CA Embedded Entitlements Manager

Guía de procedimientos iniciales

r8.4 SP3

Esta documentación y todos los programas informáticos de ayuda relacionados (en adelante, "Documentación") se ofrecen exclusivamente con fines informativos, pudiendo CA proceder a su modificación o retirada en cualquier momento.

Queda prohibida la copia, transferencia, reproducción, divulgación, modificación o duplicación de la totalidad o parte de esta Documentación sin el consentimiento previo y por escrito de CA. Esta Documentación es información confidencial, propiedad de CA, y no puede ser divulgada por Vd. ni puede ser utilizada para ningún otro propósito distinto, a menos que haya sido autorizado en virtud de un acuerdo de confidencialidad suscrito aparte entre Vd. y CA.

No obstante lo anterior, si dispone de licencias de los productos informáticos a los que se hace referencia en la Documentación, Vd. puede imprimir un número razonable de copias de la Documentación, exclusivamente para uso interno de Vd. y de sus empleados, uso que deberá guardar relación con dichos productos. En cualquier caso, en dichas copias deberán figurar los avisos e inscripciones relativos a los derechos de autor de CA.

El derecho a realizar copias de la Documentación está sujeto al plazo de vigencia durante el cual la licencia correspondiente a los productos informáticos esté en vigor. En caso de terminarse la licencia por cualquier razón, Vd. es el responsable de certificar por escrito a CA que todas las copias, totales o parciales, de la Documentación, han sido devueltas a CA o, en su caso, destruidas.

EN LA MEDIDA EN QUE LA LEY APLICABLE LO PERMITA, CA PROPORCIONA ESTA DOCUMENTACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO INCLUIDAS, ENTRE OTRAS PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN CONCRETO Y NO INCUMPLIMIENTO. CA NO RESPONDERÁ EN NINGÚN CASO NI ANTE EL USUARIO FINAL NI ANTE NINGÚN TERCERO EN CASOS DE DEMANDAS POR PÉRDIDAS O DAÑOS, DIRECTOS O INDIRECTOS, DERIVADOS DEL USO DE ESTA DOCUMENTACIÓN, INCLUYENDO, ENTRE OTRAS PERO SIN LIMITARSE A ELLAS, LA PÉRDIDA DE BENEFICIOS Y DE INVERSIONES, LA INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL, LA PERDIDA DE PRESTIGIO O DE DATOS, INCLUSO CUANDO CA HUBIERA PODIDO SER ADVERTIDA EXPRESAMENTE DE LA POSIBILIDAD DE DICHA PÉRDIDA O DAÑO.

El uso de cualquier producto informático al que se haga referencia en la documentación se regirá por el acuerdo de licencia aplicable. Los términos de este aviso no modifican, en modo alguno, dicho acuerdo de licencia.

CA es el fabricante de este Documentación.

Esta Documentación presenta "Derechos Restringidos". El uso, la duplicación o la divulgación por parte del gobierno de los Estados Unidos está sujeta a las restricciones establecidas en las secciones 12.212, 52.227-14 y 52.227-19(c)(1) - (2) de FAR y en la sección 252.227-7014(b)(3) de DFARS, según corresponda, o en posteriores.

Copyright © 2010 CA. Todos los derechos reservados. Todas las marcas registradas, nombres comerciales, marcas de servicio y logotipos a los que se haga referencia en la presente documentación pertenecen a sus respectivas compañías

Referencias a productos de CA

Este documento hace referencia a los siguientes productos de CA:

- CA® Embedded Entitlements Manager (CA EEM)
- CA® Directory
- CA® SiteMinder® Web Access Manager (CA SiteMinder)
- CA® Identity Manager
- CA® Security Command Center
- CA® Integrated Threat Management
- CA® Enterprise Log Manager

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.

Contenido

Capítulo 1: Introducción

Esta sección contiene los siguientes temas:

Información general

Gracias a CA Embedded Entitlements Manager (CA EEM), las aplicaciones pueden compartir servicios comunes de autorización, autenticación y gestión de políticas de acceso.

