirá nuevos usuarios y establecerá políticas de contraseñas para estas cuentas de usuario desde CA Enterprise Log Manager. La utilización de contraseñas seguras le ayuda a proteger los recursos de los equipos. Las políticas de contraseñas le ayudan a crear contraseñas seguras y le impiden utilizar contraseñas de seguridad baja.

Las políticas de contraseñas predeterminadas proporcionadas con CA Enterprise Log Manager ofrecen una seguridad muy *débil* de protección de contraseñas. Por ejemplo, la política predeterminada permite que los usuarios utilicen su nombre de usuario como contraseña y les permite desbloquear las contraseñas. También permite que las contraseñas no caduquen y que no se bloqueen cuando se producen varios intentos fallidos de inicio de sesión. Las opciones predeterminadas se establecen intencionadamente con un nivel de seguridad de contraseña muy bajo para permitirle crear sus propias políticas de contraseñas personalizadas.

Importante: Debe modificar las políticas de contraseñas predeterminadas para que coincidan con las restricciones de contraseñas en uso de su empresa. No le recomendamos ejecutar CA Enterprise Log Manager en entornos de producción con las políticas de contraseñas predeterminadas.

Puede rechazar estas actividades, aplicar políticas en los atributos de contraseña (por ejemplo, longitud, tipo de carácter, duración y reutilización) y establecer una política de bloqueo en función de un número configurable de intentos fallidos de inicio de sesión como parte de su política de contraseñas personalizada

Más información:

Configuración de políticas de contraseñas (en la página 140)

Nombre de usuario como contraseña

Para que las contraseñas sean más seguras, se recomienda que las contraseñas no contengan el nombre de usuario o no coincidan con él. La política de contraseñas predeterminada activa esta opción. Aunque esta opción parezca útil al configurar las contraseñas temporales para nuevos usuarios, se recomienda desactivar esta selección de política de contraseñas. Con la desactivación de esta opción, se evita que los usuarios utilicen este tipo de contraseña de seguridad baja.

Reutilización y duración de contraseñas

Tenga en cuenta las siguientes directrices cuando determine las políticas sobre la reutilización y la duración de las contraseñas:

- La política de reutilización de contraseñas garantiza que una determinada contraseña no se vuelva a utilizar de forma habitual. Esta política crea un historial de contraseñas. Un ajuste de 0 significa que no se aplica el historial de contraseñas. Un ajuste superior a 0 especifica el número de contraseñas que se guardan y se utilizan para realizar la comparación cuando se cambia la contraseña. Una política de contraseñas segura debe impedir que los usuarios vuelvan a utilizar una contraseña durante, al menos, un año.
- La *duración máxima* recomendada de una contraseña depende de la longitud y de la complejidad de la contraseña. Por lo general, una contraseña aceptable no se puede romper a la fuerza antes de que finalice la duración máxima permitida de la contraseña. Un estándar aceptable para la duración máxima es de 30 a 60 días.
- La configuración de una *duración mínima* impide que los usuarios restablezcan las contraseñas numerosas veces durante una sola sesión para solventar una política de restricción de reutilización. Se recomienda que sean tres días.
- Si configura una duración de contraseña, se recomienda que avise a los usuarios para que restablezcan sus contraseñas. Puede configurar la advertencia para que se muestre en el punto medio de la duración de la contraseña o poco antes de caducar la contraseña.
- Debe bloquear las cuentas de usuario una vez sobrepasado un número razonable de inicios de sesión fallidos. De esta forma, puede evitar que los piratas informáticos adivinen las contraseñas. Tres o cinco intentos es un número estándar tras el cual se bloquea una cuenta.

Formato y longitud de la contraseña

Tenga en cuenta las siguientes directrices cuando desee aplicar requisitos de longitud:

- Debido al modo en que se cifran las contraseñas, las contraseñas más seguras tienen de siete a 14 caracteres de longitud.
- No supere los límites de longitud de las contraseñas impuestos por los sistemas operativos antiguos de su red.

Tenga en cuenta las siguientes directrices cuando desee aplicar políticas sobre el número máximo o mínimo de caracteres que se repite o sobre los caracteres numéricos.

- Las contraseñas seguras no aparecen en ningún diccionario.
- Las contraseñas seguras incluyen uno o más caracteres de al menos tres de los cuatro conjuntos de minúsculas, mayúsculas, dígitos y caracteres especiales.

Planificación de actualizaciones de suscripción

La actualización del servidor de CA Enterprise Log Manager se realiza de forma automática a través de las actualizaciones de suscripción proporcionadas por el servidor de suscripción de CA. Las actualizaciones de suscripción pueden incluir lo siguiente:

- Actualizaciones del producto y del sistema operativo, que todos los servidores de CA Enterprise Log Manager autoinstalan.

  Nota: Puede seleccionar qué actualizaciones del producto y del sistema operativo se deben aplicar durante cada ciclo de actualización.

- Actualizaciones de contenido y configuración, como las que se muestran a continuación, que se insertan en el servidor de gestión.
  - Consultas de informes
  - Informes
  - Archivos de asignación de datos (DM) y archivos de análisis de mensajes (XMP)
  - Escuchas, conectores y otros servicios
  - Integraciones
  - Actualizaciones de configuración de módulos de CA Enterprise Log Manager
  - Actualizaciones de claves públicas
- Actualizaciones destinadas para los agentes

  Nota: Actualice los servidores de CA Enterprise Log Manager antes de actualizar los agentes. Los servidores de CA Enterprise Log Manager admiten agentes con el mismo número de versión o un número inferior al actual. Para ayudar a garantizar un almacenamiento adecuado de los eventos recopilados al configurar o actualizar agentes, compruebe que el agente sólo envía eventos a servidores de CA Enterprise Log Manager cuyo nivel es igual o superior al del agente.

El primer servidor de CA Enterprise Log Manager que instala es el proxy de suscripción en línea predeterminado para las actualizaciones de suscripciones. Los posteriores servidores de CA Enterprise Log Manager se instalan como clientes de suscripción. Si es necesario, puede configurar cualquier servidor de CA Enterprise Log Manager para que actúe como proxy de suscripción *sin conexión*. También puede configurar más servidores proxy de suscripción en línea.

La planificación de suscripción implica lo siguiente:

- Evaluar la necesidad de un proxy HTTP
- Evaluar la necesidad de un proxy de suscripción sin conexión
- Evaluar la necesidad de una lista de servidores proxy

Puertos y componentes de suscripción

La suscripción incluye los siguientes componentes:

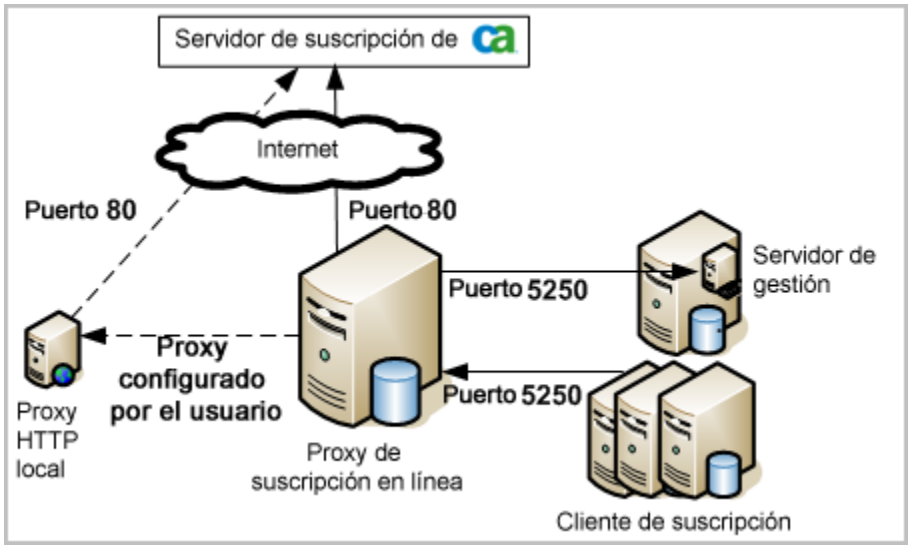
- Servidor de suscripciones de CA
- (Opcional) Proxy HTTP
- Servidores de CA Enterprise Log Manager, que se pueden configurar como:
  - Proxy de suscripción (en línea)
  - Cliente de suscripción
  - (Opcional) Proxy de suscripción sin conexión
- Servidor de gestión de CA Enterprise Log Manager, que normalmente es el proxy de suscripción predeterminado.

  El primer servidor de CA Enterprise Log Manager instalado se suele instalar con un CA EEM local, y el primer CA Enterprise Log Manager instalado es, de forma predeterminada, el proxy de suscripción predeterminado.

CA Enterprise Log Manager utiliza un proxy, o un cliente y servidor, para proporcionar contenido y actualizaciones binarias. El primer servidor de CA Enterprise Log Manager que instala se configura automáticamente como el proxy de suscripción predeterminado. Este proxy de suscripción en línea contacta periódicamente con el servidor de suscripciones de CA para comprobar las actualizaciones. El contacto puede ser directo o a través de un proxy HTTP. De forma predeterminada, el resto de servidores de CA Enterprise Log Manager son clientes de suscripción del proxy de suscripción predeterminado. Los clientes de suscripción contactan con el proxy de suscripción predeterminado para comprobar las actualizaciones. Los clientes y servidores proxy autoinstalan los módulos que solicitan.

El almacén de usuarios de CA Enterprise Log Manager recibe actualizaciones de contenido y configuración y almacena todas las configuraciones del servicio de suscripción.

El puerto 80, el conocido puerto del protocolo HTTP, se utiliza para las solicitudes de Internet con el servidor de suscripciones de CA. El puerto 5250 se utiliza para el tráfico interno entre los servidores de CA Enterprise Log Manager. El puerto desde el proxy de suscripción en línea al proxy HTTP se configura con otra información del proxy HTTP.



Más información:

Configuración de un proxy de suscripción en línea (en la página 189)
Asignaciones de puertos predeterminados (en la página 108)

Cuándo configurar una suscripción

No se recomienda configurar una suscripción hasta haber instalado y planeado los servidores de CA Enterprise Log Manager. Si prefiere obtener actualizaciones de suscripción al momento, piense en la posibilidad de sobrescribir el valor del tiempo (valor predeterminado de 30 días) que se van a retener las actualizaciones descargadas con un intervalo que permita que todos los servidores de CA Enterprise Log Manager planeados se instalen y actualicen antes de realizar la primera limpieza. Los nuevos servidores agregados a los clientes de suscripción después de haber realizado una o varias limpiezas se perderán las actualizaciones disponibles antes de la limpieza. Si instala nuevos servidores después de realizar la limpieza, configúrelos como sus propios servidores proxy de suscripción para que se puedan aplicar todas las actualizaciones disponibles del servidor de suscripciones de CA. Posteriormente, podrá volver a configurar los nuevos servidores como clientes de suscripción.

Planificación del espacio en disco

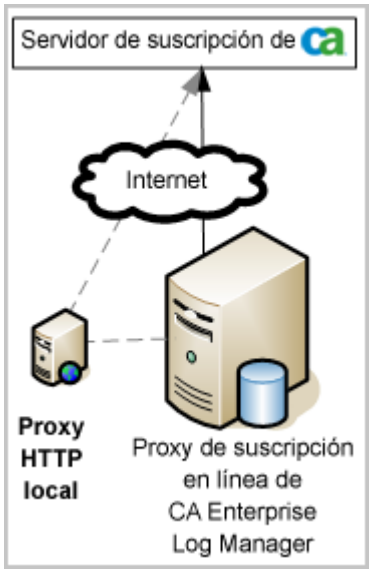
Le recomendamos que compruebe habitualmente el espacio libre en disco para disponer del espacio necesario a la hora de descargar actualizaciones de suscripción. Si el espacio en disco utilizado en un CA Enterprise Log Manager configurado como cliente de suscripción supera el 90% cuando el motor de suscripción trate de realizar la actualización, el servicio de suscripción emitirá un evento autocontrolado y suspenderá el proceso de descarga.

Puede programar una alerta de acción basada en la consulta Espacio en disco disponible bajo.

Nota: Para ver un ejemplo, consulte la sección sobre alertas de acción en la *Guía de administración de CA Enterprise Log Manager* .

Evaluación de la necesidad de un proxy HTTP

Antes de configurar los ajustes globales de suscripción, determine si va a descargar actualizaciones de suscripción en su red interna a través de un servidor proxy HTTP. Numerosas empresas requieren que las conexiones a Internet de salida se realicen a través de un servidor proxy HTTP. Puede especificar las credenciales del servidor proxy HTTP como parte de la configuración de suscripción. De este modo, el proxy de suscripción omite el proxy HTTP cuando comprueba las actualizaciones desde el servidor de suscripciones de CA. Gracias a la omisión automática, ninguno tiene que estar presente durante el proceso de actualizaciones de suscripción.



Si utiliza un proxy HTTP, debe contar con una dirección IP, un número de puerto y credenciales a la hora de iniciar esta configuración.

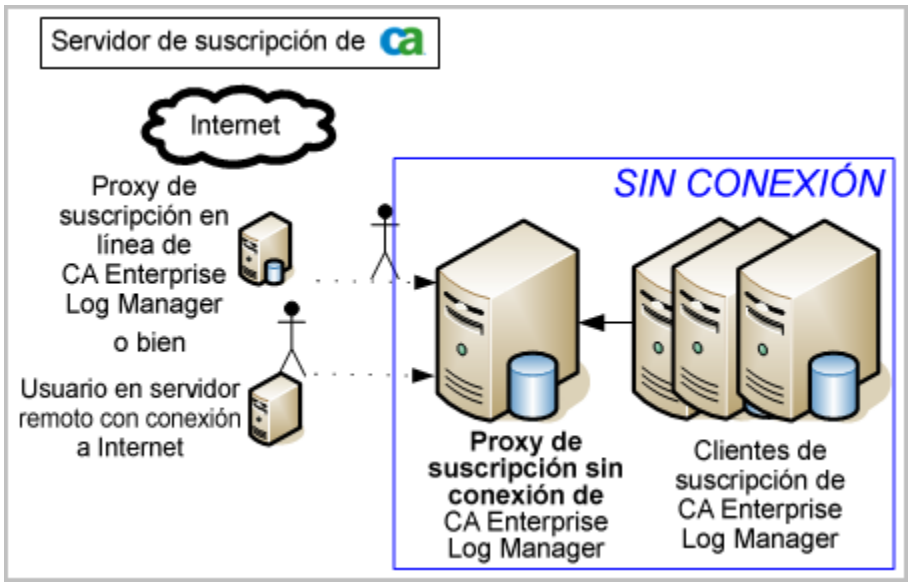
Comprobación del acceso a la fuente RSS para la suscripción

Cuando inicie la configuración de los ajustes globales de suscripción, compruebe que el servidor proxy de suscripción predeterminado pueda acceder a la URL de fuente RSS predefinida. Si se ha generado la lista de módulos para descargar, el acceso ha sido correcto.

Si no se genera el área de módulos para descargar y el servidor está protegido por cortafuegos, configure los ajustes del proxy HTTP para que los servidores proxy en línea puedan contactar con la fuente RSS.

Evaluación de la necesidad de un proxy de suscripción sin conexión

Antes de configurar una suscripción, determine si necesita designar servidores proxy de suscripción sin conexión. Los servidores proxy de suscripción sin conexión son necesarios cuando los servidores de CA Enterprise Log Manager configurados como clientes de suscripción no tienen acceso a ningún proxy de suscripción en línea debido a las políticas que no permiten que estos servidores accedan a ningún servidor mediante acceso a Internet. Estas políticas incluso pueden establecer que ningún servidor de CA Enterprise Log Manager sea un proxy de suscripción en línea. En ambos casos, es necesario un proxy de suscripción sin conexión. La diferencia entre estos escenarios es el modo en que se recupera la actualización de suscripción desde el servidor de suscripciones de CA; en un caso, el proxy en línea recupera las actualizaciones de forma programada y, en el otro, es una persona en un servidor remoto la que recupera las actualizaciones manualmente.



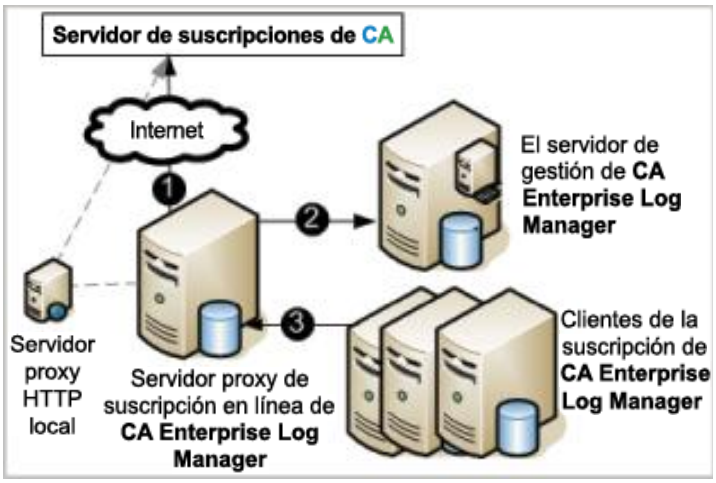
Más información:

Configuración de un proxy de suscripción sin conexión (en la página 190)

Cómo funciona la suscripción con clientes en línea

El servidor proxy de suscripción en línea predeterminado y otros proxy de suscripción configurados por usted obtienen actualizaciones de suscripción del servidor de suscripción de CA. Omiten un servidor proxy HTTP, si está configurado.

La ilustración siguiente muestra un escenario en línea simple con el servidor de suscripción de CA, el proxy de suscripción en línea predeterminado, el servidor de gestión de CA Enterprise Log Manager y algunos clientes de suscripción:



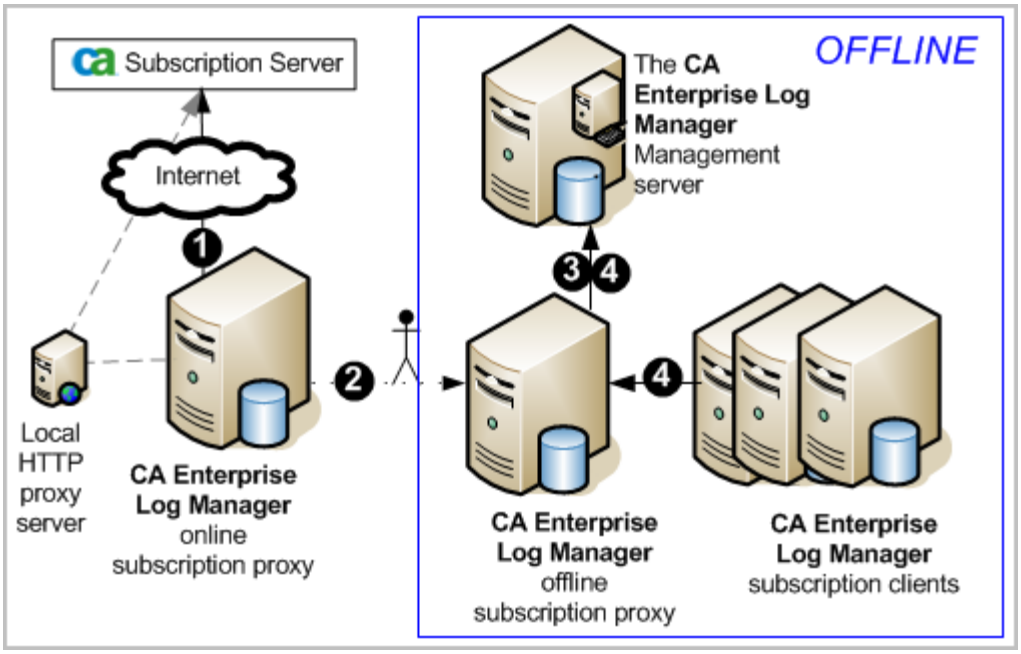
A continuación, se muestra una descripción del proceso indicado por las flechas numeradas:

1. Cuando el administrador configura por primera vez la Configuración del servicio global: módulo de suscripción y especifica la URL de fuente RSS, el proxy de suscripción accede al servidor de suscripción de CA a través de la URL de fuente RSS para obtener la lista de módulos disponibles de descarga. Cuando el administrador selecciona los módulos para descargar, el sistema determina las actualizaciones que todavía no se han descargado en el proxy en línea. El proxy de suscripción en línea descarga las nuevas actualizaciones de suscripción, probablemente a través de un servidor proxy HTTP local. Las actualizaciones de suscripción incluyen actualizaciones del contenido y actualizaciones del producto y del sistema operativo.

2. El proxy de suscripción en línea inserta las actualizaciones de contenido y configuración en el componente del servidor de gestión de CA Enterprise Log Manager que almacena este tipo de información para todos los servidores CA Enterprise Log Manager del entorno.
3. Los clientes de suscripción sondean el servidor proxy de suscripción. Si hay nuevas actualizaciones disponibles, los clientes de suscripción las descargarán. La descarga es un archivo zip que contiene actualizaciones del producto y del sistema operativo, un script para realizar la instalación y un archivo de información de componente (componentinfo.xml). En caso de que sea necesario realizar una copia de seguridad, los clientes de suscripción crearán una copia de seguridad de la instalación más reciente de las actualizaciones del producto y también crearán un script que restaura el estado de las actualizaciones por si necesita deshacer los cambios (la copia de seguridad no incluye las actualizaciones del sistema operativo). A continuación, los clientes de suscripción ejecutan el script de instalación que instalará las actualizaciones del producto.

Cómo funciona la suscripción con clientes sin conexión

La ilustración siguiente muestra un escenario sin conexión simple con el servidor de suscripción de CA, el proxy de suscripción en línea predeterminado, un proxy de suscripción sin conexión, un servidor de gestión con el usuario de CA Enterprise Log Manager y algunos clientes de suscripción.

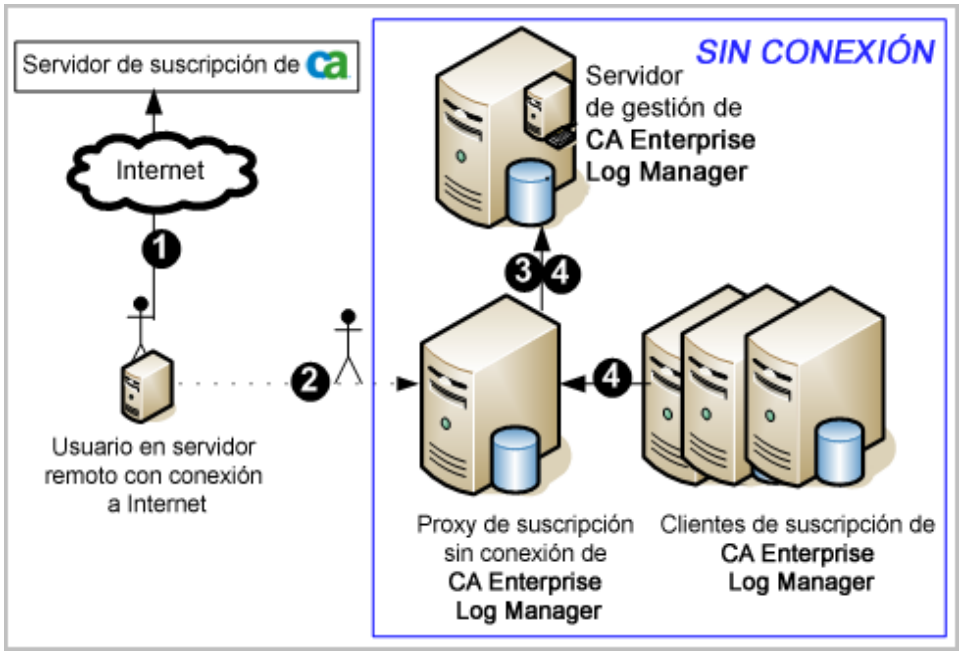


A continuación, se muestra el proceso representado por las flechas enumeradas:

1. El proxy de suscripción en línea accede al servidor de suscripción de CA y descarga actualizaciones de contenido así como actualizaciones del producto y del sistema operativo, probablemente a través de un servidor HTTP local. Las actualizaciones del producto descargadas se basan en los módulos para descargar seleccionados; esta configuración forma parte de la Configuración global de servicios: módulo de suscripción
2. Copie todo lo que se encuentra en la ruta de descarga del proxy en línea en la ruta de descarga del proxy sin conexión. La utilidad *scp* (copia segura) se proporciona para realizar esta acción. También puede emplear la utilidad sftp. El contenido copiado incluye actualizaciones de contenido así como actualizaciones del sistema operativo y del producto binario. Después de realizar la copia, cambie la propiedad de los archivos en el usuario de caelmservice.
3. El servidor proxy de suscripción sin conexión inserta las actualizaciones de contenido en el servidor de gestión de CA Enterprise Log Manager.
4. Los clientes de suscripción sondean el servidor proxy de suscripción *sin conexión*. Si hay nuevas actualizaciones disponibles, los clientes de suscripción las descargarán. La descarga es un archivo zip que contiene actualizaciones del producto y del sistema operativo, un script para realizar la instalación y un archivo de información de componente (componentinfo.xml). En caso de que sea necesario realizar una copia de seguridad, los clientes de suscripción crearán una copia de seguridad de la instalación más reciente de las actualizaciones del producto y también crearán un script que restaura el estado de las actualizaciones por si necesita deshacer los cambios (la copia de seguridad no incluye las actualizaciones del sistema operativo). A continuación, los clientes de suscripción ejecutan el script de instalación que instalará las actualizaciones del producto.

Funcionamiento de la suscripción con proxy sin conexión

Es posible ejecutar un sistema de servidores de CA Enterprise Log Manager, del cual ninguno de ellos tenga acceso a Internet. En esta excepción, incluso el primer servidor instalado, que se configura automáticamente como el proxy de suscripción predeterminado, no puede tener acceso en línea. Ha configurado el proxy de suscripción predeterminado como proxy sin conexión. Para realizar las actualizaciones, debe acceder manualmente al sitio FTP de CA especificado. Este sitio FTP contiene una carpeta para las versiones más importantes. Las carpetas con las versiones anteriores, como r12.0, contienen un archivo tar o de núcleo con la versión, los Service Pack y todas las actualizaciones agregadas durante el ciclo de la versión. La carpeta para la versión actual contiene un archivo de núcleo, actualizado con cada Service Pack, y un archivo suplementario que contiene las actualizaciones y correcciones del contenido acumulativo. Se puede obtener el archivo tar deseado a través de FTP desde cualquier servidor de la red. A continuación debe extraerlo en la ruta de descarga del servidor proxy sin conexión. La actualización de los clientes y del repositorio de contenido se realiza tal y como se ha configurado.



A continuación, se muestra el proceso representado por las flechas enumeradas:

1. Desde un servidor remoto con una conexión de Internet o en un servicio que ejecuta FTP, acceda al sitio FTP que contiene el archivo tar para cada versión y Service Pack de CA Enterprise Log Manager. Abra la carpeta de la versión actual o deseada. Descargue el archivo de núcleo, subscription_12.x.x.x.tar, si no lo ha descargado ya anteriormente. Si ha descargado este archivo, descargue el archivo suplementario.
2. Rellene la ruta de descarga del proxy sin conexión con las actualizaciones siguientes:
   a. Si ha descargado el archivo tar de núcleo, copie este archivo en el directorio /opt/CA/LogManager/data del proxy sin conexión. La utilidad scp (copia segura) se proporciona para realizar esta acción. También puede emplear la utilidad sftp.
   b. Cambie el nombre del directorio de suscripción existente a subscription.bak
   c. Descomprima el archivo tar.

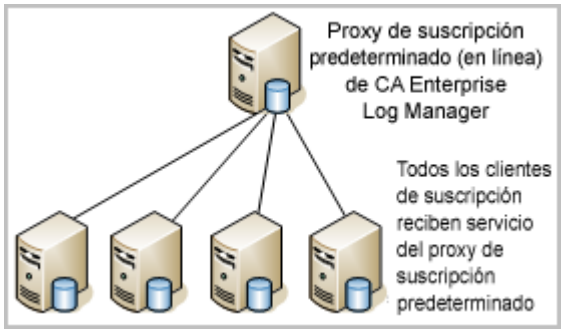
      ```
      tar -xvf subscription_x_x_x_x.tar
      ```

      La estructura de directorios /opt/CA/LogManager/data/subscription se crea con los últimos archivos binarios y contenido. Se configuran los permisos y propiedad.
   d. Si ha descargado el archivo tar suplementario, copie este archivo en el directorio /opt/CA/LogManager/data/subscription del proxy sin conexión y descomprima el tar. Esta acción actualizará módulos y archivos con las últimas versiones.
   e. Reiniciar el servicio iGateway.
3. El servidor proxy de suscripción sin conexión envía las actualizaciones de contenido al servidor de gestión de CA Enterprise Log Manager.
4. Los clientes de suscripción, incluyendo el cliente en el servidor de gestión y el proxy sin conexión, se ponen en contacto con el servidor proxy de suscripción *sin conexión* para obtener actualizaciones. Si hay nuevas actualizaciones disponibles, los clientes de suscripción las descargarán. La descarga es un archivo zip que contiene actualizaciones del producto y del sistema operativo, un script para realizar la instalación y un archivo de información de componente (componentinfo.xml). Si se requiere una copia de seguridad, los clientes de suscripción crearán una copia de seguridad a partir de la última instalación de las actualizaciones del producto y también establecerán un script que permitirá la recuperación de los cambios. (la copia de seguridad no incluye las actualizaciones del sistema operativo). A continuación, los clientes de suscripción ejecutan el script de instalación que instalará las actualizaciones del producto.

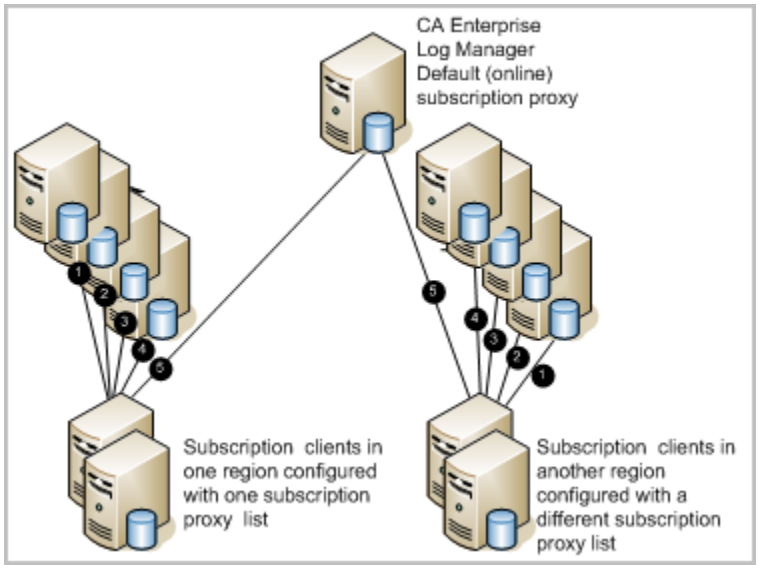
Evaluación de la necesidad de una lista de servidores proxy

Antes de configurar los clientes de suscripción, determine el origen desde el que los clientes de suscripción recuperan actualizaciones de contenido. Los clientes de suscripción pueden obtener actualizaciones directamente desde el proxy de suscripción o puede configurar una lista de servidores proxy intermedios para descargar solicitudes de actualizaciones.

- En las empresas con pocos servidores de CA Enterprise Log Manager que están muy próximos en la red, le recomendamos que los clientes de suscripción utilicen el proxy de suscripción predeterminado.



- En las empresas con un gran número de servidores de CA Enterprise Log Manager o donde los servidores de CA Enterprise Log Manager se encuentran muy dispersos, le recomendamos que configure una lista de servidores proxy de suscripción para cada cliente de suscripción. Cuando una lista de servidores proxy está configurada, cada cliente contacta con los miembros de la lista, uno a uno, y sólo cuando no puede realizar la conexión, contacta con el proxy de suscripción predeterminado.



Ejemplo: configuración de suscripción con seis servidores

Cuando vaya a realizar la configuración de suscripción, tenga en cuenta las otras funciones que estén realizando los servidores antes de decidir la función de suscripción. De forma predeterminada, el servidor de gestión, el primer servidor que instala, es el proxy de suscripción predeterminado. El resto de servidores son clientes de suscripción del proxy de suscripción predeterminado. Aunque esto es aceptable, se recomienda configurar un proxy de suscripción en línea y tener el proxy predeterminado como proxy redundante o de conmutación por error. Se recomienda asignar el rol de proxy en línea al servidor menos activo.

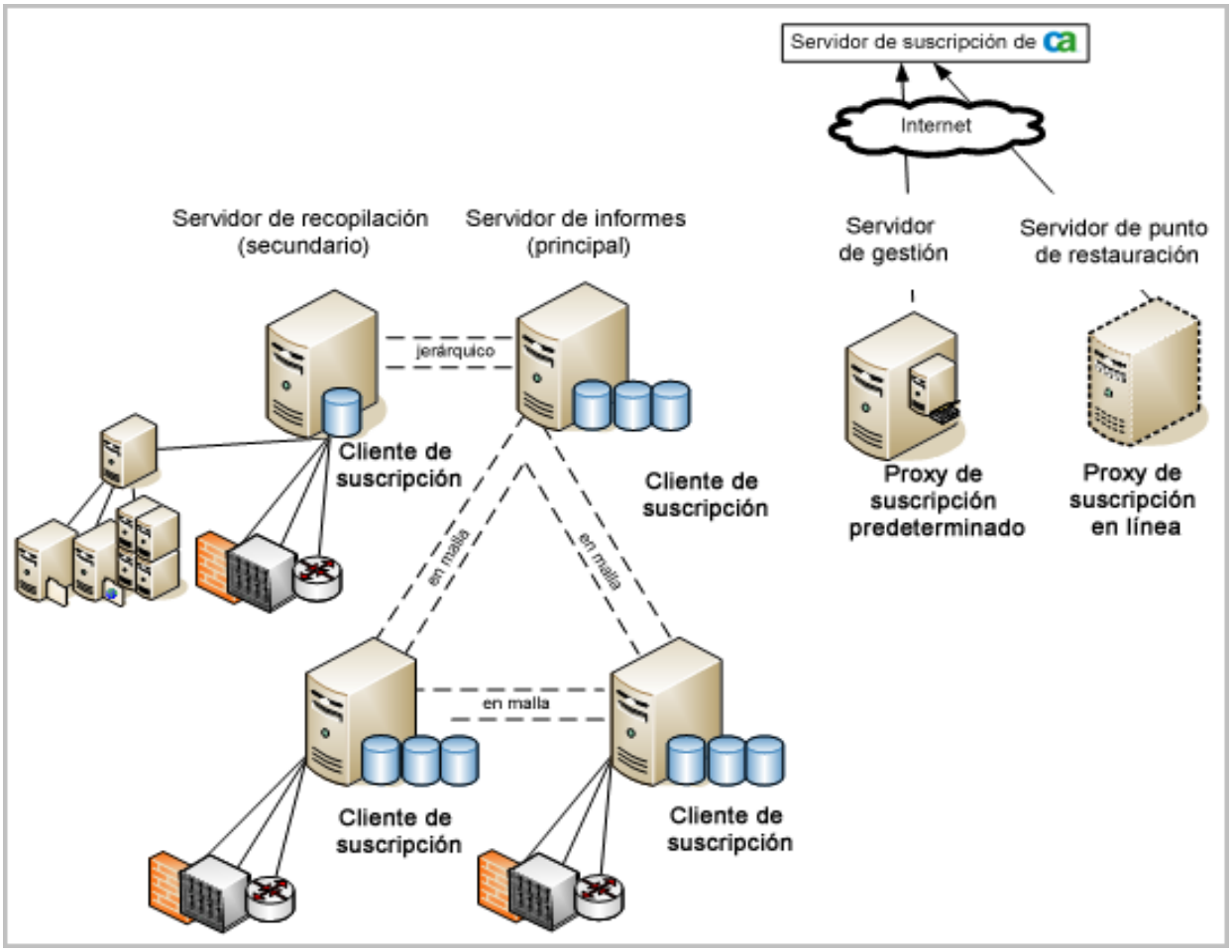
Ejemplo: seis servidores donde el servidor menos ocupado es el proxy de suscripción en línea

Piense en un escenario de seis servidores de CA Enterprise Log Manager. El servidor de gestión se dedica a autenticar y a autorizar usuarios en el contenido de la aplicación de inicio de sesión y de almacenamiento. Cuatro servidores federados gestionan el procesamiento de eventos y la generación de informes. Un sexto servidor es un punto de restauración dedicado para investigar eventos de bases de datos restauradas. Una de las ventajas de contar con un punto de restauración dedicado es que puede evitar que los datos antiguos se incluyan en los informes actuales no incluyendo este servidor en la federación.

En este ejemplo, los dos servidores de recopilación y de informes representan una configuración con unos requisitos de procesamiento excepcionalmente altos. Estos servidores están federados en una configuración jerárquica, donde el servidor de recopilación es el servidor secundario del servidor de informes. Los dos servidores que actúan como servidores de recopilación y de informes representan una configuración con volúmenes de eventos normales y con informes programados. Estos servidores se encuentran federados entre ellos y con el servidor de informes dedicado en una federación en malla; es decir, los tres servidores son del mismo nivel. El objetivo de federar servidores es ampliar la capacidad de obtener resultados de las consultas de los servidores que se federan. Una consulta federada desde cualquier servidor en malla devuelve eventos de sí misma y de los tres servidores de la federación.

Nota: Si desea ejecutar informes consolidados en eventos autocontrolados, incluya el servidor de gestión en la federación.

En este escenario, la solución recomendada es configurar el punto de restauración como proxy de suscripción en línea, dado que es el servidor menos activo. A continuación, dirija cada cliente a este proxy en línea de modo que el proxy predeterminado pueda actuar como copia de seguridad en caso de que el proxy en línea esté ocupado o no esté disponible.



Más información:

Configuración de una federación de CA Enterprise Log Manager (en la página 215)
Configuración de servidores de CA Enterprise Log Manager para la suscripción (en la página 188)
Funciones de servidor (en la página 23)

Planificación de agentes

Los agentes utilizan conectores para recopilar eventos y transportarlos al servidor de CA Enterprise Log Manager. Puede configurar un conector en el agente predeterminado que está instalado con el servidor de CA Enterprise Log Manager o puede instalar un agente en un servidor o en un origen de evento de la red. La decisión de utilizar agentes externos se basa en el volumen de eventos, en la ubicación de agentes, en las necesidades de filtrado de datos y en otras consideraciones. La planificación de la instalación de agentes implica lo siguiente:

- Conocer las relaciones entre los siguientes componentes:
  - Integraciones y escuchas
  - Agentes
  - Conectores
- Ajustar el tamaño de la red para decidir cuántos agentes se van a instalar

Debe instalar los agentes relativamente cerca de los orígenes de eventos desde los que desee recopilar los registros de eventos. La mayoría de conectores recopila eventos desde un único origen de eventos. Para los eventos syslog, una única escucha syslog puede recibir eventos desde varios tipos de orígenes de eventos. Un agente puede controlar y gestionar el tráfico de eventos de más de un conector.

Acerca de la recopilación de eventos syslog

CA Enterprise Log Manager puede recibir eventos directamente desde orígenes de syslog. La recopilación de syslog es distinta al resto de métodos de recopilación porque varios orígenes de registros pueden enviar eventos a CA Enterprise Log Manager al mismo tiempo. Considere el enrutador de red y el concentrador VPN como dos orígenes de eventos posibles. Ambos pueden enviar eventos a CA Enterprise Log Manager directamente utilizando syslog, pero las estructuras y los formatos de registros son diferentes. Un agente de syslog puede recibir ambos tipos de eventos al mismo tiempo utilizando la escucha de syslog proporcionada.

Por lo general, la recopilación de eventos se divide en dos categorías:

- CA Enterprise Log Manager *escucha* los eventos syslog en los puertos configurables.
- CA Enterprise Log Manager *controla* los eventos de otros orígenes de eventos, por ejemplo, utilizando WMI para recopilar eventos de Windows.

Varios orígenes de eventos syslog puede transmitir eventos a través de un solo conector dado que la escucha recibe todo el tráfico en un puerto especificado. CA Enterprise Log Manager puede escuchar eventos syslog en cualquier puerto (si está ejecutando un agente como un usuario que no es raíz, podría haber restricciones al utilizar los puertos que están por debajo del 1024). Es posible que los puertos estándar reciban un flujo de eventos formado por diversos tipos de eventos syslog como, por ejemplo, UNIX, Linux, Snort, Solaris, CiscoPIX, Check Point Firewall 1, etc. CA Enterprise Log Manager gestiona los eventos syslog utilizando escuchas que están especializadas en un tipo especializado de componente de integración. Cree conectores syslog en función de las escuchas y de las integraciones:

- La escucha proporciona la información de conexión como, por ejemplo, puertos o host de confianza.
- La integración define los archivos de análisis de mensajes (XMP) y los archivos de asignación de datos (DM).

Dado que un solo conector de syslog puede recibir eventos desde varios orígenes de eventos, debe considerar si desea redirigir eventos syslog en función de su tipo u origen. El tamaño y la complejidad de su entorno determinarán como equilibrará la recepción de eventos syslog:

Numerosos tipos de syslog: un conector

Si un solo conector tiene que procesar eventos de distintos orígenes de syslog, y el volumen de eventos es alto, el conector tiene que analizar todas las integraciones aplicadas (archivos XMP) hasta encontrar un evento. Esto puede provocar un rendimiento inferior dado que el procesamiento que hay que realizar es abundante. Sin embargo, si el volumen de eventos no es demasiado alto, puede bastar con un solo conector en el agente predeterminado para recopilar todos los eventos requeridos para el almacenamiento.

Un tipo de syslog: un conector

Si configura una serie de conectores únicos para procesar eventos de un solo tipo de syslog, puede aligerar la carga de procesamiento expandiéndola por varios conectores. No obstante, si demasiados conectores se ejecutan en un solo agente, el rendimiento podría verse afectado ya que cada uno es una instancia independiente que requiere un procesamiento individual.

Varios tipos de syslog: un conector

Si su entorno cuenta con un gran volumen de eventos con determinados tipos de eventos syslog, es posible que desee configurar un conector para que sólo recopile ese tipo de eventos. Por lo tanto, podría configurar uno o más conectores para que recopilen varios tipos de eventos syslog que presenten un volumen de eventos inferior en el entorno. De este modo, puede equilibrar la carga de recopilación de eventos syslog en un número más pequeño de conectores por lo que puede obtener un mayor rendimiento.

No es necesario que cree sus propias escuchas de syslog, aunque puede hacerlo si lo considera oportuno. Podría crear escuchas de syslog independientes con distintos valores predeterminados para los puertos, host de confianza, etc. De este modo, puede simplificar la creación de conectores si necesita crear numerosos conectores para cada tipo de evento syslog, por ejemplo.

Más información:

Cuentas de usuarios predeterminadas (en la página 106)
Asignaciones de puertos predeterminados (en la página 108)
Redireccionamiento de puertos del cortafuegos para eventos syslog (en la página 113)

Certificado de agente y agentes

Todos los agentes utilizan el certificado de CAELM_AgentCert.cer predeterminado con tal de comunicarse con su servidor de CA Enterprise Log Manager.

Si desea reemplazar este certificado por un certificado personalizado, recomendamos que lo sustituya antes de instalar un agente. Si se implementa un certificado personalizado después de instalar y registrar los agentes en un servidor de CA Enterprise Log Manager, deberá desinstalar todos los agentes, suprimir la entrada de agente desde el explorador de agentes, reinstalar el agente, y reconfigurar los conectores.

Acerca de los agentes

Los agentes se ejecutan como servicio o daemon después de la instalación y son componentes opcionales del producto utilizados en una o varias de las siguientes situaciones:

- Un sitio remoto y pequeño necesita recopilar datos de eventos pero no requiere un dispositivo de software completo de CA Enterprise Log Manager.
- Es necesario que filtre los datos en el origen de eventos para reducir el tráfico de red de la cantidad de datos que se almacena.

- Es necesario que garantice la entrega de eventos para el almacenamiento del registro de eventos por conformidad.
- Es necesario que proteja la transmisión de registros por la red con el cifrado de datos.

Los agentes actúan como gestores de procesos de los conectores que recopilan datos de eventos de distintas aplicaciones, sistemas operativos o bases de datos. Los agentes proporcionan comandos de gestión de conectores como, por ejemplo, iniciar, detener y reiniciar desde la interfaz del explorador de agente de CA Enterprise Log Manager. Los agentes también aplican cambios en la configuración y actualizaciones binarias.

Puede instalar agentes en orígenes de eventos individuales o en servidores de host remoto para recopilar eventos de más de un origen de eventos. La instalación del servidor de CA Enterprise Log Manager instala automáticamente su propio agente. Puede utilizar este agente predeterminado para realizar la recopilación de eventos syslog directa.

También puede ver el estado de cualquier agente desde el explorador de agente en cualquier servidor de CA Enterprise Log Manager de la red. Los agentes cuentan con un servicio de vigilancia que reinicia un agente cuando se detiene de forma inesperada y controla las actualizaciones binarias de agentes y conectores. Los agentes también envían eventos autocontrolados al almacenamiento del registro de eventos para realizar el seguimiento de cambios y estados.

Acerca de los grupos de agentes

También puede crear grupos de agentes, que son agrupaciones lógicas de agentes que facilitan la gestión. Después de incluir un agente en un grupo de agentes, podrá cambiar las configuraciones e iniciar y detener todos los conectores de un grupo al mismo tiempo. Por ejemplo, podría agrupar agentes por su región física o geográfica.

Puede crear grupos y mover agentes entre grupos en el explorador de agente. Si no define un grupo de agentes, entonces todos los agentes residirán en un grupo predeterminado que se crea cuando instala CA Enterprise Log Manager.

Los registros de configuraciones de agentes y de grupos de agentes se almacenan en el servidor de gestión. Cada vez que instala un agente, el servidor de gestión pone a disposición el nuevo agente en el explorador de agente para cada servidor de CA Enterprise Log Manager que ha registrado con el mismo nombre de instancia de aplicación. De esta forma, podrá configurar y controlar cualquier agente desde el servidor de CA Enterprise Log Manager de la red.

Privilegios de cuentas de usuarios de agentes

Los agentes pueden ejecutarse con cuentas de usuarios con privilegios bajos. Debe crear un grupo y una cuenta de usuario de servicio en el host de destino antes de instalar un agente. Especificará el nombre de usuario durante la instalación del agente y el programa de instalación establecerá los permisos adecuadamente. En los sistemas Linux, el usuario del agente es propietario de todos los binarios del agente, excepto el binario del servicio de vigilancia, que es propiedad del usuario raíz.

Acerca de las integraciones

El conjunto de integraciones predeterminadas es básicamente una biblioteca de plantillas. Estas plantillas proporcionan el código específico para recopilar eventos desde un tipo particular de origen de registros. Una integración se convierte en conector cuando se extrae de la biblioteca, se configura y se aplica a un origen de eventos. Las integraciones incluyen los siguientes tipos de información:

- Archivo de acceso a datos con la información de un determinado tipo de origen de eventos
- Archivo de análisis de mensajes que crea pares de nombre y valor desde los registros de eventos recopilados
- Archivo de asignación de datos que asigna los pares de nombre y valor a la gramática de eventos comunes que forma el esquema de la base de datos para el almacenamiento del registro de eventos del servidor de CA Enterprise Log Manager

CA Enterprise Log Manager proporciona una serie de integraciones de orígenes de eventos populares y comunes entre los que se incluyen productos de CA, cortafuegos populares, bases de datos, sistemas operativos, aplicaciones, etc. Puede obtener más integraciones de las siguientes maneras:

- Actualizaciones de suscripción que incluyen nuevas integraciones o nuevas versiones de las existentes
- Creación de integraciones personalizadas utilizando el asistente proporcionado

Utilice las integraciones para especificar el tipo de recopilación de eventos que desee realizar al configurar conectores.

Acerca de los conectores

Los conectores escuchan los eventos y también envían eventos de estado al agente de forma periódica para que los transporte al servidor de CA Enterprise Log Manager. Un *conector* es un proceso que utiliza una integración y un sensor de registros para crear una configuración con el fin de recopilar eventos de un determinado tipo de origen de eventos. Aparte de para syslog, un conector utiliza una integración como plantilla de configuración. Los conectores de syslog se basan en escuchas.

Los agentes utilizan conectores para recopilar eventos. Después de instalar un agente, puede utilizar el explorador de agente en cualquier servidor de CA Enterprise Log Manager para configurar uno o varios conectores en ese agente (los servidores de CA Enterprise Log Manager deben registrarse en el mismo servidor de gestión [o servidor de CA EEM externo] y con el mismo nombre de instancia de aplicación para configurar los agentes de esta forma).

Normalmente, hay un conector para cada origen de eventos de la red. En los eventos syslog, es posible que haya un conector para varios orígenes de eventos en función de las opciones de configuración. Puede crear varios conectores que utilicen la misma integración pero que presenten detalles de configuración ligeramente diferentes para acceder a distintos orígenes de eventos. Algunos conectores proporcionan ayudantes de la configuración que recopilan la información necesaria para acceder al origen de eventos. Si necesita un conector que no cuente con ninguna integración, puede crear una integración utilizando el asistente de la integración.

Acerca de los sensores de registros

Un *sensor de registro* es el componente de un conector que sabe cómo acceder a los orígenes de eventos. CA Enterprise Log Manager proporciona sensores de registros para los distintos tipos de orígenes de eventos y formatos de registros que se mencionan a continuación:

ACLogsensor

Este sensor de registro lee eventos de CA Access Control cuando CA Access Control emplea selogrd para enrutar eventos.

FileLogSensor

Este sensor de registro lee los eventos de un archivo.

LocalSyslog

Este sensor de registro recopila eventos de cualquier archivo de syslog local del servidor de UNIX.

ODBCLogSensor

Este sensor de registro utiliza ODBC para conectarse a un origen de eventos de la base de datos y recuperar eventos de éste.

OPSECLogSensor

Este sensor de registro lee eventos de un origen de eventos de OPSEC de Check Point.

SDEELogSensor

Este sensor de registro lee eventos de dispositivos de Cisco.

Syslog

Este sensor de registro escucha los eventos syslog.

TIBCOLogSensor

Este sensor de registro lee eventos de una cola de servicio de mensajes de eventos (EMS) de TIBCO en implementaciones de CA Access Control.

W3CLogSensor

Este sensor de registro lee eventos de un archivo con formato de registro W3C.

WinRMLinuxLogSensor

Este sensor de registro activa el agente (Linux) predeterminado en el servidor de CA Enterprise Log Manager para recopilar eventos de Windows.

WMILogSensor

Este sensor de registro recopila eventos de orígenes de eventos de Windows mediante la Instrumentación de administración de Windows (WMI).

El resto de sensores de registro pueden ponerse a disposición a través de actualizaciones de suscripción. Si desea obtener más información acerca de la configuración de los sensores de registros, consulte la ayuda en línea y la *Guía de administración*.

Ajuste de tamaño de la red de CA Enterprise Log Manager

Cuando planifica el número de agentes necesarios, puede utilizar un esquema simple de ajuste de tamaño como el que se indica a continuación. En primer lugar, determine el número de conectores que necesita. No tiene que instalar un agente en todos los orígenes de eventos. Sin embargo, será necesario configurar un conector para cada origen de eventos que no sea syslog desde el que vaya a recopilar los eventos. (Puede recopilar eventos WMI desde múltiples orígenes de eventos en un único conector mediante la adición de un sensor de registro para cada origen de evento. Asegúrese de tener en cuenta los volúmenes de eventos agregados al configurar un conector de este modo.)

Puede configurar los conectores de syslog de varias maneras. Por ejemplo, puede configurar un solo conector de syslog para que reciba todos los eventos syslog independientemente del tipo. Sin embargo, se recomienda basar los conectores de syslog en los volúmenes de eventos de orígenes de eventos de syslog específicos.

Puede instalar agentes en un origen de evento individual. Recomendamos este procedimiento cuando el recuento de eventos de dicho origen sea elevado. Su planificación debe distinguir los agentes de un origen de eventos y los agentes de un host que actúan como recopiladores de distintos tipos de eventos.

Efectos de las reglas de supresión

Durante la planificación, es posible que desee tener en cuenta los efectos de las *reglas de supresión*, que evitan que los eventos se introduzcan en el sistema de almacenamiento de registro de eventos o que se recopilen mediante un conector. Las reglas de supresión siempre están vinculadas a un conector. Puede aplicar las reglas de supresión en el ámbito del agente, del grupo o del propio servidor de CA Enterprise Log Manager. Las ubicaciones tienen diferentes efectos:

- Las reglas de supresión aplicadas a los agentes o a los grupos evitan que los eventos se recopilen y, por lo tanto, reducen el volumen de tráfico de red *enviado* al servidor de CA Enterprise Log Manager.
- Las reglas de supresión aplicadas al servidor de CA Enterprise Log Manager evitan que los eventos se *inserten* en la base de datos y, por lo tanto, redicen la cantidad de información almacenada.

Existen consideraciones de rendimiento potencial a la hora de aplicar reglas de supresión a eventos una vez que hayan llegado al servidor de CA Enterprise Log Manager, especialmente si crea múltiples reglas de supresión o la tasa de flujo de eventos es elevada.

Por ejemplo, puede que desee eliminar *algunos* de los eventos de un cortafuegos o de algunos servidores de Windows que producen eventos duplicados para una misma acción. La no recopilación de estos eventos puede acelerar la transmisión de los registros de eventos que desea guardar y reduce el tiempo de procesamiento en el servidor de CA Enterprise Log Manager. En estos casos, aplicaría una o varias reglas de supresión adecuadas en los componentes del agente.

Si deseara suprimir todos los eventos de determinado tipo en múltiples plataformas o en todo el entorno, aplicaría una o varias reglas de supresión adecuadas en el servidor de CA Enterprise Log Manager. La evaluación de eventos con respecto a la supresión se produce cuando los eventos llegan al servidor de CA Enterprise Log Manager. La aplicación de un gran número de reglas de supresión en el servidor puede provocar un rendimiento más lento, ya que el servidor tiene que aplicar reglas de supresión, además de insertar eventos en el sistema de almacenamiento de registro de eventos.

Para implementaciones más pequeñas, puede llevar a cabo la supresión en el servidor de CA Enterprise Log Manager. También puede decidir aplicar la supresión en el servidor en el caso de implementaciones en las que se emplean resúmenes (acumulaciones). Si sólo introduce algunos de los eventos de un origen de eventos que genera grandes cantidades de información, puede decidir suprimir los eventos no deseados en el agente o en el grupo de agentes para reducir el tiempo de procesamiento del servidor de CA Enterprise Log Manager.

Capítulo 3: Instalación de CA Enterprise Log Manager

Esta sección contiene los siguientes temas:

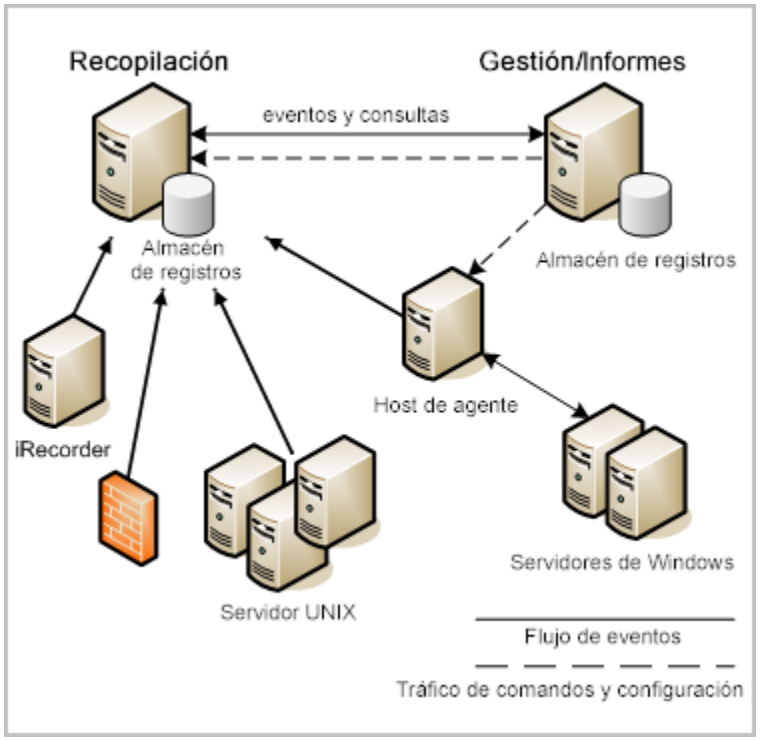
Descripción del entorno de CA Enterprise Log Manager

CA Enterprise Log Manager se ha diseñado para que esté listo y se pueda ejecutar poco después de instalarse; es decir, el tiempo que transcurre desde el comienzo de la instalación hasta que el producto recopila información de registros y genera informes es mínimo. Debe instalar el dispositivo de software de CA Enterprise Log Manager en un sistema dedicado.

Importante: Dado que el servidor de CA Enterprise Log Manager se dedica a la recopilación de registros de eventos de alto rendimiento, no debe instalar ninguna otra aplicación en el servidor. Si lo hace, el rendimiento podría verse afectado.

Existen varias formas de configuración del entorno. Le recomendamos la configuración específica que se muestra a continuación para garantizar una gestión adecuada de altos volúmenes de eventos en los entornos empresariales.

En un nivel empresarial básico, en el entorno de producción, instale al menos dos servidores de CA Enterprise Log Manager en la red existente. Los servidores de CA Enterprise Log Manager utilizan los servidores DNS existentes en la red para que funcionen con los host de agentes y de orígenes de eventos mencionados Un servidor se centra en la recopilación y, el otro, en la generación de informes de los registros de eventos recopilados. En un entorno de dos servidores, el servidor de gestión que instala primero adopta la función de servidor de informes. Como servidor de gestión, realiza la autorización y la autenticación de usuario así como otras funciones de gestión. La ilustración siguiente muestra este entorno básico con algunos orígenes de eventos:



Las líneas continuas de este diagrama muestran el flujo de eventos desde los orígenes de eventos al servidor de recopilación, o a un host de agente y al servidor de recopilación. Puede recopilar eventos syslog directamente utilizando el agente predeterminado del servidor de recopilación de CA Enterprise Log Manager. También podría configurar uno o más conectores en un host de agente independiente para realizar la recopilación a partir de varios orígenes de syslog (no se muestra en este diagrama).