Funciones

CA EEM pone a disposición del usuario un conjunto de servicios de seguridad. Entre éstos, se encuentran los siguientes:

- Servicios de configuración:
  - Registro y anulación del registro de instancias de aplicación
  - Definición del ámbito administrativo de los Administrators de aplicaciones
  - Delegación de derechos administrativos
  - Gestión de usuarios y grupos
- Servicios de seguridad de la administración:
  - Gestión de políticas de obligación, evento y acceso
  - Gestión de calendarios
- Servicios de seguridad en tiempo de ejecución:
  - Autenticación de los usuarios
  - Autorización del acceso
  - Registro de los eventos de seguridad

Características

CA EEM se compone de las siguientes características:

Generales

- Gracias al aislamiento de políticas, cada una de las instancias de aplicación registrada dispone de su propio espacio para almacenar los datos específicos de la misma.
- SDK de tiempo de ejecución disponible para Java, C++ y C#.
- SDK administrativo disponible para Java, C++ y C#.
- Compatibilidad con la interfaz de línea de comandos para funciones administrativas (insertar, modificar o quitar objetos):
  - Importación y exportación de XML
  - Comprobaciones en tiempo de ejecución
  - Herramientas de migración
- Compatibilidad con interfaces Web para el acceso independiente y de ejecución en contexto.
- Comunicaciones HTTP seguras.
- Integración con CA Security Command Center y CA Audit para hacer posible la gestión de los eventos de seguridad.
- Integración con CA SiteMinder para recuperar información concerniente a los grupos y usuarios del almacén de datos de CA SiteMinder.

Gestión de identidades

- Usuarios globales y atributos compartidos por todas las aplicaciones.
- Compatibilidad con distintos modos para los usuarios globales:
  - Usuarios globales internos, cuyas funciones se completan con la gestión de políticas de contraseñas
  - Usuarios globales externos de los servidores de directorios LDAP
  - Usuarios globales externos de CA Identity Manager
- Integración con CA Identity Manager para brindar una gestión y configuración de los usuarios basadas en funciones.
- Compatibilidad con la importación y exportación de sesiones transportables para el inicio de sesión único.

Gestión del acceso

- En la gestión del acceso se incluyen tanto las listas de control de acceso como las políticas de empresa.
- El lenguaje de políticas permite utilizar atributos de usuario, sesión, entorno y recurso a la hora de tomar las decisiones de las políticas.

- Ámbito administrativo integrado de todos los objetos.
- Compatibilidad integrada con la administración delegada.
- Compatibilidad integrada con comprobaciones de obligaciones personalizadas que requieran acciones específicas de la aplicación:
  - Evaluación en proceso local de las comprobaciones de permisos
  - SDK e interfaz Web para definir políticas de acceso, listas de control de acceso, políticas de ámbito administrativo y autoridad delegada

Acceso del cliente

Es posible obtener acceso al servidor de CA EEM mediante interfaces Web estándar y de servicios Web capaces de integrar productos de terceros, sin necesidad de contar con el módulo del cliente. Las interfaces son:

- HTML e iTechnology para la configuración y administración
- iTechnology para el suministro de eventos de CA Audit

iTechnology es una tecnología de CA basada en estándares Web, como HTTP, HTTPS, HTML, XML y SSL. Proporciona un marco de trabajo para crear e implantar servicios Web en Internet.

Compatibilidad con almacenes de datos

CA EEM permite identificar un origen único de usuario externo, como Microsoft Active Directory. CA EEM almacena tanto su configuración como sus políticas en CA Directory, con independencia de dónde se hayan almacenado los objetos de usuario.

Capítulo 2: Instalación en Windows

Esta sección contiene los siguientes temas:

Información general de la instalación

Para instalar CA EEM en entornos operativos Windows, deben instalarse las siguientes aplicaciones:

Servidor de CA EEM

Puede utilizar el servidor de CA EEM para definir políticas de autorización con respecto a los recursos de las aplicaciones mediante una interfaz Web. La interfaz administrativa basada en la Web le permite gestionar políticas de acceso e identidades. La infraestructura de seguridad existente se utiliza para implantar reglas en virtud de la lógica empresarial, mediante recursos y atributos del usuario, definidas en almacenes centralizados de usuarios y otros sistemas empresariales.