La recopilación de eventos de Windows utiliza la Instrumentación de administración de Windows (WMI) para controlar los eventos de los servidores de Windows. Es necesario que configure un conector WMI en un agente instalado en un host de Windows como punto de recopilación de eventos. Con algunos tipos de eventos, podría utilizar un iRecorder de CA independiente en un servidor host.

Puede configurar y gestionar los agentes y conectores de estos orígenes de eventos desde cualquier servidor de CA Enterprise Log Manager de la red. Las líneas discontinuas del diagrama representan el tráfico de control y de configuración entre el servidor de gestión, los agentes y el resto de servidores de CA Enterprise Log Manager. En el entorno que se representa en este diagrama, podrá realizar las configuraciones desde el servidor de gestión. De este modo, el servidor de recopilación se puede centrar en el procesamiento de eventos.

El entorno de recopilación de registros en el que instala los servidores de CA Enterprise Log Manager presenta las siguientes características:

- El servidor de gestión de CA Enterprise Log Manager realiza la autorización y la autenticación del usuario y, además, gestiona las configuraciones de todos los servidores CA Enterprise Log Manager, agentes y conectores de la red utilizando el servidor de CA EEM local.

  En función del tamaño de la red y del volumen del evento, es posible instalar más de un servidor de gestión y crear federaciones de servidores de recopilación en cada uno. También puede dedicar varios servidores para la generación de informes, donde todos los servidores de informes se registran con su servidor de gestión. En este escenario, el flujo de eventos pasa de los orígenes de eventos al servidor de recopilación configurado hasta el servidor de informes configurado.

- Uno o más servidores de recopilación de CA Enterprise Log Manager procesan y almacenan los eventos entrantes.
- Los eventos pasan por la red de recopilación de registros desde diversos orígenes de eventos *después de* configurar sus conectores o adaptadores correspondientes.

Más información:

Planificación de servidores (en la página 22)

Creación de DVD de instalación

El software de CA Enterprise Log Manager se encuentra disponible como imágenes ISO descargables y comprimidas. Una vez descargado el software, es necesario crear el DVD para poder realizar la instalación. Siga este procedimiento para descargar las imágenes ISO y, a continuación, cree los discos de instalación.

Para crear DVD de instalación

1. Acceda al servidor de descarga http://ca.com/support desde un equipo conectado a Internet.
2. Haga clic en el vínculo Technical Support (Soporte técnico) y, a continuación, haga clic en el vínculo Download Center (Centro de descargas).
3. Seleccione CA Enterprise Log Manager en el campo Select a Product (Seleccionar un producto) y, a continuación, seleccione la versión en el campo Select a Release (Seleccionar una versión).
4. Active la casilla de verificación Select all components (Seleccionar todos los componentes) y, a continuación, haga clic en Go (Ir).

   Se mostrará la página de descargas de soluciones publicadas
5. Seleccione el paquete de descarga.

   Aparecerá la página de soluciones.
6. Desplácese hasta la parte inferior de la página y seleccione el vínculo Download (Descargar) que está en frente al nombre del paquete.

   Se iniciará la descarga del paquete.

   Nota: Es posible que la descarga tarde algún tiempo en completarse en función de la velocidad de la conexión.
7. Descomprima las dos imágenes de instalación.
8. Cree dos discos de instalación independientes grabando las imágenes de disco ISO de CA Enterprise Log Manager y del sistema operativo en DVD-RW.

   Los dos discos de instalación contienen todos los componentes del sistema operativo y del producto, respectivamente, para su entorno de CA Enterprise Log Manager. Puede utilizar otros componentes como SAPI Recorder o iRecorder en su entorno. Estas descargas se encuentran disponibles por separado en el sitio Web de soporte de CA.
9. Utilice los discos de instalación creados para realizar las instalaciones.

Instalación de un servidor de CA Enterprise Log Manager

El proceso de instalación incluye los siguientes pasos:

- Complete la hoja de trabajo del servidor de CA Enterprise Log Manager.
- Instale el servidor de gestión de CA Enterprise Log Manager.

  Nota: Si se utiliza el almacenamiento SAN, tome precauciones para evitar la instalación de una unidad de SAN.

- Instale uno o más servidores de recopilación de CA Enterprise Log Manager.
- (Opcional) Instale uno o más servidores de informes.

  Nota: Si no instala un servidor dedicado a generar informes, puede utilizar el servidor de gestión para que realice esta función del servidor de informes.
- (Opcional) Instale un servidor de punto de restauración.
- Compruebe la instalación.
- Vea los eventos autocontrolados.

Importante: Configure los discos de almacenamiento de una matriz RAID *antes de* comenzar la instalación de CA Enterprise Log Manager. Configure los dos primeros discos como RAID 1 y configure esta matriz como la matriz de arranque. Configure los discos restantes como una única matriz RAID 5. Si la matriz RAID no se configura correctamente, podrían perderse datos.

Como parte de la seguridad global del propio servidor de CA Enterprise Log Manager, la utilidad GRUB está protegida con contraseña durante la instalación.

Hoja de trabajo del servidor de CA Enterprise Log Manager

Antes de instalar un servidor de CA Enterprise Log Manager, recopile la información de la siguiente tabla. Cuando complete la hoja de trabajo, podrá utilizarla para incluir la información solicitada en los mensajes de instalación. Puede imprimir y completar una hoja de trabajo distinta para cada servidor de CA Enterprise Log Manager que tenga pensado instalar.

Información de CA Enterprise Log Manager	Valor	Comentarios
Disco de SO		
Tipo de teclado	*valor apropiado*	Especifique el tipo de teclado que desee utilizar en función de su idioma. El valor predeterminado utiliza la configuración de hardware del teclado conectado al servidor cuando se inicia.
Selección de zona horaria	*su zona horaria deseada*	Seleccione la zona horaria en la que reside el servidor.
Contraseña raíz	*nueva contraseña raíz*	Cree y confirme una nueva contraseña raíz para este servidor.

Información de CA Enterprise Log Manager	Valor	Comentarios
Disco de aplicación		
Nombre de host nuevo	*nombre de host para este servidor de CA Enterprise Log Manager* Por ejemplo: CA-ELM1	Especifique el nombre de host para este servidor utilizando únicamente caracteres compatibles para host. La normativa del sector recomienda el uso de A-Z (con distinción de mayúsculas y minúsculas), 0-9 y guión, donde el primer carácter es una letra y el último carácter es alfanumérico. No utilice el carácter de subrayado en un nombre de host. **Nota:** No añada un nombre de dominio al valor de este nombre de host.
Selección de un dispositivo	*nombre de dispositivo*	Seleccione el nombre del adaptador de red para utilizar con las comunicaciones y con las recopilaciones de registros de eventos. Pulse la barra espaciadora para introducir la configuración del dispositivo.
Dirección IP, máscara de subred y puerta de enlace predeterminada	*valores IP relevantes*	Introduzca una dirección IP válida para este servidor. Introduzca una máscara de subred válida y una puerta de enlace predeterminada para utilizar con este servidor.
Nombre de dominio	*su nombre de dominio*	Introduzca un nombre de dominio completo en el que opere este servidor, por ejemplo, mycompany.com **Nota:** El nombre de dominio debe estar registrado como servidor DNS (servidor de nombres de dominio) en su red para permitir la resolución del nombre de host en la dirección IP.
Lista de servidores DNS	*direcciones IPv4 o IPv6 relevantes*	Introduzca una o más direcciones IP en uso del servidor DNS de su

Información de CA Enterprise Log Manager	Valor	Comentarios
		red. La lista está separada por comas y *no* tiene espacios entre las entradas Si sus servidores DNS utilizan direccionamiento IPv6, introduzca estas direcciones con ese formato.
Fecha y hora del sistema	*fecha y hora local*	Introduzca una nueva fecha y hora del sistema si es necesario.
¿Actualización de hora a través de NTP?	Sí (recomendado) o No	Indique si desea configurar el servidor de CA Enterprise Log Manager para que actualice la fecha y hora desde un servidor NTP (Protocolo de tiempo de redes) establecido. **Nota:** La sincronización de fecha y hora asegura que las alertas contengan datos completos.
Nombre o dirección del servidor NTP	*nombre de host o dirección IP relevante*	Introduzca el nombre de host o la dirección IP válida del servidor NTP desde el que este servidor de CA Enterprise Log Manager obtiene la información de fecha y hora.
Sun Java JDK EULA	Sí	Lea el acuerdo de licencia hasta que llegue a la pregunta: ¿Acepta los términos de licencia mencionados? [sí o no].
CA EULA	Sí	Lea el acuerdo de licencia de CA hasta que llegue a la pregunta: ¿Acepta los términos de licencia mencionados? [sí o no].
¿Servidor de CA Embedded Entitlements Manager local o remoto?	Local: para el primer servidor instalado (servidor de gestión) Remoto: para cada servidor adicional	Indique si desea utilizar un servidor de CA EEM local o remoto. Para un servidor de gestión de CA Enterprise Log Manager, seleccione Local. La instalación le solicitará que cree una contraseña para la cuenta de usuario de EiamAdmin predeterminada. Para cada servidor adicional, seleccione Remoto. La instalación

Información de CA Enterprise Log Manager	Valor	Comentarios
		le solicitará el nombre del servidor de gestión. Independientemente de si selecciona local o remoto, debe utilizar el ID y la contraseña de la cuenta EiamAdmin para iniciar sesión la primera vez en *cada* servidor de CA Enterprise Log Manager.
Introducción del nombre del servidor de CA EEM	*Dirección IP o nombre de host*	Este mensaje sólo se muestra si selecciona Remoto en el mensaje del servidor local o remoto. Introduzca la dirección IP o el nombre de host del servidor de gestión de CA Enterprise Log Manager que ha instalado primero. El nombre de host debe estar registrado como servidor DNS.
Contraseña del administrador del servidor de CA EEM	*Contraseña de la cuenta EiamAdmin*	Registre la contraseña de la cuenta predeterminada del administrador, EiamAdmin El servidor de CA Enterprise Log Manager *requiere* las credenciales de esta cuenta para el inicio de sesión inicial. Si está instalando el servidor de gestión, creará y confirmará aquí una nueva contraseña de EiamAdmin. Apunte esta contraseña ya que la utilizará de nuevo durante las instalaciones de otros agentes y servidores de CA Enterprise Log Manager. **Nota:** La contraseña introducida aquí también es la contraseña inicial de la cuenta de caelmadmin predeterminada que utilizará para acceder directamente al servidor de CA Enterprise Log Manager a través de ssh. Si lo desea, puede crear más

Información de CA Enterprise Log Manager	Valor	Comentarios
		cuentas de administrador para acceder a las funciones de CA EEM después de realizar la instalación.
Nombre de instancia de aplicación	CAELM	Cuando instale el primer servidor de CA Enterprise Log Manager en la red, creará un valor de instancia de aplicación en este mensaje. El resto de servidores de CA Enterprise Log Manager utilizan este valor para registrarse con el servidor de gestión. El nombre predeterminado de la instancia de aplicación es CAELM. Puede utilizar cualquier nombre con este valor. Apunte el nombre de instancia de aplicación para utilizar con instalaciones de CA Enterprise Log Manager posteriores.
¿Desea que el servidor de CAELM se ejecute en modo FIPS?	Sí o No	La respuesta a esta petición determina si el servidor de CA Enterprise Log Manager se inicia en modo FIPS. **Nota:** Si se agrega un servidor a una implementación de CA Enterprise Log Manager existente, el servidor de gestión de CA Enterprise Log Manager o el servidor remoto de CA EEM también deben encontrarse en modo FIPS. De lo contrario, el nuevo servidor no podrá registrarse, por lo que deberá instalarse de nuevo el servidor.

Nota: La instalación le permite revisar y cambiar los detalles del servidor de CA EEM antes de realizar la conexión.

Si el programa de instalación no puede conectarse con el servidor de gestión especificado y decide continuar con la instalación, puede registrar manualmente el servidor de CA Enterprise Log Manager con la funcionalidad de CA EEM incrustada. Si es así, también debe importar el contenido, la Gramática de eventos comunes y los archivos de gestión de agentes. Consulte la sección acerca de la solución de problemas de la instalación para obtener más información e instrucciones.

Más información:

Registro del servidor de CA Enterprise Log Manager con el servidor de CA EEM (en la página 126)
Adquisición de certificados desde el servidor de CA EEM (en la página 127)
Importación de informes de CA Enterprise Log Manager (en la página 127)
Importación de archivos de asignación de datos de CA Enterprise Log Manager (en la página 128)
Importación de archivos de análisis de mensajes de CA Enterprise Log Manager (en la página 129)
Importación de archivos de gramática de eventos comunes (CEG) (en la página 129)
Importación de archivos de gestión de agentes comunes (en la página 130)

Instalación de CA Enterprise Log Manager

Siga este procedimiento para instalar un servidor de CA Enterprise Log Manager.

Para instalar el software de CA Enterprise Log Manager, siga estos pasos:

1. Inicie el servidor con el DVD de instalación del sistema operativo.

   La instalación del sistema operativo se iniciará automáticamente.

2. Responda a los mensajes utilizando la información de la hoja de cálculo del servidor de CA Enterprise Log Manager.

   Si rechaza el acuerdo de licencia, se detendrá la instalación y se apagará el servidor.

3. Cuando aparezca el mensaje de reinicio, extraiga primero el medio y, a continuación, haga clic en Reiniciar.

4. Cuando se le solicite, inserte el disco de la aplicación de CA Enterprise Log Manager y pulse la tecla Intro.

5. Responda a los mensajes utilizando la información de la hoja de cálculo.

   El proceso de instalación continuará. Cuando aparezca el mensaje: "Instalación de CA Enterprise Log Manager correcta.", la instalación habrá finalizado.

   Nota: Cuando instale otro servidor de CA Enterprise Log Manager, es posible que aparezca un mensaje de error en el registro de instalación que indique que el nombre de la aplicación que trató de registrar la instalación con el servidor de CA EEM ya existe. Puede ignorar este error ya que cada instalación de CA Enterprise Log Manager trata de crear el nombre de la aplicación, como si fuese nueva.

Cuando finalice la instalación, debe configurar el servidor de CA Enterprise Log Manager para poder recibir eventos. Es posible que sea necesario configurar un conector en el agente predeterminado para recibir eventos syslog.

Más información

Solución de problemas de instalación (en la página 123)
Configuración del agente predeterminado (en la página 196)

Comprobación de que el proceso de iGateway se esté ejecutando

Si no puede acceder a la interfaz Web del servidor de CA Enterprise Log Manager después de la instalación y está seguro de que los puertos de la interfaz de red están configurados correctamente, es posible que el proceso de iGateway no se esté ejecutando.

Puede comprobar de forma rápida el estado del proceso de iGateway a través de este procedimiento. El proceso de iGateway debe estar ejecutándose para que el servidor de CA Enterprise Log Manager pueda recopilar eventos y para que se pueda acceder a la interfaz de usuario.

Para comprobar el daemon 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 raíz con el siguiente comando:

   ```
   su - root
   ```

4. Utilice el siguiente comando para comprobar que el proceso de iGateway se esté ejecutando:

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

   El sistema operativo devuelve la información del proceso de iGateway así como una lista de procesos que también se están utilizando.

Más información:

Resolución de un error de configuración de la interfaz de red (en la página 125)

Inicio del servicio o del daemon de iGateway

El servicio o el daemon de iGateway es el proceso que gestiona todas las llamadas a la interfaz de usuario de CA EEM y CA Enterprise Log Manager. El proceso debe estar ejecutándose para que pueda acceder a la aplicación. Siga este procedimiento para iniciar el proceso de iGateway en caso de que no se esté ejecutando.

Nota: Si no puede iniciar iGateway, compruebe que la carpeta "/" cuente con espacio en disco disponible. Si no hay espacio suficiente, es posible que no pueda iniciar iGateway correctamente.

Para iniciar 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 raíz con el siguiente comando:

   ```
   su -
   ```

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

   ```
   $IGW_LOC/S99igateway start
   ```

   S99igateway es el script de inicio del proceso de iGateway y es propiedad de la cuenta raíz. Cuando se inicia el proceso de iGateway, éste se ejecuta en la cuenta de usuario de caelmservice.

Detención del servicio o del daemon de iGateway

El servicio o el daemon de iGateway es el proceso que gestiona todas las llamadas a la interfaz de usuario de CA EEM y CA Enterprise Log Manager. El proceso debe estar ejecutándose para que pueda acceder a la aplicación. Siga este procedimiento para detener el proceso de iGateway. Debe seguir este procedimiento cuando reinicie el proceso o cuando elimine un servidor de CA Enterprise Log Manager de la red.

Para detener 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 raíz con el siguiente comando:

   ```
   su -
   ```

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

   ```
   $IGW_LOC/S99igateway stop
   ```

   S99igateway es el script de cierre del proceso de iGateway y es propiedad de la cuenta raíz. Cuando se inicia el proceso de iGateway, éste se ejecuta en la cuenta de usuario de caelmservice.

Inicio del servicio o del daemon del agente de CA Enterprise Log Manager

El servicio o el daemon del agente de CA Enterprise Log Manager es el proceso que gestiona los conectores que envían eventos recopilados a un servidor de CA Enterprise Log Manager. El proceso debe estar ejecutándose para que los conectores puedan recopilar eventos. Siga este procedimiento para iniciar el proceso del agente de CA Enterprise Log Manager en caso de que no se esté ejecutando.

Para iniciar el servicio o el daemon del agente de CA ELM

1. Inicie sesión como usuario raíz o administrador de Windows.
2. Acceda a un símbolo del sistema e introduzca el siguiente comando:

   ```
   Linux, UNIX, Solaris:  /opt/CA/ELMAgent/bin/S99elmagent start

   Windows:  net start ca-elmagent
   ```

Detención del servicio o del daemon del agente de CA Enterprise Log Manager

El servicio o el daemon del agente de CA Enterprise Log Manager es el proceso que gestiona los conectores que envían eventos recopilados a un servidor de CA Enterprise Log Manager. El proceso debe estar ejecutándose para que los conectores puedan recopilar eventos. Siga este procedimiento para detener el proceso del agente de CA Enterprise Log Manager. Normalmente, los comandos de inicio y detención se envían desde el explorador de agente de cualquier servidor de CA Enterprise Log Manager. Podría utilizar este comando para reiniciar un proceso del agente además de todos sus conectores.

Para detener el servicio o el daemon del agente de CA ELM

1. Inicie sesión como usuario raíz o administrador de Windows.
2. Acceda a un símbolo del sistema e introduzca el siguiente comando:

   ```
   Linux, UNIX, Solaris:  /opt/CA/ELMAgent/bin/S99elmagent stop

   Windows:  net stop ca-elmagent
   ```

Comprobación de la instalación del servidor de CA Enterprise Log Manager

Puede comprobar la instalación del servidor de CA Enterprise Log Manager utilizando un explorador Web. Puede realizar una comprobación inicial de la instalación iniciando sesión en el servidor de CA Enterprise Log Manager.

Nota: Cuando inicie sesión en la aplicación de CA Enterprise Log Manager por primera vez, debe utilizar las credenciales de usuario de EiamAdmin con las que instaló el servidor de CA Enterprise Log Manager. Después de iniciar sesión con esta cuenta de usuario, sólo podrá ver y utilizar las funciones de gestión de usuarios y accesos específicas. A continuación, debe configurar el almacén de usuarios y crear una nueva cuenta de usuario de CA Enterprise Log Manager para acceder a la otra funcionalidad de CA Enterprise Log Manager.

Para comprobar la instalación del servidor de CA Enterprise Log Manager

1. Abra el explorador Web e introduzca la siguiente dirección URL.

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

   Aparecerá la pantalla de inicio de sesión de CA Enterprise Log Manager.
2. Inicie sesión como usuario administrativo de EiamAdmin.

   Aparecerá la ficha Administración y la subficha Gestión de usuarios y accesos. Si puede iniciar sesión en el servidor de CA Enterprise Log Manager, la instalación se ha realizado correctamente.

   Nota: Debe configurar uno o más servicios de orígenes de eventos para poder recibir datos de eventos y ver informes.

Visualización de eventos autocontrolados

Puede utilizar eventos autocontrolados para comprobar que el servidor de CA Enterprise Log Manager está instalado correctamente. Tiene que completar algunas tareas de configuración para que CA Enterprise Log Manager pueda recopilar y generar informes sobre los datos del registro de eventos de la red. No obstante, puede ver al momento eventos autocontrolados generados por el servidor de CA Enterprise Log Manager.

Iniciar sesión en el servidor de CA Enterprise Log Manager es la mejor forma de comprobar si la instalación se ha realizado correctamente. Los eventos autocontrolados son otra forma de comprobar el estado del servidor de CA Enterprise Log Manager. Existen una serie de tipos de eventos autocontrolados. Siga este procedimiento para ver más datos de los eventos generados por el propio servidor de CA Enterprise Log Manager.

Para ver eventos autocontrolados

1. Inicie sesión en el servidor de CA Enterprise Log Manager.
2. Seleccione la ficha Informes.
3. Haga clic en la etiqueta Sistema y seleccione el informe Detalles de los eventos autocontrolados del sistema.

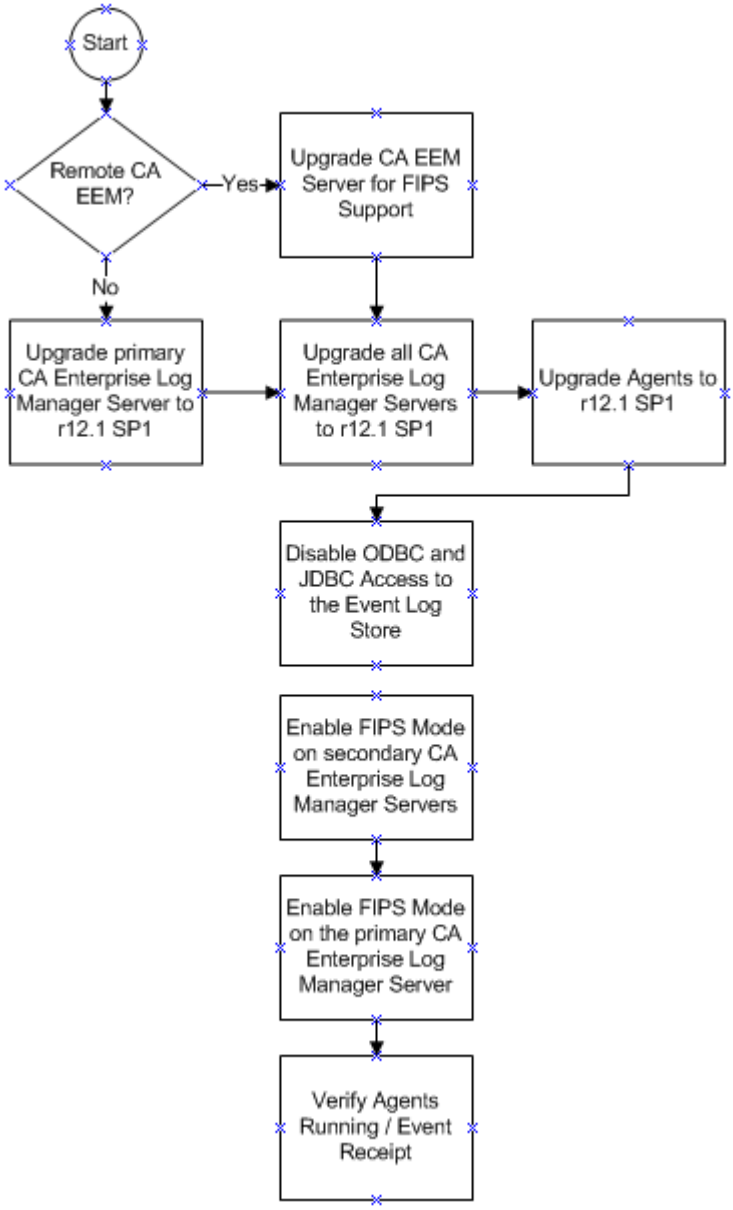
   Se cargará el informe de eventos autocontrolados.
4. Compruebe que los eventos autocontrolados para iniciar sesión y otras acciones de configuración preliminares estén presentes en el informe.

Actualización de los servidores y agentes de CA Enterprise Log Manager para el soporte de FIPS

Se pueden actualizar servidores y agentes existentes de CA Enterprise Log Manager para la compatibilidad con FIPS mediante el módulo de suscripción. Este proceso de actualización comprende los siguientes puntos:

- Ha instalado CA Enterprise Log Manager r12.1 o ha actualizado a este nivel desde r12.0 SP3.
- Ha activado el modo FIPS para la federación de CA Enterprise Log Manager.

Utilice el proceso siguiente para actualizar los servidores:



La actualización y el proceso de activación de FIPS incluye los pasos siguientes:

1. Actualice el servidor primario o de gestión a r12.1 SP1.

   Si usa un servidor de CA EEM remoto, asegúrese de que está en un nivel de versión que es compatible con la operación de FIPS. Consulte las *Notas de la versión de CA EEM* para obtener más información acerca de la actualización para la compatibilidad con FIPS.

   Encontrará instrucciones detalladas para el uso del módulo de suscripción para actualizar tanto servidores como agentes de CA Enterprise Log Manager en la sección *Guía de Administración* de la suscripción.

2. Actualice a r12.1 SP1 todos los otros servidores de CA Enterprise Log Manager en la federación.

3. Actualice todos los agentes a r12.1 SP1 y, si es necesario, actualice los sensores de registro de conector.

   Importante: Si ha implementado un conector que utiliza el sensor de registro de syslog en un host de Windows, actualice todas estas configuraciones de conector para que, al ejecutarse en el modo FIPS, se utilice el último sensor de syslog para esta versión. Consulte la Matriz de integración del producto https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8238/8238_integration_certmatrix.html de CA Enterprise Log Manager para obtener la última lista de integraciones que utilizan el sensor de registro de syslog.

4. Desactive el acceso a ODBC y a JDBC en el almacenamiento de registro de eventos.

5. Active el modo FIPS en cada uno de los servidores de CA Enterprise Log Manager secundarios de la federación.

   Los agentes detectan automáticamente el modo operativo desde el servidor de CA Enterprise Log Manager que los gestiona.

6. Active el modo FIPS en el servidor primario o de gestión.

7. Verifique que los agentes están ejecutándose en el modo FIPS a través del cuadro de mandos del explorador de agentes.

   También se puede verificar que los agentes estén enviando eventos mediante una consulta o un informe, o a través de un examen de la ficha de eventos controlados automáticamente en el área del servicio Estado del sistema.

Cuando se actualiza un agente existente a r12.1 SP1, el procesamiento de suscripción actualizará, de forma predeterminada, el agente en el modo no FIPS. Configure el modo FIPS para el servidor de CA Enterprise Log Manager que gestiona un agente. Un agente detecta el modo FIPS del servidor que gestiona y se reinicia en el modo correspondiente, según sea necesario. Utilice el cuadro de mandos Explorador de agentes en la interfaz de usuario de CA Enterprise Log Manager con el fin de consultar el modo FIPS para un agente, si dispone de privilegios de usuario de Administrador. Para obtener más información, consulte la información de actualización en la sección *Guía de implementación* acerca de la instalación de CA Enterprise Log Manager, o la ayuda en línea para las tareas de gestión de agente.

Más información:

Activación de la operación en modo FIPS (en la página 92)
Visualización del cuadro de mandos de los agentes (en la página 94)

Requisitos previos para la actualización de la compatibilidad con FIPS

Los siguientes requisitos previos son necesarios para la actualización de CA Enterprise Log Manager con tal de ser compatible con FIPS 140-2:

- Empiece bien con una instalación de CA Enterprise Log Manager r12.0 SP3 o r12.1
- Actualización a CA Enterprise Log Manager r12.1 SP1 mediante suscripción

Más información:

Cómo agregar servidores de CA Enterprise Log Manager nuevos en una federación existente en el modo FIPS (en la página 96)

Directrices de actualización

Las siguientes directrices se aplican para actualizar CA Enterprise Log Manager con la compatibilidad con FIPS:

- Si dispone de más de un servidor de CA Enterprise Log Manager en una federación, actualice primero el servidor primario o de gestión de CA Enterprise Log Manager a r12.1 SP1. A continuación, ya podrá actualizar el resto de servidores en cualquier orden. El servidor actualizado se inicia únicamente en el modo no FIPS. La activación del modo FIPS requiere que un usuario Administrador configure el modo operativo de manera manual.

  Importante: No se cambie al modo FIPS en ningún servidor secundario de CA Enterprise Log Manager durante el procesamiento de suscripción. Esto puede producir un error en el procesamiento de suscripción.

- Los servidores de CA Enterprise Log Manager en r12.1 SP1 pueden comunicarse con los agentes de r12.1, pero la compatibilidad con FIPS de nivel de agente no está disponible hasta la actualización a r12.1 SP1.
- Cuando se activa el modo FIPS, solamente los agentes activados de FIPS de r12.1 SP1 y posteriores podrán comunicarse con el servidor de CA Enterprise Log Manager. Cuando se activa el modo *no* FIPS, el servidor de CA Enterprise Log Manager es totalmente compatible con las versiones anteriores que contienen agentes más antiguos. Sin embargo, la operación en modo FIPS no estará disponible. Recomendamos que se instale *solamente* agentes de r12.1 SP1 después de la actualización de los servidores de CA Enterprise Log Manager a r12.1 SP1.
- Los agentes asociados con un servidor de CA Enterprise Log Manager detectan automáticamente cambios en el modo del servidor y se reinician del modo correspondiente.
- Agregar un servidor de CA Enterprise Log Manager nuevo en una federación existente que se ejecuta en el modo FIPS requiere un tratamiento especial. Para obtener más información, consulte la sección de la *Guía de Implementación* acerca de la agregación de un servidor de CA Enterprise Log Manager nuevo en una federación existente.

Actualización de un servidor de CA EEM remoto

Si utiliza un servidor de CA EEM independiente junto con la instalación de CA Enterprise Log Manager, actualícelo para que sea compatible con FIPS antes de la actualización de cualquiera de los servidores o agentes de CA Enterprise Log Manager. Consulte las instrucciones en la *Guía de introducción de CA EEM*, para obtener más detalles e instrucciones.

Desactive el acceso a ODBC y a JDBC en el almacenamiento de registro de eventos.

Se puede prevenir el acceso de ODBC y JDBC a los eventos en el almacenamiento de registro de eventos a través de las opciones en el cuadro de diálogo de configuración del servicio ODBC. Si desea ejecutar la red federada en el modo FIPS, desactive el acceso a ODBC y JDBC para continuar con el cumplimiento de los estándares federales.

Para desactivar el acceso de ODBC y JDBC

1. Inicie sesión en el servidor de CA Enterprise Log Manager y acceda a la ficha Administración.
2. Haga clic en la subficha Servicios y, a continuación, amplíe el nodo de servicio ODBC.

3. Seleccione el servidor que desee.
4. Borre la casilla de verificación Activar servicio y, a continuación, haga clic en Guardar.

   Nota: Desactive la opción de ODBC para *todos* los servidores de CA Enterprise Log Manager en una federación con tal de verificar que ODBC y JDBC se han desactivado.

Activación de la operación en modo FIPS

El usuario puede utilizar las opciones en modo FIPS en el servicio de Estado del sistema para activar o desactivar el modo FIPS. El modo FIPS predeterminado es no FIPS. Los usuarios Administrador deben configurar el modo FIPS para cada servidor de CA Enterprise Log Manager en una federación.

Importante: No se puede operar con modos mixtos dentro de la misma federación de servidores. Cualquier servidor de una federación que se ejecute en un modo diferente no puede recopilar datos de consultas e informes, o responder a solicitudes, desde otro servidor.

Para cambiar entre modos FIPS y no FIPS

1. Inicie sesión en el servidor de CA Enterprise Log Manager.
2. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
3. Amplíe el nodo del servicio Estado del sistema y seleccione el servidor de CA Enterprise Log Manager deseado.

   Aparecerá el cuadro de diálogo Configuración del servicio Estado del sistema.

4. Seleccione el modo FIPS deseado, Activado o Desactivado, de la lista desplegable.
5. Haga clic en Guardar.

   El servidor de CA Enterprise Log Manager se reiniciará en el modo seleccionado. Puede iniciar sesión otra vez para consultar el modo FIPS del agente desde el Explorador de agente.
6. Verifique el modo de funcionamiento del servidor de CA Enterprise Log Manager seleccionando el cuadro de diálogo Servicio Estado del sistema después de que el servidor se haya reiniciado.

   También puede utilizar eventos autocontrolados para verificar que el servidor de CA Enterprise Log Manager se inicia en el modo deseado. Busque los eventos siguientes en la ficha de Eventos autocontrolados en el cuadro de diálogo Estado del sistema:

   ```
   Modo FIPS del servidor activado correctamente
   Modo FIPS del servidor desactivado correctamente
   Error al activar el modo FIPS del servidor
   Error al desactivar el modo FIPS del servidor
   ```

La desactivación del modo FIPS para los servidores de gestión o primario detiene la devolución de datos de consultas e informes federados. Asimismo, los informes programados no se ejecutan. Esta condición continúa hasta que todos los servidores de la federación se ejecutan en el mismo modo otra vez.

Nota: La desactivación del modo FIPS en el servidor remoto de CA EEM o en el servidor de gestión es uno de los requisitos para la agregación de un nuevo servidor de CA Enterprise Log Manager para una federación del servidor que se ejecute en modo FIPS.

Más información:

Desactive el acceso a ODBC y a JDBC en el almacenamiento de registro de eventos. (en la página 91)

Visualización del cuadro de mandos de los agentes

El usuario puede consultar el cuadro de mandos de agente para visualizar el estado de los agentes en el entorno. El cuadro de mandos también muestra detalles como el modo de FIPS actual (FIPS o no-FIPS), y los detalles de uso. Éstos incluyen eventos por segunda carga, uso del porcentaje de CPU, y la fecha y hora de actualización más recientes.

Para visualizar el cuadro de mandos de agentes

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

   Aparece la lista de la carpeta Recopilación de registros.

2. Seleccione la carpeta Explorador de agente.

   Los botones de la gestión de agentes aparecerá en el panel de detalles.

3. Haga clic en Cuadro de mandos y controlador de estado de los agentes:


   Aparece el panel de búsqueda de agentes, que muestra el estado de todos los agentes disponibles en un gráfico detallado. Por ejemplo:

   ```
   Total: 10; En ejecución: 8; Pendiente: 1; Detenido: 1; No responde: 0
   ```

4. (Opcional) Seleccione criterios de búsqueda de agentes para restringir la lista de agentes mostrados. Puede seleccionar uno o más de los criterios siguientes:
   - Grupo de agentes: sólo devuelve los agentes asignados al grupo seleccionado
   - Plataforma: sólo devuelve los agentes que se ejecutan en la plataforma seleccionada
   - Estado: sólo devuelve los agentes que tengan el estado seleccionado como, por ejemplo, En ejecución.
   - Patrón de nombres de agentes: sólo devuelve los agentes que contienen el patrón especificado
5. Haga clic en Mostrar estado.

   Aparece una lista de agentes que cumplen los criterios de búsqueda, en la que aparece, entre otra, la información siguiente:
   - Nombre y versión del conector local
   - Servidor de CA Enterprise Log Manager actual
   - Modo de FIPS de agente (FIPS o no-FIPS)
   - Último dato de carga de eventos registrados por segundo realizada por el agente
   - Último valor registrado de uso de la CPU
   - Último valor registrado de uso de la memoria
   - Actualización de configuración más reciente
   - Estado de la actualización de configuración

Cómo agregar servidores de CA Enterprise Log Manager nuevos en una federación existente en el modo FIPS

Hay algunas directrices especiales para agregar un servidor de CA Enterprise Log Manager nuevo a una federación de servidores que ya están ejecutándose en el modo FIPS. A menos que se especifique el modo FIPS durante la instalación, de forma predeterminada los nuevos servidores de CA Enterprise Log Manager instalados se ejecutan en modo *no* FIPS. Los servidores que se ejecutan en el modo no FIPS no pueden comunicarse con los servidores que se ejecutan en el modo FIPS.

Como parte de la instalación, un nuevo servidor de CA Enterprise Log Manager debe registrarse con el servidor de CA EEM local, incrustado en el servidor de gestión, o con un servidor de CA EEM remoto e independiente. Los procesos para agregar un servidor a una red existente se basan en la ubicación del servidor de CA EEM que gestiona.

Tenga en cuenta el siguiente flujo de trabajo:

El proceso para agregar un servidor nuevo incluye los pasos siguientes:

1. Comprobación de la activación del modo no FIPS en el servidor de CA Enterprise Log Manager de gestión (primario) o en el servidor remoto de CA EEM.
2. Instalación de uno o más servidores secundarios nuevos de CA Enterprise Log Manager mediante la imagen ISO o los DVD para CA Enterprise Log Manager 12.1 SP1 o superior.

   Importante: Asegúrese de que se especifica modo FIPS durante la instalación. De lo contrario, el servidor instalado de nuevo no podrá comunicarse con el servidor de gestión o el servidor remoto de CA EEM y deberá instalarse de nuevo el servidor de CA Enterprise Log Manager.

En el caso de que el servidor de gestión de CA Enterprise Log Manager o el servidor remoto de CA EEM operen en el modo FIPS, el nuevo servidor de CA Enterprise Log Manager puede registrarse y unirse a la federación.

Más información:

Activación de la operación en modo FIPS (en la página 92)
Visualización del cuadro de mandos de los agentes (en la página 94)

Consideraciones acerca de la instalación para un sistema con unidades de SAN

Cuando se instala el sistema operativo para el dispositivo de CA Enterprise Log Manager en un sistema con unidades de SAN, tome precauciones para evitar la instalación de CA Enterprise Log Manager en una unidad de SAN. Una instalación tal puede producir un error.

Elija uno de los siguientes enfoques con tal de ayudar a garantizar una instalación correcta:

- Desactive las unidades de SAN. Instale el sistema operativo y la aplicación de CA Enterprise Log Manager, como es habitual. A continuación, configure las unidades de SAN para CA Enterprise Log Manager y recicle CA Enterprise Log Manager para activar la configuración de SAN.
- Deje las unidades de SAN activadas. Inicie la instalación del sistema operativo. Salga de este procedimiento, tal y como se ha descrito, con el fin de cambiar la secuencia de operaciones que se definen en el archivo kickstart. Reanude el proceso de instalación y complételo, siguiendo la documentación.

Desactive las unidades de SAN para realizar la instalación.

En la actualidad, CA Enterprise Log Manager es compatible con las configuraciones de hardware fijo que proporciona Dell, IBM y HP. El ejemplo siguiente supone que el hardware está formado por HP Blade Servers que utilizan una tarjeta QLogic Fiber Channel a fin de conectarse a una red de área de almacenamiento (SAN) para el almacenamiento de datos. Los HP Blade Servers incluyen unidades de disco duro de SATA que se configuran mediante RAID-1 (reflejado).

Si se utiliza el archivo de arranque kickstart tal y como aparece, asegúrese de desactivar las unidades de SAN antes de iniciar la instalación. Inicie el proceso de instalación con el DVD OS5 y complete la instalación, siguiendo la documentación.

Nota: Si no se inicia la instalación habiendo desactivado las unidades de SAN, CA Enterprise Log Manager se instalará en SAN. En este caso, aparecerá una pantalla roja con el mensaje, Illegal Opcode, después del reinicio de CA Enterprise Log Manager.

Utilice la secuencia siguiente de procedimientos para la instalación de un dispositivo en un sistema con unidades de SAN, en el cual se desactivarán las unidades de SAN antes de la instalación del sistema operativo.

1. Desactive las unidades de SAN.
2. Instale el sistema operativo en el dispositivo.
3. Instale el servidor de CA Enterprise Log Manager.
4. Establezca una configuración de múltiples rutas para el almacenamiento de SAN.
5. Cree un volumen lógico.
6. Prepare el volumen lógico para CA Enterprise Log Manager.
7. Recicle CA Enterprise Log Manager.
8. Verifique que la instalación se ha realizado correctamente.

Al instalar el sistema operativo con unidades de SAN desactivadas, trabajará con los archivos siguientes:

lvm.conf

El archivo de configuración para el gestor de volumen lógico de Linux (LVM2).

multipath.conf (/etc/multipath.conf)

El archivo de configuración para las múltiples rutas de Linux.

fstab (/etc/fstab)

El archivo de tabla de sistemas de archivo que asigna dispositivos a directorios en un sistema de Linux.

Desactive las unidades de SAN.

Utilice los procedimientos que recomienda el distribuidor de la unidad de SAN con el fin de desactivar las unidades de SAN en el hardware en el cual desea instalar el dispositivo de software.

Desactive las unidades de SAN antes de instalar el sistema operativo del dispositivo de software o la aplicación de CA Enterprise Log Manager.

Establezca una configuración de múltiples rutas para el almacenamiento de SAN.

La instalación de una configuración de múltiples rutas es necesaria para un sistema de CA Enterprise Log Manager que se instala en un sistema RAID que debe utilizar el almacenamiento de SAN. Se dividen discos físicos de SAN en espacios de almacenamiento lógicos denominados números de unidad lógica (LUNs).

Establezca una configuración de múltiples rutas para el almacenamiento de SAN.

1. Inicie sesión en el dispositivo de CA Enterprise Log Manager y establezca SU como root.
2. (Opcional) Haga un listado del directorio /dev/mapper para consultar el estado de la configuración antes de instalar las múltiples rutas y los volúmenes lógicos. Los resultados se asemejan a los siguientes:

```
drwxr-xr-x  2 root root     120 Jun 18 12:09 .
drwxr-xr-x 11 root root    3540 Jun 18 16:09 ..
crw-------  1 root root  10, 63 Jun 18 12:09 control
brw-rw----  1 root disk 253,  0 Jun 18 16:09 VolGroup00-LogVol00
brw-rw----  1 root disk 253,  2 Jun 18 12:09 VolGroup00-LogVol01
brw-rw----  1 root disk 253,  1 Jun 18 16:09 VolGroup00-LogVol02
```

3. Abra el archivo .../etc/multipath.conf para editar y continuar como se describe a continuación:

   a. Agregue la sección siguiente bajo "dispositivo {" para los LUN que proporciona el administrador de SAN:

```
device {
    vendor                "NETAPP"
    product               "LUN"
    path_grouping_policy  multibus
    features              "1 queue_if_no_path"
    path_checker          readsector0
    path_selector         "round-robin 0"
    failback              immediate
    no_path_retry         queue
         }
```

   b. Elimine el comentario de la sección de 'lista negra' para todos los dispositivos. La sección de lista negra activa las múltiples rutas en los dispositivos predeterminados.

```
blacklist {
    devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
    devnode "^hd[a-z]"
    devnode "^cciss!c[0-9]d[0-9]*"
}
```

   c. Guarde y cierre el archivo multipath.conf.

4. Verifique que el archivo Multipath está activado y de que los LUN se enumeran al ejecutar lo siguiente:

```
multipath -l
```

   Nota: Las rutas se muestran como 'mpath0' y 'mpath1'. Si los LUN no se muestran, debe reiniciarse y ejecutarse de nuevo el archivo Multipath.

5. Consulte las unidades disponibles.

```
fdisk -l
```

6. Enumere las particiones disponibles y verifique que se enumeran 'mpath0' y 'mpath1'.

```
Es -la /dev/mapper
```

7. Asigne la primera partición de la manera siguiente:

```
kpartx -a /dev/mapper/mpath0
```

8. Asigne la segunda partición de la manera siguiente:

```
kpartx -a /dev/mapper/mpath1
```

Cree un volumen lógico

Se puede utilizar el software de gestor de volumen para combinar los LUN múltiples en un volumen lógico al cual tenga acceso CA Enterprise Log Manager. El gestor de volumen lógico (LVM) gestiona las unidades de disco y los dispositivos de almacenamiento masivo similares en el sistema operativo de Linux. Se puede cambiar el tamaño o mover las columnas de almacenamiento creadas bajo el gestor de volumen lógico a dispositivos backend como el almacenamiento de SAN.

Para crear un volumen lógico.

1. Cree el primer volumen físico:

   ```
   pvcreate /dev/mapper/mpath0
   ```

2. Cree el segundo volumen físico:

   ```
   pvcreate /dev/mapper/mpath1
   ```

3. Muestre todos los volúmenes físicos del sistema:

   ```
   pvdisplay
   ```

4. Cree el grupo de volumen VolGroup01. (El grupo de volumen VolGroup00 ya existe.)

   ```
   vgcreate VolGroup01 /dev/mapper/mpath0 /dev/mapper/mpath1
   ```

   Nota: Este comando crea un volumen y hace de los dos volúmenes físicos parte del grupo.

5. Cree un volumen lógico dentro del grupo de volumen:

   ```
   lvcreate –n LogVol00 –l 384030 VolGroup01
   ```

6. Cree un sistema de archivos:

   ```
   mkfs –t ext3 /dev/VolGroup01/LogVol00
   ```

Prepare el volumen lógico para CA Enterprise Log Manager

Después de la creación de un volumen lógico, rellénelo con la estructura de directorios esperada y asigne las asociaciones de propiedad y grupo que CA Enterprise Log Manager necesita. Debe utilizar vi con tal de modificar el archivo fstab para señalar el volumen lógico que ha creado y, a continuación, monte el nuevo directorio de datos.

Para preparar el volumen lógico de CA Enterprise Log Manager.

1. Cree un directorio provisional, /data1, cambie la propiedad del directorio /data1 a caelmservice y modifique el grupo asociado con este directorio a caelmservice:

   ```
   mkdir /data1
   chown caelmservice /data1
   chgrp caelmservice /data1
   ```

2. Detenga los procesos de iGateway del servidor de CA Enterprise Log Manager:

   ```
   /opt/CA/SharedComponents/iTechnology/S99igateway stop
   ```

3. Cambie los directorios al directorio en el que está ejecutándose el agente de CA Enterprise Log Manager. Detenga el agente y verifique que los servicios se paran:

   ```
   cd /opt/CA/ELMAgent/bin/
   ./caelmagent –s
   ps –ef | grep /opt/CA
   ```

4. Cambie el directorio a /directory.

5. Monte el sistema de archivos nuevo en /data1, copie el contenido del directorio /data en el directorio /data1 y verifique que los dos directorios sean los mismos:

   ```
   mount –t ext3 /dev/VolGroup01/LogVol00 /data1
   cp –pR /data/* /data1
   diff –qr /data /data1
   ```

6. Desmonte el punto de montaje de los datos existentes y, a continuación, desmonte el punto de montaje de data1:

   ```
   umount /data
   umount /data1
   ```

7. Suprima el directorio /data y cambie el nombre del directorio /data1 a /data.

   ```
   rm –rf /data
   datos de mv /data1
   ```

8. Modifique la línea /etc/fstab que hace referencia al directorio /data y señala el volumen lógico nuevo. Es decir, cambie /dev/VolGroup00/LogVol02 a /dev/VolGroup01/LogVol00. Los datos modificados aparecerán en negrita en la siguiente representación de un archivo fstab de muestra.

nombre de dispositivo	**punto de montaje**	**fs-type**	**opciones**	**dump-freq pass-num**
none	/dev/VolGroup00/LogVol00/	ext3	valores predeterminados	1 1
none	**/dev/VolGroup01/LogVol00/data**	ext3	valores predeterminados	2 1
LABEL=/boot	/boot	ext3	valores predeterminados	2 1
tmpfs	/dev/shm	tmpfs	valores predeterminados	0 0
devpts	/dev/pts	devpts	gid=5,mode=620	0 0
sysfs	/sys	sysfs	valores predeterminados	0 0
proc	/proc	proc	valores predeterminados	0 0
none	/dev/VolGroup00/LogVol01	swap	valores predeterminados	0 0

9. Monte el directorio de datos nuevo y verifique que todas las particiones estén montadas en /etc/fstab:

```
mount -a

mount
```

Recicle el servidor de CA Enterprise Log Manager.

Después de la creación de un volumen lógico, recicle CA Enterprise Log Manager con tal de poder utilizar el volumen lógico. Para asegurarse de que funciona correctamente, busque CA Enterprise Log Manager y consulte los eventos que devuelve la consulta Detalles de todos los eventos del sistema.

Para reciclar el servidor de CA Enterprise Log Manager

1. Inicie los procesos de iGateway del servidor de CA Enterprise Log Manager:

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

2. Inicie el servicio ELMAgent
   ```
   /opt/CA/ELMAgent/bin/caelmagent –b
   ```

3. Reinicie el servidor de CA Enterprise Log Manager.

Active las unidades de SAN para realizar la instalación

El tema, Ejemplo: Establezca un almacenamiento de SAN para CA Enterprise Log Manager, incluye la recomendación para desactivar las unidades de SAN (LUN) antes de la instalación del sistema operativo en el dispositivo de CA Enterprise Log Manager.

Una alternativa es dejar activadas las unidades de SAN, modificando el archivo kickstart, ca-elm-ks.cfg, mediante una herramienta de edición ISO, una vez haya iniciado la instalación del sistema operativo. Las modificación asegura que la instalación y el reinicio se realizan a partir del disco duro local, y no desde el SAN.

Para iniciar desde el disco local (no desde SAN)

1. Inicie el servidor con el DVD de instalación del sistema operativo
2. Responda a la primera solicitud sobre el tipo de teclado.
3. Pulse Alt-F2 para mostrar la solicitud Anaconda/Kickstart.

4. Escriba lo siguiente:

   ```
   list-hardrives
   ```

   Aparecerá la lista de unidades disponibles y podrá ver los siguientes:

   ```
   cciss/c0d0 – 68GB RAID 1 (cciss is HP Smart Array)
   Sda – 500GB SAN  (sda – h is the SAN Multipathed)
   Sdb – 500GB SAN
   Sdc – 500GB SAN
   Sdd – 500GB SAN
   Sde – 500GB SAN
   Sdf – 500GB SAN
   Sdg – 500GB SAN
   Sdh – 500GB SAN
   ```

5. Identifique la unidad de disco duro local. En este caso, es cciss/c0d0.

6. Realice los pasos siguientes:

   a. Abra el archivo kickstart del sistema operativo de CA Enterprise Log Manager, ca-elm-ks.cfg para editar. Utilice un editor ISO.

   b. Localice la línea siguiente para editar:

      ```
      bootloader --location=mbr --driveorder=sda,sdb
      ```

      Modifíquela por la siguiente:

      ```
      bootloader --location=mbr --driveorder=cciss/c0d0
      ```

      Este cambio especifica el reinicio únicamente desde el disco local.

   c. Localice las líneas siguientes para editar:

      ```
      clearpart --all --initlabel
      part /boot --fstype "ext3" --size=100
      part pv.4 --size=0 –grow
      ```

      Modifique estas líneas por las siguientes:

      ```
      part /boot --fstype "ext3" --size=100 --ondisk cciss/c0d0
      part pv.4 --size=0 --grow --ondisk cciss/c0d0
      ```

      Esta modificación en las líneas de definición de partición ayudan a asegurar que las particiones se crean en el disco cciss/c0d0 por nombre. Mediante --ondisk, podrá reemplazar las variables $disk1 y $disk2 existentes.

   d. Si es adecuado para su caso, elimine la cláusula de Si/Cuando para el número de unidades de disco, reteniendo solamente el primer conjunto de comandos de disco (líneas 57 - 65).

   e. Guarde la nueva imagen ISO.

7. Salga de la solicitud Anaconda para volver a las solicitudes de instalación del sistema operativo.

8. Continúe con la instalación, mediante los procedimientos documentados.

Configuraciones iniciales del servidor de CA Enterprise Log Manager

La instalación del servidor de CA Enterprise Log Manager crea un nombre de aplicación cuyo valor predeterminado es CAELM. La instalación registra este nombre con el servidor de CA EEM incrustado. Cuando las instalaciones posteriores utilicen el mismo nombre de instancia de aplicación, el servidor de gestión de CA Enterprise Log Manager gestionará todas las configuraciones que tengan el mismo nombre de instancia de aplicación.

Cuando finalice la instalación, el servidor contará con un sistema operativo y con un servidor de CA Enterprise Log Manager. El sistema operativo de 32 bits admite hardware de 32 y 64 bits. Las configuraciones iniciales incluyen las siguientes áreas:

- Cuentas de usuarios predeterminadas
- Estructura de directorios predeterminados
- Imagen de sistema operativo personalizada
- Asignaciones de puertos predeterminados

Cuentas de usuarios predeterminadas

La instalación de CA Enterprise Log Manager crea un usuario administrativo predeterminado, caelmadmin, que cuenta con su propia contraseña. Cuando necesite acceder directamente al servidor host, debe utilizar esta cuenta para iniciar sesión ya la función de inicio de sesión en cuenta raíz se restringe después de la instalación. La cuenta caelmadmin sólo le permite iniciar sesión una vez. Desde aquí, debe cambiar los usuarios a la cuenta raíz utilizando una contraseña distinta para acceder a las utilidades de la administración del sistema al nivel del sistema operativo.

La contraseña predeterminada de esta contraseña es la misma contraseña creada para la cuenta EiamAdmin. Le recomendamos que cambie la contraseña de la cuenta caelmadmin justo después de realizar la instalación.

La instalación también crea una cuenta de usuario de servicio predeterminada, caelmservice, que *no puede* utilizar para iniciar sesión en el sistema. Puede cambiar los usuarios a este usuario para iniciar y detener procesos, si es necesario. El proceso de iGateway y el servidor de CA EEM incrustado (si uno está instalado en el servidor de CA Enterprise Log Manager) se ejecutan en esta cuenta de usuario para proporcionar una capa adicional de seguridad.

El proceso de iGateway no se ejecuta en una cuenta de usuario raíz. El reenvío de puertos se activa automáticamente para que las solicitudes de HTTPS en los puertos 80 y 443 puedan acceder a la interfaz de usuario de CA Enterprise Log Manager, además del puerto 5250.

Estructura de directorios predeterminados

La instalación de CA Enterprise Log Manager sitúa binarios de software por debajo de la estructura de directorios, /opt/CA. Si el sistema cuenta con una segunda unidad de disco, se configura como /data. La instalación crea un vínculo simbólico desde el directorio /opt/CA/LogManager/data al directorio /data. A continuación, se representa la estructura de directorios de instalación predeterminada:

Tipos de archivo	Directorio
Archivos relacionados con iTechnology (iGateway)	/opt/CA/SharedComponents/iTechnology
Archivos relacionados con servidor de EEM de CA Enterprise Log Manager	/opt/CA/LogManager/EEM
Archivos relacionados con instalación de CA Enterprise Log Manager	/opt/CA/LogManager/install
Archivos de datos (vincula a /data en caso de varias unidades)	/opt/CA/LogManager/data
Archivos de registro	/opt/CA/SharedComponents/iTechnology

En circunstancias normales, no debería ser necesario acceder a la utilidad *ssh* en el servidor de CA Enterprise Log Manager excepto para mover archivos de almacenamiento para realizar una copia de seguridad y para su almacenamiento a largo plazo, así como para agregar unidades de disco.

Imagen de sistema operativo personalizada

El proceso de instalación personaliza el sistema operativo creando una imagen mínima y limitando el acceso al menor número de canales posible. Los servicios que no son esenciales no se instalan. El servidor de CA Enterprise Log Manager realiza la escucha en una serie de puertos y desactiva específicamente los puertos no utilizados.

Durante la instalación del sistema operativo, usted crea una contraseña para la cuenta raíz. Después de finalizar la instalación de CA Enterprise Log Manager, la raíz se restringe para no permitir posteriores inicios de sesión. La instalación de CA Enterprise Log Manager crea un usuario predeterminado, *caelmadmin*, que sólo cuenta con el permiso de iniciar sesión pero que no dispone de ningún otro permiso.

Para acceder al nivel raíz del servidor de CA Enterprise Log Manager, puede acceder al servidor con esta cuenta y, a continuación, cambiar los usuarios a la cuenta raíz para que utilicen las herramientas de administración. Es necesario que conozca las contraseñas de *caelmadmin* y de *raíz* para poder acceder al sistema como usuario raíz.

No se instala ningún otro software de seguridad específica con CA Enterprise Log Manager. Para mantener un rendimiento alto, no instale ninguna otra aplicación en el servidor de CA Enterprise Log Manager.

Asignaciones de puertos predeterminados

El servidor de CA Enterprise Log Manager se configura de forma predeterminada para que realice la escucha en el puerto 5250 y en los puertos 80 y 443 mediante el protocolo HTTPS. Los daemon y procesos de CA Enterprise Log Manager no se ejecutan en la cuenta raíz de modo que no pueden abrir los puertos que estén por debajo del 1024. Como consecuencia, la instalación crea automáticamente un redireccionamiento (a través de iptables) al puerto 5250 para las solicitudes entrantes de la interfaz de usuario en los puertos 80 y 443.

El daemon de syslog del sistema operativo local del servidor de CA Enterprise Log Manager no está configurado, ya que CA Enterprise Log Manager utiliza sus eventos autocontrolados para realizar el seguimiento del estado del sistema. Puede ver otros eventos locales y generar informes sobre acciones realizadas en el servidor local de CA Enterprise Log Manager mediante eventos autocontrolados.

A continuación, se muestra una lista de puertos utilizados por el entorno de CA Enterprise Log Manager:

Puerto	Componente	Descripción
53	Servidor de CA Enterprise Log Manager	El puerto TCP/UDP que debe estar disponible para las comunicaciones de DNS con el fin de resolver los nombres de host en las direcciones IP de servidores, como los servidores de CA Enterprise Log Manager, el servidor de CA EEM remoto, si se configura, y el servidor de NTP si ha seleccionado la sincronización de tiempo de NTP en instalar tiempo. Las comunicaciones de DNS no son necesarias si se asignan los

Puerto	Componente	Descripción
		nombres de host a las direcciones IP en el archivo local /etc/hosts.
80	Servidor de CA Enterprise Log Manager	Comunicaciones de TCP con la interfaz de usuario del servidor de CA Enterprise Log Manager mediante HTTPS; redirigido automáticamente al puerto 5250.
111	Asignador de puertos (SAPI)	Las comunicaciones del cliente de Audit con el asignador de puertos se procesan para recibir asignaciones de puerto dinámicas.
443	Servidor de CA Enterprise Log Manager	Comunicaciones de TCP con la interfaz de usuario del servidor de CA Enterprise Log Manager mediante HTTPS; redirigido automáticamente al puerto 5250.
514	Syslog	Puerto de escucha de protocolo UDP predeterminado de syslog; el valor de este puerto es configurable. Para que el agente predeterminado se ejecute como usuario no-root, el puerto predeterminado se establece como 40514 y la instalación aplica una regla de cortafuegos al servidor de CA Enterprise Log Manager.
1468	Syslog	Puerto de escucha de protocolo TCP predeterminado de syslog; el valor de este puerto es configurable.
2123	DXadmin	Puerto de LDAP DXadmin de CA Directory si utiliza un servidor de CA EEM en el mismo servidor físico que el servidor de CA Enterprise Log Manager (el servidor de gestión).

Puerto	Componente	Descripción
5250	Servidor de CA Enterprise Log Manager	Comunicaciones de TCP con la interfaz de usuario del servidor de CA Enterprise Log Manager mediante iGateway. Comunicaciones de TCP entre: ■ Servidor de CA Enterprise Log Manager y servidor de CA EEM ■ Servidores de CA Enterprise Log Manager federados ■ Agente y servidor de CA Enterprise Log Manager para las actualizaciones de estado
6789	Agente	Comando de agente y puerto de escucha de control. **Nota:** Si no se permite el tráfico saliente, será necesario abrir este puerto para permitir que se realicen las operaciones adecuadas.
17001	Agente	Puerto TCP para agente seguro para comunicaciones de servidor de CA Enterprise Log Manager; el valor de este puerto es configurable. **Nota:** Si no se permite el tráfico saliente, será necesario abrir este puerto para permitir que se realicen las operaciones adecuadas.
17002	ODBC/JDBC	Puerto TCP predeterminado empleado para las comunicaciones entre el controlador de ODBC o JDBC y el almacén de registro de eventos de CA Enterprise Log Manager.
17003	Agente	Puerto TCP empleado para las comunicaciones del bus de mensajes para agentes r12.1.
57000	Agente de escucha de SME de distribuidor	Puerto TCP empleado para el servicio de distribuidor en el host local del agente para escuchar eventos autocontrolados entre procesos de agentes.
57001	Escucha de eventos del distribuidor	El puerto TCP empleado para el servicio de distribuidor es compatible con SSL (mediante ETPKI) para escuchar eventos de conectores de cliente.
aleatorio	SAPI	Puertos UDP utilizados para la recopilación de eventos asignados por el asignador de puertos; también puede configurar el recopilador y el enrutador de SAPI para que utilicen cualquier valor de puerto fijo superior a 1024.

Lista de procesos relacionados

La siguiente tabla representa una lista de procesos que se ejecutan como parte de una implementación de CA Enterprise Log Manager. La lista no incluye los procesos del sistema relacionados con el sistema operativo básico.

Nombre de proceso	Puerto predeterminado	Descripción
caelmagent	6789, 17001	Éste es el proceso del agente de CA Enterprise Log Manager.
caelmconnector	Depende de lo que escucha o a lo que se conecta.	Éste es el proceso del conector de CA Enterprise Log Manager. Habrá un proceso independiente del conector para cada conector que se configure en un agente.
caelmdispatcher		Este proceso de CA Enterprise Log Manager gestiona la información de estado y de envío de eventos entre el conector y el agente.
caelmwatchdog	Ninguno	Proceso de vigilancia de CA Enterprise Log Manager que controla otros procesos para garantizar la continuidad de las operaciones.
caelm-eemsessionsponsor		Proceso principal de CA EEM que gestiona todas las comunicaciones con los patrocinadores locales de CA EEM que se ejecutan con red segura en el servidor de CA Enterprise Log Manager. Este proceso se puede ejecutar con red segura.
caelm-logdepot	17001	Proceso del almacenamiento del registro de eventos de CA Enterprise Log Manager que gestiona el almacenamiento de eventos, la creación de archivos de almacenamiento y otras funciones. Este proceso se puede ejecutar con red segura.
caelm-sapicollector		Éste es el proceso del servicio del recopilador de SAPI. Este proceso se puede ejecutar con red segura.
caelm-sapirouter		Éste es el proceso del servicio de enrutador de SAPI. Este proceso se puede ejecutar con red segura.
caelm-systemstatus		Este proceso recopila el estado del sistema para mostrarlo en la interfaz de usuario de CA Enterprise Log Manager.

Nombre de proceso	Puerto predeterminado	Descripción
		Este proceso se puede ejecutar con red segura.
dxadmind		Proceso de CA Directory que se ejecuta en el servidor donde está instalado CA EEM.
dxserver		Proceso de CA Directory que se ejecuta en el servidor donde está instalado CA EEM.
igateway	5250	Proceso principal de CA Enterprise Log Manager; debe estar ejecutándose para recopilar y almacenar eventos.
broker de mensajes		Proceso de CA Enterprise Log Manager que se comunica entre el agente y el servidor de CA Enterprise Log Manager para enviar eventos.
oaserver	17002	Proceso de CA Enterprise Log Manager que se ejecuta para gestionar el procesamiento por parte del servidor de consultas de ODBC y JDBC para acceder al almacén de registro de eventos.
red segura		Marco de trabajo del proceso de CA Enterprise Log Manager que se ejecuta para garantizar la continuidad de las operaciones.
ssld		Proceso de CA Directory que se ejecuta en el servidor donde está instalado CA EEM.

Protección del sistema operativo

El dispositivo de software de CA Enterprise Log Manager contiene una copia racionalizada y endurecida del sistema operativo de Red Hat Linux. Las técnicas de protección que se aplican son las siguientes:

- Se desactiva tanto el acceso a SSH como el usuario root.
- Se desactiva el uso de la secuencia de teclas Ctrl-Alt-Del para reiniciar el servidor desde la consola sin iniciar sesión.
- Se aplican redireccionamientos en iptables para los puertos siguientes:
  - Se redireccionan los puertos TCP 80 y 443 a 5250
  - El puerto UDP 514 se redirecciona a 40514

- El paquete de GRUB está protegido con contraseña.
- La instalación agrega los siguientes usuarios con privilegios bajos:
  - caelmadmin - una cuenta de sistema operativo con derechos de inicio de sesión en la consola del servidor de CA Enterprise Log Manager
  - caelmservice - cuenta de servicio bajo la cual se ejecutan los procesos de iGateway y de agente. No es posible iniciar sesión directamente mediante esta cuenta

Redireccionamiento de puertos del cortafuegos para eventos syslog

Puede redireccionar el tráfico de puertos estándar a otro puerto si está utilizando un cortafuegos entre un agente y el servidor de CA Enterprise Log Manager.

Las recomendaciones de seguridad establecen los privilegios de usuarios mínimos requeridos para ejecutar daemons y procesos de aplicación. Los daemons de UNIX y Linux que se ejecutan en cuentas que no son raíz no pueden abrir puertos por debajo del 1024. El puerto de UDP estándar de syslog es el 514. Esto puede suponer un problema para los dispositivos (como enrutadores y modificadores) que no pueden utilizar puertos que no son estándar.

Para resolver este problema, puede configurar el cortafuegos para que escuche el tráfico entrante en el puerto 514 y, a continuación, lo envíe al servidor de CA Enterprise Log Manager en un puerto diferente. El redireccionamiento se produce en el mismo host que la escucha de syslog. Si decide utilizar un puerto que no es estándar, tendrá que volver a configurar cada origen de eventos para enviar los eventos a ese puerto.

Para redireccionar el tráfico de eventos a través de un cortafuegos

1. Inicie sesión como usuario raíz.
2. Acceda a un símbolo del sistema.
3. Escriba un comando para redireccionar los puertos de su cortafuegos específico.

   Un ejemplo de las entradas de la línea de comandos para la herramienta de filtrado del paquete netfilter/iptables que se ejecuta en un sistema operativo Red Hat Linux sería similar a lo que se muestra a continuación:

   ```
   chkconfig --level 345

   iptables on iptables -t nat -A PREROUTING -p udp --dport 514 -j REDIRECT --to <yournewport>

   service iptables save
   ```

4. Reemplace el valor de la variable, <*yournewport*> con un número de puerto superior a 1024.

   Para realizar otras implementaciones, consulte las instrucciones sobre la gestión de puertos proporcionadas por su distribuidor de cortafuegos.

Instalación del cliente de ODBC

La instalación de un cliente de ODBC en sistemas Windows consta de los pasos siguientes:

1. Compruebe que cuenta con los permisos necesarios y obtenga una clave de licencia para el controlador del cliente de ODBC (requisitos previos).
2. Instale el cliente de ODBC.
3. Cree un origen de datos mediante la utilidad de origen de datos de Windows (ODBC).
4. Configure los detalles de la conexión para el cliente de ODBC.
5. Compruebe la conexión a la base de datos.

Requisitos previos

El acceso de ODBC al almacén de registro de eventos sólo está disponible en CA Enterprise Log Manager r12.1 y versiones posteriores. Consulte las consideraciones sobre orígenes de datos de ODBC para obtener la información necesaria antes de iniciar la instalación.

Los usuarios de esta función deben pertenecer a un grupo de usuarios que cuente con el privilegio de *acceso a datos* en la política de acceso a datos predeterminado (en las políticas de acceso a CALM). Consulte la *Guía de administración de CA Enterprise Log Manager r12.1* para obtener más información sobre las políticas de acceso.

En el caso de un cliente de ODBC, se aplican los requisitos previos siguientes:

- Debe contar con privilegios de administrador para instalar el cliente de ODBC en un servidor Windows.
- La instalación del cliente de ODBC requiere el servicio Microsoft Windows Installer y muestra un mensaje si no lo detecta.
- Configure el servicio del servidor de ODBC en CA Enterprise Log Manager y asegúrese de que selecciona la casilla de verificación Activar servicio.
- Configure un origen de datos de ODBC para sistemas Windows mediante la utilidad de orígenes de datos (ODBC) del Panel de control.
- Debe contar con derechos para crear archivos en el directorio en el que desea instalar en cliente en el caso de sistemas UNIX y Linux.

Consulte la matriz de certificación de asistencia técnica de CA Enterprise Log Manager en http://www.ca.com/Support para obtener detalles sobre las plataformas que disponen de asistencia técnica para su uso con la función de ODBC y JDBC.

Configuración del servicio del servidor de ODBC

Puede configurar el acceso de ODBC y JDBC al almacén de registro de eventos de CA Enterprise Log Manager mediante este procedimiento.

Para configurar el acceso de ODBC y JDBC

1. Inicie sesión en el servidor de CA Enterprise Log Manager como usuario Administrator.
2. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.
3. Haga clic en el servicio Servidor ODBC para abrir la configuración global o expanda el nodo y seleccione un servidor de CA Enterprise Log Manager determinado.
4. Defina un valor de puerto en el campo de puerto de servicio si decide emplear un puerto distinto del valor predeterminado.
5. Especifique si desea permitir que SSL cifre el transporte de datos entre el cliente de ODBC y el servidor de CA Enterprise Log Manager.

   Nota: Los ajustes del puerto de servicio y de la activación de SSL deben coincidir tanto en el servidor como en el cliente de ODBC. El valor predeterminado del puerto es 17002, y el cifrado SSL está activado. Si estos ajustes no coinciden con los del cliente de ODBC, el intento de conexión no será correcto.

Instalación del cliente de ODBC en sistemas Windows

Emplee este procedimiento para instalar el cliente de ODBC en un sistema Windows.

Nota: Debe disponer de una cuenta de administrador de Windows para instalar el cliente de ODBC.

Para instalar el cliente de ODBC

1. Busque el directorio de cliente de ODBC en el DVD de la aplicación o en la imagen de instalación, en el directorio \CA\ELM\ODBC.
2. Haga doble clic en la aplicación, Setup.exe.

3. Acepte el acuerdo de licencia y haga clic en Siguiente.

   Aparece el panel Elegir ubicación de destino.

4. Introduzca la ubicación de destino o acepte la ubicación predeterminada y haga clic en Siguiente.

   Aparece el panel Seleccionar carpeta de programas.

5. Seleccione una carpeta de programa o acepte la selección predeterminada y haga clic en Siguiente.

   Aparece el panel Iniciar la copia de archivos.

6. Haga clic en Siguiente para empezar a copiar archivos.

   Aparece el panel Estado de la instalación, donde se muestra el progreso de la instalación. Cuando la instalación termina de copiar archivos, aparece el panel Asistente de instalación terminado.

7. Haga clic en Finalizar para completar la instalación.

Creación de un origen de datos de ODBC en sistemas Windows

Emplee este procedimiento para crear el origen de datos de ODBC necesario en sistemas Windows. Puede crear el origen de datos como DSN de usuario o DSN de sistema.

Para crear orígenes de datos

1. Acceda al Panel de control de Windows y abra Herramientas administrativas.
2. Haga doble clic en la utilidad Orígenes de datos (ODBC). Aparece la ventana Administrador de orígenes de datos ODBC.
3. Haga clic en Agregar para mostrar la ventana Crear nuevo origen de datos.
4. Seleccione la entrada CA Enterprise Log Manager ODBC Driver y haga clic en Finalizar.

   Aparece la ventana de configuración del controlador de ODBC de CA Enterprise Log Manager.

5. Introduzca los valores de los campos tal y como se describe en la sección Consideraciones de origen de datos de ODBC y, a continuación, haga clic en Aceptar.

Consideraciones de origen de datos de ODBC

A continuación, se indican descripciones de los campos de origen de datos de ODBC según su relación con CA Enterprise Log Manager:

Nombre de origen de datos

Cree un nombre para este origen de datos. Las aplicaciones cliente que desean emplear este dato utilizan este nombre para conectarse al origen de datos.

Host de servicio

Indica el nombre del servidor de CA Enterprise Log Manager al que se conecta el cliente. Puede emplear un nombre de host o una dirección IPv4.

Puerto de servicio

Especifica el puerto de servicio de TCP en el que el servidor de CA Enterprise Log Manager escucha las conexiones de clientes de ODBC. El valor predeterminado es 17002. El valor definido aquí debe coincidir con la configuración del servicio del servidor de ODBC; si no es así, la conexión no será correcta.

Origen de datos de servicio

Deje este campo en blanco; si no lo hace, el intento de conexión fallará.

Cifrado SSL

Especifica si se debe emplear cifrado en las comunicación entre el cliente y el servidor de CA Enterprise Log Manager. El valor predeterminado es tener SSL activado. El valor definido aquí debe coincidir con la configuración del servicio del servidor de ODBC; si no es así, la conexión no será correcta.

Propiedades personalizadas

Indica las propiedades de conexión para su empleo con el almacén de registro de eventos. El delimitador de las propiedades es un punto y coma sin espacio. Los valores predeterminados recomendados incluyen los siguientes:

querytimeout

Indica el valor del tiempo de espera en segundos sin obtención de datos tras el que se cierra la consulta. A continuación, se muestra la sintaxis de esta propiedad:

```
querytimeout=300
```

queryfederated

Indica si se va a realizar una consulta federada. El establecimiento de este valor como falso sólo realiza una consulta en el servidor de CA Enterprise Log Manager en el que se realiza la conexión de la base de datos. A continuación, se muestra la sintaxis de esta propiedad:

```
queryfederated=true
```

queryfetchrows

Define la cantidad de filas que se deben recuperar en una sola operación de recuperación si la consulta es correcta. El valor mínimo es 1 y el máximo, 5000. El valor predeterminado es 1000. A continuación, se muestra la sintaxis de esta propiedad:

```
queryfetchrows=1000
```

offsetmins

Especifica la diferencia de zona horaria del cliente de ODBC. El valor 0 aplica GMT. Puede emplear este campo para definir su propia diferencia de zona horaria con respecto a GMT. A continuación, se muestra la sintaxis de esta propiedad:

```
offsetmins=0
```

suppressNoncriticalErrors

Indica el comportamiento del proveedor de la interfaz en el caso de errores no críticos como que una base de datos no responda o que un host no responda.

A continuación, se muestra la sintaxis de esta propiedad:

```
suppressNoncriticalErrors=false
```

Comprobación de la conexión del cliente de ODBC a la base de datos

El cliente de ODBC se instala con una herramienta de consultas de SQL de línea de comandos interactiva, ISQL. Puede emplear esta herramienta para comprobar los ajustes de la configuración y la conexión entre el cliente de ODBC y el almacén de registro de eventos de CA Enterprise Log Manager.

Para comprobar la conexión del cliente a la base de datos

1. Acceda al símbolo del sistema y vaya al directorio en el que ha instalado el cliente de ODBC.
2. Inicie la utilidad ISQL, odbcisql.exe.
3. Introduzca el comando siguiente para comprobar la conexión del cliente a la base de datos:

```
connect User*Password@DSN_name
```

Utilice el nombre del origen de datos creado para esta conexión de ODBC a la base de datos para el valor DSN_name. Si los parámetros de la conexión son correctos, verá un mensaje similar al siguiente:

```
SQL: connecting to database: DSN_name
Elapsed time 37 ms.
```

Comprobación de la recuperación de servidores desde la base de datos

Utilice esta consulta de comprobación para determinar si una aplicación cliente de ODBC puede recuperar datos de un almacén de registro de eventos de CA Enterprise Log Manager mediante la conexión establecida a la base de datos. Este proceso emplea la misma utilidad ISQL utilizada para comprobar la conexión de ODBC.

Nota: No copie ni utilice las consultas SQL incluidas en las consultas e informes de CA Enterprise Log Manager para comprobar la conexión de ODBC. Estas instrucciones SQL sólo sirven para que el servidor de CA Enterprise Log Manager las emplee en el almacén de registro de eventos. Cree las consultas SQL de ODBC mediante construcciones estándar según la norma de ANSI SQL.

Para comprobar la recuperación de datos de los componentes del servidor

1. Acceda al símbolo del sistema y vaya al directorio en el que ha instalado el cliente de ODBC.
2. Inicie la utilidad ISQL, odbcisql.exe.
3. Introduzca la instrucción SELECT siguiente para comprobar la recuperación desde el almacén de registro de eventos:

   ```
   select top 5 event_logname, receiver_hostname, SUM(event_count) as Count from
   view_event where event_time_gmt < now() and event_time_gmt >
   timestampadd(mi,-15,now()) GROUP BY receiver_hostname, event_logname;
   ```

Instalación del cliente de JDBC

El cliente de JDBC ofrece acceso a JDBC a través de cualquier subprograma compatible con Java, aplicación o servidor de aplicaciones. Ofrece un alto rendimiento punto a punto y acceso de n niveles a los orígenes de datos. El cliente está optimizado para entornos Java, lo que le permite incorporar la tecnología Java, así como ampliar la funcionalidad y el rendimiento del sistema existente.

El cliente de JDBC se ejecuta en plataformas de 32 bits y 64 bits. No es necesario realizar cambios en las aplicaciones existentes para que se puedan ejecutar en plataformas de 64 bits.

La instalación del cliente de JDBC consta de los pasos siguientes:

1. Compruebe que el servidor de aplicaciones Web con capacidad de configuración de conexiones de almacén está instalado y en ejecución.
2. Obtenga la clave de licencia del controlador del cliente de JDBC.
3. Instale el cliente de JDBC.
4. Configure la conexión a la base de datos mediante las funciones de gestión de conexiones de almacén del servidor de aplicaciones Web.
5. Compruebe la conexión a la base de datos.

Requisitos previos del cliente de JDBC

El acceso de ODBC al almacén de registro de eventos sólo está disponible en CA Enterprise Log Manager r12.1 y versiones posteriores. Puede instalar el cliente de JDBC en sistemas Windows y UNIX.

Los usuarios de esta función deben pertenecer a un grupo de usuarios de CA Enterprise Log Manager que cuente con el privilegio de *acceso a datos* en la política de acceso a datos predeterminado (en las políticas de acceso a CALM). Consulte la *Guía de administración de CA Enterprise Log Manager r12.1* para obtener más información sobre las políticas de acceso.

En el caso de un cliente de JDBC, se aplican los requisitos previos siguientes:

- Debe contar con privilegios de administrador para instalar el cliente de JDBC en un servidor Windows.
- Compruebe que la ventana de configuración del servidor de ODBC muestra que la casilla de verificación Activar servicio está seleccionada (activada).
- Debe contar con derechos para crear archivos en el directorio en el que desea instalar en cliente en el caso de sistemas UNIX y Linux.
- En el caso de aplicaciones que se ejecuten con J2SE v 1.4.2.x, defina las conexiones de la base de datos de forma programada, tal y como se define en una aplicación específica.
- En el caso de las aplicaciones que se ejecuten con J2EE 1.4.2.x y versiones posteriores, utilice un servidor de aplicación Web como BEA WebLogic o Red Hat JBoss para configurar la gestión de conexiones de almacén.

Consulte la matriz de certificación de asistencia técnica de CA Enterprise Log Manager en http://www.ca.com/Support para obtener detalles sobre las plataformas que disponen de asistencia técnica para su uso con la función de ODBC y JDBC.

Instalación del cliente de JDBC en sistemas Windows

Emplee este procedimiento para instalar el controlador del cliente de JDBC en un sistema Windows.

Para instalar el controlador de JDBC

1. Busque los dos archivos .jar siguientes en el DVD de la aplicación o en la imagen de instalación, en el directorio CA/ELM/JDBC:

   ```
   LMjc.jar
   LMssl14.jar
   ```

2. Copie los archivos .jar en el directorio deseado del servidor de destino y anote su ubicación.

Instalación del cliente de JDBC en sistemas UNIX

Emplee este procedimiento para instalar el controlador del cliente de JDBC en un sistema UNIX.

Para instalar el controlador de JDBC

1. Busque los dos archivos .jar siguientes en el DVD de la aplicación o en la imagen de instalación, en el directorio CA/ELM/JDBC:

   ```
   LMjc.jar
   LMssl14.jar
   ```

2. Copie los archivos .jar en el directorio deseado del servidor de destino y anote su ubicación.

3. Ejecute el comando siguiente (o uno parecido) de forma manual desde el directorio de instalación tras instalar el cliente de JDBC para JDBC en UNIX:

   ```
   chmod -R ugo+x file_location
   ```

   El valor de *file_location* es el directorio en el que ha instalado el cliente de JDBC. Este paso le permite ejecutar scripts shell suministrados con el cliente instalado.

Parámetros de conexión de JDBC

Diversas aplicaciones requieren que determinados parámetros de conexión empleen el controlador del cliente de JDBC. Los parámetros habituales incluyen los siguientes:

- Cadena de conexión o URL de conexión
- Nombre de clase

La cadena de conexión de JDBC (URL) tiene el formato siguiente:

```
jdbc:ca-elm://[CA-ELM_host_name]:[ODBC/JDBCport];ServerDataSource=Default;
```

El nombre de la clase de controlador de JDBC es:

```
com.ca.jdbc.openaccess.OpenAccessDriver
```

Consideraciones de URL de JDBC

Al emplear el cliente de JDBC para acceder a los datos de eventos almacenados en CA Enterprise Log Manager, necesita tanto Classpath de JDBC como URL de JDBC. Classpath de JDBC indica las ubicaciones de los archivos JAR del controlador. URL de JDBC define los parámetros que emplean las clases de los archivos JAR al cargarse.