Kit de desarrollo de software (SDK) de CA EEM

Puede utilizar el SDK de CA EEM para integrar controles de seguridad basados en identidades en las aplicaciones. El SDK consta de bibliotecas, clases de java, archivos de encabezado y un tutorial. Puede utilizar el SDK para implementar CA EEM en cualquier aplicación. Para obtener más información acerca de cómo implementar CA EEM mediante el SDK, consulte la *Guía de programación*.

Cada una de estas aplicaciones se instala por separado y su funcionamiento es independiente del resto.

Instalación del servidor

El servidor de CA EEM puede instalarse mediante el asistente de instalación o la línea de comandos. Use la línea de comandos para instalar CA EEM en el modo silencioso, y el asistente de instalación si desea efectuar una instalación interactiva.

JRE ya no constituye un requisito mínimo para la instalación y el uso de CA EEM. Es posible instalar y usar CA EEM tanto con JRE como sin él. Si opta por instalar CA EEM sin que JRE se incluya como requisito mínimo, deberá omitir la pantalla correspondiente a la selección de la ruta de JRE del asistente de instalación. Si opta por instalar el servidor de CA EEM en modo silencioso sin JRE, tendrá que usar el parámetro javahome con el valor "None".

En las secciones siguientes, se expone cómo instalar el servidor de CA EEM.

Más información

Cómo omitir la pantalla de selección de la ruta de JRE en el asistente de instalación (en la página 15)
Lista de verificación para la configuración del asistente (en la página 14)
Instalación del servidor mediante el asistente de instalación (en la página 16)
Instalación del servidor de CA EEM en modo silencioso (en la página 23)

Lista de verificación para la configuración del asistente

En el curso de la instalación del servidor de CA EEM en Windows, necesitará la siguiente información:

Campo	Valor
Ruta de instalación de CA EEM	Ubicación del equipo en el que se desea instalar CA EEM.
Ruta de instalación de JRE	Ubicación del equipo correspondiente a la instalación de JRE. **Nota**: Si desea instalar y usar CA EEM sin JRE, deberá definir la variable javahome como None en la línea de comandos antes de ejecutar el asistente de instalación de CA EEM.
Contraseña de EiamAdmin	La contraseña asociada al Administrator EiamAdmin de CA EEM.
Backup Directory (Directorio de copia de seguridad)	La ubicación del equipo en la que pretende crear una copia de seguridad de los archivos correspondientes a una instalación anterior de

Campo	Valor
	CA EEM. **Nota:** Sólo necesitará esta información si actualiza una versión anterior de CA EEM a la actual.

Cómo omitir la pantalla de selección de la ruta de JRE en el asistente de instalación

JRE ya no constituye un requisito mínimo para la instalación y el uso de CA EEM. Si desea instalar CA EEM sin JRE, debe llevar a cabo los siguientes pasos:

1. Defina el parámetro javahome como "None".

   Nota: Al definir el parámetro javahome como "None", el asistente de instalación no mostrará la pantalla de selección de la ruta de Java.

2. Instale CA EEM mediante el asistente de instalación.

Definición del parámetro javahome

Debe configurarse el parámetro javahome con el valor "none" antes de usar el asistente de instalación para instalar CA EEM. Para definir el parámetro javahome desde la línea de comandos, escriba lo siguiente:

EEMServer_*[version number]*_win32.exe -s -a /z"javahome=None; "

Instalación del servidor mediante el asistente de instalación

El asistente de instalación del servidor de CA EEM le guiará a lo largo del proceso de instalación y le proporcionará las opciones adecuadas para definir los parámetros necesarios de dicho proceso.

Para instalar el servidor de CA EEM

1. Realice una de las siguientes acciones:
   - Abra el Explorador de Windows y haga doble clic en el paquete de instalación EEMServer_[*númeroversión*].[*número_compilación*]_win32.exe en el equipo de destino.
   - Escriba el comando siguiente en el símbolo del sistema usando los parámetros de instalación:

     EEMServer_*[númeroversión].[número_compilación]*_win32.exe -s -a /z "eiampath=*<Ruta de instalación personalizada para CA EEM>*; etdirpath=*<Ruta de instalación personalizada para CA Directory>*; igpath=*<Ruta de instalación personalizada para iGateway>*;"

     Puede especificar una ruta de instalación personalizada mediante los parámetros de instalación. Para obtener más detalles acerca de los parámetros de instalación, consulte el apartado Parámetros de instalación del servidor.

     Aparecerá el asistente de instalación.
2. Siga las instrucciones del asistente de la instalación para completar esta última.

Más información:

Cómo omitir la pantalla de selección de la ruta de JRE en el asistente de instalación (en la página 15)

Actualización del servidor

Puede actualizar la instalación existente del servidor de CA EEM a la versión actual.

Para actualizar una instalación existente del servidor de CA EEM

1. Ejecute el archivo EEMServer_<version number>_win32.exe en el equipo de destino.
2. En función de la versión del servidor de CA EEM que tenga instalada, tendrá lugar una de las siguientes situaciones:
   - Si la versión existente del servidor de CA EEM es anterior a la que está instalando, el asistente de instalación creará una copia de seguridad de la primera y efectuará una actualización automática a la más reciente.
   - Si la versión existente del servidor de CA EEM es la misma que la que está instalando, el asistente de instalación le preguntará si desea desinstalar el servidor de CA EEM. Puede desinstalar y volver a instalar el servidor de CA EEM.
   - Si la versión que está instalando es anterior a la existente, el asistente de instalación mostrará un error y finalizará el proceso.

Con la actualización del servidor de CA EEM, se actualizan los siguientes elementos:

- El servidor de CA EEM de la carpeta \\CA\SharedComponents\iTechnology
- iGateway
- CA Directory

También, todos los certificados de P12 se migran a certificados PEM.

Más información:

Lista de verificación para la configuración del asistente (en la página 14)
Instalación del servidor mediante el asistente de instalación (en la página 16)

Inicio del servidor

Debe iniciar el servidor de CA EEM para gestionar las identidades y las políticas de acceso de las aplicaciones registradas.

Para empezar a usar el servidor de CA EEM

1. Realice una de las siguientes acciones:
   - En el explorador, escriba la dirección URL https://*nombrehost* o *direcciónip*:5250/spin/eiam. Si se encuentra en el equipo del servidor de CA EEM, especifique http://*hostlocal*:/5250/spin/eiam.
   - Seleccione Inicio, Programas, CA, Embedded Entitlements Manager y UI de EEM en los entornos operativos Windows.

     Aparecerá una página de inicio de sesión.
2. Escriba la información siguiente en el cuadro de diálogo de inicio de sesión:
   a. En el menú desplegable Aplicación, seleccione una instancia de aplicación que haya registrado. El valor predeterminado es <Global>. Nota: El nombre de usuario predeterminado del Administrator es EiamAdmin.

      Nota: Puede agregar otros usuarios globales para el inicio de sesión y establecer sus nombres de usuario en función de sus preferencias.
   b. Escriba la contraseña. Esta contraseña debe coincidir con la especificada para EiamAdmin en el curso de la instalación del servidor de CA EEM.
   c. Si desea iniciar la próxima sesión en el servidor de CA EEM con la misma configuración, seleccione Recordar mi configuración.
3. Haga clic en Iniciar sesión.

   Aparecerá la página inicial de la interfaz de CA EEM. Para obtener más información acerca de cómo usar el servidor de CA EEM, consulte la *Ayuda en línea*.

Cómo activar la accesibilidad en el servidor de CA EEM

Las funciones de accesibilidad del servidor de CA EEM permiten a los usuarios, sin tener en cuenta la capacidad, el uso de los productos de manera correcta y la compatibilidad con la documentación para lograr tareas de negocio vitales. Cuando se activa la accesibilidad, los usuarios pueden lograr tareas de negocio vitales únicamente mediante el teclado o el lector de pantalla.