A continuación, se indica un ejemplo completo de URL de JDBC:

```
jdbc:ca-
elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout=600;que
ryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

Las descripciones siguientes definen los componentes de URL:

jdbc.ca-elm:

Define la cadena protocol:subprotocol que designa el controlador de JDBC suministrado con CA Enterprise Log Manager.

//IP Address:Port;

Indica la dirección IP que representa al servidor de CA Enterprise Log Manager a cuyos datos desea acceder. El número de puerto es el puerto que se empleará para las comunicaciones y debe coincidir con los ajustes del panel de configuración del servicio ODBC de CA Enterprise Log Manager. Si los puertos no coinciden, el intento de conexión no es correcto.

encrypted=0|1;

Determina si el cifrado SSL se emplea para la comunicación entre el cliente de JDBC y el servidor de CA Enterprise Log Manager. El valor predeterminado es 0, sin cifrado, y no requiere una especificación en la URL. Setting encrypted=1 activa el cifrado. Defina la conexión del cifrado de forma explícita. Además, este ajuste debe coincidir con la configuración del cuadro de diálogo de servicio ODBC de CA Enterprise Log Manager. Si no es así, el intento de conexión no será correcto.

ServerDataSource=Default

Especifica el nombre del origen de los datos. Establezca este valor en *Predeterminado* para acceder al almacén de registro de eventos de CA Enterprise Log Manager.

CustomProperties=(x;y;z)

Estas propiedades son las mismas que las propiedades personalizadas de ODBC. Si no las especifica de forma explícita, se aplican los valores predeterminados en la URL de ejemplo.

Más información

Consideraciones de origen de datos de ODBC (en la página 117)

Solución de problemas de instalación

Puede revisar los siguientes registros de instalación para tratar de solucionar los problemas relacionados con la instalación:

Producto	Ubicación del archivo de registro
CA Enterprise Log Manager	/tmp/pre-install_ca-elm.log /tmp/install_ca-elm.<*timestamp*>.log /tmp/install_ca-elmagent.<*timestamp*>.log
CA Embedded Entitlements Manager	/opt/CA/SharedComponents/EmbeddedIAM/eiam-install.log
CA Directory	/tmp/etrdir_install.log

La instalación de CA Enterprise Log Manager copia contenido y otros archivos en el servidor de CA EEM para la gestión. Desde la perspectiva del servidor de CA EEM, el servidor de CA Enterprise Log Manager genera informes y *se importan* otros archivos. Si la instalación no puede conectarse al servidor de CA EEM, la instalación de CA Enterprise Log Manager continúa sin importar los archivos de contenido. Puede importar los archivos de contenido manualmente cuando finalice la instalación.

Si encuentra algún error durante la instalación, es posible que tenga que realizar alguna de las siguientes acciones para finalizar la instalación. Cada una de estas acciones implica iniciar sesión en el servidor de CA Enterprise Log Manager utilizando la cuenta predeterminada caelmadmin y, a continuación, cambiar los usuarios a la cuenta raíz.

- Resolver el error de configuración de la interfaz de red
- Comprobar que se ha instalado el paquete rpm
- Comprobar que el daemon de iGateway se esté ejecutando
- Registrar la aplicación de CA Enterprise Log Manager con el servidor de CA EEM
- Adquirir certificados digitales
- Importar informes de CA Enterprise Log Manager
- Importar archivos de asignación de datos
- Importar archivos de análisis de mensajes
- Importar archivos de gramática de eventos comunes (CEG)
- Importar archivos de gestión de agentes comunes

Resolución de un error de configuración de la interfaz de red

Después de realizar la instalación, si no puede acceder a la interfaz de usuario de CA Enterprise Log Manager, es posible que aparezca un error de configuración de la interfaz de red. Tiene dos opciones para resolver el error:

- Extraiga el cable de red físico e introdúzcalo en otro puerto.
- Vuelva a configurar los adaptadores lógicos de la interfaz de red con una línea de comandos.

Para volver a configurar los puertos de un adaptador de red con una línea de comandos

1. Inicie sesión en el dispositivo de software como usuario caelmadmin y acceda a un símbolo del sistema.
2. Cambie los usuarios a usuarios raíz con el siguiente comando:

   ```
   su -
   ```

3. Introduzca la contraseña del usuario raíz para confirmar el acceso al sistema.
4. Introduzca el siguiente comando:

   ```
   system-config-network
   ```

   Se mostrará la interfaz de usuario para configurar los adaptadores de red.
5. Defina las configuraciones de puertos tal y como desee y salga.
6. Con el siguiente comando, reinicie los servicios de red para que se implementen los cambios:

   ```
   reinicio de red de servicio
   ```

Comprobación de que el paquete RPM esté instalado

Puede observar con rapidez la instalación comprobando si se ha instalado el paquete RPM adecuado.

Para comprobar el paquete RPM

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 raíz con el siguiente comando:

   ```
   su - root
   ```

4. Compruebe que el paquete ca-elm-<version>.i386.rpm se ha instalado con los siguientes comandos:

   ```
   rpm -q ca-elm
   rpm -q ca-elmagent
   ```

   Si está instalado, el sistema operativo devuelve el nombre completo del paquete.

Registro del servidor de CA Enterprise Log Manager con el servidor de CA EEM

Síntoma:

Durante la instalación, la aplicación de CA Enterprise Log Manager no registró correctamente el servidor de CA EEM. La aplicación de CA Enterprise Log Manager depende del servidor de CA EEM para gestionar cuentas de usuario y configuraciones del servicio. Si la aplicación de CA Enterprise Log Manager no está registrada, el software no se ejecutará correctamente.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Registre manualmente la aplicación de CA Enterprise Log Manager con el servidor de CA EEM.

Para registrar la aplicación de CA Enterprise Log Manager

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM.
5. Ejecute el comando siguiente:

   ```
   ./EEMRegister.sh
   ```

   El script shell registrará la aplicación de CA Enterprise Log Manager con el servidor de CA EEM.

Adquisición de certificados desde el servidor de CA EEM

Síntoma:

Durante la instalación, los certificados digitales no se adquirieron correctamente desde el servidor de CA EEM. Los certificados digitales son necesarios para iniciar y ejecutar la aplicación de CA Enterprise Log Manager.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Adquiera manualmente los certificados desde el servidor de CA EEM.

Para adquirir los certificados digitales

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM.
5. Ejecute el comando siguiente:

   ```
   ./EEMAcqCert.sh
   ```

   El script shell realizará el procesamiento necesario para adquirir los certificados digitales necesarios.

Importación de informes de CA Enterprise Log Manager

Síntoma:

Durante la instalación, el servidor de CA EEM no importó correctamente el contenido del informe desde el servidor de CA EEM. Debe importar el contenido del informe para ver los datos de los eventos después de almacenarse en el almacenamiento del registro de eventos.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Importe el contenido del informe manualmente.

Para importar contenido del informe

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM/content.
5. Ejecute el comando siguiente:

   ```
   ./ImportCALMContent.sh
   ```

   El script shell descargará el contenido del informe desde el servidor de CA EEM.

Importación de archivos de asignación de datos de CA Enterprise Log Manager

Síntoma:

Durante la instalación, el servidor de CA EEM no importó correctamente los archivos de asignación de datos (DM). Debe tener los archivos de DM para asignar datos de eventos entrantes al almacenamiento del registro de eventos.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Importe los archivos de DM manualmente.

Para importar archivos de DM

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM/content.
5. Ejecute el comando siguiente:

   ```
   ./ImportCALMDM.sh
   ```

   El script shell importará los archivos de DM desde servidor de CA EEM.

Importación de archivos de análisis de mensajes de CA Enterprise Log Manager

Síntoma:

Durante la instalación, el servidor de CA EEM no importó correctamente los archivos de análisis de mensajes (.XMP). Los archivos de análisis de mensajes son necesarios para gestionar los registros de eventos desde varios orígenes de eventos de la red. Debe disponer de los archivos de análisis de mensajes para poder insertar eventos en el almacenamiento del registro de eventos de CA Enterprise Log Manager.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Importe los archivos de análisis de mensajes manualmente.

Para importar archivos de análisis de mensajes

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM/content.
5. Ejecute el comando siguiente:

   ```
   ./ImportCALMMP.sh
   ```

   El script shell importará el contenido del archivo de análisis de mensajes desde el servidor de CA EEM.

Importación de archivos de gramática de eventos comunes (CEG)

Síntoma:

Durante la instalación, el servidor de CA EEM no importó correctamente los archivos de gramática de eventos comunes (CEG). La gramática de eventos comunes forma el esquema básico de la base de datos del almacenamiento del registro de eventos. No podrá almacenar los eventos en el almacenamiento del registro de eventos de CA Enterprise Log Manager sin los archivos de la gramática de eventos comunes.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Importe los archivos de CEG manualmente.

Para importar archivos de CEG

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM/content.
5. Ejecute el comando siguiente:

   ```
   ./ImportCALMCEG.sh
   ```

   El script shell importará los archivos de gramática de eventos.

Importación de archivos de gestión de agentes comunes

Síntoma:

Durante la instalación, el servidor de CA EEM no importó correctamente los archivos de gramática de eventos comunes. No puede gestionar agentes en la interfaz de usuario de CA Enterprise Log Manager sin estos archivos.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Importe los archivos de gestión de agentes manualmente.

Para importar archivos de gestión de agentes comunes

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM/content.
5. Ejecute el comando siguiente:

   ```
   ./ImportCALMAgentContent.sh
   ```

   El script shell importará los archivos de gestión de agentes comunes.

Importación de archivos de configuración de CA Enterprise Log Manager

Síntoma:

Durante la instalación, el servidor de CA EEM no importó correctamente los archivos de configuración. Puede iniciar CA Enterprise Log Manager, pero algunos de los ajustes y valores no se encontrarán en las áreas de configuración de servicios y no podrá configurar host individuales de forma central sin estos archivos.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Importe los archivos de configuración manualmente.

Para importar archivos de configuración

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM/content.
5. Ejecute el comando siguiente:

   ```
   ./ImportCALMConfig.sh
   ```

   El script shell importa los archivos de configuración.

Importación de archivos de supresión y resumen

Síntoma:

Durante la instalación, el servidor de CA EEM no importó correctamente los archivos de supresión y resumen. No podrá emplear las reglas predeterminadas de supresión y resumen de la interfaz de usuario de CA Enterprise Log Manager sin estos archivos.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Importe los archivos de supresión y resumen manualmente.

Para importar archivos de supresión y resumen

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM/content.
5. Ejecute el comando siguiente:

   ```
   ./ImportCALMSAS.sh
   ```

   El script shell importa los archivos de supresión y resumen.

Importación de archivos de tokens de análisis

Síntoma:

Durante la instalación, el servidor de CA EEM no importó correctamente los archivos de tokens de análisis. No podrá emplear los tokens de análisis predeterminados en el asistente de análisis de mensajes sin estos archivos.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Importe los archivos de tokens de análisis manualmente.

Para importar archivos de tokens de análisis

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM/content.
5. Ejecute el comando siguiente:

   ```
   ./ImportCALMTOK.sh
   ```

   El script shell importa los archivos de tokens de análisis.

Importación de archivos de la interfaz de usuario de CA Enterprise Log Manager

Síntoma:

Durante la instalación, el servidor de CA EEM no importó correctamente los archivos de la interfaz de usuario. No podrá visualizar ni utilizar los valores de los campos desplegables de intervalo de tiempo dinámico sin estos archivos.

El script shell del siguiente procedimiento se copia automáticamente en el directorio mencionado durante la instalación.

Solución:

Importe los archivos de la interfaz de usuario manualmente.

Para importar archivos de la interfaz de usuario

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 usuarios raíz con el siguiente comando:

   ```
   su -
   ```

4. Desplácese al directorio /opt/CA/LogManager/EEM/content.
5. Ejecute el comando siguiente:

   ```
   ./ImportCALMFlexFiles.sh
   ```

   El script shell importa los archivos de la interfaz de usuario.

Capítulo 4: Configuración de accesos y usuarios básicos

Esta sección contiene los siguientes temas:

Acerca de los accesos y usuarios básicos

La configuración comienza con el ajuste del almacén de usuarios, con la creación de uno o más usuarios con la función predefinida de administrador y con la configuración de políticas de contraseñas. Normalmente, esta configuración la realiza el instalador, que puede iniciar sesión en CA Enterprise Log Manager con las credenciales de EiamAdmin. Una vez finalizada la configuración, los usuarios definidos como administradores configuran CA Enterprise Log Manager.

Si se acepta la configuración predeterminada del almacén de usuarios, la configuración mínima que debe ser completada por el usuario de EiamAdmin es la cuenta del primer administrador. El primer administrador puede configurar políticas de contraseñas para poder configurar el resto de componentes de CA Enterprise Log Manager.

Nota: Si desea obtener más información acerca de la creación de otros usuarios o acerca de las funciones personalizadas y de las políticas de acceso personalizadas, consulte la *Guía de administración de CA Enterprise Log Manager*.

Configuración del almacén de usuarios

El almacén de usuarios es el repositario de la información global de los usuarios. Puede configurar el almacén de usuarios en cuanto instale un servidor de CA Enterprise Log Manager. Sólo el usuario de EiamAdmin puede configurar el almacén de usuarios, algo que normalmente se realiza después de iniciar sesión la primera vez.

Configure el almacén de usuarios de una de las siguientes maneras:

- Acepte el almacén predeterminado en el almacén de datos interno.

  Nota: La opción predeterminada podría mostrarse como la base de datos de gestión de CA si, durante la instalación, ha marcado un CA EEM independiente.

- Seleccione Referencia en un directorio externo, que puede ser un directorio de LDAP como Microsoft Active Directory, Sun One o Novell CA Directory.

- Seleccione Referencia en CA SiteMinder.

Si configura el almacén de usuarios como directorio externo, no podrá crear usuarios nuevos. Sólo podrá agregar grupos de aplicaciones, o funciones, predefinidas o definidas por el usuario a los registros de usuarios globales de sólo lectura. Debe agregar nuevos usuarios del almacén de usuarios externos y, a continuación, agregar los permisos de CA Enterprise Log Manager a los registros de usuarios globales.

Aceptación del almacén de usuarios predeterminado

No es necesario que configure el almacén de usuarios si acepta el predeterminado, que es el almacén de datos interno. Esto se aplica si no existe ningún almacén de usuarios para utilizar.

Para comprobar que el repositorio está configurado como el almacén de usuarios

1. Inicie sesión en un servidor de CA Enterprise Log Manager como usuario con privilegios de administrador o con el nombre de usuario y la contraseña asociada de EiamAdmin.
2. Haga clic en la ficha Administración.

   Si inicia sesión como usuario de EiamAdmin, esta ficha se mostrará automáticamente.

3. Seleccione la subficha Gestión de usuarios y accesos y, a continuación, haga clic en el botón Almacén de usuarios en el panel izquierdo.

   Se mostrará la configuración del servidor de EEM para usuarios y grupos globales.

4. Compruebe que la opción Guardar en almacén de datos interno esté seleccionada.

5. Haga clic en Guardar y, a continuación, en Cerrar.

Nota: Cuando está establecido el almacén de usuarios predeterminado, puede crear nuevos usuarios, definir contraseñas temporales y establecer políticas de contraseñas.

Más información:

Planificación del almacén de usuarios (en la página 43)

Utilización de un directorio de LDAP

Configure el almacén de usuarios como referencia a un directorio de LDAP cuando los detalles de los usuarios globales se almacenen en Microsoft Active Directory, Sun One o Novell Directory.

Nota: Los detalles de la aplicación se almacenan en el repositorio predeterminado. La utilización de un almacén de usuarios externo no actualiza ese almacén de usuarios.

Para utilizar un directorio de LDAP como almacén de usuarios

1. Inicie sesión en un servidor de CA Enterprise Log Manager como usuario con privilegios de administrador o como usuario de EiamAdmin.

2. Haga clic en la ficha Administración.

   Si inicia sesión como usuario de EiamAdmin, esta ficha se mostrará automáticamente.

3. Seleccione la subficha Gestión de usuarios y accesos y, a continuación, haga clic en Almacén de usuarios en el panel izquierdo.

   Se mostrará la configuración del servidor de CA EEM del almacén de usuarios.

4. Seleccione Referencia en un directorio externo.

   Se mostrarán los campos de la configuración de LDAP.

5. Complete debidamente estos campos en la hoja de trabajo del directorio externo.

   Tenga en cuenta el siguiente ejemplo para realizar el enlace a objetos de Active Directory con la siguiente cadena de enlace:

   Set objUser = Get Object ("LDAP://cn=Bob, cn=Users, ou=Sales, dc=MyDomain, dc=com"), donde cn es el nombre común, ou es la unidad organizativa y dc está formado por dos componentes de dominio que completan el nombre DNS. Para el nombre de dominio de usuario, debe introducir:

   ```
   cn=Bob,cn=Users,ou=Sales,dc=MyDomain,dc=com
   ```

6. Haga clic en Guardar.

   Al guardar esta referencia, la información de cuenta del usuario se cargará en CA EEM. De esta forma, podrá acceder a estos registros de usuarios como usuario global y agregar detalles de la aplicación como, por ejemplo, el grupo de usuarios de aplicaciones o el nombre de la función del usuario.

7. Revise el estado que se muestra para comprobar si el enlace del directorio externo es correcto y si se han cargado los datos.

   Si el estado muestra una advertencia, haga clic en el estado Actualizar. Si el estado muestra un error, corrija la configuración, haga clic en Guardar y repita este paso.

8. Haga clic en Cerrar.

Más información:

Planificación del almacén de usuarios (en la página 43)
Hoja de trabajo del directorio de LDAP (en la página 45)

Utilización de CA SiteMinder como almacén de usuarios

Si sus cuentas de usuario ya se han definido en CA SiteMinder, utilice este directorio externo cuando configure el almacén de usuarios.

Para utilizar CA SiteMinder como el almacén de usuarios

1. Inicie sesión en un servidor de CA Enterprise Log Manager como usuario con privilegios de administrador o como usuario de EiamAdmin.
2. Haga clic en la ficha Administración.

   Si inicia sesión como usuario de EiamAdmin, esta ficha se mostrará automáticamente.

3. Seleccione la subficha Gestión de usuarios y accesos y, a continuación, haga clic en el botón Almacén de usuarios en el panel izquierdo.

   Se mostrará la configuración del servidor de CA EEM del almacén de usuarios.

4. Seleccione la opción Referencia en CA SiteMinder.

   Aparecerán los campos específicos de CA SiteMinder.

   a. Complete debidamente estos campos en la hoja de trabajo de SiteMinder.

   b. Para ver o cambiar las conexiones y puertos utilizados por CA SiteMinder, haga clic en los puntos suspensivos para mostrar el panel de atributos de conexión.

5. Haga clic en Guardar.

   Al guardar esta referencia, la información de cuenta del usuario se cargará en CA EEM. De esta forma, podrá acceder a estos registros de usuarios como usuario global y agregar detalles de la aplicación como, por ejemplo, el grupo de usuarios de aplicaciones o el nombre de la función del usuario.

6. Revise el estado que se muestra para comprobar si el enlace del directorio externo es correcto y si se han cargado los datos.

   Si el estado muestra una advertencia, haga clic en el estado Actualizar. Si el estado muestra un error, corrija la configuración, haga clic en Guardar y repita este paso.

7. Haga clic en Cerrar.

Más información:

Planificación del almacén de usuarios (en la página 43)
Hoja de trabajo de CA SiteMinder (en la página 46)

Configuración de políticas de contraseñas

Puede establecer políticas de contraseñas para asegurarse de que las contraseñas creadas por los usuarios cumplan los estándares configurados y para que cambien con la frecuencia definida. Establezca políticas de contraseñas después de configurar el almacén de usuarios interno. Sólo el usuario de EiamAdmin o un usuario con privilegios de administrador puede definir o modificar las políticas de contraseñas.

Nota: Las políticas de contraseñas de CA Enterprise Log Manager no se aplican a las cuentas de usuario creadas en un almacén de usuarios externo.

Para configurar las políticas de contraseñas

1. Inicie sesión en un servidor de CA Enterprise Log Manager como usuario con privilegios de administrador o como usuario de EiamAdmin.
2. Haga clic en la ficha Administración.

   Si inicia sesión como usuario de EiamAdmin, esta ficha se mostrará automáticamente.
3. Seleccione la subficha Gestión de usuarios y accesos y, a continuación, haga clic en el botón Políticas de contraseñas en el panel izquierdo.

   Aparecerá el panel de políticas de contraseñas.
4. Especifique si desea que las contraseñas sean iguales a los nombres de usuario.
5. Especifique si desea que se apliquen requisitos de longitud.
6. Especifique si desea aplicar políticas sobre el número máximo o mínimo de caracteres que se repite o sobre los caracteres numéricos.
7. Especifique la duración y reutilice las políticas.
8. Compruebe los distintos parámetros y, a continuación, haga clic en Guardar.
9. Haga clic en Cerrar.

   Las políticas de contraseñas configuradas se aplican a todos los usuarios de CA Enterprise Log Manager.

Más información:

Planificación de políticas de contraseñas (en la página 48)
Nombre de usuario como contraseña (en la página 49)
Reutilización y duración de contraseñas (en la página 49)
Formato y longitud de la contraseña (en la página 50)

Conservación de políticas de acceso predefinidas

Si sólo va a utilizar las funciones o los grupos de usuarios de aplicaciones predefinidos con las políticas predefinidas asociadas, el riesgo de que las políticas se eliminen o se dañen debe ser mínimo. Sin embargo, si sus administradores van a crear funciones definidas por el usuario y políticas de acceso asociadas, se podrá acceder a las políticas predefinidas, se podrán editar y, por lo tanto, serán vulnerables a cambios no deseados. Se recomienda realizar una copia de seguridad de las políticas originales predefinidas para poder restaurarlas en caso de que sea necesario.

Cree un archivo de copia de seguridad que contenga cada tipo de política predefinida utilizando la función de exportación. Puede copiar estos archivos a un medio externo o dejarlos en el disco del servidor en el que se inició la exportación.

Nota: Para obtener más información sobre los procedimientos de realización de copias de seguridad de políticas predefinidas, consulte la *Guía de administración de CA Enterprise Log Manager*.

Creación del primer administrador

Al primer usuario que crea debe asignársele la función de administrador. Sólo los usuarios a los que se les asigna la función de administrador pueden realizar la configuración. Puede asignar una función de administrador a una nueva cuenta de usuario que cree o a una cuenta de usuario existente recuperada en CA Enterprise Log Manager.

Siga el siguiente proceso:

1. Inicie sesión en el servidor de CA Enterprise Log Manager como usuario predeterminado de EiamAdmin.
2. Cree el primer administrador.

   El método utilizado para crear el primer administrador de CA Enterprise Log Manager depende de cómo configure el almacén de usuarios.

   - Si configura CA Enterprise Log Manager para que utilice el almacén de usuarios interno, cree una nueva cuenta de usuario con la función de administrador.
   - Si configura CA Enterprise Log Manager para utilizar un almacén de usuarios externo, utilice un usuario de LDAP existente para vincular al directorio. Cuando lo vincule a un directorio externo, recupere la cuenta del usuario al que desee asignar una función de CA Enterprise Log Manager del almacén de usuarios externo. Las cuentas de usuarios de almacenes de usuarios externos se recuperan como usuarios globales. No puede modificar la información de una cuenta de usuario existente, pero puede agregar una función o un grupo de usuarios de aplicaciones de CAELM. Al primer usuario le asigna la función de administrador.

   Nota: No puede crear nuevos usuarios de CA Enterprise Log Manager cuando configura un almacén de usuarios externo.
3. Cierre sesión del servidor de CA Enterprise Log Manager.
4. Vuelva a iniciar sesión en el servidor de CA Enterprise Log Manager con las credenciales de la nueva cuenta de usuario.

   A continuación, podrá realizar las tareas de configuración.

Creación de una nueva cuenta de usuario.

Puede crear una cuenta de usuario para cada persona que utilice CA Enterprise Log Manager. Usted proporciona las credenciales con las que el usuario va a iniciar sesión la primera vez y especifica su función. Las tres funciones principales son: administrador, analista y auditor. Cuando un usuario al que se le ha asignado la función de analista o auditor inicia sesión, CA Enterprise Log Manager autentica al usuario con las credenciales guardadas y le permite utilizar varias funcionalidades según la función asignada.

Para crear un nuevo usuario

1. Inicie sesión en el servidor de CA Enterprise Log Manager como usuario predeterminado de EiamAdmin.

   Se mostrará la ficha Administración y la subficha Gestión de usuarios y accesos.

2. Haga clic en Usuarios en el panel izquierdo.
3. Haga clic en Nuevo usuario a la izquierda de la carpeta Usuarios.

   La pantalla de detalles Nuevo usuario se mostrará a la derecha de la ventana.

4. Escriba un nombre de usuario en el campo Nombre. Los nombres de usuario no distinguen mayúsculas de minúsculas.
5. Haga clic en Agregar detalles de usuarios de aplicaciones.
6. Seleccione la función asociada a las tareas que va a realizar el usuario. Utilice el control de cambios para moverlo a la lista Grupos de usuarios seleccionados.
7. Introduzca los valores de los campos restantes en la pantalla según sea necesario. Debe incluir una contraseña que distingue mayúsculas de minúsculas con confirmación en el cuadro de grupo de autenticación.
8. Haga clic en Guardar y, a continuación, en Cerrar.

Más información:

Asignación de funciones a usuarios globales (en la página 143)

Asignación de funciones a usuarios globales

Puede buscar una cuenta de usuario existente y asignar el grupo de usuarios de la aplicación de la función que desee que lleve a cabo el usuario. Si emplea un almacén de usuarios externo, la búsqueda da como resultado registros globales cargados desde dicho almacén de usuarios. Si el almacén de usuarios configurado es el de CA Enterprise Log Manager, la búsqueda obtiene registros creados para usuarios en CA Enterprise Log Manager.

Los administradores son los únicos que pueden editar cuentas de usuario.

Para asignar una función o un grupo de usuarios de la aplicación a un usuario existente

1. Haga clic en la ficha Administración y en la subficha Gestión de usuarios y accesos.
2. Haga clic en Usuarios en el panel de la izquierda.

   Aparecen los paneles Buscar usuarios y Usuarios.
3. Seleccione Usuarios globales, introduzca los criterios de búsqueda y haga clic en Ir.

   Si la búsqueda es de cuentas de usuario cargadas, el panel Usuarios muestra la ruta y las etiquetas de la ruta indican el directorio externo al que se hace referencia.

   Importante: Introduzca siempre criterios al realizar una búsqueda para evitar que aparezcan todas las entradas de un almacén de usuarios externo.
4. Seleccione un usuario global que no pertenezca al grupo de aplicaciones de CA Enterprise Log Manager.

   La página Usuario muestra, con el nombre de carpeta, los detalles de usuarios globales y, si procede, la pertenencia a grupos globales.
5. Haga clic en Agregar detalles del usuario de la aplicación.

   El panel de detalles del usuario de "CAELM" se expande.
6. Seleccione el grupo deseado en los grupos de usuarios disponibles y haga clic en la flecha hacia la derecha.

   El grupo seleccionado aparece en el cuadro de grupos de usuarios seleccionados.
7. Haga clic en Guardar.
8. Verifique la adición.
   a. En el panel Buscar usuarios, haga clic en Detalles del usuario de la aplicación y haga clic en Ir.
   b. Verifique que el nombre del nuevo usuario de la aplicación aparece en los resultados que se muestran.
9. Haga clic en Cerrar.

Capítulo 5: Configuración de servicios

Esta sección contiene los siguientes temas:

Configuraciones y orígenes de eventos

La mayoría de las redes cuenta con algunos dispositivos basados en syslog y en Windows cuyos registros de eventos se deben recopilar, almacenar, controlar y auditar. Su red también puede disponer de otros tipos de dispositivos, entre los que se incluyen aplicaciones, bases de datos, lectores de tarjetas, dispositivos biométricos, así como Recorders o iRecorders de CA Audit existentes. Los servicios, adaptadores, agentes y conectores de CA Enterprise Log Manager representan las configuraciones necesarias para conectarse a estos orígenes de eventos para recibir datos de eventos.

Los servicios de CA Enterprise Log Manager incluyen las siguientes áreas de configuración:

- Configuraciones globales
- Configuración y filtros globales
- Configuración del almacenamiento del registro de eventos
- Configuración del servidor de ODBC
- Configuración del servidor de informes
- Configuración del módulo de suscripción
- Panel de acceso al estado del sistema

Las configuraciones de servicio pueden ser globales, lo que significa que pueden afectar a todos los servidores de CA Enterprise Log Manager instalados con un solo nombre de instancia de aplicación en el servidor de gestión. Las configuraciones también pueden ser locales de modo que sólo afecten a un servidor seleccionado. Las configuraciones se almacenan en el servidor de gestión con una copia local en el servidor de recopilación de CA Enterprise Log Manager. De esta forma, si la conectividad de red se pierde o el servidor de gestión se apaga por alguna razón, la generación de registros de eventos no se detiene en los servidores de recopilación.

El panel de acceso al estado del sistema ofrece herramientas para asignarlas al servidor de CA Enterprise Log Manager y sus servicios, así como para recopilar información para el soporte. Puede disponer de más información sobre esta área en la guía de administración y en la ayuda en línea.

Edición de configuraciones globales

Puede definir configuraciones globales para todos los servicios. Si intenta guardar valores que se encuentran fuera del intervalo permitido, CA Enterprise Log Manager adoptará de forma predeterminada al valor mínimo o máximo, según corresponda. Algunos de los ajustes son interdependientes.

Para editar configuraciones globales

1. Haga clic en la ficha Administración y, a continuación, en la subficha Servicios.

   Aparece la lista de servicios.

2. Haga clic en Configuración global en la lista de servicios.

   Se abre el panel de detalles de la configuración del servicio global.

3. Cambie cualquiera de los ajustes de configuración siguientes:

   Intervalo de actualización

   Especifica la frecuencia, en segundos, con la que los componentes del servidor aplican actualizaciones de configuración.

   Mínimo: 30

   Máximo: 86.400

   Tiempo de espera de sesión

   Especifica la duración máxima de una sesión inactiva. Si se activa la actualización automática, la sesión nunca caduca.

   Mínimo: 10

   Máximo: 60

Permitir actualización automática

Permite a los usuarios actualizar los informes y las consultas de forma automática. Este valor permite a los administradores desactivar la actualización automática de forma global.

Frecuencia de la actualización automática

Especifica el intervalo (en minutos) en el que se actualiza la visualización del informe. Este valor depende de la selección de Permitir actualización automática.

Mínimo: 1

Máximo: 600

Permitir actualización automática

Establece la actualización automática en todas las sesiones. De forma predeterminada, la actualización automática no está activada.

La visualización de las alertas de acción requiere autenticación

Evita que los auditores o los productos de terceros vean las fuentes RSS de las alertas de acción. Este ajuste está activado de forma predeterminada.

Informe predeterminado

Especifica el informe predeterminado.

Activar inicio de informe predeterminado

Muestra el informe predeterminado cuando se hace clic en la ficha Informes. Este ajuste está activado de forma predeterminada.

4. Cambie cualquiera de los valores de etiquetas de informe y consulta siguientes:

Ocultar etiquetas de informe

Evita que las etiquetas especificadas aparezcan en una lista de etiquetas. Al ocultar las etiquetas de informe se simplifica la visión de los informes disponibles.

Ocultar etiquetas de consulta

Permite ocultar las etiquetas seleccionadas. Las etiquetas ocultas no aparecen en la lista de consultas principal ni en la lista de consultas sobre la programación de alertas de acción. Al ocultar las etiquetas de consulta se personaliza la vista de las consultas disponibles.

5. Cambie cualquiera de los ajustes de perfil siguientes:

   Activar perfil predeterminado

   Permite definir el perfil predeterminado.

   Perfil predeterminado

   Especifica el perfil predeterminado.

   Ocultar perfiles

   Permite ocultar los perfiles seleccionados. Cuando la interfaz se actualiza o caduca el intervalo de actualización, los perfiles ocultos no aparecen. Al ocultar los perfiles se personaliza la vista de los perfiles disponibles.

   Nota: Haga clic en Restablecer para almacenar los últimos valores guardados. Hasta que guarde los cambios, puede restablecer un solo cambio o varios. Una vez que haya guardado los cambios, deberá restablecerlos de forma individual.

6. Haga clic en Guardar.

Empleo de filtros y valores de configuración globales

Puede definir filtros y valores de configuración globales como parte de la configuración del servidor de CA Enterprise Log Manager. Los valores globales sólo se guardan en la sesión actual y no se conservan cuando cierra la sesión del servidor, a no ser que seleccione la opción Utilizar como predeterminado.

Un *filtro rápido* controla el intervalo de tiempo inicial sobre el que generar un informe, proporciona un filtrado sencillo de texto coincidente y le permite utilizar campos específicos y sus valores que afectan a los datos que se muestran en un informe.

Un *filtro avanzado* global le permite utilizar operadores y sintaxis SQL para ampliar los datos del informe. La configuración global le permite establecer una zona horaria y utilizar consultas especiales para recuperar datos de otros servidores de CA Enterprise Log Manager de una federación, así como activar la actualización automática de informes durante la visualización.

Debe establecer filtros globales que se puedan utilizar en varias áreas de informes. Al configurar las opciones que limitan el filtro global, podrá controlar los datos que se muestren en un informe. Entre las tareas iniciales de filtros y valores de configuración globales se incluyen las siguientes:

- Configure filtros rápidos globales para proporcionar una hora inicial que afecte a los informes que verá en el servidor de CA Enterprise Log Manager.
- Seleccione las consultas federadas en la ficha Configuración para ver los datos de los servidores de CA Enterprise Log Manager que ha federado en este servidor.
- Decida si desea que los informes se actualicen automáticamente.
- Defina el intervalo con el que desea que se actualicen los datos de los informes.

Nota: Si la configuración del filtro global es demasiado limitada o específica, es posible que no se muestren datos en algunos informes.

Para obtener más información sobre los filtros globales y su empleo, consulte la ayuda en línea.

Más información:

Edición de configuraciones globales (en la página 146)

Selección de uso de consultas federadas

Puede seleccionar si desea ejecutar consultas en los datos federados. Si va a utilizar más de un servidor de CA Enterprise Log Manager en una red federada, es posible que active la casilla de verificación Utilizar consultas federadas. Esta opción le permite recopilar datos de eventos para generar informes desde todos los servidores de CA Enterprise Log Manager federados (que actúan como servidores secundarios) con este servidor de CA Enterprise Log Manager.

También puede desactivar las consultas federadas para realizar una determinada consulta si sólo desea ver los datos del servidor de CA Enterprise Log Manager actual.

Para definir el uso de consultas federadas

1. Inicie sesión en el servidor de CA Enterprise Log Manager.
2. Haga clic en el botón Mostrar/editar filtros globales.

   El botón se encuentra a la derecha del nombre del servidor de CA Enterprise Log Manager actual y por encima de las fichas principales.
3. Haga clic en la ficha Configuración.

4. Seleccione si desea utilizar consultas federadas.

   Si desactiva la opción de selección de consultas federadas, los informes que vea *no* contendrán datos de eventos de los otros servidores que ha configurado como secundarios de este servidor.

Más información:

Configuración de una federación de CA Enterprise Log Manager (en la página 215)
Configuración de un servidor de CA Enterprise Log Manager como servidor secundario (en la página 216)

Configuración del intervalo de actualización global

Puede establecer el intervalo en el que los servicios de CA Enterprise Log Manager comprueban los cambios de configuración. El valor predeterminado, después de la instalación, es de cinco minutos y se expresa en segundos. Si el intervalo de tiempo es demasiado largo, algunos cambios de configuración necesarios podrían retrasarse.

Para configurar el intervalo de actualización

1. Inicie sesión en el servidor de CA Enterprise Log Manager y haga clic en la ficha Administración.
2. Haga clic en la ficha Servicios y, a continuación, haga clic en el nodo de servicio Configuración global.
3. Introduzca un nuevo valor para el intervalo de actualización.

   El valor predeterminado y recomendado es 300 segundos.

Acerca de los filtros locales

Los filtros locales funcionan en un informe en tiempo real cuando lo ve y sobrescribe temporalmente la configuración global. Puede utilizar los filtros locales para refinar los datos de un informe y así poder resolver los incidentes de seguridad o buscar un informe específico en una lista de informes generados. Las tareas de configuración local incluye las siguientes acciones:

- Definir un nuevo filtro para un informe en tiempo real mientras lo ve
- Definir un filtro de una lista de informes generados para ver un subconjunto de la lista por hora y tipo de informe

La ayuda en línea contiene más información sobre los filtros de configuración local mientras ve un informe o una lista de informes.

Configuración del almacenamiento del registro de eventos

El almacenamiento del registro de eventos es la base de datos básica de propietario que contiene registros de eventos recopilados. Las opciones de configuración definidas para el servicio de almacenamiento del registro de eventos pueden ser globales o locales y pueden afectar al almacenamiento y archivado de eventos de los servidores de CA Enterprise Log Manager. El proceso de configuración del almacenamiento del registro de eventos incluye lo siguiente:

- Entender el servicio de almacenamiento del registro de eventos
- Entender el modo en que el almacenamiento del registro de eventos gestiona los archivos de almacenamiento
- Configurar los valores globales y locales del almacenamiento del registro de eventos

  También se incluye la configuración del tamaño de la base de datos, los valores de retención de archivos de almacenamiento básicos, las reglas de resumen para agregar eventos similares, las reglas de supresión para evitar que eventos específicos se almacenen en la base de datos, las relaciones de federación y las opciones de autoarchivación.

CA Enterprise Log Manager cierra automáticamente los archivos de la base de datos activa y crea archivos de almacenamiento cuando las bases de datos activas alcanzan la capacidad definida para este servicio. A continuación, CA Enterprise Log Manager abre nuevos archivos activos para continuar con las operaciones de registro de eventos. Puede configurar opciones de autoarchivación para gestionar estos archivos, pero sólo como una configuración local en cada servidor de CA Enterprise Log Manager.

Acerca del servicio de almacenamiento del registro de eventos

El servicio de almacenamiento del registro de eventos gestiona interacciones de la base de datos como las que se muestran a continuación:

- Inserción de nuevos eventos en la base de datos actual (caliente)
- Recuperación de eventos de las bases de datos federadas locales y remotas para realizar consultas e informes
- Creación de nuevas bases de datos cuando la base de datos actual esté completa
- Creación de nuevos archivos de almacenamiento y eliminación de archivos de almacenamiento antiguos
- Gestión de la caché de consultas de archivos
- Aplicación de reglas de resumen y de supresión
- Aplicación de reglas de transferencia de eventos seleccionados
- Definición de los servidores de CA Enterprise Log Manager que actúan como servidores secundarios federados respecto a este servidor de CA Enterprise Log Manager

Acerca de los archivos de almacenamiento

El servidor de CA Enterprise Log Manager crea automáticamente archivos de bases de datos tibias denominados archivos de *almacenamiento* cuando una base de datos caliente alcanza el parámetro Número máximo de filas especificado en el servicio de almacenamiento del registro de eventos. Los archivos de bases de datos calientes no se comprimen.

Cuando cambia la autoarchivación de un servidor de recopilación a un servidor de informes, las bases de datos tibias se eliminan del servidor de recopilación después de copiarse en el servidor de informes. El valor Número máximo de días de archivado no se aplica aquí.

Cuando cambia la autoarchivación de un servidor de informes a un servidor de almacenamiento remoto, las bases de datos tibias del servidor de informes no se eliminan después de copiarse al servidor de almacenamiento remoto. Por el contrario, estas bases de datos tibias se retienen en el servidor de informes hasta que se alcanza el valor Número máximo de días de archivado. Posteriormente, se *eliminan*. Sin embargo, se retiene un registro de estas bases de datos frías eliminadas para que pueda obtener detalles de la base de datos de almacenamiento en caso de que necesite esta información para realizar una restauración.

Cuando determine cómo configurar el valor Número máximo de días de archivado, tenga en cuenta el espacio en disco disponible en el servidor de informes. La configuración de Archivar espacio en disco establece el umbral. Si el espacio en disco disponible cae por debajo del porcentaje establecido, los datos del registro de eventos se eliminarán para disponer de más espacio cuando el valor Número máximo de días de archivado de esos datos no haya pasado.

Cuando no cambie la autoarchivación de un servidor de informes a un servidor de almacenamiento remoto, debe realizar manualmente las copias de seguridad de las bases de datos tibias y mover la copia a una ubicación de almacenamiento remota con una mayor frecuencia que el valor configurado Número máximo de días de archivado. De lo contrario, podría perder datos. Le recomendamos que realice diariamente copias de seguridad de los archivos para evitar una posible pérdida de datos y para conservar el espacio adecuado en disco. El servicio de almacenamiento del registro de eventos gestiona su propia caché interna de las consultas de bases de datos archivadas para mejorar el rendimiento cuando se ejecuta en consultas muy amplias o repetitivas.

Para obtener más información acerca de los archivos de almacenamiento, consulte la *Guía de administración de CA Enterprise Log Manager*.

Más información:

Ejemplo: Almacenamiento automático en tres servidores (en la página 167)

Acerca de la autoarchivación

La gestión de registros de eventos almacenados requiere una manipulación adecuada de las copias de seguridad y de los archivos restaurados. La configuración del servicio del almacenamiento del registro de eventos le proporciona un lugar centralizado para configurar y ajustar los tamaños de las bases de datos internas, las retenciones, y para definir opciones de autoarchivación. CA Enterprise Log Manager proporciona los siguientes scripts para ayudarle con estas tareas:

- backup-ca-elm.sh
- restore-ca-elm.sh
- monitor-backup-ca-elm.sh

Nota: Al utilizar estos scripts se da por hecho que ha establecido una autenticación no interactiva entre los dos servidores a través de claves RSA.

Los scripts de *copia de seguridad* y *restauración* utilizan la utilidad LMArchive para facilitar la copia de bases de datos tibias a o desde host remotos. Cuando finalizan las tareas, los scripts actualizan automáticamente los archivos de catálogo correspondientes. Puede copiarlos a servidores remotos o a otros servidores de CA Enterprise Log Manager. Si el host remoto al que envía los archivos es un servidor de CA Enterprise Log Manager, los scripts también actualizarán automáticamente los archivos de catálogo en el servidor de recepción. Además, los scripts eliminarán los archivos de almacenamiento del equipo local para evitar la duplicación de informes federados. De esta forma, los datos estarán disponibles para las consultas y para los informes. El almacenamiento fuera del sistema se denomina almacenamiento en frío. Puede restaurar archivos movidos al almacenamiento en frío para realizar consultas y generar informes.

El script de *control* ejecuta automáticamente el script de copia de seguridad utilizando la configuración especificada en la parte de autoarchivación de la configuración de servicio del almacenamiento del registro de eventos.

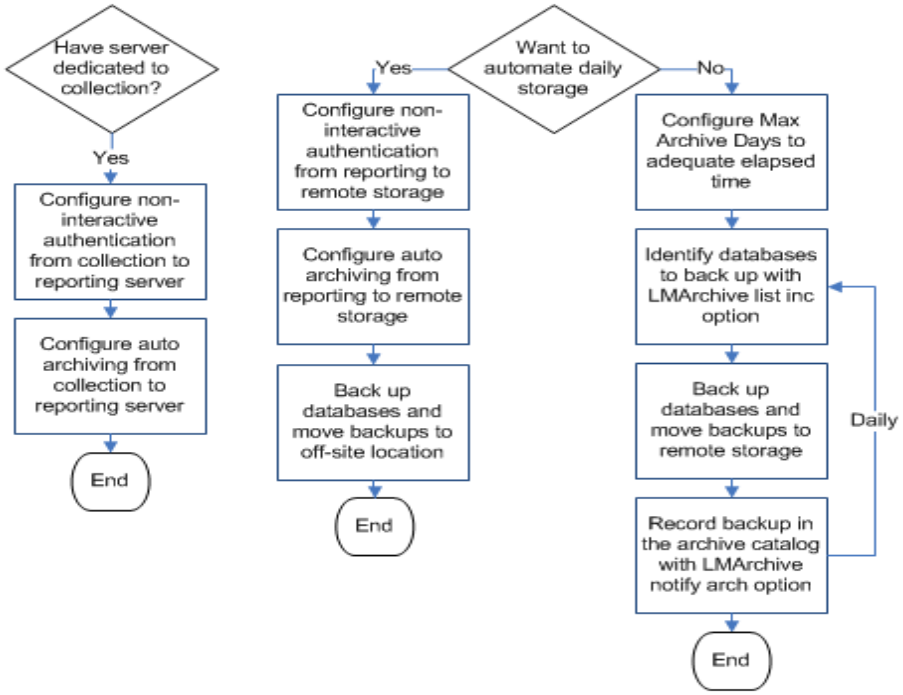
Más información:

Ejemplo: Almacenamiento automático en tres servidores (en la página 167)

Desplazamiento de la base de datos y copia de seguridad del diagrama de flujo de estrategia

Se puede ejecutar la recopilación y la generación de informes de eventos de cada servidor de CA Enterprise Log Manager o puede utilizar varios servidores diferentes para estas acciones. Si utiliza servidores para la recopilación, a continuación la automatización moverá cada hora desde servidores de recopilación a un servidor de informe; de lo contrario, no es aplicable. Si no tiene ningún rol de servidor específico, se interpretarán las referencias del diagrama de flujo "del servidor de informes al servidor de almacenamiento remoto" como "del servidor de CA Enterprise Log Manager no específico al servidor de almacenamiento remoto."

Una estrategia de copia de seguridad consiste en tener dos copias de cada base de datos; una de las dos es considerada como la copia de seguridad. Este objetivo puede lograrse con o sin archivado automático a un servidor de almacenamiento remoto. La estrategia de copia de seguridad con resultados de archivado automático en las bases de datos originales del servidor de almacenamiento remoto y en las copias de seguridad de una ubicación externa. La estrategia de copia de seguridad sin resultados de archivado automático en las bases de datos originales del servidor de CA Enterprise Log Manager y las copias de seguridad en un servidor de almacenamiento remoto. La posibilidad de almacenar las bases de datos originales en CA Enterprise Log Manager donde inicialmente se archivaron, depende del espacio disponible para el almacenamiento a largo plazo y de las políticas de almacenamiento. Si se cumplen estos criterios, la decisión dependerá de las preferencias personales.



Configuración de la autenticación no interactiva para el archivado automático

Se puede configurar el archivado automático entre servidores que tienen roles diferentes. Por ejemplo:

- Desde uno o más servidores de recopilación a un único servidor de informes.
- Desde uno o más servidores de informes a un único servidor de almacenamiento remoto.

Antes de configurar el archivado automático de un servidor a otro, debería configurar la autenticación *ssh* no interactiva desde el servidor de origen al servidor de destino. *No interactivo* significa que un servidor puede mover archivos a otro servidor sin que se requieran contraseñas.

- Si solamente dispone de tres servidores, un servidor de recopilación, un servidor de informes y un servidor de almacenamiento remoto, es recomendable configurar dos veces la autenticación no interactiva:
  - Desde el servidor de recopilación al servidor de informes
  - Desde el servidor de informes al servidor de almacenamiento remoto.
- Si dispone de seis servidores con cuatro servidores de recopilación, un servidor de informe y un servidor de almacenamiento remoto, debería configurar cinco veces la autenticación no interactiva:
  - Desde el servidor de recopilación 1 al servidor de informes.
  - Desde el servidor de recopilación 2 al servidor de informes.
  - Desde el servidor de recopilación 3 al servidor de informes.
  - Desde el servidor de recopilación 4 al servidor de informes.
  - Desde el servidor de informes al servidor de almacenamiento remoto.

Configuración de la autenticación ssh no interactiva entre dos servidores que utilizan pares de clave de RSA, una clave privada y una clave pública. Copie la primera clave pública que genere al servidor de destino como authorized_keys. Al configurar varias instancias de autenticación no interactiva al mismo servidor de informes de destino, debe copiar las claves públicas adicionales a los nombres de archivo únicos para evitar sobrescribir el archivo original authorized_keys. A continuación, concatene estos nombres de archivo a authorized_keys. Por ejemplo, debería anexar authorized_keys_ELM-C2 y authorized_keys_ELM-C3 al archivo authorized_keys desde ELM-C1.

Ejemplo: Configuración de la autenticación no interactiva para concentrador y periferia

La existencia de la autenticación no interactiva entre dos servidores es un requisito previo para el archivado automático desde el servidor de origen al de destino. Un escenario común para la configuración de la autenticación no interactiva consiste en un escenario en el cual los diversos servidores de origen específicos para la recopilación disponen de un servidor de destino común dedicado a la generación de informes/gestión. Este ejemplo comprende una federación mediana de CA Enterprise Log Manager con un servidor de informes/gestión (periferia), cuatro servidores de recopilación (concentrador) y un servidor de almacenamiento remoto. Los nombres para los servidores en cada rol de servidor son los siguientes:

- Servidor de informes/gestión de CA Enterprise Log Manager: ELM-RPT
- Servidores de recopilación de CA Enterprise Log Manager: ELM-C1, ELM-C2, ELM-C3, ELM-C4
- Servidor de almacenamiento remoto: RSS.

Los procedimientos para activar la autenticación no interactiva de la federación de CA Enterprise Log Manager son los siguientes:

1. Desde el primer servidor de recopilación, genere un par de claves de RSA como caelmservice y copie la clave pública como authorized_keys al directorio /tmp en el servidor de informes de destino.
2. Desde cada servidor de recopilación adicional, si hay alguno, genere un par de claves de RSA y copie la clave pública como authorized_keys_n, donde n únicamente identifica el origen.
3. Desde el servidor de informes del directorio /tmp, concatene el contenido de estos archivos de clave pública al archivo original authorized_keys. Cree un directorio .ssh y cambie la propiedad del directorio a caelmservice, mueva authorized_keys al directorio .ssh, y establezca la propiedad del archivo clave y los permisos necesarios.
4. Verifique que exista la autenticación no interactiva entre cada servidor de recopilación y el servidor de informes.
5. Desde el servidor de almacenamiento remoto, cree una estructura de directorios para el directorio .ssh, en el cual el valor predeterminado es /opt/CA/LogManager. Cree un directorio .ssh en el destino, cambie la propiedad a caelmservice.
6. Desde el servidor de informes, genere un par de claves de RSA como caelmservice y copie la clave pública como authorized_keys al directorio /tmp en el servidor de almacenamiento remoto de destino.
7. Desde el servidor de almacenamiento remoto, mueva authorized_keys de /tmp al directorio .ssh y configure la propiedad del archivo clave a caelmservice con los permisos necesarios.

8. Verifique que exista la autenticación no interactiva entre el servidor de informes y el servidor de almacenamiento remoto.

Configuración de las claves para el primer par de informes de recopilación

Configurar la autenticación no interactiva para una arquitectura de periferia y concentrador empieza con la generación de un par de claves públicas/privadas de RSA en un servidor de recopilación y la copia de la clave pública al servidor de informes. Copie el archivo de clave pública con el nombre *authorized_keys.* Suponga que esta clave es la primera clave pública copiada al servidor de informes especificado.

Para generar un par de claves en el primer servidor de recopilación, copie la clave pública en el servidor de informes.

1. Inicie sesión en ELM-C1 a través de ssh como usuario caelmadmin.
2. Cambie los usuarios a root.

   ```
   su –
   ```

3. Cambie los usuarios a la cuenta de caelmservice.

   ```
   su – caelmservice
   ```

4. Genere el par de claves RSA utilizando el siguiente comando:

   ```
   ssh-keygen –t rsa
   ```

5. Pulse Intro para aceptar los valores predeterminados cuando aparezcan las siguientes solicitudes:
   - Introduzca el archivo donde se guardará la clave (/opt/CA/LogManager/.ssh/id_rsa):
   - Introduzca la frase de contraseña (queda vacío si no se utiliza frase de contraseña):
   - Introduzca de nuevo la misma frase de contraseña:
6. Cambie los directorios a /opt/CA/LogManager.
7. Cambie los permisos del directorio .ssh utilizando el siguiente comando.

   ```
   chmod 755 .ssh
   ```

8. Vaya a .ssh, donde se guardará la clave id_rsa.pub.

   ```
   cd .ssh
   ```

9. Copie el archivo id_rsa.pub en ELM-RPT, el servidor de CA Enterprise Log Manager de destino, mediante el comando siguiente:

   ```
   scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys
   ```

   Así se creará el archivo authorized_keys en el servidor de informes con el contenido de la clave pública.

Configuración de las claves para los pares de informes de recopilación adicionales

El segundo paso de la configuración de la autenticación no interactiva para una arquitectura de concentrador y periferia consiste en la generación de un par de claves de RSA en cada servidor de recopilación adicional. También puede copiarse al directorio /tmp del servidor de generación de informes común como authorized_keys_n, en el cual n sólo se refiere al servidor de recopilación de origen.

Para generar un par de claves de RSA en servidores de recopilación adicionales y copiar la clave pública a un servidor de generación de informes común.

1. Inicie sesión en el segundo servidor de recopilación ELM-C2 a través de ssh como caelmadmin.
2. Cambie los usuarios a root.
3. Cambie los usuarios a la cuenta de caelmservice.

   ```
   su – caelmservice
   ```

4. Genere el par de claves RSA utilizando el siguiente comando:

   ```
   ssh-keygen –t rsa
   ```

5. Pulse Intro para aceptar los valores predeterminados cuando aparezcan las siguientes solicitudes:
   - Introduzca el archivo donde se guardará la clave (/opt/CA/LogManager/.ssh/id_rsa):
   - Introduzca la frase de contraseña (queda vacío si no se utiliza frase de contraseña):
   - Introduzca de nuevo la misma frase de contraseña:
6. Cambie los directorios a /opt/CA/LogManager.
7. Cambie los permisos del directorio .ssh utilizando el siguiente comando.

   ```
   chmod 755 .ssh
   ```

8. Vaya a .ssh, donde se guardará la clave id_rsa.pub.

9. Copie el archivo id_rsa.pub en ELM-RPT, el servidor de CA Enterprise Log Manager de destino, mediante el comando siguiente:

   ```
   scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C2
   ```

   Así se creará el archivo authorized_keys_ELM-C2 en el servidor de informes con el contenido de la clave pública.

10. Escriba Sí seguido de la contraseña caelmadmin de ELM-RPT
11. Escriba Salir.
12. Repita los pasos 1-11 de este procedimiento en los servidores de recopilación ELM-C3. Para el paso 9, especifique los siguientes valores:

    ```
    scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C3
    ```

13. Repita los pasos 1-11 de este procedimiento en los servidores de recopilación ELM-C4. Para el paso 9, especifique los siguientes valores:

    ```
    scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C4
    ```

Creación de un único archivo de clave pública en el servidor de informes y configuración de la propiedad de archivo

En el proceso que hemos seguido en este escenario, hasta este momento, se han generado pares de clave en cada servidor de recopilación y se ha copiado la parte de clave pública en el servidor de informes, así como los siguientes archivos:

- authorized_keys
- authorized_keys_ELM-C2
- authorized_keys_ELM-C3
- authorized_keys_ELM-C4

El paso 3 es concatenar estos archivos, mover el archivo de clave pública de RSA resultante al directorio correcto y configurar en caelmservice la propiedad de directorio y archivo.

Para crear el archivo de clave pública combinado en el directorio correcto del servidor de informes y establecer la propiedad del archivo

1. Inicie sesión en el servidor de informes de CA Enterprise Log Manager a través de ssh como usuario caelmadmin.
2. Cambie los usuarios a root.

3. Modifique los directorios de la carpeta de CA Enterprise Log Manager:

   ```
   cd /opt/CA/LogManager
   ```

4. Cree la carpeta .shh:

   ```
   mkdir .ssh
   ```

5. Cambie la propiedad de la nueva carpeta al grupo y al usuario caelmservice:

   ```
   chown caelmservice:caelmservice .ssh
   ```

6. Modifique los directorios a /tmp
7. Agregue el contenido de las claves públicas desde los servidores de recopilación ELM-C2, ELM-C3, and ELM-C4 al archivo authorized_keys que contiene la clave pública desde ELM-C1.

   ```
   cat authorized_keys_ELM-C2 >> authorized_keys
   ```

   ```
   cat authorized_keys_ELM-C3 >> authorized_keys
   ```

   ```
   cat authorized_keys_ELM-C4 >> authorized_keys
   ```

8. Cambie los directorios a /opt/CA/LogManager/.ssh
9. Copie el archivo authorized_keys desde la carpeta /tmp a la carpeta actual, .ssh:

   ```
   cp /tmp/authorized_keys .
   ```

10. Cambie la propiedad del archivo authorized_keys en la cuenta caelmservice:

    ```
    chown caelmservice:caelmservice authorized_keys
    ```

11. Cambie los permisos del archivo:

    ```
    chmod 755 authorized_keys
    ```

    755 medios leen y ejecutan el acceso para todos y el acceso de lectura, ejecución y escritura para el propietario del archivo

De esta forma, se completa la configuración de la autenticación que no requiere contraseñas entre los servidores de recopilación y el servidor de informes.

Cómo validar la autenticación no interactiva entre servidores de informes y de recopilación.

Puede validar la configuración de una autenticación no interactiva entre los servidores de origen y de destino de ambas fases de la autoarchivación.

Para validar la configuración entre los servidores de recopilación y de informes

1. Inicie sesión en el servidor de recopilación ELM-C1 a través de ssh como caelmadmin.
2. Cambie los usuarios a root.
3. Cambie los usuarios a la cuenta de caelmservice.

   ```
   su – caelmservice
   ```

4. Introduzca el siguiente comando:

   ```
   ssh caelmservice@ELM-RPT
   ```

   Iniciar sesión en ELM-RPT sin la introducción de una frase de contraseña confirma la autenticación no interactiva entre ELM-C1 y ELM-RPT.
5. Inicie sesión en ELM-C2 y repita.
6. Inicie sesión en ELM-C3 y repita.
7. Inicie sesión en ELM-C4 y repita.

Creación de una estructura de directorios con propiedades en el servidor de almacenamiento remoto

El procedimiento siguiente da por hecho que el servidor de almacenamiento remoto no es un servidor de CA Enterprise Log Manager y que se necesita crear usuarios nuevos, un grupo y una estructura de directorios que imite la del servidor de CA Enterprise Log Manager. Puesto que se utiliza la cuenta caelmadmin que se creó para comunicarse con el servidor de informes, debe ejecutarse este procedimiento antes de enviar la clave del servidor de informes.

Para crear una estructura de archivo y configurar propiedades de archivo en el servidor de almacenamiento remoto

1. Inicie sesión en el servidor de almacenamiento remoto, RSS, mediante ssh como root.
2. Cree un nuevo usuario denominado caelmadmin.
3. Cree un grupo denominado caelmservice y, a continuación, cree un nuevo usuario denominado caelmservice.

4. Cree el directorio que se utilizará como Ubicación remota, cuyo valor predeterminado es /opt/CA/LogManager.

   Nota: Para utilizar un directorio diferente, debe asegurarse de especificar el directorio, siempre que configure Ubicación remota para el archivado automático.

5. Modifique el directorio principal para caelmservice en /opt/CA/LogManager o el directorio Ubicación remota planificado. El ejemplo siguiente contiene el directorio predeterminado:

   ```
   usermod -d /opt/CA/LogManager caelmservice
   ```

6. Configure los permisos de archivo para caelmservice. El ejemplo siguiente contiene el directorio Ubicación remota predeterminado:

   ```
   chown -R caelmservice:caelmservice /opt/CA/LogManager
   ```

7. Modifique los directorios en /opt/CA/LogManager o la alternativa a Ubicación remota.

8. Cree la carpeta .shh.

9. Cambie la propiedad de la carpeta .ssh al grupo y al usuario caelmservice:

   ```
   chown caelmservice:caelmservice .ssh
   ```

10. Cierre la sesión del servidor de almacenamiento remoto.

Configure las claves para el par de almacenamiento remoto de informes

Después de la configuración y de la validación de la autenticación no interactiva desde cada servidor de recopilación al servidor de informes, configure y valide la autenticación no interactiva desde el servidor de informes al servidor de almacenamiento remoto.

Para el escenario de ejemplo, la configuración empieza con la generación de un par nuevo de claves de RSA en el servidor de informes, ELM-RPT, y con la copia de la clave pública como authorized_keys al directorio /tmp del servidor de almacenamiento remoto, RSS.

Para generar un par de claves de RSA en el servidor de informes y copiarlo en el servidor de almacenamiento remoto

1. Inicie sesión en el servidor de informes como caelmadmin.
2. Cambie los usuarios a root.

3. Cambie los usuarios a la cuenta de caelmservice.

   ```
   su – caelmservice
   ```

4. Genere el par de claves RSA utilizando el siguiente comando:

   ```
   ssh-keygen –t rsa
   ```

5. Pulse Intro para aceptar los valores predeterminados cuando aparezcan las siguientes solicitudes:

   - Introduzca el archivo donde se guardará la clave (/opt/CA/LogManager/.ssh/id_rsa):
   - Introduzca la frase de contraseña (queda vacío si no se utiliza frase de contraseña):
   - Introduzca de nuevo la misma frase de contraseña:

6. Cambie los directorios a /opt/CA/LogManager.

7. Cambie los permisos del directorio .ssh utilizando el siguiente comando.

   ```
   chmod 755 .ssh
   ```

8. Desplácese a la carpeta .ssh.

9. Copie el archivo id_rsa.pub en RSS, el servidor de almacenamiento remoto de destino, mediante el comando siguiente:

   ```
   scp id_rsa.pub caelmadmin@RSS:/tmp/authorized_keys
   ```

   Automáticamente se creará el archivo authorized_keys en el directorio /tmp en el servidor de almacenamiento remoto con el contenido de la clave pública.

Configuración de propiedad de archivo clave en el servidor de almacenamiento remoto

Se puede configurar la propiedad y los permisos de archivo clave en un servidor de almacenamiento remoto, después de la generación de un par de claves en el servidor de informes. Previamente, también debe hacerse una copia de la clave pública en el servidor de almacenamiento remoto.

Para mover el archivo de clave pública a la ubicación correcta del servidor de almacenamiento remoto y cómo establecer la propiedad del archivo

1. Inicie sesión en el servidor de almacenamiento remoto como caelmadmin.
2. Cambie los usuarios a root.

3. Modifique los directorios a /opt/CA/LogManager/.ssh.
4. Copie el archivo authorized_keys desde el directorio /tmp al directorio actual .ssh:

   ```
   cp /tmp/authorized_keys .
   ```

5. Cambie la propiedad del archivo authorized_keys con el siguiente comando:

   ```
   chown caelmservice:caelmservice authorized_keys
   ```

6. Cambie los permisos en el archivo authorized_keys:

   ```
   chmod 755 authorized_keys
   ```

   La autenticación no interactiva está ahora configurada entre un servidor de informes de CA Enterprise Log Manager y el host remoto utilizado para el almacenamiento.

Cómo validar la autenticación no interactiva entre los servidores de informes y de almacenamiento

Verifique la correcta configuración de la autenticación no interactiva entre el servidor de informes y el servidor de almacenamiento remoto. Para el escenario de ejemplo, el servidor de almacenamiento remoto se denominará RSS.

Para validar la autenticación no interactiva entre el servidor de informes de CA Enterprise Log Manager y el servidor de almacenamiento

1. Inicie sesión en el servidor de informes como root.
2. Modifique los usuarios a caelmservice.

   ```
   su – caelmservice
   ```

3. Introduzca el siguiente comando:

   ```
   ssh caelmservice@RSS
   ```

   De esta manera iniciará sesión en el servidor de almacenamiento remoto sin introducir una frase de contraseña.

Ejemplo: Configuración de una autenticación no interactiva en tres servidores

El escenario más sencillo para la configuración de la autenticación no interactiva, un requisito previo para el archivado automático, consiste en uno de los dos servidores de CA Enterprise Log Manager, un servidor de recopilación y un servidor de informes/de gestión y un sistema de almacenamiento remoto en un servidor de UNIX o de Linux. En este ejemplo se detalla que tres servidores están preparados para el archivado automático. Éstos son:

- NY-Recopilación-ELM
- NY-Informes-ELM
- NY-Almacenamiento-Svr

Los procedimientos para la activación de la autenticación no interactiva son los siguientes:

1. Desde NY-Recopilación-ELM, se generará el par de claves de RSA como caelmservice y se copiará la clave pública de este par como authorized_keys al directorio /tmp en NY-Informes-ELM.
2. Cree un directorio de .ssh en NY-Informes-ELM, cambie la propiedad a caelmservice, mueva authorized_keys del directorio /tmp al directorio de .ssh y configure el archivo clave de propiedad a caelmservice con los permisos necesarios.
3. Compruebe la autenticación no interactiva desde NY-Recopilación-ELM a NY-Informes-ELM.
4. Desde NY-Informes-ELM, se generará otro par de claves de RSA como caelmservice y se copiará la clave pública como authorized_keys al directorio /tmp de NY-Almacenamiento-Svr.
5. Desde NY-Almacenamiento-Svr, se creará la estructura de directorios /opt/CA/LogManager. A partir de esta ruta, cree un directorio de .ssh, cambie la propiedad a caelmservice, mueva authorized_keys al directorio y configure la propiedad de archivo clave a caelmservice con los permisos necesarios.
6. Compruebe la autenticación no interactiva desde NY-Informes-ELM a NY-Almacenamiento-Svr.

Los detalles para estos pasos son similares a los del escenario de concentrador y periferia. Para un escenario de tres servidores, omita el paso 2 en pares de informes de recopilación adicionales y omita las instrucciones del paso 3 acerca de la concatenación de archivos a authorized_keys.

Ejemplo: Almacenamiento automático en tres servidores

Al emplear la arquitectura de recopilación-informes, debe configurar el almacenamiento automático del servidor de recopilación en un servidor de informes. Esta configuración automatiza el traslado de una base de datos tibia de datos de registro de eventos refinados al servidor de informes, donde podrá realizar informes de ella. Es conveniente programar el almacenamiento automático cada hora, en lugar de cada día, para evitar destinar una gran cantidad de tiempo al día a la realización de grandes transferencias de datos. Seleccione una programación basada en la carga que tenga y en si prefiere unificar el procesamiento o extenderlo a lo largo del día. Cuando se copian bases de datos mediante el almacenamiento automático de un servidor de recopilación al servidor de informes correspondiente, dichas bases de datos se eliminan del servidor de recopilación.

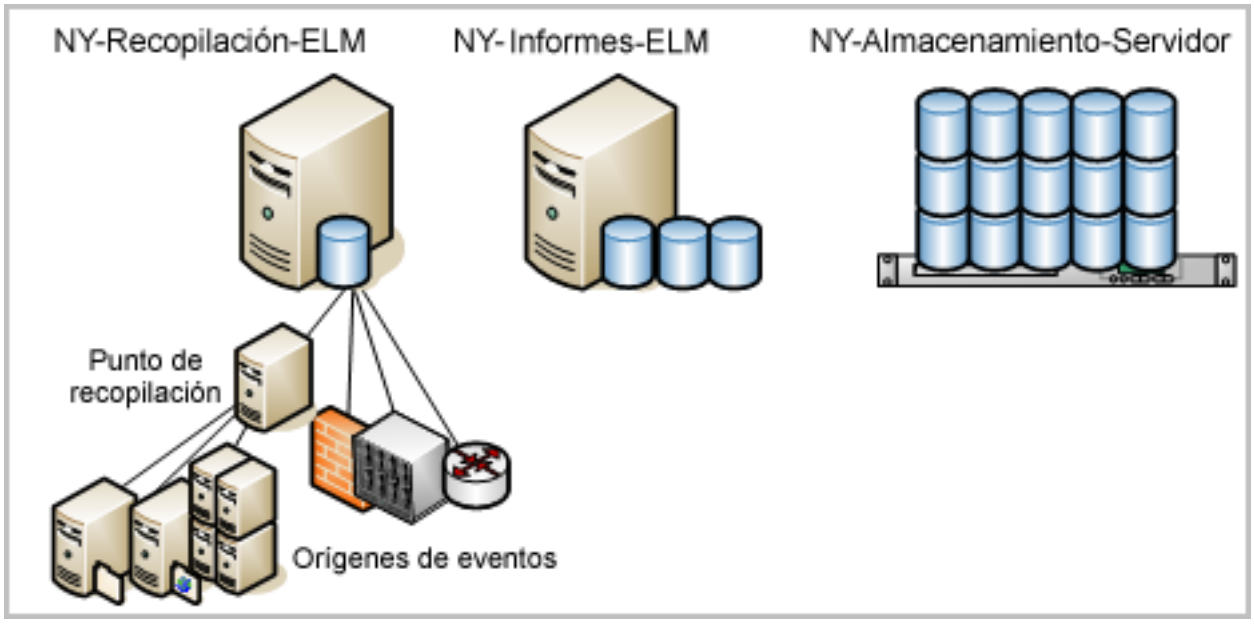
Después de identificar un servidor local con una gran cantidad de espacio de almacenamiento, puede configurar el almacenamiento automático desde el servidor de informes a este servidor de almacenamiento remoto. Cuando las bases de datos se copian mediante almacenamiento automático de un servidor de informes a un servidor de almacenamiento remoto, dichas bases de datos permanecen inalteradas en el servidor de informes hasta que se alcance la fecha configurada en Número máximo de días de archivado. En ese momento, se eliminan. La ventaja de esta fase de almacenamiento automático es la protección de las bases de datos frente a pérdidas por no trasladarlas de forma manual a una ubicación de almacenamiento a largo plazo antes de la eliminación automática.

Nota: Antes de configurar un servidor remoto para recibir bases de datos almacenadas automáticamente, debe establecer una estructura de directorios en este servidor de destino igual a la del servidor de CA Enterprise Log Manager de origen y asignar varios permisos y pertenencias para la autenticación. Para obtener detalles, consulte el apartado de configuración de autenticaciones no interactivas en la *Guía de implementación*. Asegúrese de seguir las instrucciones descritas en el apartado de establecimiento de la propiedad del archivo clave en un host remoto.

En este caso de ejemplo, asumiremos que el usuario es un administrador de CA Enterprise Log Manager en un centro de datos de Nueva York con una red de servidores de CA Enterprise Log Manager, cada uno de los cuales tiene una función dedicada, y con un servidor remoto con una gran capacidad de almacenamiento. A continuación, se indican los nombres de los servidores empleados en el almacenamiento automático:

- NY-Recopilación-ELM
- NY-Informes-ELM
- NY-Almacenamiento-Svr

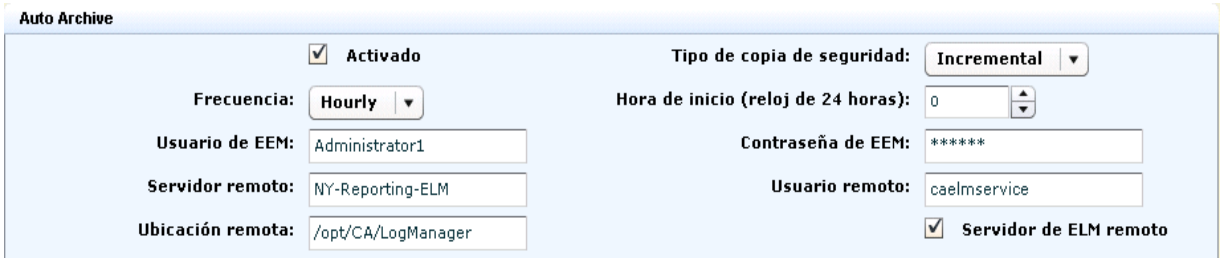
Nota: En este ejemplo, se supone la existencia de un servidor de gestión dedicado a la gestión del sistema de servidores de CA Enterprise Log Manager. Este servidor no se muestra aquí porque no desempeña un papel directo en el almacenamiento automático.



Para configurar el almacenamiento automático desde un servidor de recopilación a un servidor de informes y, a continuación, desde el servidor de informes a un servidor de almacenamiento remoto, utilice el ejemplo siguiente como guía:

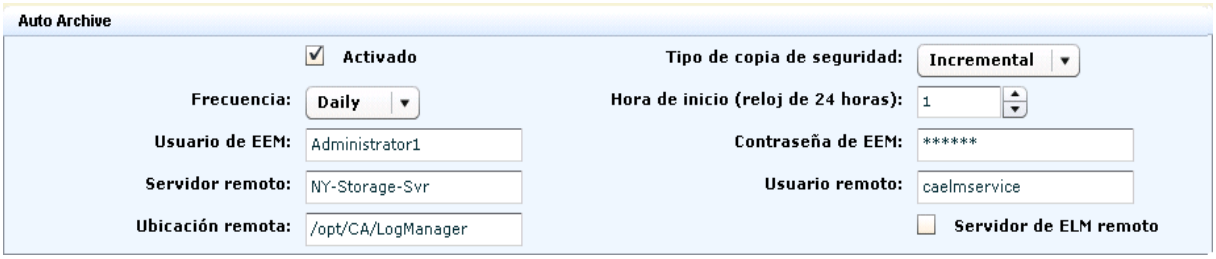
1. Seleccione la ficha Administración y la subficha Recopilación de registros.
2. Expanda la carpeta Almacenamiento de registro de eventos y seleccione un servidor de recopilación.

3. Especifique una frecuencia de almacenamiento automático horaria y designe como destino el servidor de informes. Introduzca las credenciales de un usuario de CA Enterprise Log Manager con función Administrator. Si tiene políticas personalizadas, debe ser un usuario con derechos de edición del recurso de la base de datos para poder eliminar la base de datos almacenada.

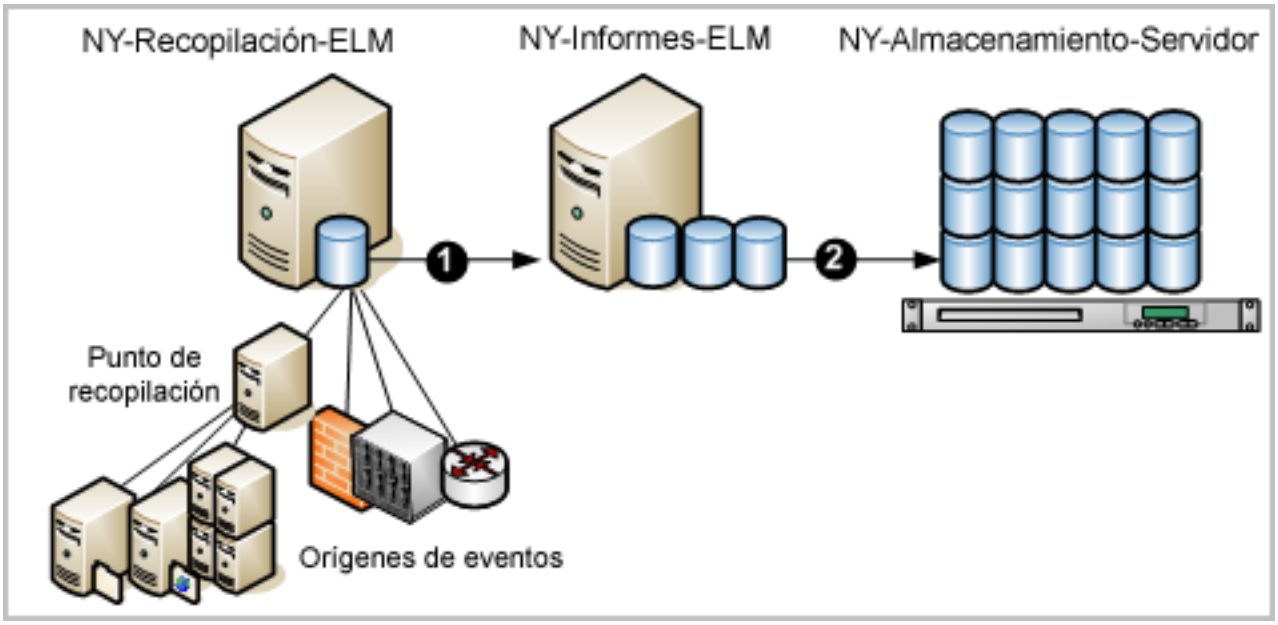


4. Seleccione el servidor de informes en la lista de servicios.

5. Especifique una frecuencia de almacenamiento automático diaria en la que el destino sea un servidor remoto empleado para el almacenamiento. Introduzca las credenciales de una cuenta de usuario con función Administrator. También puede crear una política de acceso a CALM con acción de edición en el recurso de la base de datos y asignar un usuario como identidad. Introduzca aquí las credenciales de dicho usuario con pocos privilegios.



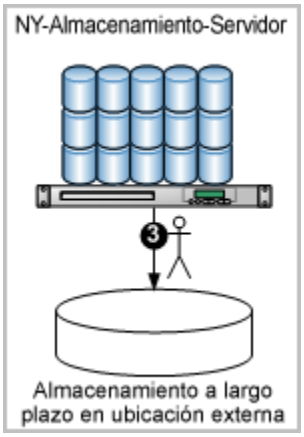
Los números del diagrama siguiente muestran dos configuraciones de almacenamiento automático: una del servidor de recopilación al servidor de informes, y otra del servidor de informes a un servidor remoto de la red.



Tras dicha confirmación, ese procesamiento automático funciona del modo siguiente:

1. NY-Recopilación-ELM, el servidor de recopilación de CA Enterprise Log Manager, recopila y refina eventos y los introduce en la base de datos caliente. Cuando la base de datos caliente alcanza el número configurado de registros, la base de datos se comprime en forma de base de datos tibia. Como el almacenamiento automático se ha programado con una frecuencia horaria, cada hora el sistema copia las bases de datos tibias y las traslada al servidor NY-Informes-ELM, el servidor de informes de CA Enterprise Log Manager. Las bases de datos tibias se eliminan de NY-Recopilación-ELM cuando se trasladan.
2. NY-Informes-ELM retiene las bases de datos que pueden recibir consultas hasta que alcancen la antigüedad configurada en Número máximo de días de archivado, tras lo cual, las elimina. Como el almacenamiento automático se ha programado con una frecuencia diaria, cada día el sistema copia las bases de datos tibias y las traslada como bases de datos frías a NY-Almacenamiento-Svr. Las bases de datos frías pueden permanecer en el servidor de almacenamiento remoto durante un largo período de tiempo.
3. Desplace las bases de datos frías almacenadas en el servidor NY-Almacenamiento-Svr de la red a una solución de almacenamiento a largo plazo exterior en la que puedan permanecer durante el número de años necesario.

   El motivo del almacenamiento es que los registros de eventos estén disponibles para su restauración. Las bases de datos frías se pueden restablecer si es necesario para investigar eventos antiguos que se han registrado. El paso manual para desplazar bases de datos almacenadas del servidor de almacenamiento interno a una ubicación de almacenamiento a largo plazo externa se ilustra en el diagrama siguiente.

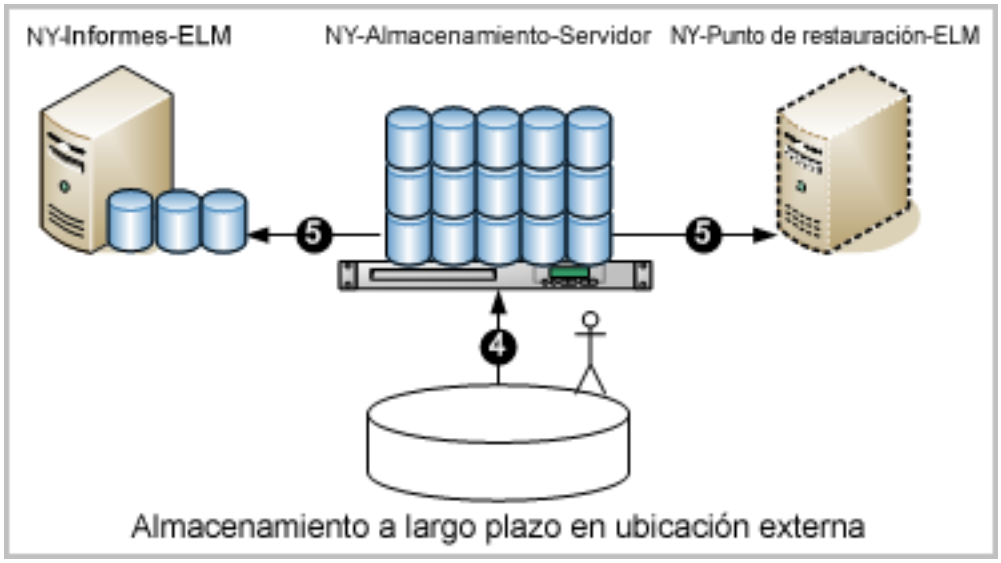


4. Supongamos que se produce una situación que hace necesario examinar registros que tienen copia de seguridad y se han trasladado a una ubicación exterior. Para identificar el nombre de la base de datos almacenada que se va a restaurar, busque el catálogo de archivos local en NY-Informes-ELM. (Haga clic en la ficha Administración, seleccione Consulta de catálogo de archivos en el explorador de recopilación de registros y haga clic en Consulta.)

5. Recupere la base de datos almacenada identificada del almacenamiento externo. Vuelva a copiarla en el directorio /opt/CA/LogManager/data/archive del servidor NY-Almacenamiento-Svr. A continuación, modifique la pertenencia del directorio de archivos al usuario caelmservice.

6. Restaure la base de datos en el servidor de informes original o en un punto de restauración dedicado para investigar los registros de las bases de datos restauradas del modo siguiente:

   - Si la restaura en NY-Informes-ELM, ejecute el script restore-ca-elm.sh desde NY-Informes-ELM y especifique NY-Almacenamiento-Svr como host remoto.
   - Si la restaura en NY-PuntoRestauración-ELM, ejecute el script restore-ca-elm.sh desde NY-PuntoRestauración-ELM y especifique NY-Almacenamiento-Svr como host remoto.



Nota: Ahora, podrá realizar consultas en los datos restaurados.

Más información:

Acerca de la autoarchivación (en la página 153)
Acerca de los archivos de almacenamiento (en la página 152)
Configuración del almacenamiento del registro de eventos en el entorno básico (en la página 173)
Ejemplo: Mapa de federación para una gran empresa (en la página 38)

Configuración del almacenamiento del registro de eventos en el entorno básico

En un entorno con servidores de CA Enterprise Log Manager independientes que tienen funciones de servidor de recopilación y servidor de informes, debe configurar los almacenamientos de registros de eventos de forma individual como configuraciones locales. Si también decide que el servidor de informes gestione el tráfico de conmutación por error, es posible que desee establecer un valor mayor para el campo Número máximo de filas que el que se muestra en la tabla. Si utiliza el servidor de gestión como servidor de informes, tenga en cuenta que el servidor de gestión genera alguna información de eventos como eventos autocontrolados.

Nota: Debe configurar cada par de servidores que participan en la autoarchivación para que la autenticación no interactiva de la configuración de autoarchivación funcione correctamente.

La siguiente tabla es un ejemplo. El servidor de recopilación de CA Enterprise Log Manager se denomina CollSrvr-1. El servidor de informes de CA Enterprise Log Manager se denomina RptSrvr-1. En este ejemplo, existe un servidor de almacenamiento remoto denominado RemoteStore-1 para almacenar archivos de bases de datos fríos, y esos archivos fríos se ubican en el directorio /CA-ELM_cold_storage.

Almacenamiento de registro de eventos campo	Servidor de recopilación valores	Valores del servidor de informes
Máximo de filas	2000000 (predeterminado)	No aplicable a la autoarchivación
Máximo de días de archivo	1 (no aplicable a la autoarchivación)	30 (aplicable a la autoarchivación cuando ésta no está configurada)
Archivar espacio en disco	10	10
Exportar política	24	72
Puerto de servicio seguro	17001	17001

Almacenamiento de registro de eventos campo	Servidor de recopilación valores	Valores del servidor de informes
Opciones de autoarchivación		
Activado	Sí	Sí
Tipo de copia de seguridad	Incremental	Incremental
Frecuencia	Cada hora	Diario
Hora de inicio	0	23
Usuario de EEM	<CA Enterprise Log Manager_Administrator>	<CA Enterprise Log Manager_Administrator>
Contraseña de EEM	*<contraseña>*	*<contraseña>*
Servidor remoto	RptSrvr-1	RemoteStore-1
Usuario remoto	caelmservice	user_X
Ubicación remota	/opt/CA/LogManager	/CA-ELM_cold_storage
Servidor remoto de CA-ELM	Sí	No

Las opciones de autoarchivación de este ejemplo mueven archivos de almacenamiento (archivos de bases de datos tibias) del servidor de recopilación al servidor de informes cada hora. De esta forma, hay espacio disponible en disco para los eventos entrantes. Ambos servidores utilizan un copia de seguridad incremental para evitar mover grandes volúmenes de datos en cualquier momento. Después de mover la base de datos tibia al servidor de informes, ésta se elimina automáticamente del servidor de recopilación.

Nota: El valor 0 para la hora de inicio no tiene ninguna repercusión cuando la frecuencia de la copia de seguridad se establece cada hora.

Para el usuario de EEM y para la contraseña de EEM, usted especifica las credenciales de un usuario de CA Enterprise Log Manager asignando la función predefinida de administrador o una función personalizada asociada a una política personalizada que permite realizar la acción de edición en el recurso de la base de datos.

En el servidor de informes, especifique /opt/CA/LogManager para la ubicación remota y caelmservice como usuario remoto si se realiza la autoarchivación desde el servidor de informes al servidor de almacenamiento remoto. Esta ruta y este usuario los crea cuando configura la autenticación no interactiva entre estos servidores.

Las opciones de autoarchivación de este ejemplo mueven diariamente los archivos de almacenamiento del servidor de informes al servidor de almacenamiento remoto a partir de las 11:00 p. m. Cuando una base de datos se mueve al almacenamiento en frío del servidor remoto, ésta se retiene en el servidor de informes durante el número máximo de días de archivado.

Si la autoarchivación no está activada, las bases de datos tibias se retienen en función de los umbrales configurados para el número máximo de días y para el espacio en disco, lo que ocurra primero. Las bases de datos archivadas se retendrían en el servidor de informes durante 30 días antes de eliminarse a no ser el espacio en disco esté por debajo del 10%. En ese caso, el servidor de informes generará un evento autocontrolado y eliminará las bases de datos más antiguas hasta que el espacio en disco esté por encima del 10%. Puede crear una alerta para que se le notifique por correo electrónico o por fuente RSS cuando esto se produzca.

Cuando se restaura una base de datos desde un servidor de almacenamiento remoto en el servidor de informes original, ésta se retiene durante tres días (72 horas).

Si desea obtener más información acerca de estos campos y de sus valores, consulte la ayuda en línea.

Opciones de la configuración del almacenamiento del registro de eventos

El cuadro de diálogo de la configuración del almacenamiento del registro de eventos le permite definir opciones globales para todos los servidores de CA Enterprise Log Manager. También puede hacer clic en la flecha que se encuentra al lado de la entrada para expandir el nodo del almacenamiento del registro de eventos. Esta acción muestra los servidores de CA Enterprise Log Manager individuales de la red. Con sólo hacer clic en los nombres de los servidores, podrá establecer las opciones de configuración local específicas de cada servidor, si lo desea.

Los usuarios que son administradores pueden configurar cualquier servidor de CA Enterprise Log Manager a partir de otro servidor de CA Enterprise Log Manager.

Para configurar las opciones del almacenamiento del registro de eventos

1. Inicie sesión en el servidor de CA Enterprise Log Manager y seleccione la ficha Administración.

   La subficha Recopilación de registros se mostrará de forma predeterminada.

2. Haga clic en la subficha Servicios.

3. Seleccione la entrada Almacenamiento del registro de eventos.

   Las opciones predeterminadas le proporcionan una configuración inicial adecuada para una red de tamaño medio con rendimiento moderado.

   En la ayuda en línea, podrá obtener más información sobre cada uno de los campos.

   Nota: Las tablas Secundarios de la federación y Autoarchivación sólo aparecen cuando muestra las opciones locales de un servidor de CA Enterprise Log Manager individual.

Consideraciones sobre el servidor ODBC

El usuario puede instalar un cliente de ODBC o de JDBC para acceder al almacén de registro de eventos de CA Enterprise Log Manager desde una aplicación externa, como Crystal Reports de SAP BusinessObjects.

En la zona de configuración, se pueden llevar a cabo las tareas siguientes:

- Activar o desactivar el acceso de ODBC y JDBC al almacén de registro de eventos.
- Establecer el puerto utilizado para comunicaciones entre el cliente de ODBC o JDBC y el servidor de CA Enterprise Log Manager.
- Especificar si las comunicaciones entre el cliente de ODBC o JDBC y el servidor de CA Enterprise Log Manager estarán cifrados.

Las descripciones de los campos son las siguientes:

Activar servicio

Indica si los clientes de ODBC y JDBC pueden acceder a los datos en el almacén de registro de eventos. Seleccione esta casilla de verificación para activar el acceso externo a los eventos. Anule la selección de la casilla de verificación para desactivar el acceso externo.

Actualmente, el servicio de ODBC no es compatible con FIPS. Si pretende ejecutarlo en el modo FIPS, elimine esta casilla de verificación para prevenir el acceso de ODBC y JDBC. Con ello se previene el acceso no compatible con los datos del evento. Si pretende desactivar el servicio de ODBC y JDBC para las operaciones en modo FIPS, asegúrese de que configura este valor para *cada uno* de los servidores en una federación.

Puerto de escucha del servidor

Especifica el número de puerto utilizado por los servicios de ODBC o JDBC. El valor predeterminado es 17002. El servidor de CA Enterprise Log Manager rechaza los intentos de conexión cuando se especifica un valor diferente en el origen de datos de Windows o en la cadena de la dirección URL de JDBC.

Cifrado (Capa de sockets seguros)

Indica si se debe utilizar cifrado para las comunicaciones entre el cliente de ODBC y el servidor de CA Enterprise Log Manager. El servidor de CA Enterprise Log Manager rechaza los intentos de conexión cuando el valor correspondiente del origen de datos de Windows o la dirección URL de JDBC no coincide con este valor.

Tiempo de espera de sesión (minutos)

Especifica el número de minutos que se mantiene abierta una sesión inactiva antes de que se cierre automáticamente.

Nivel de registro

Define el tipo y el nivel de detalle incluidos en el archivo de registro. La lista desplegable se ordena según el detalle, donde la primera opción ofrece la información menos detallada.

Aplicar a todos los registradores

Controla si la configuración del nivel de registro anula todos los ajustes de registro del archivo de propiedades de registro. Este ajuste sólo se aplica cuando la configuración del nivel de registro es inferior (muestra más detalles) a la configuración predeterminada.

Consideraciones del servidor de informes

El servidor de informes controla la administración de informes enviados de manera automática y su visualización en formato PDF, así como las alertas de acción y la retención de informes. En la zona de configuración del servidor de informes, puede llevar a cabo las tareas siguientes:

- Crear listas definidas por el usuario:

  Listas definidas por el usuario (valores clave)

  Le permiten crear agrupaciones relevantes para emplearlas en los informes, así como controlar los períodos de tiempo a los que hacen referencia.

- Establecer el servidor de correo, el correo electrónico de administración, así como la información del puerto SMTP y de autenticación del informe en el área de configuración de correo electrónico.
- Controlar el nombre y el logotipo de la empresa, las fuentes y otros ajustes de informes PDF en el área de configuración del informe.
- Establecer las alertas de acciones totales retenidas, así como el número de días que se mantendrán en el área de retención de alertas:

  Número máximo de alertas de acción

  Define el número máximo de alertas de acción que retiene el servidor de informes para su revisión.

  Mínimo: 50

  Máximo: 1.000

  Retención de alertas de acción

  Define el número de días durante los que se retienen las alertas de acción, hasta la cantidad máxima indicada.

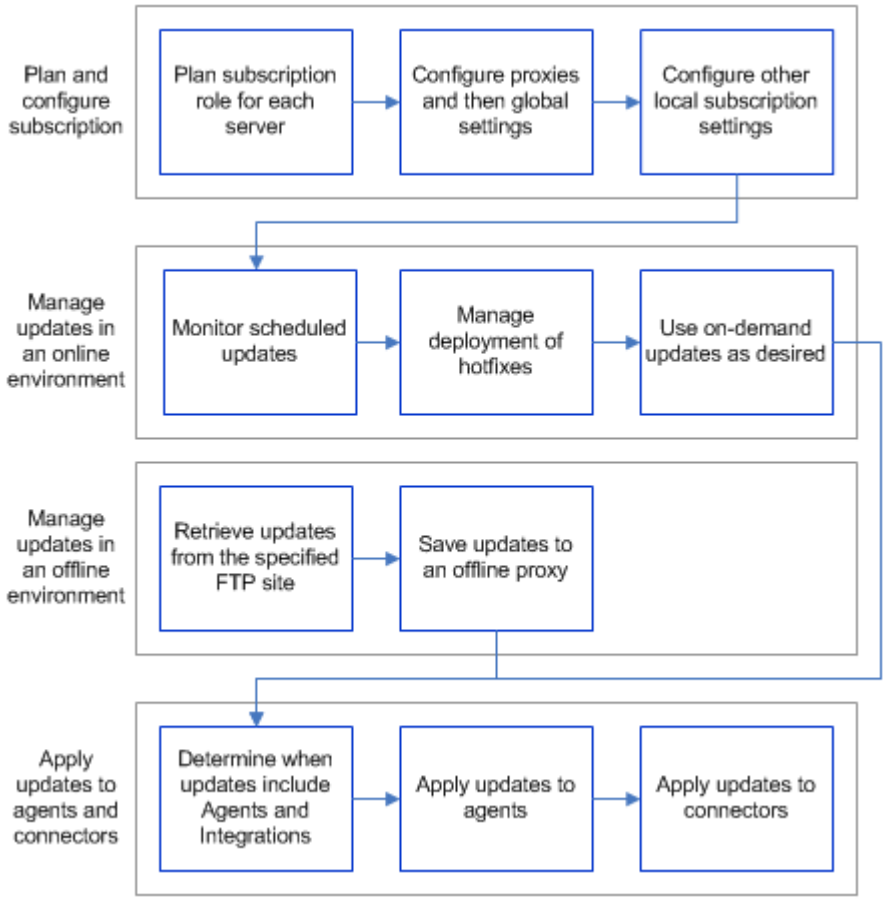
  Mínimo: 1

  Máximo: 30
- Establecer la política de retención de cada tipo de repetición de informe programado en el área de retención de informes.
- Establecer la frecuencia con que la utilidad de retención busca informes para eliminarlos de forma automática en función de dichas políticas. Por ejemplo, si la utilidad de retención de informes se ejecuta diariamente, suprimirá los informes diarios con una antigüedad superior a la máxima especificada.
- Establecer la configuración del proceso de CA IT PAM
- Establecer configuración de trap de SNMP

Diagrama de flujo de la implementación de suscripción

Si gestiona actualizaciones al dispositivo de CA Enterprise Log Manager, se realizan las actualizaciones en agentes y conectores el contenido se actualiza mediante la función Suscripción. El diagrama de flujo siguiente está en relación con la planificación, la configuración, la gestión de las actualizaciones en un entorno sin conexión y la aplicación de las actualizaciones a agentes y conectores. En esta guía, también se mencionan la planificación y la configuración.

Nota: Para obtener más detalles acerca del uso de las actualizaciones a petición, la gestión de las actualizaciones en un entorno sin conexión y la aplicación de las actualizaciones a los agentes y conectores, consulte la *Guía de administración*.



Configuración de la suscripción

El módulo de suscripción es similar al de otros servicios en los que hay una configuración global y local.

El módulo de suscripción es distinto a otros servicios por lo siguiente:

- La configuración global que requiere la selección de servidores proxy depende de la configuración realizada a nivel local. Usted define los servidores proxy para las actualizaciones de contenido a nivel local pero la lista disponible de servidores proxy no se genera hasta que estos servidores están configurados. Configura los servidores que van a actuar como proxy a nivel local, como proxy o proxy sin conexión.
- Todos los servidores locales de CA Enterprise Log Manager no son similares en cuanto a su configuración. Los distintos servidores tienen funciones diferentes. La función del servidor establece los parámetros que es necesario configurar.

La configuración de suscripción global varía en aplicabilidad de la siguiente forma:

- Las configuraciones que no se pueden sobrescribir a nivel local (sólo a nivel global) se indican a continuación:
  - Proxy de suscripción predeterminado
  - URL de fuente RSS: utilizada por todos los proxy en línea
  - Clave pública: utilizada por todos los proxy en línea

    Importante: No actualice esta configuración manualmente.
  - Limpiar actualizaciones antiguas a n días: se aplica a todos los servidores proxy (en línea y sin conexión)
  - Reiniciar automáticamente tras la actualización del SO: se aplica a todos los clientes

    Nota: Todos los CA Enterprise Log Manager son clientes, incluidos aquéllos que son servidores proxy en línea o sin conexión.
  - Servidores proxy de suscripción para actualizaciones de contenido
- Configuraciones que sólo se pueden configurar a nivel local
  - Proxy de suscripción
  - Proxy de suscripción sin conexión

Para aquellos parámetros de la configuración global que pueden sobrescribirse a nivel local, la capacidad de sobrescritura dependerá de si el servidor está definido como proxy en línea o como cliente. A continuación, se muestran más detalles:

- Configuraciones que se aplican a servidores proxy en línea que puede sobrescribir
  - Cinco configuraciones relacionadas con el proxy HTTP
  - Módulos que se van a descargar
- Configuración que se aplica a loa clientes de suscripción que pueden sobrescribirse
  - Servidores proxy de suscripción para el cliente

Configuración de los valores de la configuración global de la suscripción

Una vez instalados todos los servidores de CA Enterprise Log Manager, podrá configurar los valores de la configuración global de la suscripción.

Piense en configurar los ajustes de los servidores que vaya a asignar como servidores proxy de suscripción (en línea o sin conexión) antes de configurar los valores de la configuración global de la suscripción. Esta configuración genera las listas globales disponibles de servidores proxy para los clientes y de servidores proxy para las actualizaciones de contenido.

Para configurar los valores de la configuración global de la suscripción

1. Haga clic en la ficha Administración, haga clic en Servicios, haga clic en el módulo de suscripción y examine los ajustes de Configuración global de servicios: módulo de suscripción en el panel derecho.
2. Acepte o cambie la configuración del proxy de suscripción predeterminado. Normalmente, el *proxy de suscripción predeterminado* es el servidor de CA Enterprise Log Manager que se instala primero y también puede ser el servidor de gestión de CA Enterprise Log Manager. Cada cliente de suscripción en línea en el que no se ha configurado ninguna lista de servidores proxy de suscripción contactará con este servidor. Sin embargo, si existe una lista de servidores proxy de suscripción, pero se agota cuando se realizan búsquedas, el cliente obtendrá actualizaciones desde el servidor proxy predeterminado.

   Nota: Esta configuración no se puede sobrescribir a nivel local. Lo que aquí se especifica se aplica a todos los servidores de CA Enterprise Log Manager que utilizan el mismo servidor de gestión de CA Enterprise Log Manager.

3. Defina la programación para que el servidor proxy predeterminado y los servidores proxy en línea contacte con el servidor de suscripción de CA para descargar actualizaciones. Los clientes se ponen en contacto con los proxies una vez que han descargado la actualización del servidor de suscripción de CA.

   a. Especifique la frecuencia en horas con la que el servidor proxy predeterminado va a contactar con el servidor de suscripción de CA en busca de actualizaciones en el campo Frecuencia de la actualización.

   b. Utilice las siguientes directrices para configurar la hora de inicio de la actualización.

      - Si especifica un valor inferior a 24 en Frecuencia de actualización, no realice ninguna selección con el control de hora de inicio de la actualización. Las actualizaciones de suscripción comenzarán cuando se inicie iGateway.
      - Si especifica un valor igual o superior a 24 en Frecuencia de actualización, especifique la hora en un reloj de 24 horas a la que desee que se inicie la actualización.

4. Acepte la URL de fuente RSS preconfigurada, que se vincula con el servidor de suscripción de CA. Esta URL permite la generación de los módulos para descargar disponibles.

5. Acepte la clave pública que se muestre o seleccione la versión correcta. Dado que todos los servidores proxy de suscripción utilizan esta clave, no se puede modificar a nivel local.

   Importante: No modifique estos valores a no ser que lo haga bajo la supervisión del soporte técnico. Cuando se requiere cambiar una clave de una determinada descarga, este campo se actualizará automáticamente antes de que comience la descarga.

6. Especifique un valor en días o acepte el valor predeterminado 30; éste es el tiempo que las actualizaciones descargadas se retendrán en el sistema. Conceda suficiente tiempo para copiar el directorio de descarga desde el proxy de suscripción de origen a todos los servidores proxy de suscripción sin conexión y para que todos los clientes descarguen e instalen todas las actualizaciones.

   Nota: La configuración de actualizaciones de limpieza se aplica a todos los servidores proxy de suscripción y a todos lo servidores proxy sin conexión y no se puede modificar a nivel local.

7. Tenga en cuenta las siguientes indicaciones a la hora de configurar Reiniciar automáticamente tras la actualización del SO, que se aplican a todos los servidores de CA Enterprise Log Manager cuando se descarga y se instala un sistema operativo:

   - Acepte el valor predeterminado No para que el servidor de CA Enterprise Log Manager no se reinicie automáticamente si las actualizaciones binarias incluyen la instalación de parches en el sistema operativo que requieren reiniciar el servidor para finalizar la actualización. Cuando selecciona No, los usuarios serán notificados con un evento que les indicará que reinicien el sistema manualmente.
   - Seleccione Sí para que el servidor de CA Enterprise Log Manager se apague automáticamente y se reinicie después de la instalación de cada parche del sistema operativo (cuando el parche requiera que se reinicie el sistema para poder completar la instalación).

8. En Módulos para descargar, seleccione aquellos módulos que se apliquen a su entorno operativo. Por ejemplo, si no cuenta con servidores de CA Enterprise Log Manager que ejecuten una determinada aplicación o un determinado sistema operativo, no seleccionará el correspondiente módulo de descarga.

   Nota: La lista disponible se genera en el ciclo de actualización después de introducir una URL de fuente RSS válida. Esto viene determinado por la hora de inicio de actualización especificada y por la frecuencia de actualización especificada. Si la URL de fuente RSS está establecida y no se han generado los módulos para descargar, compruebe que la URL es válida. Si la red está protegida por cortafuegos, compruebe que el ajuste Proxy HTTP esté activado y que los ajustes asociados con el proxy de suscripción en línea sean correctos.

9. En la lista de proxies de suscripción disponibles para clientes, seleccione uno o más proxies con los que van a contactar los clientes en una operación por turnos rotativos para obtener las actualizaciones del sistema operativo y del software de CA Enterprise Log Manager. En una empresa grande, este ajuste se modificaría a nivel local. Baraje la opción de proporcionar la lista que utilizarán la mayor parte de clientes o de proporcionar una "superlista" que incluye los servidores proxy que se pueden seleccionar en las configuraciones locales.

   Nota: Esta configuración también se puede utilizar para crear una arquitectura de servidores proxy por niveles, donde un proxy de suscripción contacta con los servidores proxy de suscripción seleccionados para que las actualizaciones pasen a los clientes, en lugar de contactar con el servidor de suscripción de CA directamente.

10. En los proxies de suscripción para las actualizaciones de contenido disponibles, seleccione el proxy que va a enviar actualizaciones no binarias al almacén de usuarios de CA Enterprise Log Manager. Es recomendable seleccionar un segundo proxy para garantizar el envío de las actualizaciones si el servidor que suele realizar esta tarea deja de funcionar. Las actualizaciones no binarias incluyen archivos XMP, archivos DM, integraciones, actualizaciones de configuración de módulos de CA Enterprise Log Manager y actualizaciones de claves públicas. En un entorno sin conexión, puede seleccionar el proxy sin conexión que envía las actualizaciones al almacén de usuario de CA Enterprise Log Manager.