Para activar la accesibilidad

1. A continuación, realice una de las siguientes acciones:
   - En el explorador, escriba la dirección URL https://*nombrehost* o *direcciónip*:5250/spin/eiam. Si se encuentra en el equipo del servidor de CA EEM, especifique http://*hostlocal*:/5250/spin/eiam.
   - Seleccione Inicio, Programas, CA, Embedded Entitlements Manager y UI de EEM en los entornos operativos Windows.

     Aparecerá una página de inicio de sesión.
2. Escriba la información siguiente en el cuadro de diálogo de inicio de sesión:
   a. En el menú desplegable Aplicación, seleccione una instancia de aplicación que haya registrado. El valor predeterminado es <Global>. Nota: El nombre de usuario predeterminado del Administrator es EiamAdmin.

      Nota: Puede agregar otros usuarios globales para el inicio de sesión y establecer sus nombres de usuario en función de sus preferencias.
   b. Escriba la contraseña. Esta contraseña debe coincidir con la especificada para EiamAdmin en el curso de la instalación del servidor de CA EEM.
   c. Si desea iniciar la próxima sesión en el servidor de CA EEM con la misma configuración, seleccione Recordar mi configuración.
3. Haga clic en Activar accesibilidad.

   La accesibilidad se activa en la interfaz gráfica de usuario de CA EEM.
4. Haga clic en Inicio de sesión.

   Aparecerá la página inicial de la interfaz de CA EEM.

Eliminación del servidor

El servidor de CA EEM puede desinstalarse mediante la opción Agregar o quitar programas del Panel de control.

Nota: Si hay alguna aplicación registrada en CA EEM, no podrá eliminar el servidor de CA EEM. Debe eliminar las aplicaciones del registro antes de desinstalar el servidor de CA EEM. Para obtener más información acerca de cómo eliminar una aplicación del registro, consulte la *Ayuda en línea*.

Instalación del SDK

El asistente de instalación del SDK de CA EEM le guiará a lo largo del proceso de instalación.

Para instalar el SDK de CA EEM

1. Abra el Explorador de Windows y haga doble clic en el paquete de instalación EEMSDK_<version number>_win32.exe, o ejecute el archivo de instalación desde el símbolo del sistema.

   Aparecerá el asistente de instalación.

2. Pulse el botón Acepto para aceptar los Términos y condiciones.

   Nota: El botón Acepto se activa únicamente después de haber leído el texto de los Términos y condiciones, o tras haberse desplazado por él.

   Aparecerá el cuadro de diálogo Seleccionar ubicación de destino. De forma predeterminada, el asistente de instalación instala el SDK de CA EEM en la siguiente ubicación: C:\Program Files\CA\Embedded IAM SDK.

3. Haga clic en Siguiente.

   Or

   Haga clic en Explorar, seleccione el directorio de su equipo en el que desee instalar el SDK de CA EEM y, a continuación, haga clic en Siguiente.

   Con ello, comenzará a instalarse el SDK de CA EEM.

4. Haga clic en Finalizar.

   Tras ello, el SDK de CA EEM ya estará instalado.

   Nota: Durante la instalación se crea una variable de entorno %EIAM_SDK% que dirige a la ruta de instalación Utilice esta variable en la ruta del explorador para abrir la carpeta de instalación.

Inicio del SDK

Para iniciar el SDK de CA EEM, haga clic en Inicio, Programas, CA, Embedded Entitlements Manager y SDK de EEM.

Aparecerá la ventana de la documentación del SDK de CA EEM.

Eliminación del SDK

El SDK de CA EEM puede desinstalarse mediante la opción Agregar o quitar programas del Panel de control.

Parámetros de instalación del servidor

Durante la instalación de CA EEM en Windows, deberá recopilar información relacionada con los siguientes parámetros de la línea de comandos:

-eiampath

Especifica la ruta en la que se instalará el servidor de CA EEM. La ruta predeterminada es C:\Archivos de programa \CA\SharedComponents\Embedded IAM.