11. Si su red está protegida por un cortafuegos y cuenta con un servidor proxy HTTP, cambie el valor a Sí y rellene los cuatro campos relacionados. Haga clic en Probar proxy para comprobar la conectividad. Los servidores configurados como servidores proxy de suscripción en línea pueden sobrescribir estos ajustes.
12. Haga clic en Guardar.

Más información:

Consideraciones de la suscripción (en la página 184)
Evaluación de la necesidad de un proxy HTTP (en la página 54)
Comprobación del acceso a la fuente RSS para la suscripción (en la página 55)
Puertos y componentes de suscripción (en la página 52)

Consideraciones de la suscripción

Las actualizaciones las ofrece un sistema de servidor proxy/cliente. El primer servidor instalado se establece como el servidor proxy de suscripción predeterminado, y es el que contacta periódicamente con el servidor de suscripciones de CA para comprobar si hay actualizaciones. Las instalaciones posteriores se configurarán como clientes de ese servidor proxy y se pondrán en contacto con él para obtener actualizaciones.

El sistema predeterminado reduce el tráfico de red al eliminar la necesidad de que cada servidor se ponga en contacto directo con el servidor de suscripciones de CA y se puede configurar por completo. Puede agregar tantos servidores proxy como necesite.

También puede reducir aún más el tráfico de Internet mediante la creación de servidores proxy sin conexión, que almacenan la información sobre las actualizaciones de forma local y la ofrecen a los clientes que se ponen en contacto. Para ofrecer soporte a los servidores proxy sin conexión, copie de forma manual todo el contenido de la ruta de descarga del proxy en línea en la ruta de descarga del proxy sin conexión. Los servidores proxy sin conexión deben configurarse en entornos en los que hay servidores de CA Enterprise Log Manager que no pueden acceder a Internet o a un servidor conectado a Internet.

Al configurar el servicio de suscripción, tenga en cuenta la información siguiente sobre determinados ajustes y sus interacciones:

Proxy de suscripción predeterminado

Define el servidor proxy predeterminado para el servicio de suscripción. El proxy de suscripción predeterminado debe tener acceso a Internet. Si no se define ningún otro proxy de suscripción, este servidor obtiene las actualizaciones de suscripción del servidor de suscripciones de CA, descarga las actualizaciones de archivos binarios para todos los clientes y distribuye las actualizaciones de contenido. Si se definen otros servidores proxy, los clientes se pondrán en contacto con este servidor para obtener actualizaciones cuando no se haya configurado una lista de servidores proxy de suscripciones o cuando la lista configurada se haya agotado. El valor predeterminado es el primer servidor instalado en el entorno. Este valor sólo está disponible como configuración global.

Proxy de suscripción

Controla si el servidor local es un proxy de suscripción. Un servidor proxy de suscripción en línea emplea el acceso a Internet para obtener actualizaciones de suscripción del servidor de suscripciones de CA. Los servidores proxy de suscripciones en línea se pueden configurar para descargar actualizaciones de archivos binarios para clientes y para cargar actualizaciones de contenido en el servidor de gestión. Los servidores proxy en línea también se pueden emplear como origen para la copia de actualizaciones en servidores proxy de suscripciones sin conexión. Si se selecciona, debe cancelarse la selección de la casilla de verificación Proxy de suscripción sin conexión. Este valor sólo está disponible como configuración local.

Nota: Si ambas casillas de verificación del proxy de suscripción están sin seleccionar, el servidor es un cliente de suscripción.

Proxy de suscripción sin conexión

Controla si el servidor local es un proxy de suscripción sin conexión. Un proxy de suscripción sin conexión es un servidor que obtiene actualizaciones de suscripción a través de una copia de directorios manual (mediante scp) de un proxy de suscripción en línea. Puede configurar los servidores proxy de suscripciones sin conexión para que descarguen actualizaciones de archivos binarios en los clientes. Los servidores proxy de suscripciones sin conexión no necesitan tener acceso a Internet. Si se selecciona, debe cancelarse la selección de la casilla de verificación Proxy de suscripción. Este valor sólo está disponible como configuración local.

Nota: Si no está seleccionada ninguna de las casillas de verificación del proxy de suscripción, el servidor será un cliente de suscripción.

Hora de inicio de la actualización

Sólo es válida cuando la función Frecuencia de la actualización es 24 o superior.

Define la hora a la que se iniciará la primera comprobación de la actualización, en horas completas, según la hora local del servidor. El valor corresponde a un reloj de 24 horas. Este valor se aplica a la comprobación de actualización inicial. La Frecuencia de actualización controla el tiempo de todas las comprobaciones posteriores de la actualización. Esta configuración sólo se aplica al servicio de proxy de suscripción.

Límites: 0-23, donde 0 equivale a la medianoche y 23 equivale a las 11.00 p.m.

Frecuencia de la actualización

Define la frecuencia, en horas, con la que el servidor proxy en línea se pone en contacto con el servidor de suscripciones de CA y la frecuencia con la que el cliente de suscripción se pone en contacto con el proxy. Esta configuración sólo se aplica al servicio de proxy de suscripción.

Ejemplos: 0,5 quiere decir cada 30 minutos; 48 quiere decir cada dos días.

Actualizar ahora

Haga clic en este botón para iniciar un ciclo de actualización a petición del servidor seleccionado de forma inmediata. Sólo puede realizar una actualización a petición de los servidores de uno en uno. Actualice el servidor del proxy de suscripción antes de actualizar un cliente de suscripción.

URL de fuente RSS

Define la URL del servidor de suscripciones de CA. Los servidores proxy de suscripciones en línea emplean esta URL para acceder al servidor de suscripciones de CA y descargar las actualizaciones de suscripción. Este valor sólo está disponible como configuración global.

Servidor proxy HTTP

Controla si este servidor se pone en contacto con el servidor de suscripciones de CA a través de un proxy HTTP para obtener las actualizaciones, en lugar de hacerlo directamente.

Dirección proxy que se va a utilizar

Especifica la dirección IP completa del proxy HTTP.

Puerto

Especifica el número de puerto empleado para ponerse en contacto con el proxy HTTP.

Id de usuario del proxy HTTP

Especifica el ID de usuario empleado para ponerse en contacto con el proxy HTTP.

Contraseña de proxy HTTP

Especifica la contraseña empleada para ponerse en contacto con el proxy HTTP.

Clave pública

Define la clave empleada para comprobar y verificar la firma empleada para firmar las actualizaciones. No actualice este valor manualmente nunca. Cuando se actualiza una clave pública-privada, el proxy descarga la actualización al valor de clave pública y actualiza la clave pública. Este valor sólo está disponible como configuración global.

Limpiar actualizaciones de más de

Controla el número de días que el servidor proxy retiene los paquetes de actualización. Este valor sólo está disponible como configuración global.

Reiniciar automáticamente tras la actualización del SO

Controla si CA Enterprise Log Manager se reinicia de forma automática tras una actualización del SO. Este valor sólo está disponible como configuración global.

Módulos para descargar

Permite seleccionar los módulos que se aplicarán al entorno operativo. Los módulos seleccionados para los servidores proxy determinan los módulos descargados del servidor de suscripciones de CA como parte de las actualizaciones de suscripción. Los módulos seleccionados para clientes se emplean para actualizar los módulos correspondientes instalados en el cliente. Puede seleccionar un módulo para descargarlo en un cliente aunque no se haya seleccionado como su servidor proxy. El proxy lo recuperará para el cliente, pero no lo instalará en dicho proxy.

Nota: Si el campo está vacío, defina una URL de fuente RSS. Esta configuración permite que el sistema lea la fuente RSS y, en el siguiente intervalo de actualización, muestre la lista de módulos que se pueden descargar.

Servidores proxy de suscripción para el cliente

Permite definir los servidores proxy a los que se conectarán los clientes o un cliente seleccionado para obtener actualizaciones del sistema operativo y de los productos. Puede emplear las teclas de flecha hacia arriba/abajo para controlar el orden en el que el cliente se pone en contacto con los servidores proxy de suscripciones. El cliente descarga actualizaciones del primer servidor proxy con el que se conecta de forma correcta. Si ninguno de los servidores proxy configurados está disponible, el cliente se pone en contacto con el proxy de suscripción predeterminado.

Servidores proxy de suscripción para actualizaciones de contenido

Le permite seleccionar qué servidores proxy se emplean para distribuir actualizaciones de contenido en el almacén de usuarios. Puede seleccionar los servidores proxy sin conexión y en línea. Este valor sólo está disponible como configuración global.

Nota: Le recomendamos seleccionar más de uno para disponer de varias alternativas.

Configuración de servidores de CA Enterprise Log Manager para la suscripción

En el módulo de suscripción se enumeran uno o más servidores de CA Enterprise Log Manager. Cada servidor hereda la configuración de suscripción local. Cuando se muestra por primera vez, todos los ajustes están desactivados. Para sobrescribir cualquier ajuste, haga clic en el botón de alternar global/local para editar el campo.

Cada servidor enumerado debe estar configurado como uno de los siguientes:

- Proxy de suscripción (en línea)
- Proxy de suscripción sin conexión
- Cliente de suscripción

Los servidores proxy de suscripción en línea y sin conexión autoinstalan actualizaciones y actúan como su propio cliente. Todos los servidores de CA Enterprise Log Manager que no son servidores proxy de suscripción deben estar configurados como clientes.

Un proxy de suscripción especial es el proxy de suscripción predeterminado. El servidor de CA Enterprise Log Manager que se instala primero se registra con el almacén de usuarios de CA Enterprise Log Manager como proxy de suscripción predeterminado, pero este ajuste se puede cambiar a nivel global. En un entorno en línea, todos los clientes descargan actualizaciones de suscripción desde el proxy de suscripción predeterminado si no se configuran más servidores proxy o cuando no están disponibles.

Más información:

Ejemplo: configuración de suscripción con seis servidores (en la página 62)
Configuración de un proxy de suscripción en línea (en la página 189)
Configuración de un proxy de suscripción sin conexión (en la página 190)

Configuración de un proxy de suscripción en línea

Puede utilizar el servidor predeterminado como su único servidor de suscripciones en línea. En este caso, el resto de servidores de CA Enterprise Log Manager competirán para descargar actualizaciones de suscripciones desde este servidor. Esta configuración es adecuada para una instalación pequeña donde no se requieren más servidores proxy de suscripción en línea.

En una instalación mayor, se recomienda configurar más servidores. Cuando varios servidores se configuran como servidores proxy de suscripción en línea en un entorno en línea, puede seleccionar los servidores proxy que podrá sondear cada cliente. Cuando un cliente puede contactar con varios servidores en una operación por turnos, es probable que pueda descargar las actualizaciones de suscripción de manera puntual.

La ruta de descarga preconfigurada es la siguiente: .../opt/CA/LogManager/data/subscription.

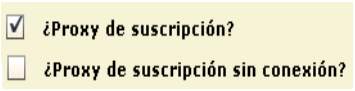
Sólo los administradores pueden configurar los servidores proxy de suscripción.

Para configurar un servidor proxy de suscripción en línea

1. Haga clic en la ficha Administración, haga clic en Servicios, expanda el módulo de suscripción y seleccione el servidor que desee configurar.

   Aparecerá la configuración del servicio del módulo de suscripción del servidor de CA Enterprise Log Manager seleccionado.

2. Active ¿Proxy de suscripción? y desactive la opción ¿Proxy de suscripción sin conexión?

3. Para sobrescribir una configuración global, haga clic en el botón de alternar global/local para cambiar a la configuración de servicio local del campo seleccionado; a continuación, realice los cambios oportunos.

   Nota: Si vuelve a hacer clic en el botón de alternar para bloquear el campo y utilizar la configuración global, el valor cambiará al valor global en el siguiente intervalo de actualización, tal y como se define en la configuración global.

4. Piense si desea aceptar la configuración global Hora de inicio de la actualización y Frecuencia de la actualización.

5. Si este servidor va a descargar actualizaciones de suscripción a través de un servidor proxy HTTP distinto al heredado, cambie a la configuración local y edite los cinco campos que configuran el proxy HTTP.

6. Si los módulos que necesita descargar para las actualizaciones del sistema operativo o del producto de CA Enterprise Log Manager difieren de la configuración heredada, cambie a la configuración local y realice los cambios oportunos.
7. Haga clic en Guardar.

Más información:

Consideraciones de la suscripción (en la página 184)

Configuración de un proxy de suscripción sin conexión

Cuando un servidor de CA Enterprise Log Manager no esté conectado a Internet, debe configurar uno o más servidores de CA Enterprise Log Manager como servidores proxy de suscripción sin conexión desde el que otros servidores cliente sin conexión puedan obtener actualizaciones de suscripción.

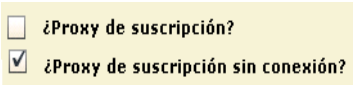
Un administrador debe copiar actualizaciones de suscripción desde un servidor proxy en línea a servidores proxy sin conexión. La ruta de descarga preconfigurada es la siguiente: .../opt/CA/LogManager/data/subscription.

Sólo los administradores pueden configurar los servidores proxy de suscripción.

Para configurar un servidor proxy de suscripción sin conexión

1. Haga clic en la ficha Administración, haga clic en Servicios, expanda el módulo de suscripción y seleccione el servidor que desee configurar.

   Aparecerá la configuración del servicio del módulo de suscripción del servidor de CA Enterprise Log Manager seleccionado.
2. Active Proxy de suscripción sin conexión

3. Haga clic en Guardar.

   Ahora podrá configurar este servidor proxy de suscripción sin conexión de la siguiente manera:

   - Añádalo a la configuración global de los servidores proxy de suscripción para las actualizaciones de contenido
   - Añádalo a la configuración global o a cualquier configuración local del cliente de los servidores proxy de suscripción del cliente

Más información:

Evaluación de la necesidad de un proxy de suscripción sin conexión (en la página 55)

Configuración de un cliente de suscripción

De forma predeterminada, todos los servidores de CA Enterprise Log Manager que no son servidores proxy de suscripción están configurados como clientes. No es necesario configurar clientes de suscripción a no ser que desee sobrescribir la lista de servidores proxy seleccionada que está configurada como global.

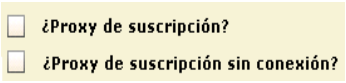
Un cliente de suscripción es un servidor de CA Enterprise Log Manager que obtiene contenido de otro servidor de CA Enterprise Log Manager denominado servidor proxy de suscripción. Los clientes de suscripción sondean el servidor proxy de suscripción configurado de manera regular y recuperan las actualizaciones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

Para configurar un cliente de suscripción

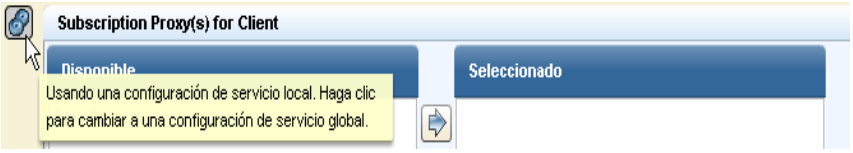
1. Haga clic en la ficha Administración, haga clic en Servicios, expanda el módulo de suscripción y seleccione el servidor que desee configurar.

   Aparecerá la configuración del servicio del módulo de suscripción del servidor de CA Enterprise Log Manager seleccionado.

2. Identifique el servidor seleccionado como cliente desactivando las dos casillas de verificación del servidor proxy de suscripción.

3. Haga clic en el botón de alternar global/local para realizar la configuración de servicio local de los servidores proxy de suscripción del cliente y seleccione los servidores proxy de suscripción con los que va a contactar este cliente en una operación por turnos para descargar actualizaciones del sistema operativo y del producto.

4. Si los módulos que necesita descargar para las actualizaciones del sistema operativo o del producto difieren de la configuración heredada, cambie a la configuración local y realice los cambios oportunos. Puede seleccionar módulos como cliente no seleccionados por su proxy.

5. Haga clic en Guardar.

Más información:

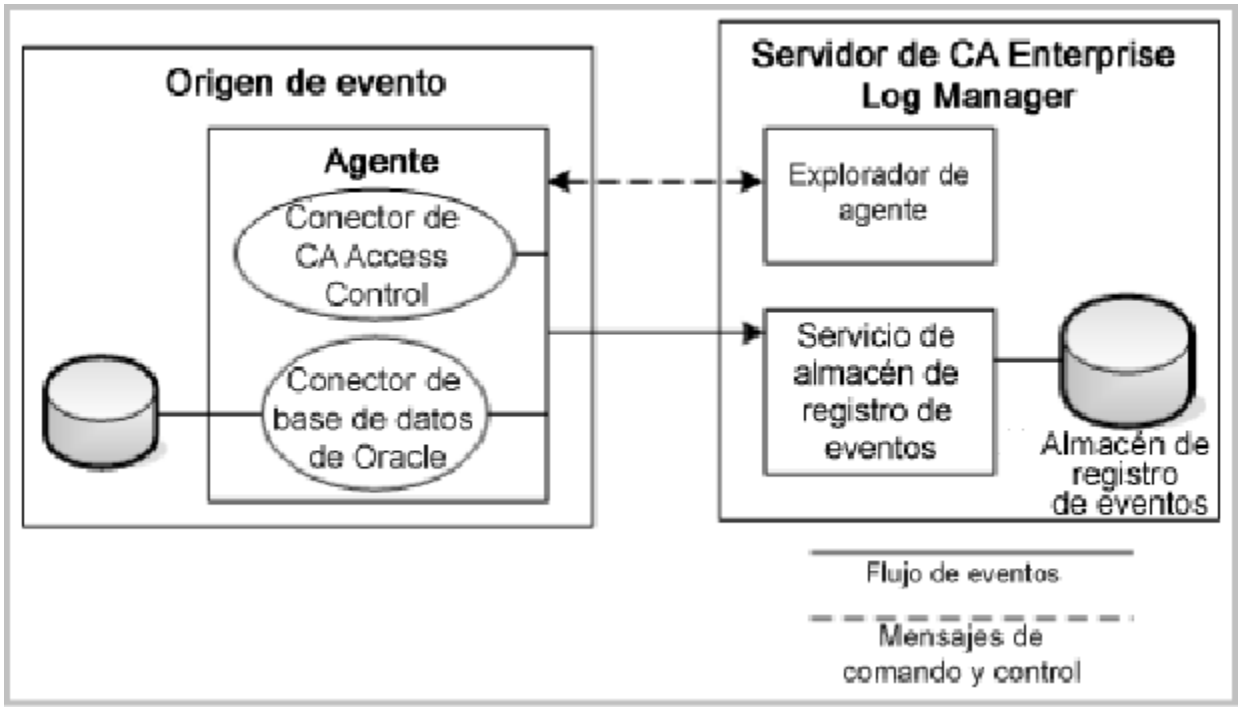
Evaluación de la necesidad de una lista de servidores proxy (en la página 61)
Consideraciones de la suscripción (en la página 184)

Capítulo 6: Configuración de la recopilación de eventos

Esta sección contiene los siguientes temas:

Instalación de agentes

Gracias a instalaciones independientes de plataformas específicas, los agentes de CA Enterprise Log Manager proporcionan la capa de transporte para pasar eventos de los orígenes de eventos al almacenamiento del registro de eventos del servidor de CA Enterprise Log Manager. Los agentes utilizan conectores para recopilar registros de eventos desde distintos orígenes de eventos. El siguiente diagrama muestra las interconexiones entre los agentes y el servidor de CA Enterprise Log Manager:



Después de instalar un agente en un origen de evento, podrá configurar uno o más conectores para que recopilen eventos desde los orígenes de eventos como, por ejemplo, dispositivos, aplicaciones, sistemas operativos y bases de datos. Los ejemplos del diagrama incluyen conectores para CA Access Control y para una base de datos de Oracle. Normalmente, sólo instalará un agente por servidor host o por origen de evento, pero puede configurar más de un tipo de conector en ese agente. Puede utilizar el explorador de agente que forma parte del servidor de CA Enterprise Log Manager para controlar agentes y configurar y controlar conectores de un agente. El explorador de agente también le permite crear grupos para que la gestión y el control sean más sencillos.

Base la configuración de un conector en una integración o en una escucha, que son plantillas que pueden incluir archivos para acceder a datos, analizar mensajes y asignar datos. CA Enterprise Log Manager proporciona una serie de integraciones de orígenes de eventos populares predeterminados.

Si desea obtener más información sobre la instalación de agentes, consulte la *Guía de instalación del Agente de CA Enterprise Log Manager*.

Más información:

Visualización y control del estado de agentes o conectores (en la página 209)

Utilización del explorador de agente

Inmediatamente después de instalar un servidor de CA Enterprise Log Manager, contará con un agente predeterminado enumerado en el explorador de agente. Este agente se instala cuando instala el servidor de CA Enterprise Log Manager y lo utiliza con la recopilación de eventos syslog directa.

El explorador de agente realiza un seguimiento de los agentes y los enumera a medida que los instala en la red. Además, proporciona una ubicación centralizada para la configuración, el comando y el control de agentes y conectores. Los agentes se registran con el servidor de CA Enterprise Log Manager especificado la primera vez que los inicia. Cuando se realiza la instalación, el nombre del agente aparece en el explorador de agente. A continuación, podrá configurar un conector para iniciar la recopilación de registros de eventos. Los conectores recopilan registros de eventos y los envían al servidor de CA Enterprise Log Manager. Un agente puede controlar varios conectores.

La utilización del explorador de agente para instalar, configurar y controlar conectores y agentes incluye los siguientes pasos básicos:

1. Descargue los agentes binarios.
2. Cree uno o varios grupos de agentes (opcional).
3. Cree y configure un conector, incluida la creación o aplicación de reglas de supresión y resumen.
4. Vea el estado del agente o del conector.

Consulte la *Guía de administración de CA Enterprise Log Manager* si desea obtener más información sobre la creación y el trabajo con grupos de agentes y conectores, y sobre cómo aplicar reglas de supresión en los agentes.

Más información:

Acerca de los agentes (en la página 66)
Acerca de los grupos de agentes (en la página 67)
Acerca de los conectores (en la página 69)
Acerca de los sensores de registros (en la página 69)
Efectos de las reglas de supresión (en la página 71)

Configuración del agente predeterminado

La instalación de CA Enterprise Log Manager crea un agente predeterminado en el servidor de CA Enterprise Log Manager que cuenta con dos conectores listos para su uso, un conector syslog_Connector y un conector Linux_local. El conector de syslog está disponible para la recopilación de eventos de syslog enviados al servidor de CA Enterprise Log Manager. El conector Linux_local está disponible para la recopilación de eventos del sistema operativo desde el servidor físico de CA Enterprise Log Manager o desde un archivo de syslog.

En el entorno básico de dos servidores, configure uno o varios conectores de syslog en el servidor de recopilación para recibir eventos.

El proceso de utilización del agente predeterminado incluye los siguientes pasos:

1. (opcional) Revise las escuchas y las integraciones de syslog.
2. Cree un conector de syslog.
3. Compruebe que el servidor de CA Enterprise Log Manager recibe eventos syslog.

Revise las escuchas y las integraciones de syslog

Puede revisar las escuchas y las integraciones de syslog predeterminadas antes de crear un conector. Básicamente, las escuchas son una plantilla para los conectores de syslog que utilizan integraciones de syslog específicas que se proporcionan como contenido predeterminado con su servidor de CA Enterprise Log Manager.

Para revisar integraciones de syslog

1. Inicie sesión en CA Enterprise Log Manager y acceda a la ficha Administración.
2. Expanda el nodo de la biblioteca de refinamiento de eventos en el panel de navegación de la izquierda.

3. Expanda el nodo de integraciones y el nodo de suscripción.
4. Seleccione una integración cuyo nombre finalice por ..._Syslog.

   Los detalles de la integración se mostrarán en la ventana de la derecha. Puede revisar el archivo de análisis de mensajes y de asignación de datos que utiliza la integración además de otros detalles como, por ejemplo, la versión y la lista de reglas de supresión.

Para revisar una escucha de syslog

1. Expanda el nodo de escuchas y el nodo de suscripción.
2. Seleccione la escucha de Syslog.

   Los detalles de la escucha predeterminada se mostrarán en la ventana de la derecha. Puede revisar detalles como, por ejemplo, versiones, una lista de reglas de supresión, puertos predeterminados en los que escuchar, una lista de host de confianza y la zona horaria de la escucha.

Creación de un conector de syslog para el agente predeterminado

Puede crear un conector de syslog para recibir eventos de syslog mediante el agente predeterminado del servidor de CA Enterprise Log Manager.

Para crear un conector de syslog para el agente predeterminado

1. Inicie sesión en CA Enterprise Log Manager y acceda a la ficha Administración.
2. Expanda el explorador de agente y un grupo de agentes.

   El agente predeterminado se instala automáticamente en el grupo de agentes predeterminado. Puede trasladar este agente a otro grupo.
3. Seleccione el nombre del agente.

   El agente predeterminado tiene el mismo nombre que el nombre asignado el servidor de CA Enterprise Log Manager durante la instalación.
4. Haga clic en Crear nuevo conector para abrir el asistente de conectores.
5. Haga clic en la opción Escuchas y asígnele un nombre a este conector.

6. Aplique o cree reglas de supresión según sea necesario en la segunda página del asistente.
7. Seleccione una o varias integraciones específicas de syslog en la lista disponible para utilizar con este conector y muévalas a la lista seleccionada.
8. Establezca valores de puertos UDP y TCP si no está utilizando los valores predeterminados y proporcione una lista de host de confianza si su implementación los utiliza.

   Nota: Cuando un agente de CA Enterprise Log Manager no se ejecuta como root, no puede abrir un puerto con un valor inferior a 1024. Por lo tanto, el conector de syslog predeterminado emplea el puerto UDP 40514. La instalación aplica una regla de cortafuegos al servidor de CA Enterprise Log Manager para redireccionar el tráfico del puerto 514 a través del puerto 40514.
9. Seleccione una zona horaria.
10. Haga clic en Guardar y cerrar para finalizar el conector.

    El conector comenzará a recopilar los eventos syslog que coincidan con las integraciones seleccionadas en los puertos que ha especificado.

Compruebe que CA Enterprise Log Manager reciba los eventos syslog

Con el siguiente procedimiento, puede comprobar si el conector en el agente predeterminado está recopilando eventos syslog con el siguiente procedimiento.

Para comprobar la recepción de eventos syslog

1. Inicie sesión en CA Enterprise Log Manager y acceda a la ficha Consultas e informes.
2. Seleccione la etiqueta de consulta Sistema y abra la consulta Detalles de todos los eventos del sistema.

   Si ha configurado el conector correctamente y el origen de eventos está enviando eventos de forma activa, debería ver los eventos enumerados para el agente predeterminado.

Ejemplo: Activación de la recopilación directa con ODBCLogSensor

Puede habilitar la recopilación directa de eventos generados mediante bases de datos específicas y productos de CA con ODBCLogSensor. Para ello, cree un conector en el agente predeterminado que esté basado en una integración que utilice ODBCLogSensor. Muchas integraciones utilizan este sensor, por ejemplo, CA_Federation_Manager, CAIdentityManager, Oracle10g, Oracle9i y MS_SQL_Server_2005.

A continuación, aparece una lista parcial de productos que genera eventos que se pueden recopilar directamente a través del agente predeterminado en un servidor de CA Enterprise Log Manager. Para cada producto, se utiliza un conector único. Todos los conectores utilizan ODBCLogSensor.

- CA Federation Manager
- CA SiteMinder
- CA Identity Manager
- Oracle 9i y 10g
- Microsoft SQL Server 2005

Para obtener una lista completa, consulte la Matriz de integración de productos en Support Online.

En este ejemplo, se muestra cómo activar la recopilación directa de eventos de una base de datos de Microsoft SQL Server. El conector implementado en el agente predeterminado está basado en la integración de MS_SQL_Server_2005. En este ejemplo, la base de datos de SQL Server reside en un servidor de ODBC. El conector implementado en el agente de CA Enterprise Log Manager recopila eventos de la tabla MSSQL_TRACE. El envío de los eventos seleccionados a esta tabla de seguimiento forma parte del proceso de activación de la base de datos de Microsoft SQL Server. Puede consultar instrucciones explícitas para ello en la *Guía del conector para Microsoft SQL Server de CA*.

Para obtener información acerca de cómo configurar el origen de evento de Microsoft SQL Server

1. Seleccione la ficha Administración.
2. Expanda Biblioteca de refinamiento de eventos, Integraciones, Suscripción y seleccione MS_SQL_Server_2005.

   En Visualización de los detalles de la integración aparece el nombre del sensor, ODBCLogSensor. Entre las plataformas compatibles, se incluyen Windows y Linux.
3. Haga clic en el vínculo Ayuda en Visualización de los detalles de la integración.

Aparecerá la Guía del conector para Microsoft SQL Server.

4. Revise las secciones Requisitos previos y Configuración de Microsoft SQL Server para obtener instrucciones.

Para configurar el origen de evento y comprobar el registro

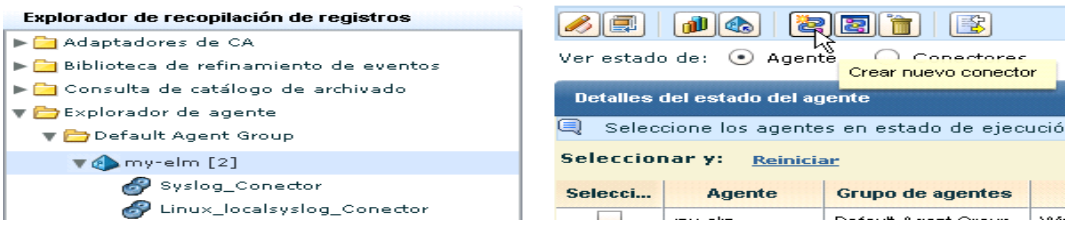
1. Recopile los siguientes detalles: la dirección IP del servidor de ODBC, el nombre de la base de datos, el nombre de usuario de administrador, y las credenciales de usuario con privilegios bajos que se utilizan para la autenticación en SQL Server. (Se trata del usuario definido para que disponga de acceso de sólo lectura a la tabla de seguimiento).
2. Inicie sesión en el servidor de ODBC con la contraseña y el nombre de usuario de administrador.
3. Asegure la conectividad a través de TCP/IP como aparece especificado en la *Guía del conector para Microsoft SQL Server*.
4. Configure SQL Server y compruebe que los eventos se envían a la tabla de seguimiento como se especifica en la *Guía del conector para Microsoft SQL Server*.

   Nota: Registre el nombre del nombre de la base de datos en la que desee crear la tabla de seguimiento. Debe especificar dicho nombre de base de datos en la cadena de conexión. Por ejemplo: principal.

Para crear un conector en el agente predeterminado que permita recuperar eventos generados por una base de datos de SQL Server en un servidor de ODBC

1. Seleccione la ficha Administración y la subficha Recopilación de registros.
2. Expanda el Explorador de agente y, a continuación, el grupo de agentes que contenga el agente predeterminado de CA Enterprise Log Manager.
3. Seleccione un agente predeterminado, es decir, un agente con el nombre de un servidor de CA Enterprise Log Manager.

   El agente predeterminado puede tener otros conectores implementados.
4. Haga clic en Crear nuevo conector.



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

5. Seleccione la integración de MS_SQL_Server_2005 en la lista desplegable Integración.

   Esta selección hace que se rellene el campo Nombre de conector con MS_SQL_Server_2005_Connector.

6. (Opcional) Sustituya el nombre predeterminado por uno que le permita identificar el conector fácilmente. Considere la posibilidad de usar un nombre exclusivo si va controlar varias bases de datos de SQL Server con el mismo agente.

7. (Opcional) Haga clic en el paso Aplicar reglas de supresión y seleccione las reglas asociadas con los eventos admitidos.

   Por ejemplo, seleccione MSSQL_2005_Authorization 12.0.44.12.

8. Haga clic en el paso Detalles del conector y, a continuación, en el vínculo Ayuda.

   Entre las instrucciones también se incluyen los requisitos de configuración del sensor de CA Enterprise Log Manager para Windows y Linux.

9. Revise los pasos para Linux, la plataforma del agente predeterminado, y configure Cadena de conexión y los demás campos como se especifica.

   a. Especifique la cadena de conexión según se especifica en Configuración del sensor (Linux), donde la dirección es el nombre de host o la dirección IP del origen de evento y la base de datos es la base de datos de SQL Server en MSSQLSERVER_TRACE

      `DSN=SQLServer Wire Protocol;Address=`*`IPaddress`*`,`*`port`*`;Database=`*`databasename`*

   b. Especifique el nombre del usuario con los derechos de acceso de recopilación de eventos de sólo lectura. El usuario debe tener asignadas las funciones db_datareader y public para disponer de acceso de sólo lectura.

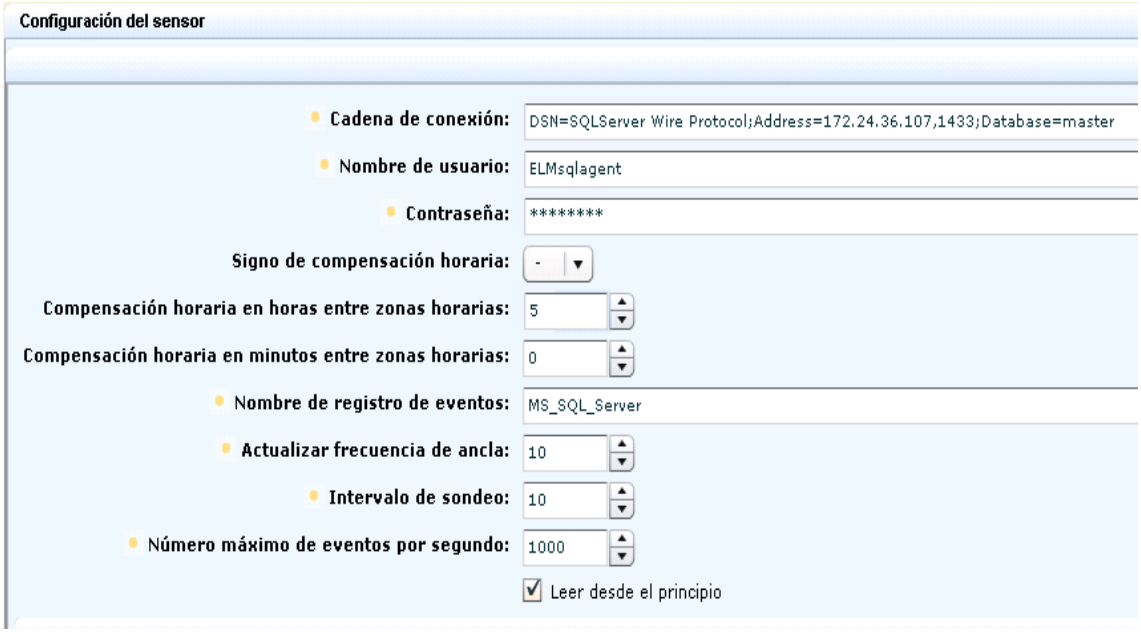
   c. Introduzca la contraseña del nombre de usuario especificado.

   d. Especifique la zona horaria de la base de datos como la diferencia con la hora GMT.

      Nota: En Windows Server, esta información aparece en la ficha Zona horaria de Propiedades de fecha y hora. Abra el reloj en la bandeja del sistema.

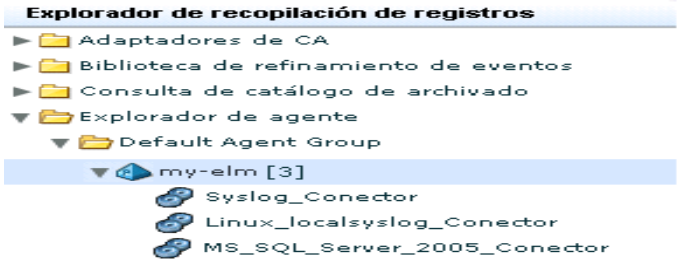
   e. Seleccione o anule la selección de Leer desde el principio dependiendo de si desea que el sensor de registro lea los eventos desde el principio de la base de datos o no.

   A continuación, puede encontrar un ejemplo parcial:



10. Haga clic en Guardar y cerrar.

    El nombre de conector nuevo aparece debajo del agente en el Explorador de agente.



11. Haga clic en MS_SQL_Server_2005_Connector para visualizar los detalles de estado.

    Inicialmente, en el estado aparece Configuración pendiente. Espere hasta que el estado sea En ejecución.

Conector	Agente	Grupo de agentes	Plataforma	Integración	Estado
MS_SQL_Server_2005_Conector	my-elm	Default Agent Group	Linux_X86_32	MS_SQL_Server_2005	En ejecución

12. Seleccione el conector y haga clic en En ejecución para visualizar los detalles de recopilación del evento.

    Nota: También puede ejecutar un informe para ver los datos de esta base de datos.

Para comprobar si el agente predeterminado recopila eventos del origen de evento de destino

1. Seleccione la ficha Consultas e informes. Aparecerá la subficha Consultas.
2. Expanda Peticiones en la Lista de consultas y seleccione Conector.
3. Especifique el nombre del conector y haga clic en Ir.

   Se mostrarán los eventos recopilados. Los dos primeros son eventos internos. Los siguientes son eventos recopilados de la tabla de seguimiento MS SQL que ha configurado.

   Nota: Si no se muestran los eventos esperados, haga clic en Configuración y filtros globales en la barra de herramientas principal, establezca Intervalo de tiempo en Sin límite, y guarde la configuración.
4. (Opcional) Seleccione Mostrar eventos sin formato y examine la cadena de resultado para los dos primeros eventos. La cadena de resultado aparece en último lugar en el evento sin procesar. Los siguientes valores indican un inicio correcto.
   - result_string=ODBCSource initiated successfully - MSSQL_TRACE
   - result_string=<nombre del conector> Connector Started Successfully

Ejemplo: Activación de la recopilación directa con WinRMLinuxLogSensor

Puede activar la recopilación directa de eventos generados por aplicaciones de Windows o el sistema operativo Windows Server 2008 con WinRMLinuxLogSensor. Para ello, cree un conector en el agente predeterminado que esté basado en una integración que utilice WinRMLinuxLogSensor. Muchas integraciones utilizan este sensor, por ejemplo: Active_Directory_Certificate_Services, Forefront_Security_for_Exchange_Server, Hyper-V, MS_OCS y WinRM. La aplicación y el sistema operativo Microsoft Windows que generan eventos que WinRMLinuxLogSensor puede recuperar son aquellos para los que se activa la Administración remota de Windows.

A continuación, aparece una lista parcial de productos que genera eventos que se pueden recopilar directamente a través del agente predeterminado en un servidor de CA Enterprise Log Manager. Para cada producto, se utiliza un conector único. Todos los conectores utilizan WinRMLinuxLogSensor.

- Servicios de certificados de Active Directory de Microsoft
- Microsoft Forefront Security para Exchange Server
- Microsoft Forefront Security para SharePoint Server
- Microsoft Hyper-V Server 2008
- Microsoft Office Communications Server
- Microsoft Windows Server 2008

Para obtener una lista completa, consulte la Matriz de integración de productos en Support Online.

En este ejemplo, se muestra cómo activar la recopilación directa de eventos con un conector basado en la integración de WinRM. Al implementar dicho conector, recopila eventos de un origen de evento del sistema operativo Windows Server 2008. La recopilación comienza una vez que haya configurado los orígenes de evento en el Visor de eventos de Windows y active la Administración remota de Windows en el servidor según se especifique en la guía del conector asociado con esta integración.

Para obtener información acerca de cómo configurar el origen de evento de Windows Server 2008

1. Seleccione la ficha Administración.
2. Expanda Biblioteca de refinamiento de eventos, Integraciones, Suscripción y seleccione WinRM.

   En Ver detalles de integraciones aparece el nombre del sensor, WinRMLinuxLogSensor. Entre las plataformas compatibles, se incluyen Windows y Linux.
3. Haga clic en el vínculo Ayuda en Visualización de los detalles de la integración de WinRM.

   Aparecerá la Guía del conector para Microsoft Windows Server 2008 (WinRM).

Para configurar el origen de evento y comprobar el registro

1. Inicie sesión en el host de destino con un sistema operativo Windows Server 2008.
2. Siga las instrucciones de la *Guía del conector para Microsoft Windows Server 2008* para asegurarse de que los eventos aparecen en el Visor de eventos de Windows y de que la opción Administración remota de Windows está activada en el servidor de destino.

   Nota: Parte de este proceso consiste en la creación del nombre de usuario y la contraseña que debe especificar al configurar el conector. Estas credenciales activan la autenticación necesaria para establecer la conectividad entre el origen de evento y CA Enterprise Log Manager.
3. Compruebe el registro.
   a. Abra eventvwr desde el cuadro de diálogo Ejecutar.

      Aparecerá el Visor de eventos.
   b. Expanda Registros de Windows y haga clic en Seguridad.

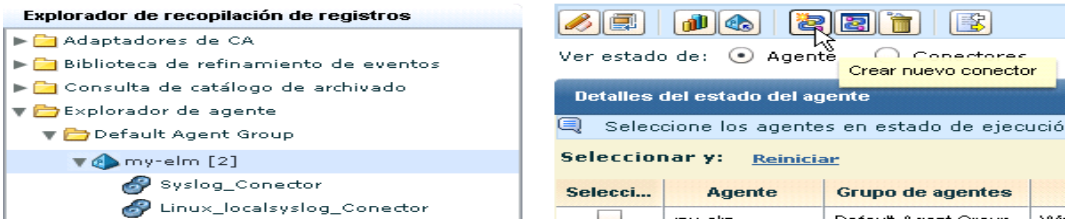
      Una pantalla parecida a la siguiente indica que se está realizando el registro.

Para activar la recopilación directa de eventos de orígenes de eventos de Windows

1. Seleccione la ficha Administración y la subficha Recopilación de registros.
2. En el Explorador de recopilación de registros, expanda el Explorador de agente y el grupo de agentes que contenga el agente predeterminado de CA Enterprise Log Manager.
3. Seleccione un agente predeterminado, es decir, un agente con el nombre de un servidor de CA Enterprise Log Manager.

   El agente predeterminado puede tener otros conectores implementados.

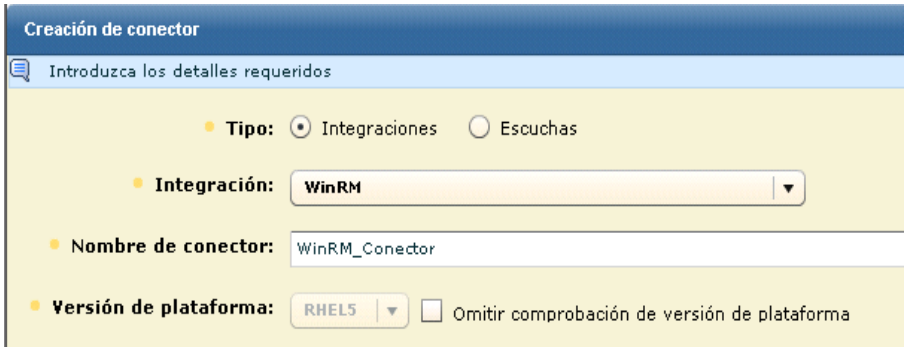
4. Haga clic en Crear nuevo conector



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

5. Seleccione una integración que utilice el sensor de registro de WinRM en la lista desplegable Integración.

   Por ejemplo, seleccione WinRM.



   Al realizar la selección, se rellena el campo Nombre de conector con WinRM_Connector.

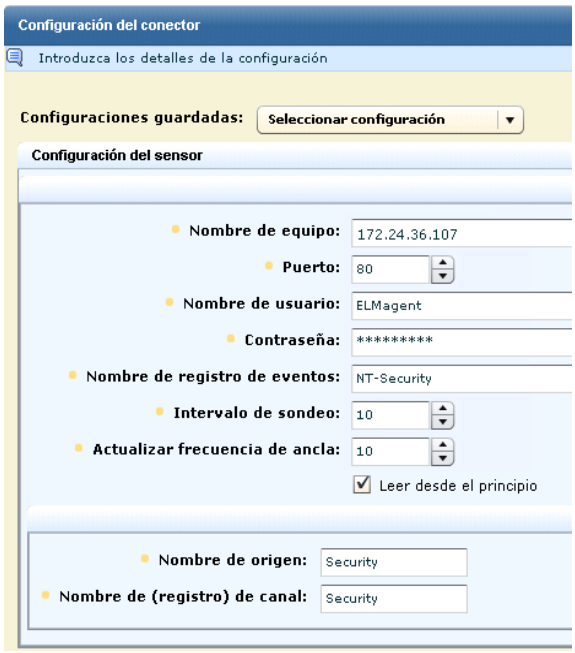
6. (Opcional) Haga clic en Aplicar reglas de supresión y seleccione las reglas asociadas con los eventos admitidos.

7. Haga clic en el paso Detalles del conector y, a continuación, en el vínculo Ayuda.

   En las instrucciones se incluye la configuración del sensor de CA Enterprise Log Manager (WinRM).

8. Siga las instrucciones de esta Guía del conector para configurar el sensor. Especifique la dirección IP (en lugar del nombre de host) del host en el que ha configurado Administración remota de Windows. En las entradas Nombre de usuario y Contraseña aparecen las credenciales que agregó durante la configuración de Administración remota de Windows.

   A continuación, se muestra un ejemplo:



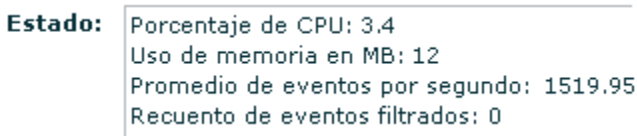
9. Haga clic en Guardar y cerrar.

10. El nombre de conector nuevo aparece debajo del agente en el Explorador de agente.

11. Haga clic en WinRM_Connector para ver los detalles de estado.

    Inicialmente, en el estado aparece Configuración pendiente. Espere hasta que el estado sea En ejecución.

12. Haga clic en En ejecución para obtener datos de resumen, como los EPS (eventos por segundo).



Para comprobar si el agente predeterminado recopila eventos del origen de evento de destino

1. Seleccione la ficha Consultas e informes. Aparecerá la subficha Consultas.
2. Expanda Peticiones en la Lista de consultas y seleccione Conector.
3. Especifique el nombre del conector y haga clic en Ir.
4. Visualice los eventos recopilados.

Visualización y control del estado de agentes o conectores

Puede controlar el estado de los agentes o conectores de su entorno, reiniciar agentes así como iniciar, detener y reiniciar conectores cuando sea necesario.

Puede ver agentes o conectores desde distintos niveles de la jerarquía de carpetas del explorador de agente. Cada nivel reducirá la vista disponible de forma correspondiente:

- Desde la carpeta del explorador de agente, podrá ver todos los agentes o conectores asignados al servidor de CA Enterprise Log Manager actual.
- Desde la carpeta de un grupo de agentes específico, podrá ver los agentes y los conectores asignados a ese grupo de agentes.
- Desde un agente individual, sólo podrá ver ese agente y los conectores asignados a éste.

Puede determinar el modo de FIPS (FIPS o no-FIPS) para un agente desde los tres niveles.

Para ver el estado del agente o del conector

1. Haga clic en la ficha Administración y, a continuación, en la subficha Recopilación de registros.

   Aparece la lista de la carpeta Recopilación de registros.

2. Seleccione la carpeta Explorador de agente.

   Los botones de la gestión de agentes aparecerá en el panel de detalles.

3. Haga clic en Estado y comando: 

   Aparecerá el panel de estado.

4. Seleccione Agentes o Conectores.

   Aparecerá el panel de búsqueda de agentes o conectores.

5. (Opcional) Seleccione los criterios de búsqueda de actualización de agentes o conectores. Si no introduce ningún término de búsqueda, aparecerán todas las actualizaciones disponibles. Puede seleccionar uno o más de los siguientes criterios para limitar la búsqueda:

   - Grupo de agentes: sólo devuelve los agentes y los conectores asignados al grupo seleccionado.
   - Plataforma: sólo devuelve los agentes y conectores que se ejecutan en el sistema operativo seleccionado.
   - Patrón de nombres de agentes: sólo devuelve los agentes y conectores que contienen el patrón especificado.
   - (Sólo conectores) Integración: sólo devuelve los conectores que utilizan la integración seleccionada.

6. Haga clic en Mostrar estado.

   Aparece un gráfico de detalles que muestra el estado de los agentes o conectores que se ajustan a la búsqueda. Por ejemplo:

   ```
   Total: 10; En ejecución: 8; Pendiente: 1; Detenido: 1; No responde: 0
   ```

7. (Opcional) Haga clic en la pantalla de estado para ver los detalles del panel Estado en la parte inferior del gráfico.

   Nota: Puede hacer clic en el botón A petición para que un agente o conector actualice la pantalla de estado.

8. (Opcional) Si ve conectores, seleccione cualquier conector y haga clic en Reiniciar, Iniciar o Detener. Si ve agentes, seleccione cualquier agente y haga clic en Reiniciar

Capítulo 7: Creación de federaciones

Esta sección contiene los siguientes temas:

Consultas e informes en un entorno federado

Un solo servidor de CA Enterprise Log Manager devuelve datos desde su base de datos de eventos interna para responder a las consultas y generar informes. Si cuenta con una federación de servidores de CA Enterprise Log Manager, puede controlar el modo en que las consultas y los informes devuelven información de eventos según la configuración de las relaciones de la federación. También puede conservar los resultados de las consultas de servidores únicos desactivando la configuración global Utilizar consultas federadas.

La configuración global Utilizar consultas federadas está activada de forma predeterminada. De esta forma, las consultas de un servidor principal de CA Enterprise Log Manager se envían a todos los servidores secundarios de CA Enterprise Log Manager. Cada servidor de CA Enterprise Log Manager secundario realiza consultas al catálogo de archivos y al almacenamiento del registro de eventos activo además de realizar consultas a todos los servidores de CA Enterprise Log Manager secundarios. A continuación, cada servidor de CA Enterprise Log Manager secundario crea un único conjunto de resultados para enviar al servidor principal de CA Enterprise Log Manager solicitante. Se crea una protección ante consultas circulares en CA Enterprise Log Manager para activar las configuraciones en malla.

La implementación típica de CA Enterprise Log Manager de una empresa dispone de uno a cinco servidores. La implementación de una gran empresa dispone de diez a más servidores. El modo en que configura la federación controla la cantidad de información visible para el servidor de CA Enterprise Log Manager que emite la consulta. El tipo de consulta más simple proviene del servidor de CA Enterprise Log Manager principal y devuelve información de todos los servidores secundarios configurados por debajo de éste.

Cuando realiza consultas en la federación desde un servidor secundario, los resultados que ve dependen de la configuración de la federación. En una federación *jerárquica*, todos los servidores configurados como secundarios de un servidor le devuelven los resultados de las consultas a éste. En una federación *en malla*, todos los servidores interconectados devuelven los datos al servidor que emite la consulta.

Federaciones jerárquicas

Las *federaciones jerárquicas* utilizan una estructura piramidal vertical para expandir las cargas de recopilación de eventos por un área amplia. La estructura es similar a un organigrama. No es necesario crear un determinado número de niveles: puede crear los niveles que mejor se ajusten a sus necesidades empresariales.

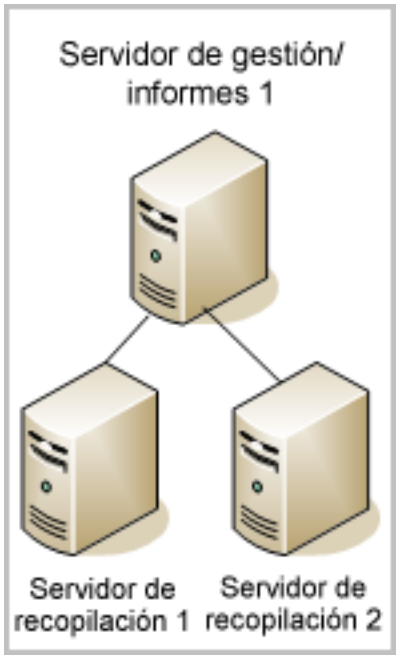
En una federación jerárquica, puede conectarse a cualquier servidor de CA Enterprise Log Manager para ver los informes de sus datos de eventos desde cualquier servidor secundario que se encuentre por debajo. El acceso a los datos es limitado en función de dónde empiece en la jerarquía. Si empieza en el medio de la jerarquía, sólo podrá ver los datos de ese servidor y los datos de sus servidores secundarios. Cuanto más ascienda en la federación jerárquica, a más datos de la red podrá acceder. En el nivel superior, podrá acceder a todos los datos de toda la implementación.

Las federaciones jerárquicas son útiles, por ejemplo, en las implementaciones regionales. Si desea que los recursos locales accedan a los datos de eventos dentro de una determinada jerarquía, o rama, de la red, pero no desea que accedan a los datos de eventos de otras ramas paralelas, podría crear una federación jerárquica con dos o más ramas paralelas que contengan los datos de cada región. Cada una de las ramas podría generar informes para un servidor de gestión de CA Enterprise Log Manager en las oficinas centrales para contar con una vista vertical de todos los informes de registro de eventos.

Ejemplo de mapa de federación

En el mapa de federación que se muestra en el siguiente diagrama, la red utiliza el servidor de gestión de CA Enterprise Log Manager como servidor de informes y varios servidores de recopilación en una configuración similar a la de un organigrama. El servidor de gestión/informes actúa como servidor principal de CA Enterprise Log Manager y proporciona autenticaciones de usuario, autorizaciones y funciones de gestión importantes además de las funciones de informes de gestionar consultas, informes y alertas. Los servidores de recopilación de este ejemplo serían los servidores secundarios del servidor de gestión/informes 1. Puede organizar más niveles en la jerarquía. Sin embargo, no puede haber más de un servidor de gestión. Los niveles adicionales se compondrían de servidores de informes que actuarían como servidores principales de los servidores de recopilación.

Como ejemplo de este estilo de federación, el servidor de gestión/informes 1 podría estar ubicado en su sede central y los servidores de recopilación podrían estar ubicados en oficinas regionales o sucursales (representados por los servidores de recopilación 1 y 2). Cada sucursal podría obtener información de sus propios datos, pero no los datos de la otra sucursal. Por ejemplo, desde el servidor de recopilación 1, sólo puede realizar consultas y generar informes sobre los datos del servidor de recopilación 1. Por el contrario, desde el servidor de gestión/informes 1, puede realizar consultas y generar informes sobre los datos del servidor de gestión/informes 1, del servidor de recopilación 1 y del servidor de recopilación 2.



En una federación jerárquica, cada servidor de CA Enterprise Log Manager puede tener uno o más servidores secundarios, pero sólo un servidor principal. Puede configurar este tipo de federación de forma vertical comenzando por el servidor de gestión. A continuación, muévase por las capas inferiores para configurar los servidores de recopilación y de informes secundarios. La clave a la hora de configurar una federación es realizar primero un mapa de los servidores y de las relaciones que se desean establecer. Posteriormente, podrá configurar un servidor de CA Enterprise Log Manager como servidor secundario para implementar las relaciones entre ellos.

Federaciones en malla

Una *federación en malla* es similar a una federación jerárquica en el sentido de que dispone de niveles. La principal diferencia es la configuración de las conexiones entre los servidores. Una federación en malla puede permitir que cualquier servidor de CA Enterprise Log Manager de la red realice consultas y genere informes sobre los datos del resto de servidores de CA Enterprise Log Manager. Las funciones de generación de informes dependen de las relaciones que cree entre los servidores.

Por ejemplo, en una federación en malla, es posible que los servidores sólo se pueden interconectar dentro de una rama vertical. Esto significa que todos los servidores de CA Enterprise Log Manager de esa rama podrían acceder al resto de servidores de CA Enterprise Log Manager de la misma rama. Esto se opone directamente a un servidor de CA Enterprise Log Manager en una federación jerárquica, que sólo puede generar informes en los servidores que se encuentran por debajo en la jerarquía.

En una formación de anillo o de estrella, cada servidor de CA Enterprise Log Manager se configura como servidor secundario del resto de servidores. Cuando solicita datos del informe desde un servidor de CA Enterprise Log Manager, verá los datos de todos los servidores de CA Enterprise Log Manager de la red.

La federación en malla asigna dos o más servidores de CA Enterprise Log Manager como principales y utiliza los servidores de la federación independientemente de su ubicación en la red. Los servidores configurados *como* secundarios también se configuran para ver los servidores secundarios de la misma rama o de otras diferentes como servidores federados a ellos. Por ejemplo, si cuenta con dos servidores de CA Enterprise Log Manager, A y B, podría crear una federación en malla haciendo que B sea un servidor secundario de A, *y* que A sea un servidor secundario de B. Ésta es la configuración esperada cuando utiliza dos o más servidores de gestión.

Ejemplo de federación en malla

Observe la siguiente ilustración de una federación en malla completa:

En la federación en malla que se muestra en este diagrama, los cuatro servidores de recopilación están federados entre ellos y con los servidores de informes. Cada servidor es un servidor principal y secundario respecto a cada servidor de la federación.

Una gran ventaja de esta implementación sobre la federación jerárquica estricta es que puede acceder a los datos desde cualquier punto de la malla y obtener resultados de todos los servidores de CA Enterprise Log Manager, independientemente de la jerarquía.

Puede combinar federaciones jerárquicas y en malla para llevar a cabo una configuración que se ajuste a sus necesidades. Por ejemplo, una configuración en malla dentro de una única rama podría ser muy útil para implementaciones globales. Podría obtener una descripción global de los datos desde los servidores de informes principales al tiempo que conserva los clústeres regionales (ramas) que sólo pueden acceder a sus propios datos.

Configuración de una federación de CA Enterprise Log Manager

Los servidores de CA Enterprise Log Manager que agrega a una federación deben utilizar el mismo nombre de instancia de aplicación del servidor de gestión. De esta forma, el servidor de gestión podrá almacenar y gestionar todas las configuraciones de forma conjunta como configuraciones globales.

Puede configurar la federación en cualquier momento, pero resulta útil hacerlo antes de comenzar a generar informes de programación, si desea informes consolidados.

La configuración de una federación incluye las siguientes actividades:

1. Cree un mapa de federación.
2. Instale el primer CA Enterprise Log Manager, el servidor de gestión.

3. Instale uno o más servidores.
4. Configure las relaciones primarias/secundarias. Por ejemplo, comience seleccionando los secundarios de la federación del servidor de gestión en esta configuración del almacenamiento del registro de eventos del servidor.

   Este primer grupo de servidores secundarios forma la segunda capa, o nivel, de la federación si está configurando una federación jerárquica.
5. Mire el gráfico de federación para comprobar que la estructura entre los servidores de los niveles principales y secundarios esté configurada como desea.

Configuración de un servidor de CA Enterprise Log Manager como servidor secundario

La configuración de un servidor de CA Enterprise Log Manager como servidor secundario es otro de los pasos esenciales a la hora de crear una federación. Siga este procedimiento para agregar servidores a la federación en cualquier momento. Debe instalar todos los servidores de CA Enterprise Log Manager que desee federar con el mismo nombre de instancia de aplicación registrado antes de realizar esta parte de la configuración. Cuando instala un servidor nuevo, el nombre aparece en la lista de servidores disponibles para la federación. Puede realizar este procedimiento tantas veces como sea necesario para crear la estructura federada que desee.

Para configurar un servidor de CA Enterprise Log Manager como servidor secundario

1. Inicie sesión en algún servidor de CA Enterprise Log Manager que esté registrado con el mismo nombre de instancia de aplicación que los otros de la federación planteada.
2. Haga clic en la ficha Administración y seleccione la subficha Servicios.
3. Expanda la carpeta de servicios Almacenamiento del registro de eventos y, a continuación, seleccione el nombre del servidor principal de CA Enterprise Log Manager.
4. Desplácese a la lista Secundarios de la federación.
5. Seleccione uno o más nombres de servidor que desee configurar como secundarios del servidor principal en los servidores de la lista disponible.
6. Utilice los botones de flecha para mover las selecciones a la lista de servidores seleccionados.

   Los servidores de CA Enterprise Log Manager seleccionados y movidos a la lista son ahora secundarios federados del servidor principal.

Más información:

Selección de uso de consultas federadas (en la página 149)

Visualización del gráfico de federación y del monitor de estado del servidor

Puede visualizar un gráfico que muestra los servidores de CA Enterprise Log Manager en el entorno, sus relaciones de federación y la información de estado sobre servidores individuales. El gráfico de federación le permite ver la estructura actual de la federación y los detalles de estado de cada servidor. También puede seleccionar el servidor local consultado durante la sesión y establecerlo como servidor principal.

Para ver un gráfico de federación, haga clic en Mostrar gráfico de federación y controlador de estado en la parte superior de la pantalla: 

Aparecerá una ventana con un gráfico de todos los host de almacenes de eventos registrados con el servidor de gestión actual:

- Los almacenes de eventos con secundarios de la federación se muestran con líneas de conexión azules claro y negras que indican la relación de federación.
- Los almacenes de eventos sin secundarios de la federación se muestran en verde claro.

Puede seleccionar un servidor local actual para realizar consultas.

También puede visualizar los detalles de estado de cualquiera de los servidores mostrados. Haga clic en un servidor del gráfico de federación para mostrar detalles del estado, incluidos los siguientes:

- Porcentaje de uso de la CPU
- Porcentaje de uso de la memoria disponible
- Porcentaje de uso del espacio disponible en el disco
- Eventos por segundo recibidos
- Gráfico principal de estado del almacén de registro de eventos

Más información:

Ejemplo: Mapa de federación para una empresa mediana (en la página 40)
Ejemplo: Mapa de federación para una gran empresa (en la página 38)

Capítulo 8: Empleo de la biblioteca de refinamiento de eventos

Esta sección contiene los siguientes temas:

Acerca de la biblioteca de refinamiento de eventos

La biblioteca de refinamiento de eventos le proporciona herramientas para crear nuevos archivos de asignación y análisis o para modificar copias de los archivos existentes; de este modo, podrá proporcionar soporte para nuevos dispositivos, aplicaciones, etc. La biblioteca incluye las siguientes opciones:

- Integraciones
- Escuchas
- Archivos de asignación y análisis
- Reglas de resumen y supresión

Las reglas de supresión evita que se recopilen datos o que se inserten en el almacenamiento del registro de eventos. Las reglas de resumen le permiten agregar eventos para reducir el número de inserciones de acciones o tipos de eventos similares. Ésta es la parte de la biblioteca utilizada más habitualmente dado que las reglas de resumen y supresión pueden ayudarle a ajustar el rendimiento de la red y de la base de datos.

Puede utilizar el área de integraciones para ver las integraciones predefinidas y para crear nuevas integraciones para sus bases de datos, archivos, aplicaciones o dispositivos de propietario o personalizados. Si desea obtener más información, consulte la *Guía de administración de CA Enterprise Log Manager* y la ayuda en línea.

Admisión de nuevos orígenes de eventos con la biblioteca de refinamiento de eventos

Si necesita admitir un dispositivo, aplicación, base de datos u otro origen de eventos todavía no admitido, utilice asistentes de archivos de asignación y análisis, así como el asistente de integraciones para crear los componentes necesarios.

El proceso consta de los pasos generales siguientes:

1. Crear archivos de análisis para recopilar datos de eventos como pares de nombre y valor.
2. Crear archivos de asignación para asignar los pares de nombre y valor en la gramática de eventos comunes.
3. Crear nuevas integraciones y escuchas para recopilar datos desde el origen de eventos.

Los archivos de integraciones, análisis y asignaciones, así como las reglas de resumen y supresión, se explican detalladamente en la *Guía de administración de CA Enterprise Log Manager* y en la ayuda en línea.

Archivos de asignación y análisis

Durante su funcionamiento, CA Enterprise Log Manager lee eventos entrantes y los divide en secciones en una acción denominada *análisis*. Existen diversos archivos de análisis de mensajes de distintos dispositivos, sistemas operativos, aplicaciones y bases de datos. Una vez analizados los eventos entrantes en pares de nombre y valor, esos datos pasan por un módulo de *asignación* que coloca los datos de eventos en los campos de la base de datos.

El módulo de asignación utiliza archivos de asignación de datos creados para orígenes de eventos específicos y que son similares a los archivos de análisis de mensajes. El esquema de la base de datos es la gramática de eventos comunes, una de las características principales de CA Enterprise Log Manager.

El análisis y la asignación son los medios por los que los datos se normalizan y se almacenan en una base de datos común independientemente del tipo de evento o del formato del mensaje.

El asistente de integración y algunos de los módulos del adaptador de CA requieren la configuración de los archivos de asignación y análisis que mejor describen los tipos de datos de eventos que escucha un conector o un adaptador. En los paneles de configuración donde aparecen estos controles, el orden de los archivos de análisis de mensajes debe reflejar el número de eventos recibidos relativo de ese tipo. El orden de los archivos de asignación de datos también debe reflejar la cantidad de eventos recibidos desde un origen determinado.

Por ejemplo, si el módulo de escucha de syslog de un determinado servidor de CA Enterprise Log Manager recibe la mayoría de eventos de Cisco PIX Firewall, debe colocar en primer lugar los archivos de CiscoPIXFW.XMPS y CiscoPIXFW.DMS en las listas respectivas.

Apéndice A: Consideraciones para los usuarios de CA Audit

Esta sección contiene los siguientes temas:

Descripción de las diferencias en las arquitecturas

A la hora de planificar la utilización de CA Audit y CA Enterprise Log Manager conjuntamente, primero debe conocer las diferencias en las arquitecturas así como los efectos que tienen en la estructura de red.

CA Enterprise Log Manager utiliza un almacenamiento del registro de eventos incrustado y proporciona un explorador de agente para configurar y gestionar los agentes. Esta nueva tecnología junto con una gramática de eventos comunes permite que el rendimiento de eventos sea más rápido para realizar el almacenamiento al tiempo que admite un mayor número de orígenes de eventos. La gramática de eventos comunes permite que CA Enterprise Log Manager normalice los eventos desde diversos orígenes de eventos en un único esquema de base de datos.

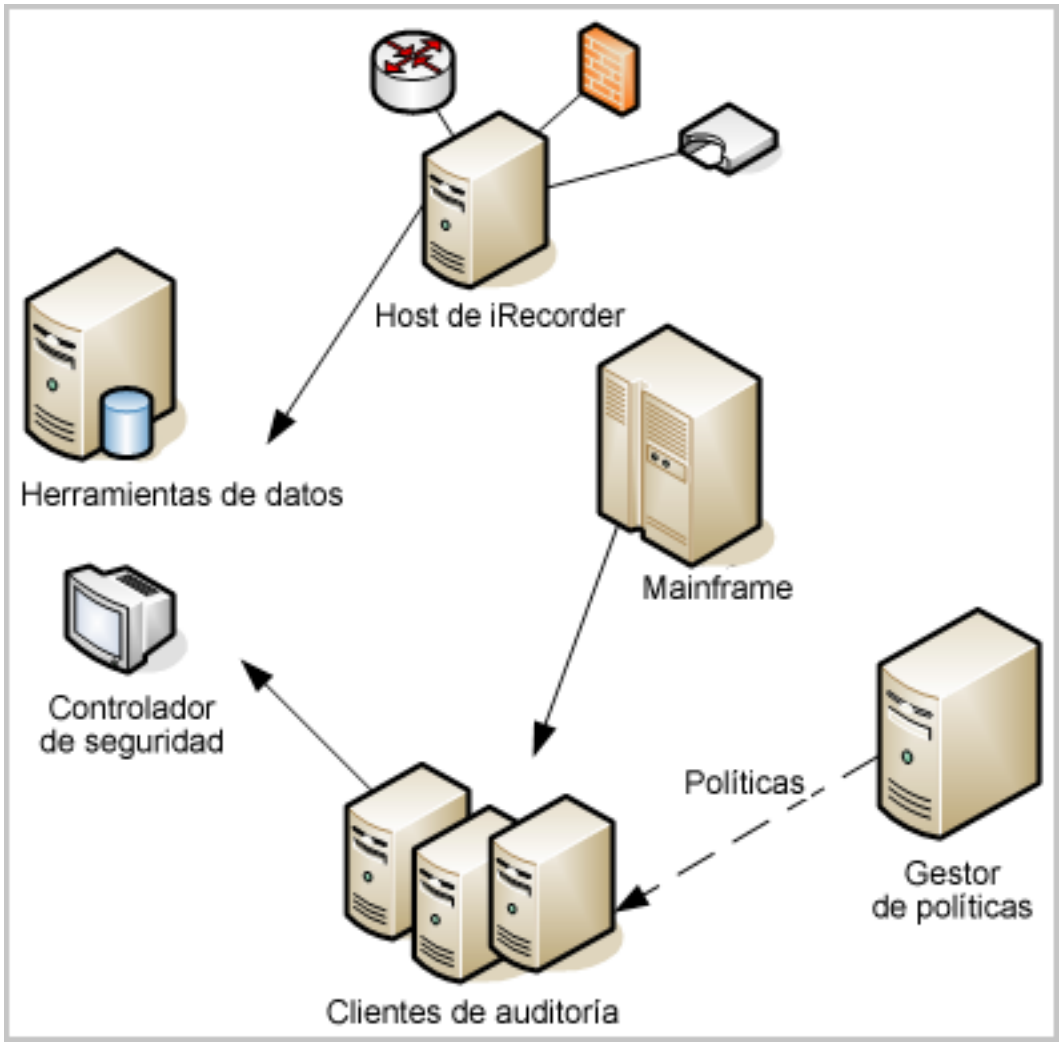
CA Enterprise Log Manager se integra a un cierto nivel con CA Audit pero, por el diseño, no es totalmente interoperable. CA Enterprise Log Manager es una nueva estructura de servidores independiente que se puede ejecutar con CA Audit, pero debe tener en cuenta las siguientes consideraciones sobre la gestión de eventos:

CA Enterprise Log Manager puede...	**CA Enterprise Log Manager *no* puede...**
Recibir registros de eventos enviados desde iRecorders y clientes de CA Audit utilizando escuchas configurables.	Acceder directamente a registros de eventos almacenados en la base de datos del recopilador de CA Audit.
Proporcionar una utilidad para importar datos de registros de eventos almacenados en la base de datos del recopilador de CA Audit (tabla SEOSDATA).	
Utilizar agentes para enviar registros de eventos	

CA Enterprise Log Manager puede...	CA Enterprise Log Manager *no* puede...
sólo a la infraestructura de servidores de CA Enterprise Log Manager.	
Permitir que los agentes de CA Enterprise Log Manager y los clientes de CA Audit junto con iRecorders se ejecuten en el mismo host físico.	Permitir que los agentes de CA Enterprise Log Manager y los clientes de CA Audit junto con iRecorders del mismo host accedan a los mismos orígenes de registros simultáneamente.
Utilizar el explorador de agente integrado para sólo gestionar los agentes de CA Enterprise Log Manager. Durante la operación conjunta de los dos sistemas, CA Audit sólo utiliza Policy Manager para gestionar clientes de CA Audit.	
	Migrar datos de CA Audit de recopiladores de tablas, plantillas de informes o informes personalizados, políticas de alertas, políticas de recopilación/filtrado o políticas de control de acceso basadas en funciones.

Arquitectura de CA Audit

La siguiente ilustración muestra una implementación de CA Audit simplificada:



En las implementaciones de CA Audit de algunas empresas, los datos de eventos son almacenados por el servicio de recopilador en una base de datos relacional que se ejecuta en el servidor de herramientas de datos. El administrador de la base de datos controla y realiza el mantenimiento de esta base de datos y trabaja con el administrador del sistema para que las políticas adecuadas recopilen los eventos deseados y excluyan los eventos no requeridos.

Las líneas continuas de este diagrama muestran los eventos que pasan de hosts de clientes, grabadoras e iRecorder de CA Audit al servidor de herramientas de datos o, en algunos casos, a una consola con monitor de seguridad opcional. La línea discontinua representa el flujo de control entre el servidor de Policy Manager y los clientes que utilizan políticas.

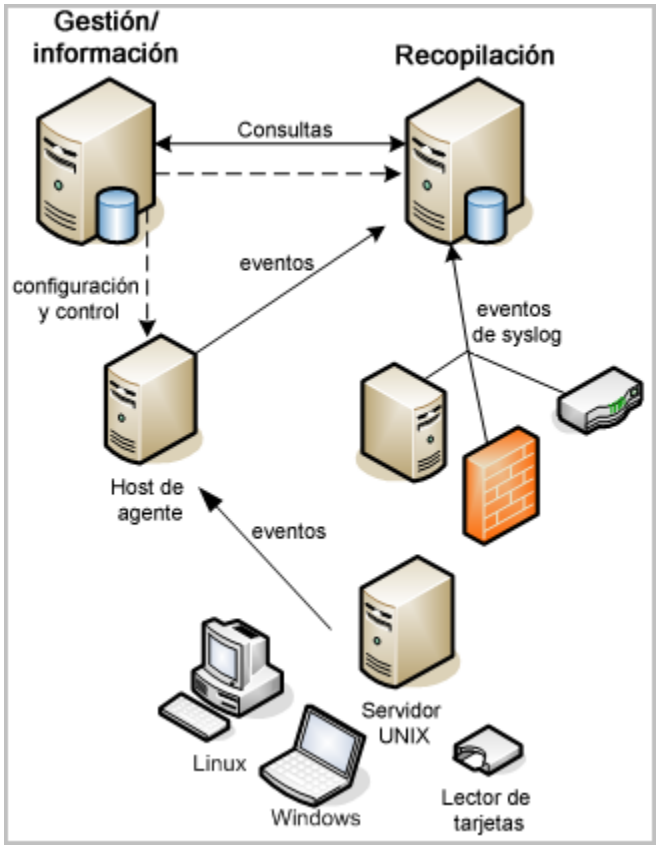
El servidor de herramientas de datos proporciona utilidades básicas de visualización y de generación de informes así como el almacenamiento de eventos. Las consultas y los informes personalizados son habituales en las implementaciones de empresas y su creación y mantenimiento requieren un tiempo considerable.

Esta topología de red permite la recopilación de diversos tipos de eventos desde distintos dispositivos, aplicaciones y bases de datos. Normalmente, cuenta con un almacenamiento central de eventos recopilados que es parte de, o está gestionado por, el servidor de herramientas de datos que también genera algunos informes.

No obstante, son necesarias otras funciones para que su solución se gestione con rapidez de modo que aumenten los volúmenes de eventos. Tiene que generar informes que cumplan una serie de regulaciones federales e internacionales. Además, tiene que encontrar estos informes de forma rápida y sencilla.

Arquitectura de CA Enterprise Log Manager

La siguiente ilustración muestra una implementación básica de dos servidores de CA Enterprise Log Manager:



Un sistema de CA Enterprise Log Manager puede contar con uno o más servidores, donde el primer servidor instalado es el servidor de gestión. No puede haber más de un servidor de gestión en un sistema, pero puede tener varios sistemas. El servidor de gestión realiza el mantenimiento del contenido y de la configuración de todos los servidores de CA Enterprise Log Manager y lleva a cabo la autenticación y la autorización de usuario.

En una implementación básica de dos servidores, el servidor de gestión realiza la función de un servidor de informes. Un servidor de informes recibe eventos refinados de uno o varios servidores de recopilación. El servidor de informes gestiona informes y consultas a petición además de alertas e informes programados. El servidor de recopilación refina los eventos recopilados.

Cada servidor de CA Enterprise Log Manager cuenta con su propia base de datos interna del almacenamiento del registro de eventos. El almacenamiento del registro de eventos es una base de datos de propiedad que utiliza la compresión para mejorar la capacidad de almacenamiento y para permitir consultas de archivos de bases de datos activas, archivos marcados para archivar y archivos descongelados. No es necesario ningún paquete DBMS para realizar el almacenamiento de eventos.

El servidor de recopilación de CA Enterprise Log Manager puede recibir eventos directamente utilizando el agente predeterminado o desde un agente que resida en el origen de eventos. Los agentes también pueden residir en un host que actúa como recopilador de otros orígenes de eventos de la red como de un host del enrutador o un concentrador VPN.

Las líneas continuas de este diagrama representan los flujos de eventos desde los orígenes de eventos a los agentes, al servidor de recopilación y a la función de generación de informes del servidor de gestión/informes. Las líneas discontinuas muestran y el tráfico de control y de configuración entre los servidores de CA Enterprise Log Manager y desde la función de gestión del servidor de gestión/informes a los agentes. Puede utilizar cualquier servidor de CA Enterprise Log Manager de la red para controlar cualquier agente de la red siempre que los servidores de CA Enterprise Log Manager hayan sido registrados con el mismo nombre de instancia de aplicación en el servidor de gestión durante la instalación.

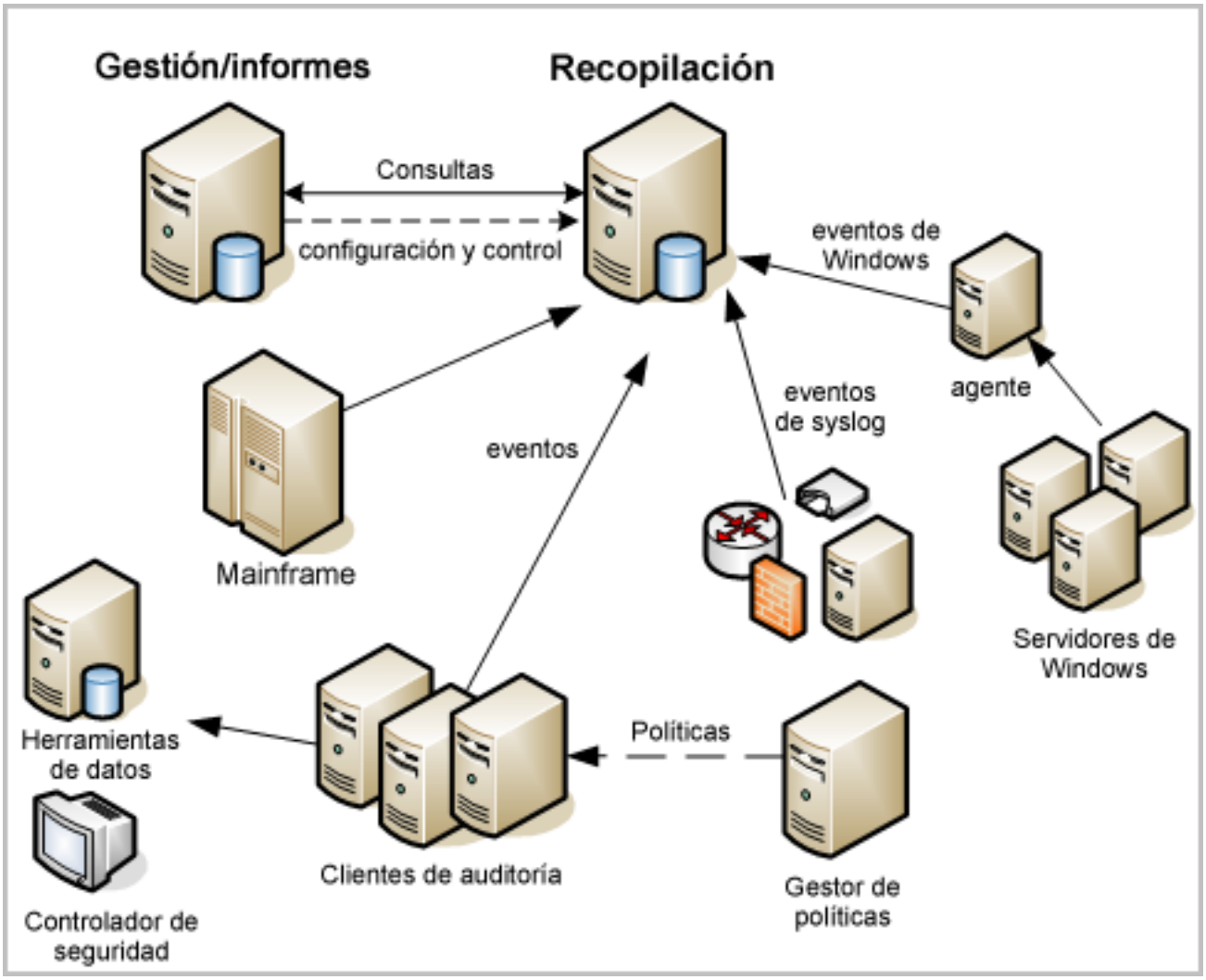
Los agentes utilizan conectores (no se muestran) para recopilar eventos. Un solo agente puede gestionar varios conectores para recopilar distintos tipos de eventos al mismo tiempo. Esto significa que un solo agente implementado en un origen de eventos individual puede recopilar distintos tipos de información. El servidor de CA Enterprise Log Manager también proporciona escuchas que permiten la recopilación de eventos desde otras aplicaciones de CA utilizando los iRecorder y SAPI Recorder de su red de CA Audit.

Puede federar servidores de CA Enterprise Log Manager para escalar la solución y para compartir datos de informes entre ellos sin tener que transportar los datos fuera de los límites. De este modo, obtiene una vista general de la red al tiempo que se cumplen las regulaciones sobre el mantenimiento de las ubicaciones de datos físicos.

Las actualizaciones de suscripción de consultas e informes predefinidos implican que ya no tendrá que realizar el mantenimiento de consultas e informes manualmente. Los asistentes proporcionados le permiten crear sus propias integraciones personalizadas para las aplicaciones y dispositivos de terceros no admitidos.

Arquitectura integrada

El siguiente diagrama muestra una red de CA Audit típica con CA Enterprise Log Manager que equilibra la gestión del alto volumen de eventos y las funciones de generación de informes basadas en la compatibilidad:



CA Enterprise Log Manager utiliza un agente de explorador integrado, un almacenamiento del registro de eventos incrustado y una única interfaz para centralizar y simplificar la recopilación de registros. La nueva tecnología de CA Enterprise Log Manager junto con una gramática de eventos comunes permite que el rendimiento de eventos sea más rápido para realizar el almacenamiento al tiempo que gestiona un mayor número de orígenes de eventos. Un único agente puede gestionar varios conectores para los orígenes de eventos, simplificar las tareas de gestión de agentes y sacar provecho de las integraciones predefinidas para los orígenes de registros de eventos populares o comunes.

En esta implementación, el servidor de recopilación de CA Enterprise Log Manager recibe los eventos syslog, los eventos basados en iTechnology y los eventos de SAPI Recorder. El servidor de recopilación recibe eventos de los orígenes de eventos de Windows a través de un agente de CA Enterprise Log Manager independiente basado en Windows. Puede disponer de varios agentes implementados en la red, cada uno de los cuales recopila distintos tipos de datos de eventos a través de sus conectores. De esta forma, podrá reducir el tráfico de eventos en la base de datos SEOSDATA y utilizar las consultas e informes disponibles en CA Enterprise Log Manager. Un simple cambio de regla de política le permite a los clientes de CA Audit enviar eventos recopilados al servidor de herramientas de datos y al servidor de CA Enterprise Log Manager.

Además de un mayor rendimiento, CA Enterprise Log Manager proporciona consultas e informes predeterminados que le ayudan a cumplir varios estándares como PCI (DSS) y SOX. Cuando combina las consultas e informes predefinidos con la implementación existente de CA Audit y CA Security Command Center, puede sacar provecho de sus inversiones en sus soluciones personalizadas al tiempo que se beneficia de los informes de CA Enterprise Log Manager y de un mayor rendimiento.

Configuración de los adaptadores de CA

Los adaptadores de CA son un grupo de escuchas que reciben eventos de los componentes heredados como, por ejemplo, clientes de CA Audit, iRecorders y SAPI Recorders además de orígenes de eventos que envían eventos a través de iTechnology de forma nativa.

Defina las opciones de configuración del adaptador de CA antes de cambiar las configuraciones de las políticas de CA Audit o de iRecorders. De esta forma, los procesos de escucha se realizan antes de que lleguen los eventos y, de esta forma, se evita que los datos de eventos se asignen incorrectamente.

Si envía eventos a través de un iRecorder a CA Audit o si utiliza un cliente de CA Audit con iRecorder, usará los adaptadores SAPI de CA Enterprise Log Manager para recibir eventos. Para enviar eventos a CA Enterprise Log Manager, modificará una política existente de CA Audit para los eventos de CA Access Control. Puede agregar una acción del recopilador o una acción de ruta a una regla existente.

- Si crea una acción del recopilador en una regla de una política de CA Audit existente, configure el adaptador de CA del recopilador de SAPI para recibir los eventos.
- Si crea una acción de ruta en una regla de una política de CA Audit existente, configure el adaptador de CA del enrutador de SAPI para recibir los eventos.

Consulte la documentación de orígenes de SAPI para obtener más información sobre cómo volver a realizar la configuración para enviar eventos directamente a CA Enterprise Log Manager.

Si va a instalar un iRecorder independiente o va a utilizar un iRecorder existente, tendrá que configurar el complemento de eventos de iTech para recibir eventos. Por ejemplo, utilice este método si no tiene CA Audit instalado pero desea utilizar un iRecorder de CA para recopilar eventos desde un origen de eventos admitido. El proceso incluye los siguientes pasos:

- Configurar el complemento de eventos iTechnology
- Configurar iRecorder o el producto basado en iTechnology para enviar eventos directamente al servidor de CA Enterprise Log Manager.

Acerca del recopilador y del enrutador de SAPI

Normalmente, los servicios de SAPI se utilizan para recibir eventos de productos integrados y clientes de CA Audit. CA Enterprise Log Manager utiliza dos instancias de servicio de una escucha de SAPI: una instalada en el recopilador de SAPI; la otra, en el enrutador de SAPI.

Los módulos de SAPI utilizan el daemon de iGateway para el comando y control. Los módulos actúan como un enrutador de SAPI y un recopilador de SAPI y utilizan puertos estáticos y dinámicos a través del asignador de puertos.

Utilice el recopilador de SAPI cuando envíe eventos desde clientes de CA Audit para poder utilizar el soporte integrado de conmutación por error en la acción de Audit Collector.

Utilice el enrutador de SAPI cuando envíe eventos desde clientes de CA Audit utilizando la acción de ruta o cuando envíe eventos desde SAPI Recorders o integraciones que admiten enviar eventos directamente a un cliente de CA Audit. En este caso, debe configurar el remitente remoto como si el servidor de CA Enterprise Log Manager fuese el cliente de CA Audit.

La escucha de SAPI abre su propio puerto y escucha pasivamente los nuevos eventos que se van a enviar. Cada instancia del módulo de SAPI cuenta con su propia configuración que especifica lo siguiente:

- Puerto en el que se escucha
- Archivos de asignación de datos (DM) que se van a cargar
- Bibliotecas de cifrado que se van a utilizar

Una vez recibido el evento, el módulo lo enviará a la biblioteca de asignación y, a continuación, CA Enterprise Log Manager lo insertará en la base de datos.

Importante: La biblioteca de asignación de datos puede contener uno o más archivos de asignación con el mismo nombre pero con números de versión diferentes. Los distintos archivos admiten diversos niveles de versión del mismo origen de datos, como un sistema operativo, una base de datos, etc. Es fundamental que sólo seleccione un archivo de asignación de versión al configurar el enrutador o el recopilador de SAPI.

Si los dos archivos con el mismo nombre se encuentran en la lista de archivos de asignación seleccionados, el motor de asignación sólo utilizará el primero de la lista. Si no se trata del archivo adecuado del flujo de eventos entrantes, el motor de asignación no podrá asignar los eventos correctamente. Por el contrario, podrían generarse consultas e informes que muestran información que no incluye los eventos sin asignar o que no incluye ningún evento.

Configuración del servicio de recopilador de SAPI

Siga este procedimiento para configurar el servicio de recopilador de SAPI.

Puede modificar las políticas de CA Audit que utiliza acciones del recopilador para enviar eventos a un servidor de CA Enterprise Log Manager además de, o en lugar de, enviar eventos a la base de datos del recopilador de CA Audit. Configure este servicio antes de modificar las políticas de Audit para que no se pierda ningún evento.

Para configurar el servicio de recopilador de SAPI

1. Inicie sesión en el servidor de CA Enterprise Log Manager y seleccione la ficha Administración.

   La subficha Recopilación de registros se mostrará de forma predeterminada.

2. Expanda la entrada Adaptadores de CA.
3. Seleccione el servicio de recopilador de SAPI.
4. Consulte la ayuda en línea para obtener descripciones de cada campo.
5. Al terminar, haga clic en Guardar.

Configuración del servicio de enrutador de SAPI

Siga este procedimiento para configurar el servicio de enrutador de SAPI.

Puede modificar las políticas de CA Audit que utilizan acciones de ruta para enviar eventos a un servidor de CA Enterprise Log Manager además de, o en lugar de, enviar eventos a otros destinos. También puede redireccionar eventos de SAPI Recorder para ir directamente a la escucha del enrutador de SAPI modificando los archivos de configuración. Configure este servicio antes de modificar los valores de configuración de las políticas de Audit o de SAPI Recorder para que no se pierda ningún evento.

Para configurar el servicio de enrutador de SAPI

1. Inicie sesión en el servidor de CA Enterprise Log Manager y seleccione la ficha Administración.

   La subficha Recopilación de registros se mostrará de forma predeterminada.

2. Expanda la entrada Adaptadores de CA.
3. Seleccione el servicio de enrutador de SAPI.
4. Consulte la ayuda en línea para obtener descripciones de cada campo.
5. Al terminar, haga clic en Guardar.

Acerca del complemento de eventos iTechnology

El complemento de eventos iTechnology recibe eventos enviados a través del mecanismo de gestión de eventos iGateway Configure el complemento de eventos iTechnology si se cumple alguna de las siguientes condiciones en su entorno:

- Cuenta con iRecorders en la red que no tienen clientes de CA Audit en el mismo sistema
- Cuenta con otros productos, como CA EEM, que pueden reenviar eventos a través de iTechnology

Una vez recibido un evento, este servicio lo envía a la biblioteca de asignación; a continuación, CA Enterprise Log Manager inserta el evento asignado en el almacenamiento del registro de eventos.

Configuración del complemento de eventos iTechnology

Siga este procedimiento para configurar el complemento de eventos iTechnology para recibir iRecorders y otros orígenes de eventos iTechnology.

Utilice el complemento iTechnology cuando configure un iRecorder independiente para enviar los eventos a un servidor de CA Enterprise Log Manager. Configure este servicio *antes de* configurar o instalar un iRecorder para que no se pierda ningún evento.

Para configurar el complemento de eventos iTechnology

1. Inicie sesión en el servidor de CA Enterprise Log Manager y seleccione la ficha Administración

   La subficha Recopilación de registros se mostrará de forma predeterminada.

2. Expanda la entrada Adaptadores de CA.
3. Seleccione el servicio de complemento de eventos iTechnology.
4. Seleccione uno o varios archivos de asignación de datos (DM) en la lista Archivos DM disponibles y utilice las flechas para moverlos a la lista Seleccionar archivos DM.

   El servicio de complemento de eventos se preconfigura para incluir la mayor parte de archivos de asignación de datos importantes.

5. Haga clic en Guardar para almacenar los cambios en los archivos de configuración del servidor de gestión.

Envío de eventos de CA Audit a CA Enterprise Log Manager

Puede integrar CA Enterprise Log Manager con su implementación de CA Audit existente de las siguientes maneras:

- Volver a configurar un iRecorder que no esté en el mismo host como cliente de CA Audit para enviar eventos a CA Enterprise Log Manager
- Modificar una política de CA Audit existente para enviar eventos a CA Audit y a CA Enterprise Log Manager

Configuración de iRecorder para enviar eventos a CA Enterprise Log Manager

CA Enterprise Log Manager recibe eventos de iRecorders a través de la escucha del complemento de eventos iTech. Debe configurar la escucha para poder cambiar la configuración de iRecorder. Si no lo hace, podría perder datos de eventos. Una vez configurada la escucha, siga este procedimiento para que iRecorder envíe eventos al servidor de CA Enterprise Log Manager.

Los iRecorders instalados en el mismo equipo que un cliente de CA Audit envían eventos al cliente directamente. En estos equipos, debe utilizar los adaptadores del enrutador o el recopilador de SAPI.

Importante: Un iRecorder independiente sólo puede enviar sus eventos a un único destino. Si vuelve a configurar un iRecorder siguiendo el procedimiento que se indica a continuación, los eventos *sólo* se almacenarán en el almacenamiento del registro de eventos de CA Enterprise Log Manager. Si necesita conservar eventos en el almacenamiento del registro de eventos y en la base de datos del recopilador de CA Audit, modifique una acción de regla en una política existente o cree una nueva política para un cliente de CA Audit.

Para configurar iRecorder para que envíe eventos a CA Enterprise Log Manager

1. Inicie sesión en el servidor que aloja el iRecorder como usuario con privilegios de administrador.
2. Desplácese al directorio de su sistema operativo:
   - UNIX o Linux: /opt/CA/SharedComponents/iTechnology
   - Windows: \Archivos de programa\CA\SharedComponents\iTechnology
3. Detenga el servicio o el daemon de iGateway con el siguiente comando:
   - UNIX o Linux: ./S99igateway stop
   - Windows: net stop igateway

4. Edite el archivo iControl.conf.
5. Especifique el siguiente valor RouteEvent:

   ```
   <RouteEvent>true</RouteEvent>
   ```

   Esta entrada le comunica al iGateway que envíe sus eventos, incluidos todos los eventos de iRecorder, al host del par de etiquetas de RouteHost.
6. Especifique el siguiente valor RouteHost:

   ```
   <RouteHost>CA_ELM_hostname</RouteHost>
   ```

   Esta entrada le comunica al iGateway que envíe sus eventos al servidor de CA Enterprise Log Manager utilizando el nombre DNS.
7. Reinicie el servicio o daemon de iGateway con el siguiente comando:
   - UNIX o Linux: ./S99igateway start
   - Windows: net start igateway

   Esta acción obliga a iRecorder a que utilice las nuevas configuraciones y a que inicie el flujo de eventos desde el iRecorder al servidor de CA Enterprise Log Manager.

Más información:

Acerca del recopilador y del enrutador de SAPI (en la página 231)
Configuración del servicio de recopilador de SAPI (en la página 232)
Configuración del servicio de enrutador de SAPI (en la página 233)

Modificación de una política de CA Audit existente para enviar eventos a CA Enterprise Log Manager

Siga este procedimiento para que un cliente de CA Audit pueda enviar eventos *tanto a* CA Enterprise Log Manager como a la base de datos del recopilador de CA Audit. Al agregar un nuevo destino a las acciones de ruta o del recopilador en una regla existente, podrá enviar eventos recopilados a ambos sistemas. Como alternativa, también puede modificar las reglas o políticas específicas para *sólo* enviar eventos al servidor de CA Enterprise Log Manager.

CA Enterprise Log Manager recopila eventos de clientes de CA Audit que utilizan el enrutador de SAPI de CA Audit y las escuchas del recopilador de SAPI de CA Audit. Los eventos recopilados se almacenan en el almacenamiento del registro de eventos de CA Enterprise Log Manager sólo *después* de que envíe la política a los clientes y de que pase a estar activa.

Importante: Debe configurar las escuchas de CA Enterprise Log Manager para recibir eventos antes de modificar y activar la política. Si no realiza primero la configuración, es posible que los eventos no se asignen correctamente si éstos llegan después de que la política esté activa y antes de que las escuchas puedan asignar los eventos correctamente.

Para modificar una acción de regla de una política existente y enviar eventos a CA Enterprise Log Manager

1. Inicie sesión en el servidor de Policy Manager y acceda a la ficha Mis políticas en el panel izquierdo.
2. Expanda la carpeta de políticas hasta ver la política deseada.
3. Haga clic en la política para mostrar la información básica en el panel de detalles de la derecha.
4. Haga clic en Editar en el panel de detalles para agregar las reglas de la política. Se iniciará el asistente para reglas.
5. Haga clic en Editar acciones al lado de la flecha del paso tres del asistente. Se mostrará la página de las acciones de regla del asistente.
6. Haga clic en la acción del recopilador en el panel Examinar acciones de la izquierda. Se mostrará la lista de acciones a la derecha.

   También puede utilizar la acción de ruta para crear una regla que envíe eventos a un servidor de CA Enterprise Log Manager.
7. Haga clic en Nueva para crear una nueva regla.
8. Introduzca la dirección IP o el nombre de host del servidor de recopilación de CA Enterprise Log Manager.

   En las implementaciones de CA Enterprise Log Manager con dos o más servidores, puede introducir una dirección IP o un nombre de host de CA Enterprise Log Manager distinto en el campo Nombre de host alternativo para poder utilizar la función de conmutación por error automática de <Aus>. Si el primer servidor de CA Enterprise Log Manager no está disponible, CA Audit enviará eventos automáticamente al servidor nombrado en el campo Nombre de host alternativo.
9. Introduzca el nombre del servidor de gestión de CA Enterprise Log Manager en el campo Nombre de host alternativo y, a continuación, cree una descripción para esta nueva regla de acción.
10. Desactive la casilla de verificación Realizar esta acción en el servidor remoto, si está activada.
11. Haga clic en Agregar para guardar la nueva acción de regla y, a continuación, haga clic en Finalizar en la ventana del asistente.
12. Seleccione la ficha Reglas en el panel inferior derecho y, a continuación, seleccione una de las reglas que desee marcar.

13. Haga clic en Comprobar políticas para comprobar la regla cambiada con las nuevas acciones y para garantizar que se compile correctamente.

    Realice las modificaciones necesarias en la regla y compruebe que se ha compilado correctamente antes de activarla.

14. Haga clic en Activar para distribuir la política marcada que contiene las nuevas acciones de regla agregadas.

15. Repita este procedimiento en cada regla y política con los eventos recopilados que desee enviar a CA Enterprise Log Manager.

Más información:

Acerca del recopilador y del enrutador de SAPI (en la página 231)
Configuración del servicio de recopilador de SAPI (en la página 232)
Configuración del servicio de enrutador de SAPI (en la página 233)

Modificación de una política de r8SP2 existente para enviar eventos a CA Enterprise Log Manager

Siga este procedimiento para que un cliente de CA Audit r8 SP2 pueda enviar eventos *tanto a* CA Enterprise Log Manager como a la base de datos del recopilador de CA Audit. Al agregar un nuevo destino a las acciones de ruta o del recopilador en una regla existente, podrá enviar eventos recopilados a ambos sistemas. Como alternativa, también puede modificar las reglas o políticas específicas para *sólo* enviar eventos al servidor de CA Enterprise Log Manager.

Si desea obtener más información acerca de las políticas, consulte la *Guía de implementación de CA Audit r8 SP2*. Consulte esta guía para obtener más información acerca de cómo seguir los pasos adecuados en el procedimiento que se indica a continuación.

CA Enterprise Log Manager recopila eventos de clientes de CA Audit que utilizan el enrutador de SAPI de CA Audit y las escuchas del recopilador de SAPI de CA Audit. Los eventos recopilados se almacenan en el almacenamiento del registro de eventos de CA Enterprise Log Manager sólo *después* de que envíe la política a los clientes y de que pase a estar activa.

Importante: Debe configurar las escuchas de CA Enterprise Log Manager para recibir eventos antes de modificar y activar la política. Si no realiza primero la configuración, es posible que los eventos no se asignen correctamente si éstos llegan después de que la política esté activa y antes de que las escuchas puedan asignar los eventos correctamente.

Para modificar una acción de regla de una política de r8 SP2 existente para enviar eventos a CA Enterprise Log Manager

1. Inicie sesión en el servidor de Policy Manager como usuario con la función de creador.
2. Acceda a la función que desee editar expandiendo la carpeta del panel de políticas y seleccionando la política adecuada.

   La política aparecerá en el panel de detalles y mostrará sus reglas.
3. Haga clic en la regla que desee editar.

   La regla aparecerá, junto con sus acciones, en el panel de detalles.
4. Haga clic en Editar.

   Aparecerá el asistente de edición de reglas.
5. Utilice el asistente de edición de reglas para cambiar la regla de modo que envíe eventos al servidor de CA Enterprise Log Manager (por ejemplo, a otros destinos o a nuevos destinos) y haga clic en Finalizar cuando termine.
6. Marque y confirme la política como usuario creador para que pueda ser aprobada por un usuario con la función de comprobador.
7. Cierre sesión y, a continuación, vuelva a iniciar sesión en el servidor de Policy Manager como usuario con la función de comprobador si su empresa utiliza la función de segregación de obligaciones.
8. Revise y apruebe la carpeta de políticas que contenga la regla y la política cambiadas.

   Una vez aprobada la política, la configuración del servidor de distribución de Policy Manager determina en qué momento se distribuirá la nueva política a los nodos de auditoría. Puede revisar el registro de activación para comprobar el estado de activación de una política.
9. Repita este procedimiento en cada regla y política con los eventos recopilados que desee enviar a CA Enterprise Log Manager.

Cuándo importar eventos

Si cuenta con un servidor de herramientas de datos de CA Audit existente con una base de datos de recopilación, dispondrá de una tabla SEOSDATA que contiene datos de eventos. Para ejecutar los sistemas de CA Audit y de CA Enterprise Log Manager conjuntamente y ver informes sobre los datos recopilados, es posible que desee importar datos de la tabla SEOSDATA.

Puede ejecutar la utilidad de importación SEOSDATA para realizar una importación de los datos de eventos desde la base de datos de recopilación al almacenamiento del registro de eventos de CA Enterprise Log Manager. Normalmente, importa datos de eventos inmediatamente después de implementar un servidor de CA Enterprise Log Manager. Si está integrando los dos sistemas, puede realizar la importación de datos más de una vez en función de la configuración de uso y de red.

Nota: La importación de datos de la tabla SEOSDATA *no* elimina ni modifica ningún dato almacenado aquí. El procedimiento de importación copia los datos, los analiza y los asigna al almacenamiento del registro de eventos de CA Enterprise Log Manager.

Acerca de la utilidad de importación SEOSDATA

La utilidad de importación, LMSeosImport, utiliza una interfaz de línea de comandos y admite los sistemas operativos Windows y Solaris. La utilidad realiza las siguientes acciones:

- Se conecta a la tabla SEOSDATA para extraer eventos de la forma especificada
- Analiza los eventos SEOSDATA seleccionados en pares de nombre y valor
- Envía los eventos al servidor CA Enterprise Log Manager a través del patrocinador de eventos de SAPI o de iTech para insertarlos en el almacenamiento del registro de eventos

Los eventos se asignan a la gramática de eventos comunes (CEG) que forma la base de las tablas de bases de datos del almacenamiento del registro de eventos. A continuación, puede utilizar las consultas e informes predefinidos para recopilar la información de los eventos almacenados.

Importación desde una tabla Live SEOSDATA

No se recomienda ejecutar la utilidad LMSeosImport con una tabla Live SEOSDATA, aunque a veces puede resultar inevitable. Si debe ejecutar la utilidad con una base de datos activa, la utilidad sólo importará una determinada sección de datos. Esto se debe a que los eventos agregados a la base de datos *después de* iniciarse la utilidad LMSeosImport no se importan durante la sesión de importación.

Por ejemplo, si no especifica los parámetros -minid y -maxid en la línea de comandos, cuando se inicie la utilidad, se realizará la consulta de los ID de entrada mínimos y máximos existentes en la base de datos. La utilidad basa las consultas y las actividades de importación en estos valores. Los eventos introducidos en la base de datos después de iniciarse la utilidad cuentan con ID de entrada que están fuera del intervalo, por lo que no se importan.

Cuando finaliza una sesión de importación, la utilidad muestra los últimos ID de entrada procesados. Es posible que sea necesario ejecutar más de una sesión de importación para obtener todos los eventos; también puede ejecutar la utilidad de importación en un momento con una menor actividad de eventos y redes. Puede ejecutar más sesiones de importación, si es necesario, utilizando el ID de entrada de finalización de la última sesión como el valor -minid de la nueva sesión.

Importación de datos desde una tabla SEOSDATA

Siga este proceso para importar datos desde una base de datos de recopilación (tabla SEOSDATA) para obtener resultados óptimos:

1. Copie la utilidad LMSeosImport en la carpeta iTechnology en un servidor de herramientas de datos de CA Audit.

   Nota: La utilidad LMSeosImport requiere las bibliotecas compatibles *etsapi* y *etbase* que se suministran con el cliente de CA Audit.

2. Estudie el funcionamiento de las opciones y de la línea de comandos de LMSeosImport.
3. Cree un informe de eventos para detectar tipos de eventos, recuentos e intervalos de ID de entrada.
4. Previsualice los resultados de la importación con los parámetros que piensa utilizar.

   Si es necesario, puede previsualizar de nuevo la importación para refinar las opciones de la línea de comandos.

5. Importe eventos desde una base de datos de recopilación utilizando las opciones refinadas de la línea de comandos.

Copia de la utilidad de importación a un servidor de herramientas de datos de Windows

Para poder importar datos desde la tabla SEOSDATA, debe copiar la utilidad LMSeosImport del DVD-ROM de instalación de la aplicación de CA Enterprise Log Manager en el servidor de herramientas de datos de Solaris.

Nota: La utilidad LMSeosImport requiere la presencia de bibliotecas *etsapi* y *etbase*. Estos archivos forman parte de la instalación básica del servidor de herramientas de datos. Para utilizar la utilidad LMSeosImport, compruebe que el directorio de instalación de CA Audit esté incluido en la instrucción PATH del sistema. El directorio predeterminado es opt/CA/eTrustAudit/bin.

Para ejecutar la utilidad, establezca las siguientes variables del entorno con el comando *env*:

- ODBC_HOME=<*directorio de instalación de herramientas de datos de CA Audit*>/odbc
- ODBCINI=<*directorio de instalación de herramientas de datos de CA Audit*>/odbc/odbc.ini

Para copiar la utilidad

1. Acceda a un símbolo del sistema en el servidor de herramientas de datos de Solaris.
2. Inserte el DVD-ROM de instalación de la aplicación de CA Enterprise Log Manager.
3. Desplácese al directorio /CA/ELM/Solaris_sparc.
4. Copie la utilidad LMSeosImport en el directorio iTechnology del servidor de herramientas de datos de CA Audit, /opt/CA/SharedComponents/iTechnology.

   La utilidad estará lista para utilizar después de que la copie en el directorio designado y establezca las variables del entorno requeridas. No es necesario ejecutar ninguna otra instalación.

Copia de la utilidad de importación en un servidor de herramientas de datos de Windows

Para poder importar datos desde la tabla SEOSDATA, debe copiar la utilidad LMSeosImport del DVD-ROM de instalación de la aplicación de CA Enterprise Log Manager en el servidor de herramientas de datos de Windows.

Nota: La utilidad LMSeosImport requiere la presencia de las bibliotecas de vínculos dinámicos *etsapi* y *etbase*. Estos archivos forman parte de la instalación básica del servidor de herramientas de datos. Antes de utilizar la utilidad LMSeosImport, compruebe que el directorio Archivos de programa\CA\eTrust Audit\bin esté incluido en la instrucción PATH del sistema.

Para copiar la utilidad

1. Acceda a un símbolo del sistema en el servidor de herramientas de datos de Windows.
2. Inserte el DVD-ROM de instalación de la aplicación de CA Enterprise Log Manager.
3. Desplácese al directorio \CA\ELM\Windows.

4. Copie la utilidad LMSeosImport.exe en el directorio de iTechnology del servidor de herramientas de datos de CA Audit, <unidad>:\Archivos de programa\CA\SharedComponents\iTechnology.

   La utilidad estará lista para utilizar cuando la copie en el directorio designado. No es necesario ejecutar ninguna otra instalación.

Descripción de la línea de comandos LMSeosImport

La utilidad LMSeosImport proporciona varios argumentos de la línea de comandos que le permiten controlar los eventos que migran. Cada evento de la tabla SEOSDATA es una fila y cuenta con un *ID de entrada* único para identificarlo. Puede utilizar la utilidad de importación para recuperar un informe que enumera distintos tipos de datos útiles. El informe enumera los eventos en la tabla SEOSDATA (como varios ID de entrada), los recuentos de eventos por tipo de registro y los intervalos de fecha de los eventos. La utilidad proporciona una opción de recuperación en caso de que se produzca un error durante la importación de un evento.

También puede ejecutar una tarea de vista previa para ver cuáles serían los resultados de la importación con una determinada estructura de comandos. Las tareas de vista previa no importan datos realmente. De esta forma, puede refinar las opciones de la línea de comandos antes de realizar la migración real.

Puede ejecutar la utilidad de migración más de una vez utilizando distintos parámetros para importar varios tipos de datos. Por ejemplo, puede migrar los datos en varias sesiones personalizadas en función de un determinado intervalo de ID de entrada, del tipo de registro o de distintos intervalos de fecha.

Nota: La utilidad *no* proporciona ningún seguimiento de la importación de sesiones anteriores. Es posible duplicar los datos de la base de datos de CA Enterprise Log Manager si ejecuta el comando con los mismos parámetros más de una vez.

Para obtener resultados óptimos, divida la importación por tipo de registro (utilizando la opción -log) o por ID de entrada (utilizando las opciones -minid y -maxid) para mejorar el rendimiento de la importación. Utilice la opción -retry para realizar la recuperación de los errores producidos durante la importación de eventos. La utilidad emplea un valor predeterminado -retry de 300 segundos para maximizar el éxito de la importación.

Opciones y comando de la utilidad de importación

La utilidad LMSeosImport admite la siguiente línea de comandos y las siguientes opciones:

```
LMSeosImport -dsn dsn_name -user user_name -password password -target target_name
{-sid nnn -eid nnnn -stm yyyy-mm-dd -etm yyyy-mm-dd -log logname -transport
(sapi|itech) -chunk nnnn -pretend -verbose -delay -report -retry}
```

-dsn

Especifica el nombre del servidor host donde se encuentra la tabla SEOSDATA. Este parámetro es obligatorio.

-user

Especifica un ID de usuario válido que cuenta al menos con acceso de lectura a la tabla SEOSDATA. Este parámetro es obligatorio.

-password

Especifica la contraseña de la cuenta de usuario especificada con el parámetro -usuario Este parámetro es obligatorio.

-target

Especifica el nombre de host o la dirección IP del servidor de CA Enterprise Log Manager para recibir los eventos migrados de la tabla SEOSDATA. Este parámetro es obligatorio.

-minid nnnn

Indica el ENTRYID de inicio utilizado al seleccionar eventos de la tabla SEOSDATA. Este parámetro es opcional.

-maxid nnnn

Indica el ENTRYID final utilizado al seleccionar eventos de la tabla SEOSDATA. Este parámetro es opcional.

-mintm YYYY-MM-DD

Indica el período de inicio (con formato AAAA-MM-DD) en el que se realiza la selección de eventos de la tabla SEOSDATA. Este parámetro es opcional.

-maxtm YYYY-MM-DD

Indica el período de finalización (con formato AAAA-MM-DD) en el que se realiza la selección de eventos de la tabla SEOSDATA. Este parámetro es opcional.

-log logname

Especifica que la utilidad sólo debe seleccionar los registros de eventos con este nombre de registro especificado. Este parámetro es opcional. Si el nombre de registro contiene espacios, deben utilizarse comillas dobles.

-transport <sapi | itech >

Especifica el método de transporte que se debe utilizar entre la utilidad de importación y CA Enterprise Log Manager. El método de transporte predeterminado es SAPI.

-chunk nnnn

Especifica el número de registros de eventos que se deben seleccionar de la tabla SEOSDATA en cada transferencia. El valor predeterminado es de 5000 eventos (filas). Este parámetro es opcional.

-preview

Genera los resultados de las selecciones de registros de eventos en STDOUT, pero no importa los datos. Este parámetro es opcional.

-port

Especifica el número de puerto que se debe utilizar si establece la opción de transporte como SAPI y si ha configurado el enrutador de SAPI de CA Enterprise Log Manager para que utilice un valor de puerto fijo (sin utilizar el asignador de puertos).

-verbose

Especifica que la utilidad envíe mensajes de procesamiento detallados a STDOUT. Este parámetro es opcional.

-delay

Especifica los segundos que se debe esperar entre el procesamiento de cada evento. Este parámetro es opcional.

-report

Muestra un informe del intervalo de tiempo, intervalo de ENTRYID y recuentos de registros en la tabla SEOSDATA. Este parámetro es opcional.

-retry

Especifica los segundos totales en los que se realizan reintentos de conexión cada vez que se produce un error durante la importación de un evento. El procesamiento continúa cuando el envío del evento vuelve a ser correcto. La utilidad utiliza automáticamente un valor predeterminado de 300 segundos. No es necesario introducir el parámetro a no ser que desee especificar un valor diferente. Los mensajes relacionados con el estado de reintento se envían a STDOUT.

Ejemplos de líneas de comandos de LMSeosImport

Puede utilizar los siguientes ejemplos de líneas de comandos para crear un comando personalizado al utilizar la utilidad de importación SEOSDATA.

Para ejecutar una importación de registros entre ENTRYIDs 1000 y 4000

Introduzca esta línea de comandos:

```
LMSeosImport –dsn eAudit_DSN –user sa –password sa –target 130.200.137.192 –minid 1000 –maxid 4000
```

Para ejecutar una importación de registros sólo para eventos de NT-Application

Introduzca esta línea de comandos:

```
LMSeosImport –dsn eAudit_DSN –user sa –password sa –target 130.200.137.192 –log NT-Application
```

Creación de informes de eventos

La ejecución de un informe de eventos de SEOSDATA antes de realizar la importación real de datos le proporciona la información necesaria acerca de los eventos de la tabla. El informe muestra el intervalo de tiempo de eventos, el recuento de eventos por tipo de registro y el intervalo de ID de entrada. Puede utilizar los valores que se muestran en el informe para refinar las opciones de línea de comandos de un comando de vista preliminar o de un comando de importación real.

Para mostrar la información de eventos de SEOSDATA actual en Windows

1. Acceda a un símbolo del sistema en el servidor de herramientas de datos de CA Audit.
2. Desplácese al directorio \Archivos de programa\CA\SharedComponents\iTechnology.
3. Introduzca esta línea de comandos:

   ```
   LMSeosImport –dsn eAudit_DSN –user sa –password sa -target <Log_Manager_host_name> –report
   ```

El informe generado es similar al siguiente ejemplo:

```
SEOSProcessor::InitOdbc: conectado correctamente a origen [eAudit_DSN]

---------- Intervalo de tiempo de eventos de SEOSDATA ----------

TIEMPO mínimo .= 2007-08-27
TIEMPO máximo .= 2007-10-06

---------- Recuento de eventos por registro ----------

com.ca.iTechnology.iSponsor : 3052
EiamSdk : 1013
NT-Application : 776
NT-System : 900

---------- Intervalo de ENTRYID de SEOSDATA ----------

ENTRYID mínimo: 1
ENTRYID máximo: 5741

Informe finalizado.
```

Vista previa de resultados de importación

Puede ejecutar una importación de prueba con resultado en STDOUT para obtener una vista previa de los resultados de importación sin importar ni migrar datos. Es una buena forma de probar los parámetros de la línea de comandos introducidos para realizar una migración de una sola vez o para realizar una tarea programada de lotes de importación.

Para ejecutar una información de prueba y obtener una vista previa de los resultados de importación

1. Acceda a un símbolo del sistema en el servidor de herramientas de datos de CA Audit.
2. Desplácese al siguiente directorio:

   Solaris: /opt/CA/SharedComponents/iTechnology

   Windows: \Archivos de programa\CA\SharedComponents\iTechnology

3. Introduzca esta línea de comandos:

   En Solaris:

   ```
   ./LMSeosImport.sh –dsn eAudit_DSN –user sa –password sa –target
   <Log_Manager_host_name_or_IP> –minid 1000 –maxid 4000 -preview
   ```

   En Windows:

   ```
   LMSeosImport.exe –dsn eAudit_DSN –user sa –password sa –target
   <Log_Manager_host_name_or_IP> –minid 1000 –maxid 4000 -preview
   ```

Importación de eventos desde una base de datos del recopilador de Windows

Puede seguir este procedimiento para importar datos de eventos desde una base de datos del recopilador que se encuentra en un servidor de herramientas de datos de Windows.

Para importar eventos desde una tabla SEOSDATA en un servidor de Windows

1. Localice el nombre del servidor en el que se encuentra la tabla SEOSDATA.
2. Compruebe que dispone de las credenciales de acceso de usuario del servidor con, al menos, acceso de lectura a la tabla SEOSDATA.
3. Acceda a un símbolo del sistema en el servidor de herramientas de datos de CA Audit.
4. Desplácese al directorio \Archivos de programa\CA\Shared Components\iTechnology.
5. Inicie la utilidad de importación utilizando la siguiente sintaxis de comandos:

   ```
   LMSeosImport.exe -dsn <dsnname> -user <UID> -password <password> -target
   <targethostname> <optional flags>
   ```

Importación de eventos desde una base de datos del recopilador de Solaris

Puede seguir este procedimiento para importar datos de eventos desde una base de datos del recopilador que se encuentra en un servidor de herramientas de datos de Solaris.

Para importar eventos desde una tabla SEOSDATA en un servidor Solaris

1. Localice el nombre del servidor en el que se encuentra la tabla SEOSDATA.
2. Compruebe que dispone de las credenciales de acceso de usuario del servidor con, al menos, acceso de lectura a la tabla SEOSDATA.
3. Acceda a un símbolo del sistema en el servidor de herramientas de datos de CA Audit.
4. Desplácese al directorio /opt/CA/SharedComponents/iTechnology.
5. Inicie la utilidad de importación utilizando la siguiente sintaxis de comandos:

   ```
   ./LMSeosImport -dsn <dsnname> -user <UID> -password <password> -target
   <targethostname> <optional flags>
   ```

Apéndice B: Consideraciones para los usuarios de CA Access Control

Esta sección contiene los siguientes temas:

Integración con CA Access Control

Puede integrar CA Enterprise Log Manager con CA Access Control utilizando uno de diversos niveles de versión. El proceso general es el siguiente:

En el caso de versiones de CA Access Control que empleen un servidor de mensajes TIBCO para el enrutamiento de eventos, lleve a cabo lo siguiente:

- Instale un agente de CA Enterprise Log Manager.
- Configure un conector que utilice el conector AccessControl_R12SP1_TIBCO_Connector.

En el caso de CA Access Control r12.5, consulte la *Guía de implementación de CA Access Control r12.5* y la *Guía de conectores de CA Enterprise Log Manager CA Access Control*.

En el caso de CA Access Control r12. SP1, consulte la *Guía de implementación de CA Access Control r12 SP1, 3.ª edición*, así como la <*Guía de conectores de CA Enterprise Log Manager para CA Access Control*.

Nota: Estas implementaciones emplean componentes que forman parte de las ediciones Premium de CA Access Control.

En el caso de versiones de CA Access Control que empleen selogrd para el enrutamiento de eventos, lleve a cabo lo siguiente:

- Instale un agente de CA Enterprise Log Manager.
- Configure un conector que utilice la integración ACSelogrd.

Si desea obtener más información acerca de la configuración de un conector para recopilar eventos de CA Access Control, consulte la *Guía de conectores de CA Access Control r8 SP1*.

Si envía eventos de CA Access Control a CA Audit, siga uno de estos métodos para hacer llegar los eventos a CA Enterprise Log Manager:

- Modifique una política de CA Audit existente para enviar eventos a CA Audit y a CA Enterprise Log Manager si utiliza un iRecorder de CA Audit para recopilar eventos. También puede modificar la política para enviar eventos sólo al servidor de CA Enterprise Log Manager si lo desea.
- Configure el archivo control.conf de un iRecorder para enviar eventos directamente a CA Enterprise Log Manager.

Nota: Si dispone de una versión de eTrust Access Control que no admite iRecorders, puede enviar eventos directamente al enrutador de CA Audit. Si desea obtener más información, consulte la información de integración de CA Audit en la *Guía del administrador de eTrust Access Control r5.3*.

Las directrices siguientes emplean r8 SP2-series para la interfaz de usuario de Policy Manager. Los procedimientos generales son los mismos que al emplear versiones anteriores de CA Audit, aunque la interfaz de usuario es distinta.

Modificación de las políticas de CA Audit para enviar eventos a CA Enterprise Log Manager

El proceso de modificar una política de CA Audit existente para enviar eventos a CA Enterprise Log Manager implica los siguientes pasos:

- Recopile la siguiente información:
  - Compruebe que cuenta con credenciales de usuario de CA Audit Policy Manager para crear, comprobar y activar políticas.
  - Obtenga la dirección IP o el nombre de host requeridos para acceder a la interfaz de usuario del administrador de Audit. La URL para acceder a la aplicación Web del servidor de Policy Manager r8 SP2-series tiene la estructura siguiente:

    `https://<IP_address_of_CA Audit_PM>:5250/spin/auditadmin`

- Configure el recopilador de SAPI o el servicio de enrutador de SAPI de CA Enterprise Log Manager en función de cómo desee crear la acción de regla.

  Si va a crear una acción del recopilador, configure el recopilador de SAPI. Si va a configurar una acción de ruta, configure el enrutador de SAPI.

  Nota: El ejemplo de esta sección utiliza la acción del recopilador.
- Localice y modifique una política de CA Access Control existente para enviar eventos a CA Enterprise Log Manager.
- Compruebe y active la política modificada para distribuirla a los nodos de auditoría.

Repita este proceso para agregar nuevas acciones de regla a otras reglas de políticas, según sea necesario.

Más información:

Acerca del recopilador y del enrutador de SAPI (en la página 231)

Configuración del adaptador del recopilador de SAPI para recibir eventos de CA Access Control

Siga este procedimiento para configurar el adaptador del recopilador de SAPI para recibir eventos de CA Access Control de una implementación de CA Audit.

Puede modificar las políticas de CA Audit que utiliza acciones del recopilador para enviar eventos a un servidor de CA Enterprise Log Manager además de, o en lugar de, enviar eventos a la base de datos del recopilador de CA Audit. Configure este servicio *antes de* modificar las políticas de CA Audit para asegurarse de que no se pierda ningún evento.

(Puede configurar un servicio de enrutador de SAPI de forma muy similar. Si utiliza los servicios de enrutador y recopilador, asegúrese de que los puertos enumerados son distintos o de que están controlados por el servicio del asignador de puertos.)

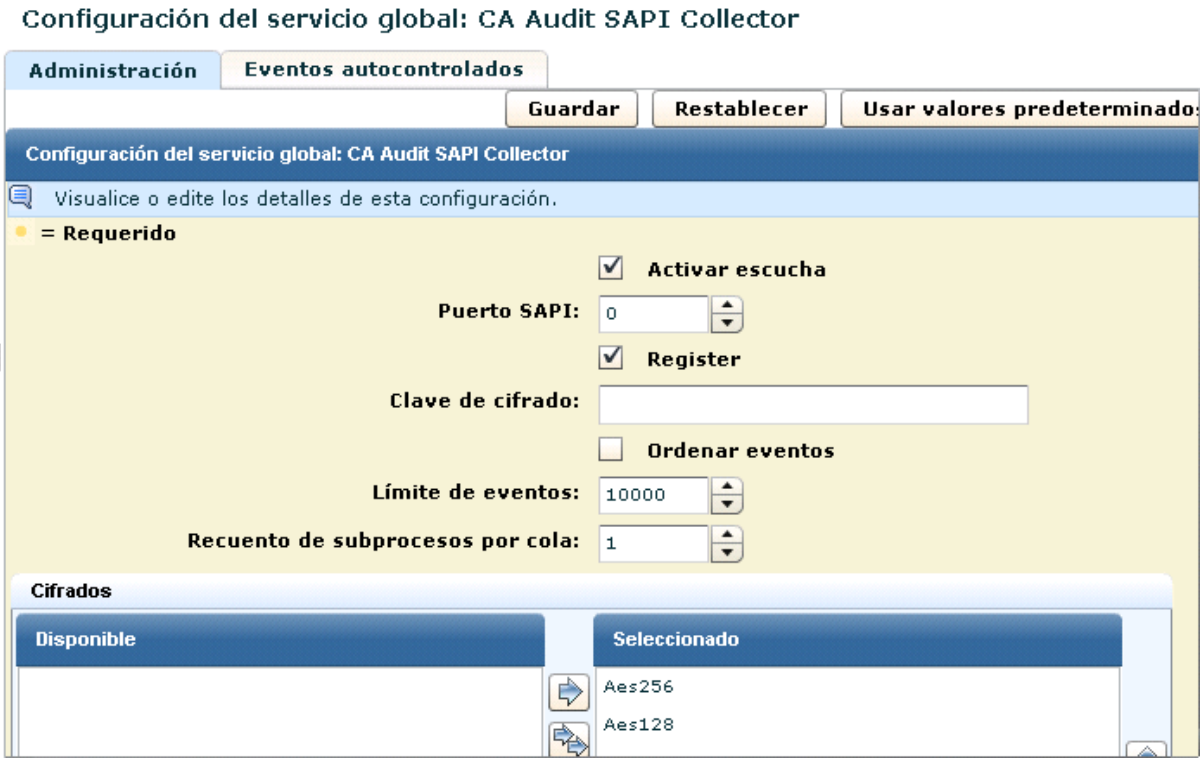
Para configurar el servicio de recopilador de SAPI

1. Inicie sesión en el servidor de CA Enterprise Log Manager como usuario Administrator y seleccione la ficha Administración.

   La subficha Recopilación de registros se mostrará de forma predeterminada.

2. Expanda la entrada Adaptadores de CA.

3. Seleccione el servicio de recopilador de SAPI



4. Seleccione la casilla de verificación Activar escucha y defina el valor de puerto SAPI con un valor que coincida con el que utiliza CA Audit.

   El valor predeterminado de CA Enterprise Log Manager, 0, emplea el servicio del asignador de puertos para asignar los puertos. Si ha definido un puerto en CA Audit, utilice esa configuración aquí.

5. Acepte el resto de los valores predeterminados del campo y desplácese por la lista de archivos de asignación.

   Si selecciona la casilla de verificación Registrar, especifique un valor de puerto SAPI.

6. Agregue la entrada del archivo de asignación de control de acceso si no está presente y elimine el resto de selecciones de la lista de archivos de asignación seleccionados.

7. Haga clic en Guardar.

Modificación de una política de CA Audit existente para enviar eventos a CA Enterprise Log Manager

Siga este procedimiento para que un cliente de CA Audit pueda enviar eventos *tanto a* CA Enterprise Log Manager como a la base de datos del recopilador de CA Audit. Al agregar un nuevo destino a las acciones de ruta o del recopilador en una regla existente, podrá enviar eventos recopilados a ambos sistemas. Como alternativa, también puede modificar las reglas o políticas específicas para *sólo* enviar eventos al servidor de CA Enterprise Log Manager.

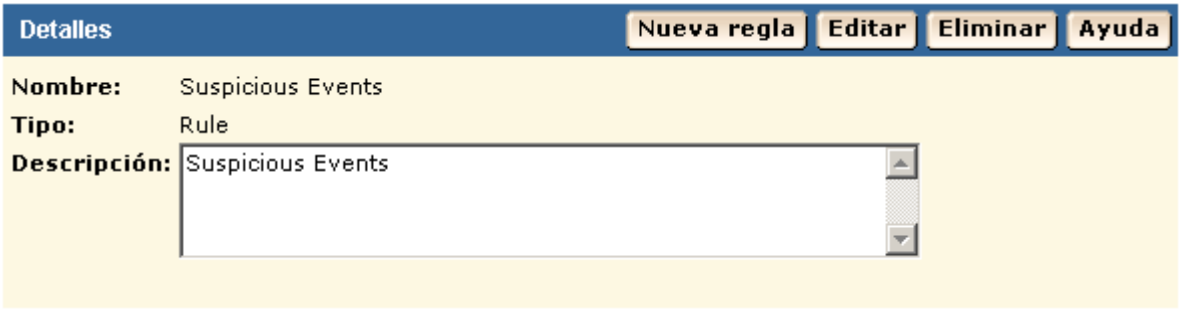
CA Enterprise Log Manager recopila eventos de clientes de CA Audit que utilizan el enrutador de SAPI de CA Audit y las escuchas del recopilador de SAPI de CA Audit. (CA Enterprise Log Manager también puede recopilar eventos directamente mediante el complemento iTech, siempre que haya configurado algún iRecorder para enviarlo directamente al servidor de CA Enterprise Log Manager.) Los eventos recopilados sólo se guardan en el almacén de registro de eventos de CA Enterprise Log Manager *después* de enviar la política a los clientes y tras activarla.

Importante: Configure las escuchas de CA Enterprise Log Manager para recibir eventos antes de modificar y activar la política. Si no realiza primero esta configuración, es posible que los eventos no se asignen correctamente si éstos llegan después de que la política esté activa y antes de que las escuchas puedan asignar los eventos correctamente.

Para modificar una acción de regla de una política existente y enviar eventos a CA Enterprise Log Manager

1. Inicie sesión en el servidor de Policy Manager y acceda a la ficha Mis políticas en el panel izquierdo.
2. Expanda la carpeta de políticas hasta ver la política deseada.

3. Haga clic en la política para mostrar la información básica en el panel de detalles de la derecha.



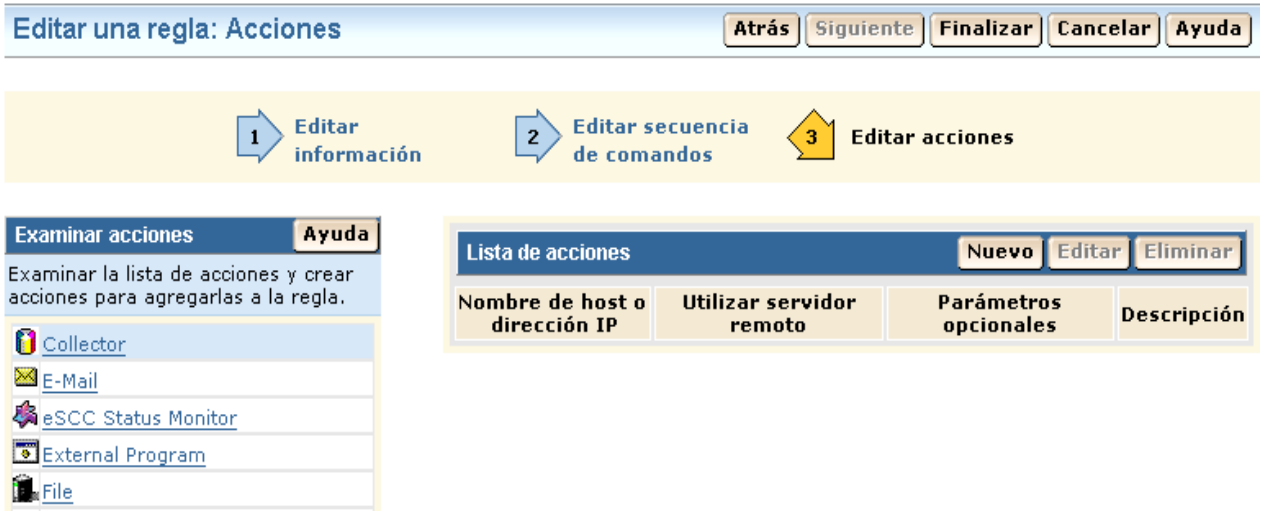
4. Haga clic en Editar en el panel de detalles para agregar reglas a la política.

   Se iniciará el asistente para reglas.

5. Haga clic en Editar acciones al lado de la flecha del paso 3.

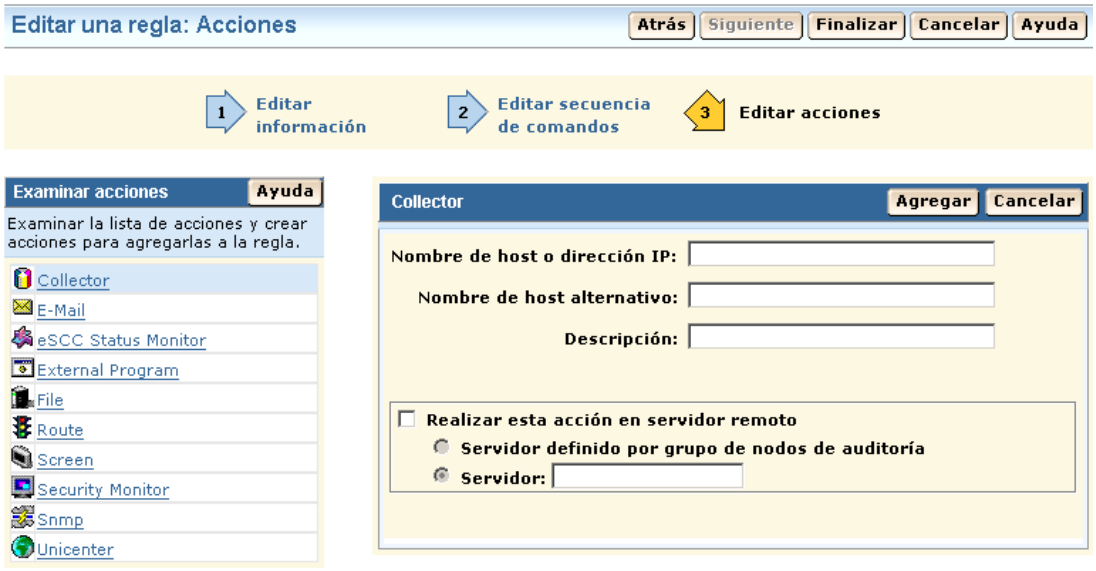
   Aparece la página de las acciones de regla.

6. Haga clic en la acción de recopilador en el panel Examinar acciones para visualizar la lista de acciones a la derecha.



También puede utilizar la acción de ruta, pero la acción del recopilador ofrece la ventaja de un nombre de host alternativo para el procesamiento de conmutación por error básico.

7. Haga clic en Nuevo para crear una nueva regla.
8. Introduzca la dirección IP o el nombre de host del servidor de recopilación de CA Enterprise Log Manager.



Para una implementación de CA Enterprise Log Manager con dos o más servidores, puede introducir un nombre de host de CA Enterprise Log Manager diferente o una dirección IP distinta en el campo Nombre de host alternativo. De este modo, se aprovecha la funcionalidad de conmutación por error automática de CA Audit. Si el primer servidor de CA Enterprise Log Manager no está disponible, CA Audit enviará eventos automáticamente al servidor nombrado en el campo Nombre de host alternativo.

9. Introduzca el nombre del servidor de gestión de CA Enterprise Log Manager en el campo Nombre de host alternativo y, a continuación, cree una descripción para esta nueva regla de acción.
10. Desactive la casilla de verificación Realizar esta acción en el servidor remoto, si está activada.
11. Haga clic en Agregar para guardar la nueva acción de regla y, a continuación, haga clic en Finalizar en la ventana del asistente.

    Nota: Posteriormente, comprobará y activará la política, así que *no* cierre la sesión en CA Audit Policy Manager.

Más información:

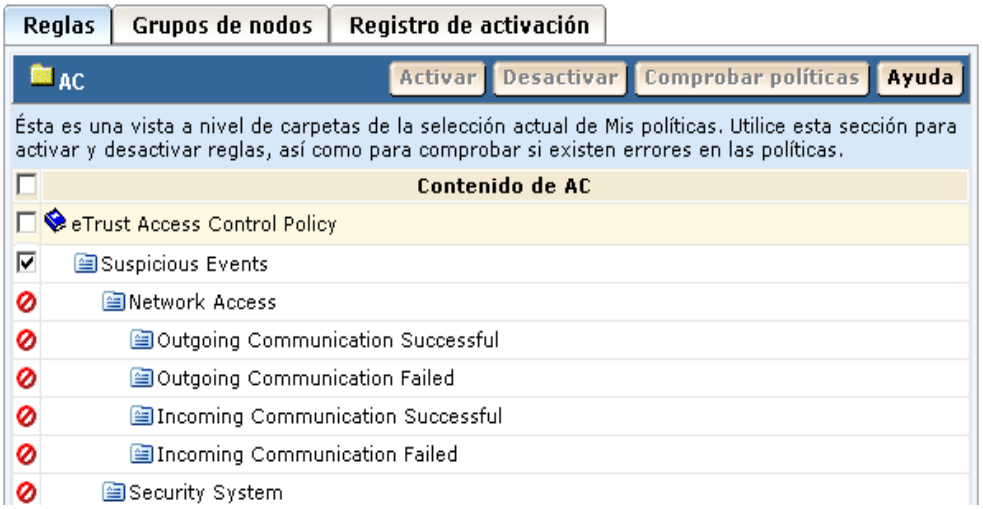
Modificación de una política de r8SP2 existente para enviar eventos a CA Enterprise Log Manager (en la página 238)

Marcado y activación de la política cambiada

Después de cambiar una política existente para agregar una acción de regla, márquela (compílela) y, a continuación, actívela.

Para marcar y activar una política de CA Access Control

1. Seleccione la ficha Reglas en el panel inferior derecho y, a continuación, seleccione una de las reglas que desee marcar.



2. Haga clic en Comprobar políticas para comprobar la regla cambiada con las nuevas acciones y para garantizar que se compile correctamente.

   Realice las modificaciones necesarias en la regla y compruebe que se ha compilado correctamente antes de activarla.

3. Haga clic en Activar para distribuir la política marcada que contiene las nuevas acciones de regla agregadas.

4. Repita este procedimiento en cada regla y política con los eventos recopilados que desee enviar a CA Enterprise Log Manager.

Configuración de un iRecorder de CA Access Control para enviar eventos a CA Enterprise Log Manager

Puede configurar un iRecorder de CA Access Control independiente para enviar los eventos que recopila directamente al servidor de CA Enterprise Log Manager para el almacenamiento y la generación de informes. El proceso incluye los siguientes pasos:

1. Configure la escucha del complemento de eventos iTech para recibir información desde un iRecorder de CA Access Control.
2. Descargue e instale un iRecorder de CA Access Control.
3. Configure iRecorder para que envíe los eventos recopilados directamente a CA Enterprise Log Manager.
4. Compruebe que CA Enterprise Log Manager reciba los eventos.

Nota: Un iRecorder sólo puede enviar sus eventos a un destino. Cuando realiza la configuración utilizando este procedimiento, el único destino será el servidor de CA Enterprise Log Manager indicado.

Configuración del complemento de eventos de iTech para los eventos de CA Access Control

Antes de volver a configurar un iRecorder para que envíe eventos directamente a CA Enterprise Log Manager, es necesario que configure una escucha para recibir estos eventos.

Para configurar la escucha

1. Inicie sesión en el servidor de CA Enterprise Log Manager como usuario con la función de administrador.
2. Acceda a la ficha Administración y, a continuación, expanda el nodo de adaptadores de CA.

3. Expanda el nodo del complemento de eventos de iTechnology.
4. Seleccione el servidor de CA Enterprise Log Manager actual para mostrar la configuración local.
5. Asegúrese de que el archivo de asignación de AccessControl esté primero en la lista de archivos de asignación seleccionados para que las operaciones sean lo más eficaces posible.
6. Compruebe que el valor Nivel de registro esté establecido como NOTSET para recopilar todos los niveles de eventos.
7. Haga clic en Guardar.

Descarga e instalación de un iRecorder de CA Access Control

Puede recopilar eventos de CA Access Control para enviar a un servidor de CA Enterprise Log Manager aunque no tenga CA Audit instalado. Cuando recopila eventos de esta forma, está utilizando un iRecorder en el modo independiente. En el sitio Web de soporte de CA puede obtener un iRecorder.

Nota: Los iRecorders sólo son compatibles con CA Access Control r8 y versiones posteriores.

Para descargar e instalar un iRecorder

1. Acceda al siguiente sitio Web de CA:

   `https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/154/cacirecr8-certmatrix.html#caacirec`

2. Seleccione el iRecorder correspondiente para su versión de CA Access Control.
3. Vea y siga las instrucciones de instalación disponibles en el vínculo de la guía de integración de la matriz.

Configuración de un iRecorder de CA Access Control independiente

Siga este procedimiento para que iRecorder envíe eventos de CA Access Control a CA Enterprise Log Manager.

Importante: Un iRecorder independiente sólo puede enviar sus eventos a un único destino. Si configura un iRecorder siguiendo el procedimiento que se indica a continuación, todos los iRecorders instalados en este sistema *sólo* enviarán sus eventos al almacenamiento del registro de eventos de CA Enterprise Log Manager.

Los iRecorders instalados en el mismo equipo que un cliente de CA Audit envían eventos al cliente directamente. En estos servidores, debe modificar una política de CA Audit existente para agregar acciones de regla después de configurar el recopilador de SAPI de CA Enterprise Log Manager o los adaptadores del enrutador.

Para configurar iRecorder para que envíe eventos a CA Enterprise Log Manager

1. Inicie sesión en el servidor que aloja el iRecorder como usuario con privilegios de administrador o privilegios raíz.
2. Desplácese al directorio de su sistema operativo:
   - UNIX o Linux: /opt/CA/SharedComponents/iTechnology
   - Windows: \Archivos de programa\CA\SharedComponents\iTechnology

3. Detenga el servicio o el daemon de iGateway con el siguiente comando:
   - UNIX o Linux: ./S99igateway stop
   - Windows: net stop igateway
4. Edite el archivo iControl.conf.

   A continuación, aparece un archivo iControl de muestra con las secciones necesarias para cambiar a negrita:

```
<?xml version='1.0' encoding='UTF-8' standalone='no'?>
<iSponsor>
    <Name>iControl</Name>
    <ImageName>iControl</ImageName>
    <Version>4.5.0.2</Version>
    <DispatchEP>iDispatch</DispatchEP>
    <ISType>DSP</ISType>
    <Gated>false</Gated>
    <PreLoad>true</PreLoad>
    <RouteEvent>false</RouteEvent>
    <RouteEventHost>localhost</RouteEventHost>
    <EventsToCache>100</EventsToCache>
    <EventUseHttps>true</EventUseHttps>
    <EventUsePersistentConnections>true</EventUsePersistentConnections>
    <EventUsePipeline>false</EventUsePipeline>
    <StoreEventHost max="10000">localhost</StoreEventHost>
    <RetrieveEventHost interval="60">localhost</RetrieveEventHost>
    <UID>ef1f44ef-r8sp1cr3596a1052-abcd28-2</UID>
    <PublicKey>Public_Key_Value</PublicKey>
    <PrivateKey>Private_Key_Value</PrivateKey>
    <EventsToQueue>10</EventsToQueue>
</iSponsor>
```

5. Especifique el siguiente valor RouteEvent:

   ```
   <RouteEvent>true</RouteEvent>
   ```

   Esta entrada le comunica al iGateway que envíe sus eventos, incluidos todos los eventos de iRecorder, al host del par de etiquetas de RouteEventHost.

6. Especifique el siguiente valor RouteEventHost:

   ```
   <RouteEventHost>Your_CA_Enterprise_Log_Manager_hostname</RouteEventHost>
   ```

   Esta entrada le comunica al iGateway que envíe sus eventos al servidor de CA Enterprise Log Manager utilizando el nombre DNS.

7. Guarde y cierre el archivo.
8. Reinicie el servicio o daemon de iGateway con el siguiente comando:
   - UNIX o Linux: ./S99igateway start
   - Windows: net start igateway

   Esta acción obliga a iRecorder a que utilice las nuevas configuraciones y a que inicie el flujo de eventos desde el iRecorder al servidor de CA Enterprise Log Manager.

Importación de eventos de CA Access Control desde una base de datos del recopilador de CA Audit

El proceso de importación de eventos de CA Access Control desde una tabla SEOSDATA existente incluye los siguientes pasos:

1. Copie la utilidad LMSeosImport al servidor de herramientas de datos de CA Audit.
2. Cree un informe de eventos para determinar si los eventos de CA Access Control están presentes en la base de datos.
3. Ejecute una vista previa de la importación con los parámetros específicos de CA Access Control.
4. Importe los eventos de CA Access Control.
5. Ejecute las consultas y los informes de CA Enterprise Log Manager en los eventos importados.

Prerrequisitos para la importación de eventos de CA Access Control

Antes de usar la utilidad LMSeosImport, siga estos pasos:

- Obtenga una cuenta de usuario de base de datos con al menos acceso de LECTURA a la tabla SEOSDATA de CA Audit.
- Copie la utilidad LMSeosImport al servidor de herramientas de datos de CA Audit.
- Acceda a un símbolo del sistema en el servidor de herramientas de datos y desplácese al directorio correspondiente:

  Solaris: /opt/CA/SharedComponents/iTechnology

  Windows: \Archivos de programa\CA\SharedComponents\iTechnology

Copia de la utilidad de importación en un servidor de herramientas de datos de Windows

Para poder importar datos desde la tabla SEOSDATA, debe copiar la utilidad LMSeosImport del DVD-ROM de instalación de la aplicación de CA Enterprise Log Manager en el servidor de herramientas de datos de Windows.

Nota: La utilidad LMSeosImport requiere la presencia de las bibliotecas de vínculos dinámicos *etsapi* y *etbase*. Estos archivos forman parte de la instalación básica del servidor de herramientas de datos. Antes de utilizar la utilidad LMSeosImport, compruebe que el directorio Archivos de programa\CA\eTrust Audit\bin esté incluido en la instrucción PATH del sistema.

Para copiar la utilidad

1. Acceda a un símbolo del sistema en el servidor de herramientas de datos de Windows.
2. Inserte el DVD-ROM de instalación de la aplicación de CA Enterprise Log Manager.
3. Desplácese al directorio \CA\ELM\Windows.
4. Copie la utilidad LMSeosImport.exe en el directorio de iTechnology del servidor de herramientas de datos de CA Audit, <unidad>:\Archivos de programa\CA\SharedComponents\iTechnology.

   La utilidad estará lista para utilizar cuando la copie en el directorio designado. No es necesario ejecutar ninguna otra instalación.

Copia de la utilidad de importación a un servidor de herramientas de datos de Windows

Para poder importar datos desde la tabla SEOSDATA, debe copiar la utilidad LMSeosImport del DVD-ROM de instalación de la aplicación de CA Enterprise Log Manager en el servidor de herramientas de datos de Solaris.

Nota: La utilidad LMSeosImport requiere la presencia de bibliotecas *etsapi* y *etbase*. Estos archivos forman parte de la instalación básica del servidor de herramientas de datos. Para utilizar la utilidad LMSeosImport, compruebe que el directorio de instalación de CA Audit esté incluido en la instrucción PATH del sistema. El directorio predeterminado es opt/CA/eTrustAudit/bin.

Para ejecutar la utilidad, establezca las siguientes variables del entorno con el comando *env*:

- ODBC_HOME=<*directorio de instalación de herramientas de datos de CA Audit*>/odbc
- ODBCINI=<*directorio de instalación de herramientas de datos de CA Audit*>/odbc/odbc.ini

Para copiar la utilidad

1. Acceda a un símbolo del sistema en el servidor de herramientas de datos de Solaris.
2. Inserte el DVD-ROM de instalación de la aplicación de CA Enterprise Log Manager.
3. Desplácese al directorio /CA/ELM/Solaris_sparc.
4. Copie la utilidad LMSeosImport en el directorio iTechnology del servidor de herramientas de datos de CA Audit, /opt/CA/SharedComponents/iTechnology.

   La utilidad estará lista para utilizar después de que la copie en el directorio designado y establezca las variables del entorno requeridas. No es necesario ejecutar ninguna otra instalación.

Creación de un informe de eventos de SEOSDATA para los eventos de CA Access Control

Para determinar si una tabla SEOSDATA existente contiene eventos de CA Access Control y para seleccionar un método de importación, debe ejecutar un informe de eventos. El nombre de registro de los eventos de CA Access Control es *eTrust Access Control*. El informe enumera todos los eventos en la base de datos separados por sus nombres de registro. La forma más sencilla de importar eventos de CA Access Control es importarlos en función de su nombre de registro.

Para crear un informe de eventos

1. Cree un informe de eventos para ver los eventos de CA Access Control presentes en la tabla SEOSDATA.

   ```
   LMSeosImport –dsn My_Audit_DSN –user sa –password sa –report
   ```

   Después de realizar el procesamiento, la utilidad mostrará un informe semejante al que se muestra a continuación:

   ```
   Importación iniciada el viernes, 2 de enero de 2009, a las 15:20:30


   Transporte no especificado, restableciendo a SAPI...

   Preparando conexiones de ODBC...

   Conectado correctamente a origen [My_Audit_DSN]

   ---------- Intervalo de tiempo de eventos de SEOSDATA ----------

   TIEMPO mínimo = 2008-05-27
   TIEMPO mínimo = 2009-01-02
   ```

```
---------- Recuento de eventos por registro ----------

Unix: 12804
ACF2: 1483
eTrust AC: 143762
com.ca.iTechnology.iSponsor: 66456
NT-Application: 5270
CISCO PIX Firewall: 5329
MS IIS: 6765
Netscape: 530
RACF: 14
Apache: 401
N/A: 28222
SNMP-recorder: 456
Check Point FW-1: 1057
EiamSdk: 2790
MS ISA: 609
ORACLE: 2742
eTrust PCM: 247
NT-System: 680
eTrust Audit: 513
NT-Security: 14714
Dispositivo CISCO: 41436
SNORT: 1089

---------- Intervalo de ENTRYID de SEOSDATA ----------


ENTRYID mínimo: 1
ENTRYID máximo: 10000010243


Informe finalizado.

Desconectado correctamente de origen [My_Audit_DSN]

Saliendo de importación...
```

2. Revise el informe para comprobar que los eventos de CA Access Control estén presentes.

   La línea en negrita de este extracto de informe muestra que hay eventos de CA Access Control en esta tabla SEOSDATA.

```
---------- Recuento de eventos por registro ----------

Unix: 12804
ACF2: 1483
eTrust AC: 143762
com.ca.iTechnology.iSponsor: 66456
NT-Application: 5270
...
```

Vista previa de una importación de eventos de CA Access Control

Puede utilizar la vista previa de importación para ajustar los parámetros de importación. Este ejemplo muestra dos tipos de vista previa que se basan en la importación de eventos a partir de un período de tiempo específico. El ejemplo da por hecho lo siguiente:

- El servidor de herramientas de datos de CA Audit reside en un equipo Windows.
- El nombre de la base de datos de la tabla SEOSDATA es My_Audit_DSN.
- El nombre de usuario de la base de datos es sa con una contraseña de sa.
- La vista previa de la importación sólo utiliza el nombre de registro como criterio de búsqueda e importación.

El resultado del comando con la opción -preview envía los resultados de importación de la muestra a STDOUT (este ejemplo utiliza el valor *My_CA-ELM_Server* para representar el nombre del servidor de CA Enterprise Log Manager).

Para realizar una vista previa de la importación

1. Realice una vista previa de la importación de eventos de CA Access Control con el siguiente comando:

   ```
   LMSeosImport.exe –dsn My_Audit_DSN –user sa –password sa -target My_CA-ELM_Server –log "eTrust Access Control" -preview
   ```

   El comando -preview mostrará información como la siguiente:

   ```
   Importación iniciada el viernes, 2 de enero de 2009, a las 15:35:37


   Transporte no especificado, restableciendo a SAPI...

   Preparando conexiones de ODBC...

   Conectado correctamente a origen [My_Audit_DSN]

   ENTRYID de inicio no especificado, utilizando ENTRYID mínimo de 1...

   Importación (vista previa) en ejecución, espere...

   .........

   Importación (vista previa) finalizada (143762 registros en 4 minutos y 12 segundos).

   ---------- Eventos importados (vista previa) por registro ----------

   eTrust AC:     143762

   Último EntryId procesado: 101234500
   ```

```
Desconectado correctamente de origen [My_Audit_DSN]

Saliendo de importación...
```

Los resultados de la vista previa muestran que hay un gran número de eventos de CA Access Control que se van a importar. Utilizando este ejemplo, suponga que sólo necesita importar los eventos que se produjeron durante un período de dos meses. Puede personalizar el comando de vista previa para importar un grupo de eventos más pequeño por fecha.

2. Cambie los parámetros de importación para incluir un intervalo de fecha y ejecute de nuevo la vista previa con el siguiente comando:

```
LMSeosImport.exe –dsn My_Audit_DSN –user sa –password sa -target My_CA-
ELM_Server –log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31 -
preview
```

El comando modificado mostrará información como la siguiente:

```
Importación iniciada el viernes, 2 de enero de 2009, a las 15:41:23


Transporte no especificado, restableciendo a SAPI...

Preparando conexiones de ODBC...

Conectado correctamente a origen [My_Audit_DSN]

ENTRYID de inicio no especificado, utilizando ENTRYID mínimo de 1...

Importación (vista previa) en ejecución, espere...

.........

Importación (vista previa) finalizada (143762 registros en 4 minutos y 37
segundos).

---------- Eventos importados (vista previa) por registro ----------

eTrust AC:     2349

Último EntryId procesado: 5167810102

Desconectado correctamente de origen [My_Audit_DSN]

Saliendo de importación...
```

Esta importación muestra los resultados del intervalo de fecha en un subconjunto más pequeño de eventos que se van a importar. Ahora está listo para ejecutar la importación real.

Más información:

Descripción de la línea de comandos LMSeosImport (en la página 243)
Vista previa de resultados de importación (en la página 247)

Importación de eventos de CA Access Control

Después de ejecutar el informe de eventos y una vista previa de importación, estará listo para importar eventos de CA Access Control desde la tabla SEOSDATA.

Para importar eventos de CA Access Control

Utilice el comando de la vista previa sin la opción -preview para recuperar los eventos de CA Access Control del intervalo de fecha especificado:

```
LMSeosImport.exe –dsn [My_Audit_DSN] –user sa –password sa -target [My-CA-ELM-Server] –log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31
```

La utilidad mostrará resultados como los siguientes:

```
Importación iniciada el viernes, 2 de enero de 2009, a las 15:41:23


Transporte no especificado, restableciendo a SAPI...

Preparando conexiones de ODBC...

Conectado correctamente a origen [My_Audit_DSN]

ENTRYID de inicio no especificado, utilizando ENTRYID mínimo de 1...

Importación (vista previa) en ejecución, espere...

.........

Importación (vista previa) finalizada (143762 registros en 5 minutos y 18 segundos).

---------- Eventos importados (vista previa) por registro ----------

eTrust AC:     2241

Último EntryId procesado: 5167810102

Desconectado correctamente de origen [My_Audit_DSN]

Saliendo de importación...
```

Más información:

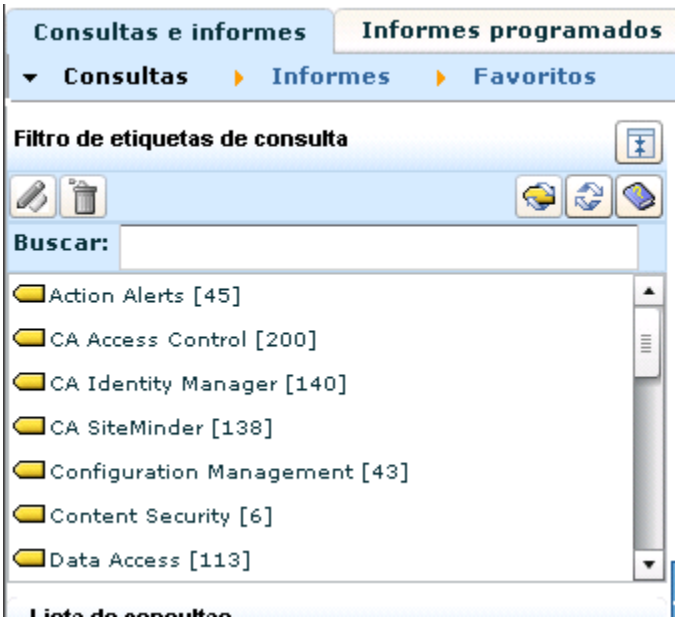
Descripción de la línea de comandos LMSeosImport (en la página 243)
Importación de eventos desde una base de datos del recopilador de Windows (en la página 248)
Importación de eventos desde una base de datos del recopilador de Solaris (en la página 248)

Visualización de consultas e informes para ver eventos de CA Access Control

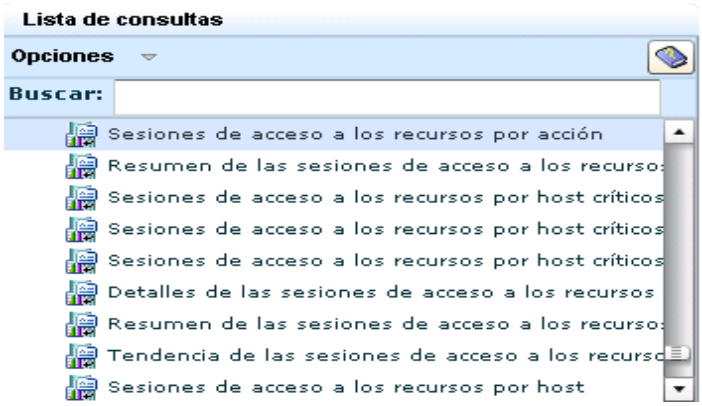
CA Enterprise Log Manager proporciona una serie de consultas e informes para examinar los eventos recopilados de CA Access Control. Siga el procedimiento que se indica a continuación para acceder a las consultas e informes de CA Access Control.

Para acceder a las consultas de CA Access Control

1. Inicie sesión en el servidor de CA Enterprise Log Manager como usuario con derechos para ver las consultas y los informes.
2. Acceda a la subficha Consultas en la ficha Consultas e informes, si todavía no aparece.



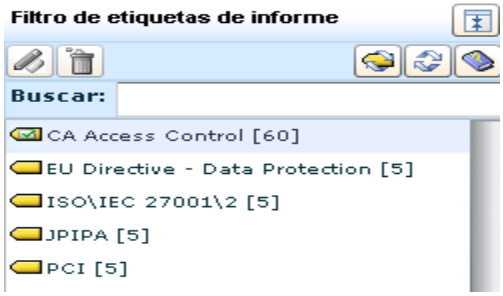
3. Haga clic en la etiqueta de consultas de CA Access Control para mostrar las consultas disponibles en una lista situada a la izquierda.



4. Seleccione una consulta para ver los datos de eventos.

Para acceder a los eventos de CA Access Control

1. Inicie sesión en el servidor de CA Enterprise Log Manager como usuario con derechos para ver las consultas y los informes.
2. Acceda a la subficha Informes en la ficha Consultas e informes, si todavía no aparece.



3. Haga clic en la etiqueta de informes de CA Access Control para mostrar los informes disponibles en una lista situada a la izquierda.

4. Seleccione un informe para ver los datos de eventos.

Apéndice C: Consideraciones de CA IT PAM

Esta sección contiene los siguientes temas:

Escenario: Cómo utilizar CA EEM en CA Enterprise Log Manager para la autenticación de CA IT PAM

Este apéndice describe el escenario en el cual desea instalar CA IT PAM en un servidor de Windows y compartir CA EEM en el servidor de CA Enterprise Log Manager para la autenticación. Estos procedimientos completan aquéllos que se documentan en la *Guía de instalación para la automatización de procesos de CA IT*.

Importante: Compartir un CA EEM *no* se admite en el modo FIPS, de la misma manera que 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.

Nota: Si se desea instalar CA IT PAM en un servidor UNIX, puede bien utilizar LDAP o un CA EEM local para la autenticación. La documentación que encontrará en este apéndice no va dirigida a usted. En estos ejemplos, no se comparte el mismo servidor de CA EEM. CA Enterprise Log Manager r12.1 SP1 se puede ejecutar en el modo FIPS y se puede comunicar con CA IT PAM; sin embargo, estos canales de comunicación no son compatibles con FIPS.

Para cualquier escenario de instalación, descargue la *Guía de instalación* de CA IT Process Automation Manager r2.1 SP03 desde el sitio Soporte en línea de CA. Además, puede descargar Adobe Acrobat Reader para abrir el documento pdf.

El proceso que permite el uso de CA EEM en CA Enterprise Log Manager para la autenticación de CA IT PAM implica dos pasos manuales. Copie un archivo del servidor de Windows al dispositivo y otro archivo desde éste al servidor de Windows. En el apéndice se describen estos pasos. No están explicados en la documentación de CA IT PAM.

Proceso de implementación de la autenticación de CA IT PAM

El proceso de implementación de la autenticación de CA IT PAM mediante CA EEM en el servidor de CA Enterprise Log Manager de gestión es el siguiente:

1. Prepárese para la implementación de la autenticación de CA IT PAM.
    a. Cargue el paquete de instalación de CA IT PAM en el servidor de Windows en el cual desee instalar este programa.
    b. (Opcional) Cambie la contraseña predeterminada para el certificado de itpamcert.p12.
2. Copie el archivo ITPAM_eem.xml del host en el cual desee instalar CA IT PAM en el dispositivo de CA Enterprise Log Manager que contiene CA EEM.

3. Registre ITPAM como instancia de la aplicación sobre el mismo CA EEM que utiliza CA Enterprise Log Manager. Si ejecuta el comando safex, se generará el certificado itpamcert.p12 y la instancia de la aplicación de ITPAM con dos cuentas de usuario, itpamadmin e itpamuser.

   Nota: Para obtener ayuda acerca del comando safex, introduzca ./safex.

4. Copie el archivo itpamcert.p12 del dispositivo de CA Enterprise Log Manager al host de Windows donde desee instalar el dominio de CA IT PAM.
5. Busque la aplicación de ITPAM y restablezca las contraseñas para itpamadmin e itpamuser.
6. Conéctese al servidor de Windows e instale los componentes de terceros a través de los procedimientos que se describen en la *Guía de instalación de CA IT Process Automation Manager*.
7. Instale el dominio de CA IT PAM mediante las directrices presentadas en este apéndice y las instrucciones de instalación de CA IT PAM.
8. Inicie el servicio del servidor de CA ITPAM.
9. Inicie la consola CA IT PAM e inicie sesión.

Prepare la implementación de la autenticación de CA IT PAM en un CA EEM compartido

Después de la carga del paquete de instalación en el servidor de Windows, en el cual desee instalar el dominio de CA IT PAM, se podrá configurar una contraseña para el certificado de itpamcert.cer.

Para preparar la implementación de la autenticación de CA IT PAM en el servidor de gestión de CA Enterprise Log Manager

1. Extraiga la imagen iso de CA IT PAM en el host del servidor de Windows 2003 en el cual desee instalar CA IT PAM.

   Nota: Podrá encontrar la imagen iso de CA IT PAM en el CD 2 del origen de instalación de CA IT PAM.

2. (Opcional) Cambie la contraseña predeterminada para el certificado de IT PAM.
   a. Vaya a la carpeta <install path>\eem.
   b. Abra el archivo ITPAM_eem.xml.
   c. Reemplace "itpamcertpass" en la línea siguiente:

      ```
      <Register certfile="itpamcert.p12" password="itpamcertpass"/>
      ```

   d. Guarde el archivo.

Copie un archivo XML en la gestión de CA Enterprise Log Manager

El comando safex genera objetos de seguridad de CA IT PAM a partir del archivo ITPAM_eem.xml. Se debe copiar este archivo en el dispositivo de CA Enterprise Log Manager, al cual será posible acceder durante el procesamiento de safex.

Para copiar el archivo ITPAM_eem.xml en el dispositivo de CA Enterprise Log Manager

Copie el archivo ITPAM_eem.xml, ubicado en el disco de instalación de CA IT PAM, en el dispositivo de CA Enterprise Log Manager que contiene CA EEM. Si se ha extraído el archivo iso en el servidor de Windows, utilice Winscp para copiar ITPAM_eem.xml en el directorio /tmp del dispositivo.

- Archivo de origen en el disco de instalación de CA IT PAM:

  `ITPAM_eem.xml`

- Ruta de destino en la gestión de CA Enterprise Log Manager:

  `/opt/CA/SharedComponents/iTechnology`

Regístrese en CA IT PAM con un CA EEM compartido

Puede registrarse en CA IT PAM con CA EEM incrustado en el servidor de gestión de CA Enterprise Log Manager. El registro con CA EEM agrega objetos de seguridad de CA IT PAM.

Los objetos de seguridad de CA IT PAM que se agregan a CA EEM durante el registro incluyen los siguientes:

- La instancia de la aplicación, ITPAM
- Las políticas relacionadas al acceso de CA IT PAM
- Grupos y Usuarios, incluyendo ITPAMAdmins predeterminado, ITPAMUsers, itpamadmin, e itpamuser
- El certificado, itpamcert.p12

Se pueden crear objetos de seguridad de CA IT PAM en el servidor de gestión de CA Enterprise Log Manager. Antes de empezar, deberá obtener la contraseña caelmadmin, en caso de que la desconozca.

Para registrarse en CA IT PAM con CA EEM en el servidor de gestión de CA Enterprise Log Manager

1. Inicie sesión en el dispositivo de CA Enterprise Log Manager mediante ssh, que no responde como el usuario caelmadmin.
2. Cambie los usuarios a la cuenta raíz.

   ```
   su -
   ```

3. Cambie los directorios a la ruta de destino y enumere los contenidos.

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

4. Verifique que los archivos siguientes se enumeran:
   - ITPAM_eem.xml
   - safex
5. Ejecute el comando siguiente:

   ```
   ./safex -h <ELM_hostname> -u EiamAdmin -p <password> -f ITPAM_eem.xml
   ```

   Este proceso crea la aplicación de CA IT PAM en el servidor de gestión de CA Enterprise Log Manager, agrega los usuarios predeterminados y genera el certificado requerido durante la instalación de CA IT PAM. El certificado se genera con la contraseña que ha especificado en el archivo ITPAM_eem.xml, o si no se modifica, itpamcertpass.

   Nota: Para obtener ayuda acerca del comando safex, introduzca ./safex.
6. Enumere los contenidos del directorio y verifique que itpamcert.cer está presente.
7. Elimine el archivo XML de configuración de CA IT PAM. Es recomendable por motivos de seguridad.

   ```
   rm ITPAM_eem.xml
   ```

Copie el certificado en el servidor de CA IT PAM

El proceso de ejecución del comando safex desde CA Enterprise Log Manager para registrar CA IT PAM en CA EEM, genera el certificado itpamcert.p12. Debe copiar este certificado en el servidor de Windows en el cual desee instalar el dominio de CA IT PAM. Durante la instalación del dominio de CA IT PAM, busque el archivo del certificado.

Para copiar el certificado a partir del dispositivo de CA Enterprise Log Manager en el servidor de Windows de destino

Copie el archivo itpamcert.p12 desde el dispositivo de CA Enterprise Log Manager que incluye CA EEM en el host, en el que desee instalar CA IT PAM.

- Archivo de origen en el servidor de gestión de CA Enterprise Log Manager:

  `/opt/CA/SharedComponents/iTechnology/itpamcert.p12`

- Ruta de destino en el servidor de Windows de destino:

  `<install path>`

  Nota: Se puede copiar este archivo en la ruta que ha elegido. Seleccione este archivo desde su ubicación, siempre que instale el dominio de CA IT PAM.

Configuración de contraseñas para las cuentas de usuario de CA IT PAM predeterminadas

La ejecución del comando safex crea lo siguiente:

- Grupos de seguridad CA IT PAM:
  - ITPAMAdmins
  - ITPAMUsers
- usuarios de CA IT PAM
  - itpamadmin con una contraseña predeterminada
  - itpamuser con una contraseña predeterminada

Se debe restablecer la contraseña para los dos usuarios de CA IT PAM predeterminados.

Para restablecer las contraseñas para itpamadmin e itpamuser en la aplicación de CA IT PAM en CA EEM

1. Busque la dirección URL del servidor, en el cual se instala CA EEM utilizado por CA Enterprise Log Manager, por ejemplo, el servidor de gestión de CA Enterprise Log Manager:

   `https://<ELM_managementserver>5250/spin/eiam`

   Aparecerá la pantalla de inicio de sesión de CA EEM. La lista desplegable de la aplicación incluye <Global>, CAELM e ITPAM.

2. Inicie sesión en la aplicación de IT PAM:
   a. Seleccione ITPAM como la aplicación.
   b. Escriba EiamAdmin como el nombre de usuario.
   c. Especifique la contraseña para la cuenta de usuario EiamAdmin.
   d. Haga clic en Iniciar sesión.

3. Haga clic en la ficha Gestionar identidades.

4. En el cuadro de diálogo Buscar usuarios, escriba itpam para Valor y haga clic en Ir.

   En la lista aparecerán los usuarios siguientes

   - itpamadmin
   - itpamuser

5. Restablezca la contraseña para itpamadmin:
   a. Seleccione itpamadmin de la lista y desplácese a Autenticación en el panel derecho.
   b. Seleccione Restablecer contraseña.
   c. Escriba la contraseña para esta cuenta en Nueva contraseña y, escríbala una vez más en Confirmar contraseña.
   d. Haga clic en Save.

6. Restablezca la contraseña para itpamuser:
   a. Seleccione itpamuser de la lista y desplácese a Autenticación en el panel derecho.
   b. Seleccione Restablecer contraseña.
   c. Escriba la contraseña para esta cuenta en Nueva contraseña y, escríbala una vez más en Confirmar contraseña.
   d. Haga clic en Save.

7. Haga clic en Cerrar sesión.

Instalación de los componentes de terceros que necesite CA IT PAM

Es necesario tener instalado JDK 1.6 o superior en el sistema antes de que se puedan instalar los componentes de terceros. Ejecute Third_Party_Installer_windows.exe en el servidor Windows Server en el vaya a instalar CA IT PAM. Consulte la *Guía de instalación de CA IT Process Automation Manager* para obtener más información.

Instale el dominio de CA IT PAM

La ejecución del asistente de CA IT PAM con las especificaciones que se han descrito aquí, establecen un vínculo con el certificado a fin de establecer confianza entre CA IT PAM y CA EEM en el servidor de gestión de CA Enterprise Log Manager.

Tenga preparada la siguiente información:

- La contraseña para el archivo de certificado de EEM, itpamcert.p12. Es posible que el valor predeterminado del archivo ITPAM_eem.xml se haya modificado durante el paso Preparación para la implementación de la autenticación de CA IT PAM en CA EEM compartido.
- El nombre de host del servidor de gestión de CA Enterprise Log Manager. Éste es el servidor al cual ha iniciado sesión para el paso Cómo iniciar sesión en CA IT PAM con CA EEM compartido.
- La contraseña itpamadmin que se ha configurado durante el paso Configuración de contraseñas para las cuentas de usuario de CA IT PAM predeterminadas.
- La contraseña de certificado que se utiliza con el fin de controlar el acceso a las claves que se utilizan para codificar contraseñas. Esta configuración es nueva: no existía.

Para obtener instrucciones sobre cómo instalar el dominio de CA IT PAM, consulte la *Guía de instalación de CA IT Process Automation Manager* que encontrará junto al software. Utilice el procedimiento siguiente para los datos específicos al establecer la configuración de seguridad de EEM.

Para instalar el dominio de CA IT PAM

1. Si no se inicia el asistente de instalación de IT PAM como una continuación de la instalación de los componentes de terceros, inicie CA_ITPAM_Domain_windows.exe.
2. Siga las instrucciones que se detallan en la documentación de CA IT PAM hasta el paso a Seleccione el tipo de servidor de seguridad.

3. Al aparecer el cuadro de diálogo Seleccione el tipo de servidor de seguridad, seleccione EEM para Server Security y haga clic en Siguiente.

   Aparecerá la página Configuración de seguridad de EEM.

4. Complete la configuración de seguridad de EEM de la manera siguiente:

   a. Introduzca el nombre de host del servidor de gestión de CA Enterprise Log Manager en el campo de servidor de EEM.

   b. Introduzca ITPAM en el campo de aplicación de EEM.

   c. Haga clic en Examinar y vaya a la carpeta en la que ha guardado itpamcert.p12.

   d. Seleccione itpamcert.p12.

   e. Complete el campo Contraseña de certificado de EEM de una de las maneras siguientes:

      – Introduzca la contraseña que ha sustituido en el archivo ITPAM_eem.xml durante el paso de preparación.

      – Escriba itpamcertpass, la contraseña predeterminada.

5. Haga clic en Probar configuración de EMM.

   Se mostrará el mensaje "Analizando...puede tardar unos minutos".

6. Haga clic en Aceptar.

   Aparecerá el cuadro de diálogo Verificar configuración de EEM.

7. Introduzca itpamadmin como el nombre de usuario. Introduzca la contraseña que ha establecido para la cuenta de usuario de itpamadmin y haga clic en Aceptar.

8. Haga clic en Siguiente. Siga las instrucciones documentadas en IT PAM para finalizar el resto del asistente.

Inicio del servicio del servidor de CA ITPAM

Inicie el servicio del servidor de CA ITPAM para que usted y otros usuarios puedan ejecutar el servidor de CA IT PAM.

Para iniciar el servicio del servidor de CA ITPAM

1. Inicie sesión en el servidor Windows Server en el que ha instalado el dominio de CA IT PAM.

2. En el menú Inicio, seleccione Programas, Dominio de ITPAM, Iniciar servicio de servidor.

   Nota: Si no aparece esta opción de menú, seleccione Herramientas administrativas, Servicios de componentes. Haga clic en Servicios, en el servidor de CA IT PAM y, a continuación, en Iniciar el servicio.

Ejecución e inicio de sesión en la consola de servidor de CA IT PAM

Puede ejecutar el servidor de CA IT PAM desde un explorador en cualquier sistema en que estén instaladas e integradas las API JRE 1.6 o JDK 1.6 de Java.

Para ejecutar la consola de gestión de CA IT PAM

1. Introduzca la siguiente URL en la barra de direcciones de un explorador:

   `http://<itpam_server_hostname>:8080/itpam/`

   Aparecerá la pantalla de inicio de sesión de CA IT Process Automation Manager.

2. Especifique itpamadmin en el campo de inicio de sesión del usuario.
3. Escriba la contraseña que ha asignado al usuario en el campo Contraseña.
4. Haga clic en Iniciar sesión.

   CA EEM en el dispositivo de CA Enterprise Log Manager realiza la autenticación de sus credenciales de inicio de sesión y abre CA IT Process Automation Manager.

Para obtener información acerca de la integración y el uso de CA IT PAM con CA Enterprise Log Manager, consulte la sección Trabajo con procesos de salida/evento de CA IT PAM del capítulo Alertas de acción en la *Guía de administración de CA Enterprise Log Manager*.

Apéndice D: Recuperación de desastres

Esta sección contiene los siguientes temas:

Planificación de la recuperación de desastres

La planificación de la recuperación de desastres es una parte necesaria en un plan de administración de redes adecuado. La planificación de la recuperación de desastres de CA Enterprise Log Manager es una tarea relativamente sencilla. La clave está en realizar copias de seguridad de forma regular.

Es necesario realizar copias de seguridad de la siguiente información:

- La instancia de aplicación de CA Enterprise Log Manager del servidor de gestión
- La carpeta /opt/CA/LogManager/data de cada servidor de CA Enterprise Log Manager
- Los archivos de certificado de la carpeta /opt/CA/SharedComponents/iTechnology de cada servidor de CA Enterprise Log Manager

Si es fundamental para la implementación mantener altos niveles de rendimiento, puede seleccionar un servidor reserva que presente las mismas características de hardware que el servidor en el que instala el resto de servidores de CA Enterprise Log Manager. Si un servidor de CA Enterprise Log Manager está desactivado, puede instalar otro utilizando el mismo nombre. Cuando se inicie el nuevo servidor, recibirá los archivos de configuración necesarios del servidor de gestión. Si este nivel de rendimiento no es fundamental para la implementación, puede instalar un servidor de CA Enterprise Log Manager en cualquier servidor en blanco que pueda albergar el sistema operativo base y que cumpla con los requisitos mínimos de memoria y disco duro.

Si desea obtener más información acerca de los requisitos de hardware y software, consulte las *Notas de la versión de CA Enterprise Log Manager*.

El servidor interno de CA EEM, instalado en el servidor de gestión, también cuenta con sus propios procesos de configuración de conmutación por error para garantizar la continuidad de las operaciones, de las que se habla detalladamente en la *Guía de introducción de CA EEM*.

Acerca de la realización de copias de seguridad del servidor de CA EEM

La configuración de cada conector, agente y servidor de CA Enterprise Log Manager, además de las consultas, informes, alertas, etc., se mantiene por separado en el repositorio de CA EEM del servidor de gestión de CA Enterprise Log Manager. Para realizar una recuperación correcta del servidor, es esencial realizar con regularidad copias de seguridad de la información almacenada en la instancia de aplicación de CA Enterprise Log Manager.

Una *instancia de aplicación* es un espacio común en el repositorio de CA EEM que almacena la siguiente información:

- Usuarios, grupos y políticas de acceso
- Agente, integración, escucha, conector y configuraciones guardadas
- Reglas personalizadas de consultas, informes, supresión y resumen
- Relaciones de federación
- Información sobre la gestión del código binario
- Claves de cifrado

Puede realizar el procedimiento de copia de seguridad de CA EEM desde la interfaz del explorador Web de CA EEM. Los servidores de CA Enterprise Log Manager de una empresa utilizan la misma instancia de aplicación. El valor predeterminado de la instancia de aplicación de CA Enterprise Log Manager es CAELM. Puede instalar servidores de CA Enterprise Log Manager con distintas instancias de aplicación, pero sólo puede federar aquellos servidores que compartan la misma instancia de aplicación. Los servidores configurados para que utilicen el mismo servidor de CA EEM pero con distintas instancias de aplicación comparten el almacén de usuarios, las políticas de contraseñas y los grupos globales.

La *Guía de introducción de CA EEM* incluye más información acerca de las operaciones de copia de seguridad y de restauración.

Realización de una copia de seguridad de una instancia de aplicación de CA EEM

Puede realizar una copia de seguridad de una instancia de aplicación de CA Enterprise Log Manager desde el servidor interno de CA EEM en el servidor de gestión.

Para realizar una copia de seguridad de una instancia de aplicación

1. Acceda al servidor de CA EEM utilizando la siguiente URL:

   `https://<servername>:5250/spin/eiam`

2. Expanda la lista de aplicaciones en la página de inicio de sesión y seleccione el nombre de la instancia de aplicación utilizado cuando instaló los servidores de CA Enterprise Log Manager.

   El nombre predeterminado de la instancia de aplicación de CA Enterprise Log Manager es CAELM.

3. Inicie sesión como usuario de EiamAdmin o como un usuario con la función de administrador de CA EEM.

4. Acceda a la ficha Configuración y, a continuación, seleccione la subficha Servidor de EEM.

5. Seleccione el elemento Exportar aplicación en el panel de navegación de la izquierda.

6. Active todas las opciones excepto la casilla de verificación Sobrescribir el tamaño máximo de búsqueda.

   Nota: Si utiliza un directorio externo, no seleccione las opciones Usuarios globales, Grupos globales y Carpetas globales.

7. Haga clic en Exportar para crear un archivo de exportación XML para la instancia de aplicación.

   El cuadro de diálogo Descarga de archivos mostrará el nombre de archivo *<AppInstanceName>*.xml.gz como, por ejemplo, CAELM.xml.gz y el botón Guardar.

8. Haga clic en Guardar y seleccione la ubicación de la copia de seguridad en un servidor asignado remoto. También puede guardar el archivo de forma local y, a continuación, copiarlo o moverlo a la ubicación de la copia de seguridad en otro servidor.

Restauración de un servidor de CA EEM para utilizar con CA Enterprise Log Manager

Puede restablecer una instancia de aplicación de CA Enterprise Log Manager en un servidor de gestión. El restablecimiento de la funcionalidad de CA EEM del servidor de gestión implica la ejecución de la utilidad Safex que importa la copia de seguridad de la instancia de aplicación.

Para restablecer una funcionalidad CA EEM del servidor de gestión a partir de una copia de seguridad

1. Instale el dispositivo de software de CA Enterprise Log Manager en un nuevo servidor de hardware.
2. Acceda a un símbolo del sistema y desplácese al directorio /opt/CA/LogManager/EEM.
3. Copie el archivo de copia de seguridad *<AppinstanceName>*.xml.gz a este directorio desde el servidor de copia de seguridad externo.
4. Ejecute el siguiente comando para recuperar el archivo de exportación XML:

   `gunzip <AppinstanceName>.xml.gz`

5. Ejecute el siguiente comando para restablecer el archivo de exportación en el nuevo servidor de gestión

   `./safex –h eemserverhostname –u EiamAdmin –p password –f AppinstanceName.xml`

   Si está realizando las operaciones en el modo FIPS, asegúrese de incluir la opción -fips.

6. Vaya al directorio /opt/CA/ELMAgent/bin.
7. Sustituya el archivo predeterminado AgentCert.cer con el archivo de copia de seguridad CAELM_AgentCert.cer para garantizar un inicio de agente adecuado.

Realización de una copia de seguridad de un servidor de CA Enterprise Log Manager

Puede realizar una copia de seguridad de un servidor de CA Enterprise Log Manager completo desde la carpeta /opt/CA/LogManager/data. Esta carpeta de datos es un vínculo simbólico de la carpeta de datos del directorio raíz (/data).

Para realizar una copia de seguridad de un servidor de CA Enterprise Log Manager

1. Inicie sesión en el servidor de CA Enterprise Log Manager como usuario caelmadmin.
2. Acceda a la cuenta raíz utilizando la utilidad "su"
3. Vaya al directorio /opt/CA/LogManager.
4. Ejecute el siguiente comando TAR para crear una copia de seguridad de los archivos del servidor de CA Enterprise Log Manager:

   ```
   tar –hzcvf backupData.tgz /data
   ```

   Este comando crea el archivo de salida comprimido backupData.tgz utilizando los archivos del directorio /data.
5. Vaya al directorio /opt/CA/SharedComponents/iTechnology.
6. Ejecute el siguiente comando TAR para crear una copia de la copia de seguridad de los certificados digitales (todos los archivos con una extensión de archivo .cer):

   ```
   tar –zcvf backupCerts.tgz *.cer
   ```

   Este comando crea el archivo de salida comprimido backupCerts.tgz.

   ```
   tar –hzcvf backupCerts.tgz /data
   ```

Restauración de un servidor de CA Enterprise Log Manager a partir de archivos de copia de seguridad

Puede restaurar un servidor de CA Enterprise Log Manager a partir de archivos de copia de seguridad después de instalar el dispositivo de software de CA Enterprise Log Manager en el nuevo servidor.

Para restaurar un servidor de CA Enterprise Log Manager a partir de copias de seguridad

1. Detenga el proceso de iGateway en el nuevo servidor.

   Para ello, desplácese a la carpeta /opt/CA/SharedComponents/iTechnology y ejecute el siguiente comando:

   ```
   ./S99igateway stop
   ```

2. Copie los archivos backupData.tgz y backupCerts.tgz en el directorio /opt/CA/LogManager en el nuevo servidor.
3. Expanda los contenidos del archivo backupData.tgz con el siguiente comando:

   ```
   tar –xzvf  backupData.tgz
   ```

   El comando sobrescribirá los contenidos de la carpeta de datos con los contenidos del archivo de copia de seguridad.

4. Desplácese al directorio /opt/CA/SharedComponents/iTechnology.
5. Expanda los contenidos del archivo backupCerts.tgz con el siguiente comando:

   ```
   tar –xzvf  backupCerts.tgz
   ```

   Este comando sobrescribe los archivos de certificado (.p12) en la carpeta actual con los archivos de certificado del archivo de copia de seguridad.

6. Inicie el proceso de iGateway:

   Para ello, ejecute el comando siguiente:

   ```
   ./S99igateway start
   ```

Reemplazo de un servidor de CA Enterprise Log Manager

Siga este procedimiento para reemplazar un servidor de recopilación de CA Enterprise Log Manager después de que se haya producido un desastre o error importante. Este procedimiento le permite recuperarse de un desastre gracias a la creación de un nuevo servidor de CA Enterprise Log Manager para reanudar la recopilación de eventos en lugar del servidor que ha fallado.

Nota: Este procedimiento no recupera los datos de eventos del almacén de registros de eventos del servidor que ha fallado. Utilice las técnicas habituales de recuperación de datos para recuperar datos de eventos del almacén de registros de eventos del servidor que ha fallado.

Para efectuar la recuperación a partir de un servidor de CA Enterprise Log Manager desactivado

1. Instale el dispositivo de software de CA Enterprise Log Manager en otro servidor utilizando el mismo nombre de host asignado al servidor que ha fallado.

   Durante la instalación, cuando se le solicite el nombre de instancia de aplicación de CA EEM, compruebe que utiliza la misma instancia de aplicación utilizada por el servidor antiguo. Cuando el registro sea correcto, se activará el servidor de CA EEM para sincronizar la configuración.

2. Inicie el servidor de CA Enterprise Log Manager e inicie sesión como usuario administrativo EiamAdmin predeterminado.

   Cuando se inicie un nuevo servidor de CA Enterprise Log Manager, se conectará automáticamente con el servidor de CA EEM que, posteriormente, descargará los archivos de configuración. Una vez recibidos los archivos de configuración, el nuevo servidor de CA Enterprise Log Manager reanudará la recopilación de registros.

Apéndice E: CA Enterprise Log Manager y virtualización

Esta sección contiene los siguientes temas:

Hipótesis de implementación

Al utilizar CA Enterprise Log Manager en un entorno virtual o en un entorno mixto que incluye servidores virtuales y de dispositivos, se da por hecho lo siguiente:

- En un entorno completamente virtual, instale al menos un servidor de CA Enterprise Log Manager como servidor de gestión. Este servidor de gestión gestiona configuraciones, contenido de la suscripción y contenido definido por el usuario, al tiempo que se comunica con los agentes. El servidor de gestión no recibe registros de eventos ni gestiona consultas ni informes.
- En un entorno mixto, instale el servidor de gestión de CA Enterprise Log Manager en un hardware certificado.
- Cada host de máquina virtual debe contar con cuatro procesadores dedicados, que es la cantidad máxima permitida por VMware ESX Server 3.5.

Consideraciones

Un servidor de CA Enterprise Log Manager dedicado logra un rendimiento óptimo con ocho o más procesadores. El servidor de VMware ESX permite hasta cuatro procesadores para una sola máquina virtual. Para lograr un rendimiento similar al de un servidor dedicado de ocho procesadores, instale CA Enterprise Log Manager en dos o más máquinas virtuales y, a continuación, fedérelas para los informes consolidados.

Dos servidores de CA Enterprise Log Manager que se ejecutan como invitados en VMware ESX Server v3.5 presentan una capacidad similar a la de un solo servidor dedicado de CA Enterprise Log Manager. Utilice la siguiente tabla para planificar su red virtual:

Función del servidor de CA Enterprise Log Manager	Número mínimo de procesadores	Memoria (por CPU)	Memoria total (requisitos mínimos)
Gestión*	4	2	8
Generación de informes	4	2	8
Recopilación	4	2	8

* La instalación de CA Enterprise Log Manager como servidor de gestión en una máquina virtual sólo se recomienda cuando es necesario instalar un entorno completamente virtual.

Creación de servidores de CA Enterprise Log Manager virtuales

Puede crear servidores de CA Enterprise Log Manager virtuales para su entorno de recopilación de registros de eventos a través de los siguientes escenarios:

- Adición de servidores virtuales a un entorno de CA Enterprise Log Manager existente; creación de un entorno mixto
- Creación de un entorno virtual de recopilación de registros
- Clonación e implementación de servidores de CA Enterprise Log Manager virtuales para una escalabilidad rápida

Adición de servidores virtuales a su entorno

Si ya cuenta con una implementación de CA Enterprise Log Manager, puede agregar servidores de recopilación de CA Enterprise Log Manager virtuales para gestionar un aumento de volumen en la red. Este escenario da por hecho que tiene instalado un servidor de gestión de CA Enterprise Log Manager y uno o varios servidores de CA Enterprise Log Manager para la recopilación y generación de informes.

Nota: Para lograr un rendimiento óptimo, instale CA Enterprise Log Manager en los servidores virtuales para gestionar únicamente las tareas de recopilación y generación de informes.

El proceso de agregar servidores de recopilación virtuales a su entorno incluye los siguiente procedimientos:

1. Cree una nueva máquina virtual.
2. Agregue unidades de disco virtuales.
3. Instale CA Enterprise Log Manager en la máquina virtual.
4. Configure el servidor de CA Enterprise Log Manager tal y como se describe en la sección de instalación.

Después de instalar el servidor de recopilación virtual, puede agregarlo a la federación para las consultas e informes.

Creación de una nueva máquina virtual

Siga este procedimiento para crear una nueva máquina virtual utilizando VMware Infrastructure Client. Utilice cuatro procesadores para cada servidor virtual de CA Enterprise Log Manager para alcanzar un rendimiento aceptable.

Para crear una máquina virtual

1. Acceda a VMware Infrastructure Client.
2. Haga clic con el botón secundario en el host de ESX en el panel izquierdo y seleccione New Virtual Machine para que aparezca el asistente de la nueva máquina virtual. Esta acción mostrará un cuadro de diálogo de tipo de configuración.
3. Seleccione la configuración personalizada y haga clic en Next. Aparecerá un cuadro de diálogo con el nombre y la ubicación.
4. Introduzca un nombre para el servidor de CA Enterprise Log Manager que va a instalar en esta máquina virtual y haga clic en Next.
5. Especifique la configuración de almacenamiento de la máquina virtual y, a continuación, haga clic en Next.

   Compruebe que la configuración de almacenamiento es lo suficientemente grande para su servidor de CA Enterprise Log Manager. Se recomienda 500 GB como mínimo.

   Nota: En otro procedimiento, configurará otras unidades de disco virtuales para almacenar los registros de eventos recopilados.
6. Seleccione Red Hat Enterprise Linux 5 (32 bits) como sistema operativo invitado y haga clic en Next.

7. Seleccione 4 como el número de procesadores virtuales en la lista desplegable Number of virtual processors.

   El servidor host físico debe ser capaz de dedicar cuatro CPU físicas *exclusivamente* a esta instancia de CA Enterprise Log Manager. Haga clic en Next.

8. Configure el tamaño de memoria de la máquina virtual y haga clic en Next. El tamaño de memoria *mínimo* aceptable para CA Enterprise Log Manager es de 8 GB u 8192 MB.

9. Configure la conexión de interfaz de red (NIC).CA Enterprise Log Manager requiere una conexión de red como mínimo. Seleccione NIC x en la lista de NIC disponible y configure el valor del adaptador a Flexible.

   Nota: No es necesario configurar un NIC independiente para cada servidor de CA Enterprise Log Manager alojado en este servidor físico. No obstante, es necesario asignar una dirección IP estática para cada uno.

10. Seleccione la opción Connect at Power On y, a continuación, haga clic en Next. Aparecerá el cuadro de diálogo I/O Adapter Types.

11. Seleccione LSI Logic para el adaptador de E/S y, a continuación, haga clic en Next. Aparecerá el cuadro de diálogo Select a Disk.

12. Seleccione la opción Create a new virtual disk y, a continuación, haga clic en Next. Aparecerá el cuadro de diálogo de la ubicación y capacidad del disco.

13. Especifique la ubicación y la capacidad del disco y haga clic en Next. Aparecerá el cuadro de diálogo de opciones avanzadas.

    Puede almacenar este disco con su máquina virtual o puede especificar otra ubicación. Se recomienda 500 GB como mínimo.

14. Acepte los valores predeterminados de las opciones avanzadas y haga clic en Next.

15. Confirme la configuración y haga clic en Finish para crear la nueva máquina virtual.

Adición de unidades de disco virtuales

Siga este procedimiento para agregar unidades de disco virtuales para el almacenamiento del registro de eventos. Utilice la misma configuración independientemente de la función que tiene en su red un servidor específico de CA Enterprise Log Manager.

Para editar la configuración

1. Haga clic con el botón secundario en VMware Infrastructure Client y seleccione Edit Settings.

   Aparecerá el cuadro de diálogo Virtual Machine Properties.

2. Resalte las propiedades de la unidad de CD/DVD 1.
3. Haga clic en el botón de selección Host Device y seleccione su unidad de DVD-ROM en la lista desplegable.
4. Seleccione la opción Connect at power on en Device Status.
5. Haga clic en Add para iniciar Add Hardware Wizard y agregue una segunda unidad de disco duro.
6. Resalte Hard Disk en la lista de dispositivos y haga clic en Next. Aparecerá el cuadro de diálogo Select a Disk.
7. Seleccione la opción Create a new virtual disk y, a continuación, haga clic en Next.
8. Especifique el tamaño del nuevo disco y seleccione la opción Specify a datastore to set its location.

   CA Enterprise Log Manager detectará esta unidad adicional durante la instalación y la asignará para el almacenamiento de datos. Se recomienda que maximice la cantidad de almacenamiento disponible en CA Enterprise Log Manager.

   Nota: La configuración predeterminada del tamaño de bloque del servidor de VMware ESX es de 1 MB, que limita el espacio máximo de disco que puede crear a 256 GB. Si necesita más espacio, hasta 512 GB, aumente la configuración de tamaño de bloque a 2 MB utilizando este comando:

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

   Reinicie el servidor de ESX para que se aplique la nueva configuración. Si desea obtener más información acerca de este y otros comandos, consulte la documentación de VMware ESX Server.

   Haga clic en Next para mostrar el cuadro de diálogo Specify Advanced Options.

9. Acepte los valores predeterminados de las opciones avanzadas y haga clic en Next. Aparecerá el cuadro de diálogo Ready to Complete.
10. Haga clic en Finish para almacenar los cambios en esta máquina virtual. Esta acción lo devolverá al cuadro de diálogo VMware Infrastructure Client.

Instalación de CA Enterprise Log Manager en la máquina virtual

Siga este procedimiento para instalar CA Enterprise Log Manager en una máquina virtual que ha creado anteriormente.

Puede configurar un servidor virtual o dedicado de CA Enterprise Log Manager después de realizar la instalación para utilizar con una de varias funciones como, por ejemplo, gestión, recopilación o generación de informes. Si instala un servidor de gestión de CA Enterprise Log Manager, no lo utilice para recibir registros de eventos ni para ejecutar consultas o informes. Instale servidores virtuales de CA Enterprise Log Manager independientes para que actúen como servidores de generación de informes y de recopilación y lograr así un rendimiento óptimo.

Revise las instrucciones de instalación habituales antes de instalar CA Enterprise Log Manager en un entorno virtual. La hoja de trabajo de instalación le ayuda a recopilar la información que necesita.

Para instalar CA Enterprise Log Manager en una máquina virtual

1. Cargue el disco de instalación del SO de CA Enterprise Log Manager en la unidad física de DVD-ROM o localice el directorio donde ha copiado la imagen de instalación.
2. Resalte la máquina virtual en la lista de inventario de la máquina virtual, haga clic con el botón secundario y, a continuación, seleccione Power On (Encender).
3. Continúe con la instalación habitual de CA Enterprise Log Manager.
4. Configure el servidor de CA Enterprise Log Manager instalado según la función que le pretenda asignar utilizando la información de la sección sobre la instalación de un servidor de CA Enterprise Log Manager.

Más información

Instalación de CA Enterprise Log Manager (en la página 82)

Creación de un entorno completamente virtual

Si todavía no ha implementado un entorno de CA Enterprise Log Manager, puede crear un entorno de recopilación de registros virtual. Este escenario da por hecho que dispone de suficientes servidores físicos disponibles, cada uno con un grupo de al menos cuatro procesadores, para instalar los servidores de CA Enterprise Log Manager deseados.

Instale un servidor de CA Enterprise Log Manager que actúe como servidor de gestión. Durante la configuración, no envíe registros de eventos a este servidor ni utilice este servidor para generar informes. La configuración del entorno de este modo mantiene el rendimiento de recopilación de registros de eventos requerido para la producción de la empresa.

Normalmente, instala dos servidores de CA Enterprise Log Manager con cuatro procesadores en sustitución de los servidores de dispositivos que instalaría al utilizar hardware certificado (los servidores de dispositivos cuentan con un mínimo de ocho procesadores).

El proceso que sigue para crear un entorno virtual incluye los siguientes procedimientos:

1. Cree una nueva máquina virtual para cada uno de los servidores de CA Enterprise Log Manager que vaya a instalar.
2. Agregue unidades de disco virtuales.
3. Instale un servidor de CA Enterprise Log Manager virtual para las funciones de gestión en uno de los hosts de la máquina virtual.
4. Instale dos o más servidores de CA Enterprise Log Manager para la recopilación y para la generación de informes.
5. Configure los servidores de CA Enterprise Log Manager tal y como se describe en la sección acerca de la instalación de un servidor de CA Enterprise Log Manager.

Creación de una nueva máquina virtual

Siga este procedimiento para crear una nueva máquina virtual utilizando VMware Infrastructure Client. Utilice cuatro procesadores para cada servidor virtual de CA Enterprise Log Manager para alcanzar un rendimiento aceptable.

Para crear una máquina virtual

1. Acceda a VMware Infrastructure Client.
2. Haga clic con el botón secundario en el host de ESX en el panel izquierdo y seleccione New Virtual Machine para que aparezca el asistente de la nueva máquina virtual. Esta acción mostrará un cuadro de diálogo de tipo de configuración.
3. Seleccione la configuración personalizada y haga clic en Next. Aparecerá un cuadro de diálogo con el nombre y la ubicación.

4. Introduzca un nombre para el servidor de CA Enterprise Log Manager que va a instalar en esta máquina virtual y haga clic en Next.
5. Especifique la configuración de almacenamiento de la máquina virtual y, a continuación, haga clic en Next.

   Compruebe que la configuración de almacenamiento es lo suficientemente grande para su servidor de CA Enterprise Log Manager. Se recomienda 500 GB como mínimo.

   Nota: En otro procedimiento, configurará otras unidades de disco virtuales para almacenar los registros de eventos recopilados.
6. Seleccione Red Hat Enterprise Linux 5 (32 bits) como sistema operativo invitado y haga clic en Next.
7. Seleccione 4 como el número de procesadores virtuales en la lista desplegable Number of virtual processors.

   El servidor host físico debe ser capaz de dedicar cuatro CPU físicas *exclusivamente* a esta instancia de CA Enterprise Log Manager. Haga clic en Next.
8. Configure el tamaño de memoria de la máquina virtual y haga clic en Next. El tamaño de memoria *mínimo* aceptable para CA Enterprise Log Manager es de 8 GB u 8192 MB.
9. Configure la conexión de interfaz de red (NIC).CA Enterprise Log Manager requiere una conexión de red como mínimo. Seleccione NIC x en la lista de NIC disponible y configure el valor del adaptador a Flexible.

   Nota: No es necesario configurar un NIC independiente para cada servidor de CA Enterprise Log Manager alojado en este servidor físico. No obstante, es necesario asignar una dirección IP estática para cada uno.
10. Seleccione la opción Connect at Power On y, a continuación, haga clic en Next. Aparecerá el cuadro de diálogo I/O Adapter Types.
11. Seleccione LSI Logic para el adaptador de E/S y, a continuación, haga clic en Next. Aparecerá el cuadro de diálogo Select a Disk.
12. Seleccione la opción Create a new virtual disk y, a continuación, haga clic en Next. Aparecerá el cuadro de diálogo de la ubicación y capacidad del disco.
13. Especifique la ubicación y la capacidad del disco y haga clic en Next. Aparecerá el cuadro de diálogo de opciones avanzadas.

    Puede almacenar este disco con su máquina virtual o puede especificar otra ubicación. Se recomienda 500 GB como mínimo.
14. Acepte los valores predeterminados de las opciones avanzadas y haga clic en Next.
15. Confirme la configuración y haga clic en Finish para crear la nueva máquina virtual.

Adición de unidades de disco virtuales

Siga este procedimiento para agregar unidades de disco virtuales para el almacenamiento del registro de eventos. Utilice la misma configuración independientemente de la función que tiene en su red un servidor específico de CA Enterprise Log Manager.

Para editar la configuración

1. Haga clic con el botón secundario en VMware Infrastructure Client y seleccione Edit Settings.

   Aparecerá el cuadro de diálogo Virtual Machine Properties.

2. Resalte las propiedades de la unidad de CD/DVD 1.
3. Haga clic en el botón de selección Host Device y seleccione su unidad de DVD-ROM en la lista desplegable.
4. Seleccione la opción Connect at power on en Device Status.
5. Haga clic en Add para iniciar Add Hardware Wizard y agregue una segunda unidad de disco duro.
6. Resalte Hard Disk en la lista de dispositivos y haga clic en Next. Aparecerá el cuadro de diálogo Select a Disk.
7. Seleccione la opción Create a new virtual disk y, a continuación, haga clic en Next.
8. Especifique el tamaño del nuevo disco y seleccione la opción Specify a datastore to set its location.

   CA Enterprise Log Manager detectará esta unidad adicional durante la instalación y la asignará para el almacenamiento de datos. Se recomienda que maximice la cantidad de almacenamiento disponible en CA Enterprise Log Manager.

   Nota: La configuración predeterminada del tamaño de bloque del servidor de VMware ESX es de 1 MB, que limita el espacio máximo de disco que puede crear a 256 GB. Si necesita más espacio, hasta 512 GB, aumente la configuración de tamaño de bloque a 2 MB utilizando este comando:

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

   Reinicie el servidor de ESX para que se aplique la nueva configuración. Si desea obtener más información acerca de este y otros comandos, consulte la documentación de VMware ESX Server.

   Haga clic en Next para mostrar el cuadro de diálogo Specify Advanced Options.

9. Acepte los valores predeterminados de las opciones avanzadas y haga clic en Next. Aparecerá el cuadro de diálogo Ready to Complete.
10. Haga clic en Finish para almacenar los cambios en esta máquina virtual. Esta acción lo devolverá al cuadro de diálogo VMware Infrastructure Client.

Instalación de CA Enterprise Log Manager en la máquina virtual

Siga este procedimiento para instalar CA Enterprise Log Manager en una máquina virtual que ha creado anteriormente.

Puede configurar un servidor virtual o dedicado de CA Enterprise Log Manager después de realizar la instalación para utilizar con una de varias funciones como, por ejemplo, gestión, recopilación o generación de informes. Si instala un servidor de gestión de CA Enterprise Log Manager, no lo utilice para recibir registros de eventos ni para ejecutar consultas o informes. Instale servidores virtuales de CA Enterprise Log Manager independientes para que actúen como servidores de generación de informes y de recopilación y lograr así un rendimiento óptimo.

Revise las instrucciones de instalación habituales antes de instalar CA Enterprise Log Manager en un entorno virtual. La hoja de trabajo de instalación le ayuda a recopilar la información que necesita.

Para instalar CA Enterprise Log Manager en una máquina virtual

1. Cargue el disco de instalación del SO de CA Enterprise Log Manager en la unidad física de DVD-ROM o localice el directorio donde ha copiado la imagen de instalación.
2. Resalte la máquina virtual en la lista de inventario de la máquina virtual, haga clic con el botón secundario y, a continuación, seleccione Power On (Encender).
3. Continúe con la instalación habitual de CA Enterprise Log Manager.
4. Configure el servidor de CA Enterprise Log Manager instalado según la función que le pretenda asignar utilizando la información de la sección sobre la instalación de un servidor de CA Enterprise Log Manager.

Más información

Instalación de CA Enterprise Log Manager (en la página 82)

Implementación rápida de servidores de CA Enterprise Log Manager virtuales

Puede clonar un servidor de CA Enterprise Log Manager virtual para crear una imagen implementable y lograr una rápida escalabilidad del entorno de recopilación de registros.

Nota: Para lograr el mejor rendimiento, es recomendable instalar CA Enterprise Log Manager en servidores virtuales para gestionar sólo tareas de recopilación. No clone una máquina virtual que contenga un servidor de CA Enterprise Log Manager de gestión.

Antes de iniciar este escenario, compruebe que tiene un entorno existente o instale un servidor de CA Enterprise Log Manager para llevar a cabo funciones de gestión en un servidor dedicado o virtual. También debe contar con la versión correcta del software VMware para admitir la función de clonación.

El proceso que debe seguir para crear y clonar un servidor de CA Enterprise Log Manager virtual para la recopilación consta de los procedimientos siguientes:

1. Cree una nueva máquina virtual.
2. Agregue unidades de disco virtuales.
3. Instale un servidor de CA Enterprise Log Manager en la máquina virtual.
4. Clone la máquina virtual que contiene el servidor de CA Enterprise Log Manager nuevo mediante las instrucciones suministradas por el proveedor.

   Nota: Cree sólo una imagen clonada completa. No utilice clones vinculados a CA Enterprise Log Manager.
5. Importe la máquina virtual clonada en un servidor físico de destino.
6. Actualice la máquina virtual clonada antes de conectarla a la red.
7. Configure el servidor de CA Enterprise Log Manager tal y como se describe en la *Guía de implementación*.

Creación de una nueva máquina virtual

Siga este procedimiento para crear una nueva máquina virtual utilizando VMware Infrastructure Client. Utilice cuatro procesadores para cada servidor virtual de CA Enterprise Log Manager para alcanzar un rendimiento aceptable.

Para crear una máquina virtual

1. Acceda a VMware Infrastructure Client.
2. Haga clic con el botón secundario en el host de ESX en el panel izquierdo y seleccione New Virtual Machine para que aparezca el asistente de la nueva máquina virtual. Esta acción mostrará un cuadro de diálogo de tipo de configuración.
3. Seleccione la configuración personalizada y haga clic en Next. Aparecerá un cuadro de diálogo con el nombre y la ubicación.

4. Introduzca un nombre para el servidor de CA Enterprise Log Manager que va a instalar en esta máquina virtual y haga clic en Next.
5. Especifique la configuración de almacenamiento de la máquina virtual y, a continuación, haga clic en Next.

   Compruebe que la configuración de almacenamiento es lo suficientemente grande para su servidor de CA Enterprise Log Manager. Se recomienda 500 GB como mínimo.

   Nota: En otro procedimiento, configurará otras unidades de disco virtuales para almacenar los registros de eventos recopilados.
6. Seleccione Red Hat Enterprise Linux 5 (32 bits) como sistema operativo invitado y haga clic en Next.
7. Seleccione 4 como el número de procesadores virtuales en la lista desplegable Number of virtual processors.

   El servidor host físico debe ser capaz de dedicar cuatro CPU físicas *exclusivamente* a esta instancia de CA Enterprise Log Manager. Haga clic en Next.
8. Configure el tamaño de memoria de la máquina virtual y haga clic en Next. El tamaño de memoria *mínimo* aceptable para CA Enterprise Log Manager es de 8 GB u 8192 MB.
9. Configure la conexión de interfaz de red (NIC).CA Enterprise Log Manager requiere una conexión de red como mínimo. Seleccione NIC x en la lista de NIC disponible y configure el valor del adaptador a Flexible.

   Nota: No es necesario configurar un NIC independiente para cada servidor de CA Enterprise Log Manager alojado en este servidor físico. No obstante, es necesario asignar una dirección IP estática para cada uno.
10. Seleccione la opción Connect at Power On y, a continuación, haga clic en Next. Aparecerá el cuadro de diálogo I/O Adapter Types.
11. Seleccione LSI Logic para el adaptador de E/S y, a continuación, haga clic en Next. Aparecerá el cuadro de diálogo Select a Disk.
12. Seleccione la opción Create a new virtual disk y, a continuación, haga clic en Next. Aparecerá el cuadro de diálogo de la ubicación y capacidad del disco.
13. Especifique la ubicación y la capacidad del disco y haga clic en Next. Aparecerá el cuadro de diálogo de opciones avanzadas.

    Puede almacenar este disco con su máquina virtual o puede especificar otra ubicación. Se recomienda 500 GB como mínimo.
14. Acepte los valores predeterminados de las opciones avanzadas y haga clic en Next.
15. Confirme la configuración y haga clic en Finish para crear la nueva máquina virtual.

Adición de unidades de disco virtuales

Siga este procedimiento para agregar unidades de disco virtuales para el almacenamiento del registro de eventos. Utilice la misma configuración independientemente de la función que tiene en su red un servidor específico de CA Enterprise Log Manager.

Para editar la configuración

1. Haga clic con el botón secundario en VMware Infrastructure Client y seleccione Edit Settings.

   Aparecerá el cuadro de diálogo Virtual Machine Properties.

2. Resalte las propiedades de la unidad de CD/DVD 1.
3. Haga clic en el botón de selección Host Device y seleccione su unidad de DVD-ROM en la lista desplegable.
4. Seleccione la opción Connect at power on en Device Status.
5. Haga clic en Add para iniciar Add Hardware Wizard y agregue una segunda unidad de disco duro.
6. Resalte Hard Disk en la lista de dispositivos y haga clic en Next. Aparecerá el cuadro de diálogo Select a Disk.
7. Seleccione la opción Create a new virtual disk y, a continuación, haga clic en Next.
8. Especifique el tamaño del nuevo disco y seleccione la opción Specify a datastore to set its location.

   CA Enterprise Log Manager detectará esta unidad adicional durante la instalación y la asignará para el almacenamiento de datos. Se recomienda que maximice la cantidad de almacenamiento disponible en CA Enterprise Log Manager.

   Nota: La configuración predeterminada del tamaño de bloque del servidor de VMware ESX es de 1 MB, que limita el espacio máximo de disco que puede crear a 256 GB. Si necesita más espacio, hasta 512 GB, aumente la configuración de tamaño de bloque a 2 MB utilizando este comando:

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

   Reinicie el servidor de ESX para que se aplique la nueva configuración. Si desea obtener más información acerca de este y otros comandos, consulte la documentación de VMware ESX Server.

   Haga clic en Next para mostrar el cuadro de diálogo Specify Advanced Options.

9. Acepte los valores predeterminados de las opciones avanzadas y haga clic en Next. Aparecerá el cuadro de diálogo Ready to Complete.
10. Haga clic en Finish para almacenar los cambios en esta máquina virtual. Esta acción lo devolverá al cuadro de diálogo VMware Infrastructure Client.

Instalación de CA Enterprise Log Manager en la máquina virtual

Siga este procedimiento para instalar CA Enterprise Log Manager en una máquina virtual que ha creado anteriormente.

Puede configurar un servidor virtual o dedicado de CA Enterprise Log Manager después de realizar la instalación para utilizar con una de varias funciones como, por ejemplo, gestión, recopilación o generación de informes. Si instala un servidor de gestión de CA Enterprise Log Manager, no lo utilice para recibir registros de eventos ni para ejecutar consultas o informes. Instale servidores virtuales de CA Enterprise Log Manager independientes para que actúen como servidores de generación de informes y de recopilación y lograr así un rendimiento óptimo.

Revise las instrucciones de instalación habituales antes de instalar CA Enterprise Log Manager en un entorno virtual. La hoja de trabajo de instalación le ayuda a recopilar la información que necesita.

Para instalar CA Enterprise Log Manager en una máquina virtual

1. Cargue el disco de instalación del SO de CA Enterprise Log Manager en la unidad física de DVD-ROM o localice el directorio donde ha copiado la imagen de instalación.
2. Resalte la máquina virtual en la lista de inventario de la máquina virtual, haga clic con el botón secundario y, a continuación, seleccione Power On (Encender).
3. Continúe con la instalación habitual de CA Enterprise Log Manager.
4. Configure el servidor de CA Enterprise Log Manager instalado según la función que le pretenda asignar utilizando la información de la sección sobre la instalación de un servidor de CA Enterprise Log Manager.

Más información

Instalación de CA Enterprise Log Manager (en la página 82)

Clonación de un servidor de CA Enterprise Log Manager virtual

Puede emplear este procedimiento para clonar un servidor de CA Enterprise Log Manager virtual. Este procedimiento presupone que ya ha creado una máquina virtual nueva, le ha agregado controladores de disco y ha instalado CA Enterprise Log Manager.

Para clonar un servidor virtual

1. Acceda a VMware VirtualCenter y busque la máquina virtual que contiene CA Enterprise Log Manager.
2. Apague la máquina virtual si está en ejecución.
3. Seleccione la opción Exportar e indique una ubicación para la máquina virtual exportada.

   VMware ESX Server ofrece otros métodos para clonar máquinas virtuales. Si desea obtener más información, consulte la documentación de VMware.

Importación de una máquina virtual clonada en un servidor de destino

Emplee este procedimiento para importar una máquina virtual clonada en otro servidor para la activación.

Para importar una máquina virtual clonada

1. Compruebe que tiene acceso de red al servidor de host de destino.
2. Acceda a VMware VirtualCenter desde el servidor que alberga VMware ESX.
3. Seleccione la opción Importar y busque el servidor de destino, al tiempo que responde a los mensajes correspondientes.

   La acción de importación desplaza la máquina virtual clonada al servidor de destino. Si desea más información, puede consultar la documentación de VMware ESX.

Actualización de un servidor de CA Enterprise Log Manager clonado antes de la implementación

Emplee este procedimiento para actualizar un servidor de CA Enterprise Log Manager virtual clonado.

Un servidor de CA Enterprise Log Manager virtual clonado mantiene el nombre de host asignado durante la instalación. Sin embargo, el nombre de host de cada servidor de CA Enterprise Log Manager activo debe ser único dentro de la implementación de recopilación de registros. Por lo tanto, antes de activar un servidor virtual clonado, debe modificar el nombre de host y la dirección IP del servidor con el script *Rename_ELM.sh*.

El script de actualización lleva a cabo acciones que incluyen las siguientes:

- Detención y reinicio automático del agente predeterminado
- Detención y reinicio automático del servicio iGateway
- Solicitud de cambio del nombre de host, la dirección IP y la dirección IP DNS
- Actualización automática de archivos de configuración con contraseñas cifradas para los diversos certificados

Para actualizar un servidor de CA Enterprise Log Manager virtual

1. Inicie sesión en el servidor físico de destino como root.
2. Acceda a la imagen ISO de la aplicación o al DVD y vaya al directorio /CA/Linux_x86.

   También puede encontrar el script en el sistema de archivos de un servidor de CA Enterprise Log Manager instalado. El script se encuentra en el directorio opt/CA/LogManager.
3. Copie el script Rename_ELM.sh en el servidor de destino.
4. Cambie la información del servidor de CA Enterprise Log Manager virtual por el comando siguiente:

   ```
   ./Rename_ELM.sh
   ```
5. Responda a los mensajes.
6. Inicie la máquina virtual que contiene el servidor virtual actualizado.

Capítulo 9: Glosario

acceso a datos

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

Acceso de ODBC y JDBC

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

actualizaciones de contenido

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

actualizaciones de suscripción

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

acumulación de eventos

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

adaptadores de CA

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

agente

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

agente predeterminado

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

alerta de acción

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

almacén de usuarios

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

almacenamiento automático

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

almacenamiento de registro de eventos

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

almacenamiento de registro de eventos

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

almacenamiento de registros

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

análisis

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

análisis de archivos XMP

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

análisis de asignaciones

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

análisis de mensajes

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

análisis de registros

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

análisis de registros

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

archivo de análisis de mensajes (XMP)

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

archivos de asignación de datos (DM)

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

asignación de datos (DM)

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

asignaciones de función

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

asistente para el archivo de análisis

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

autenticación ssh no interactiva

La autenticación *no interactiva* permite que los archivos se desplacen de un servidor a otro sin tener que introducir una frase de contraseña para la autenticación. Configure la autenticación no interactiva del servidor de origen al servidor de destino antes de configurar el archivado automático o utilizar el script restore-ca-elm.sh.

base de datos en estado tibio

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

bases de datos archivadas

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

biblioteca de análisis de mensajes

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

biblioteca de consultas

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

biblioteca de informes

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

biblioteca de refinamiento de eventos

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

CA Enterprise Log Manager

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

CA IT PAM

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

CA Spectrum

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

CAELM

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

caelmadmin

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

caelmservice

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

calendario

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

CALM

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

calmTag

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

Campos de la gramática de eventos comunes

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

carpeta

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

catálogo

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

catálogo de archivos

Consulte catálogo.

categorías de eventos

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

certificados

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

cliente de suscripción

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

compatible con FIPS 140-2

Compatible con FIPS 140-2 es una designación para un producto que puede, *de forma opcional,* utilizar las bibliotecas y algoritmos criptográficos que cumplen con FIPS que se emplean para cifrar y descifrar datos confidenciales. CA Enterprise Log Manager es un producto de recopilación de registros compatible con FIPS debido a que se puede seleccionar si se desea ejecutar el programa en modo FIPS o en modo no FIPS.

complemento de eventos iTech

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

componentes de visualización

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

conector

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

configuración global

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

configuración guardada

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

consulta

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

consulta de acción

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

consulta de archivos

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

Contenido de los trap de SNMP

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

cuenta

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

Cumple con FIPS 140-2

Cumple con FIPS 140-2 es una designación para un producto que, de modo predeterminado, utiliza *solamente* algoritmos criptográficos certificados por un laboratorio de pruebas de módulos de cifrado. CA Enterprise Log Manager puede utilizar módulos criptográficos basados en el las bibliotecas certificadas RSA BSAFE Crypto-C ME y Crypto-J en modo FIPS, pero no lo puede hacer de forma predeterminada.

descongelación

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

Destinos de traps de SNMP

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

dispositivo de software

Un *dispositivo de software* es un paquete de software completamente funcional que contiene el software, el sistema operativo subyacente y todos los paquetes dependientes. Se instala sobre hardware proporcionado por el usuario final mediante el arranque del medio de instalación de la aplicación de software.

elementos de integración

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

enrutador de SAPI

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

entrada de registro

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

entrada de registro

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

estado caliente de base de datos

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

estado descongelado de base de datos

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

estado frío de base de datos

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

estados de la base de datos

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

etiqueta

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

event_action

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

event_category

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

event_class

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

evento autocontrolado

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

evento local

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

evento nativo

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

evento observado

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

evento refinado

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

evento registrado

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

evento remoto

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

evento RSS

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

evento sin formato

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

eventos

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

explorador de agentes

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

federación en malla

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

federación jerárquica

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

filtrado de eventos

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

filtro

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

filtro de acceso

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

filtro global

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

filtro local

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

FIPS 140-2

FIPS 140-2 equivale a los Estándares Federales de Procesamiento de la Información. Estos estándares federales especifican los requisitos de seguridad para los módulos criptográficos que se utilizan en los sistemas de seguridad que protegen información confidencial pero no clasificada. Estos estándares proporcionan cuatro niveles cualitativos de seguridad, diseñados para cubrir un amplio abanico de aplicaciones y entornos potenciales.

función Administrator

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

función Analyst

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

función Auditor

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

función del usuario

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

gestión de agentes

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

gestión de la titularidad

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

gestión de los registros de seguridad de equipos

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

gramática de eventos comunes (CEG)

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

grupo de agentes

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

grupo de aplicaciones

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

grupo de usuarios

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

grupo dinámico de usuarios

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

grupo global

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

ideal_model

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

identidad

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

informe

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

Informes relacionados con EPHI

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

Instalador

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

instancia de la aplicación

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

integración

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

lista de control de acceso de identidades

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

MIB (base de información gestionada)

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

MIB personalizada

Una *MIB personalizada* es una MIB creada para una alerta de acción que se envía a un destino de mensaje SNMP, como CA NSM. El ID del mensaje SNMP personalizado que se especifica en la alerta de acción presupone la existencia de una MIB personalizada que defina los campos de la gramática de eventos comunes seleccionados, que se envían como mensaje SNMP.

modo FIPS

El modo FIPS es el valor de configuración que requiere que los servidores y agentes de CA Enterprise Log Manager utilicen módulos criptográficos certificados por FIPS de RSA para el cifrado. El valor de configuración alternativo es el modo no FIPS.

modo no FIPS

Modo no FIPS es el valor de configuración predeterminado que permite que los servidores y agentes de CA Enterprise Log Manager utilicen una combinación de técnicas de cifrado, algunas de las cuales no cumplen con FIPS. El valor de configuración alternativo es el modo FIPS.

módulo (para descargar)

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

módulo de suscripción

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

NIST

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

nombre del usuario EiamAdmin

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

Objeto seguro

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

Objetos aplicación

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

OID (identificador de objeto)

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

origen de evento

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

perfil

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

Petición

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

política de acceso

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

política de acceso a la aplicación de CALM

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

política de ámbito

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

política de delegación

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

política de obligación

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

pozFolder

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

proceso de obtención de resultados de eventos/alertas

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

proceso de valores dinámicos

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

proxy de suscripción (en línea)

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

proxy de suscripción (predeterminado)

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

proxy de suscripción (sin conexión)

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

proxys de suscripción (para actualizaciones de contenido)

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

proxys de suscripción (para el cliente)

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

punto de recopilación

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

recatalogación

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

recopilación de eventos

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

recopilación directa de registros

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

recopilador de SAPI

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

recurso de la aplicación

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

recurso global

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

refinamiento de eventos

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

registro

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

registros de auditoría

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

reglas de resumen

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

reglas de supresión

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

reglas de transferencia de eventos

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

SAPI recorder

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

sensor de registro

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

servicios

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

servidor de alertas

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

servidor de almacenamiento remoto

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

servidor de gestión

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

servidor de informes

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

servidor de informes

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

Servidor de ODBC

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

servidor de punto de restauración

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

servidor de recopilación

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

servidor de suscripciones de CA

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

servidor proxy HTTP

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

servidores de federación

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

SNMP

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

supresión

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

token de análisis de mensajes (ELM)

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

URL de fuente RSS para alertas de acción

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

URL de fuente RSS para suscripción

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

URL para CA Embedded Entitlements Manager

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

URL para CA Enterprise Log Manager

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

usuario de EEM

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

usuario de la aplicación

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

usuario global

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

utilidad LMArchive

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

utilidad LMSEOSImport

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

utilidad scp

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

valores de clave

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

varbind

Una *varbind* es un enlace variable SNMP. Cada varbind se constituye de un OID, un tipo, y un valor. Las varbinds se agregan a las MIB personalizadas.

Índice

E

F

G

H

I

P

R

S

T

U