-etdirpath [ruta]

Especifica la ruta en la que se instalará CA Directory. La ruta predeterminada es C:\Program Files\CA\Directory.

-igpath [path]

Especifica la ruta en la que se instalará iGateway. La ruta predeterminada es C:\Program Files\CA\SharedComponents\iTechnology.

backupdir

Especifica la ubicación en la que se creará la copia de seguridad de los datos correspondientes a la instalación existente.

-capkiinstalldir

Especifica la ruta de la carpeta de instalación para el módulo de CAPKI. La ruta predeterminada es C:\Archivos de programa\CA\SC\CAPKI.

-javahome [directorio]

Asigna el valor de [directorio] a la variable JAVA_HOME al llamar al instalador de iGateway. El instalador de CA EEM le solicitará la configuración de la variable aunque ya se haya configurado. Este parámetro no tiene un valor predeterminado.

Nota: Si desea instalar CA EEM sin Java, deberá definir el parámetro javahome como Ninguno.

CA EEM usa los siguientes parámetros durante la instalación de CA Directory. Podrá configurar los parámetros en función de sus necesidades.

Importante: Antes de personalizar los números de puerto predeterminados, asegúrese de que ningún otro servicio está configurado para usar los mismos puertos.

-dxadminport

Especifica el puerto en el cual DXadmind está a la escucha de solicitudes de DXmanager. Este puerto se usa para la comunicación de LDAP entre DXadmind y DXmanager. *DXadmind* es un proceso básico que se ejecuta en todos los host que contienen DSA. DXmanager utiliza DXadmind para comunicarse con los DSA.

Valor predeterminado: 2123

-dsaport

Especifica el puerto que usa DSA para atender las solicitudes dirigidas a él.

Predeterminado: 509

-ssldport

Especifica el puerto que usa CA Directory para atender al servidor SSLD. El servidor SSLD constituye un proceso que se ejecuta en segundo plano, y que controla la autenticación, el cifrado y descifrado SSL y TLS para CA Directory.

Predeterminado: 21847

-routerport

Especifica el puerto que usa DSA para conectarse al DSA de enrutador. Un DSA de enrutador no cuenta con datos locales ni con almacenes de datos. Tan sólo puede enrutar el tráfico a otros DSA.

Predeterminado: 1684

-dxdbsize

Especifica el tamaño máximo del almacén de datos para CA EEM.

Predeterminado: 500 MB

-dxuser

Especifica un usuario que, sin ser DSA, puede instalar, administrar y desinstalar CA Directory. El dxuser puede ser un usuario de la red o del sistema local.

Nota: Si ha instalado CA Directory usando, para ello, un usuario del sistema local como dxuser, es posible que dicho usuario se elimine durante la desinstalación. Por lo tanto, si usa un usuario del sistema local como dxuser para instalar CA Directory, asegúrese de que el usuario en cuestión no esté configurado para ejecutar ningún otro programa.

Nota: En un equipo con Microsoft Windows Server 2003, las cadenas del símbolo del sistema pueden tener una longitud máxima de 8.191 caracteres. Con Microsoft Windows 2000, las cadenas del símbolo del sistema pueden tener una longitud máxima de 2.047 caracteres. Para obtener más información acerca de la longitud de los comandos de InstallShield, consulte las *Notas de la versión*.

Instalación del servidor de CA EEM en modo silencioso

Para instalar el servidor de CA EEM en el modo silencioso, debe llevar a cabo dos tareas:

1. Crear el archivo de respuesta
2. Ejecutar el comando especificando el archivo de respuesta

   Durante la instalación silenciosa, se crea un archivo de registro eiaminstall.log en el que se recogen los errores de instalación que se hayan podido producir.

Nota: Si instala el servidor de CA EEM en modo silencioso, también podrá usar este último para quitarlo.

Creación del archivo de respuesta

Puede registrar los datos de la instalación en un archivo de respuesta; éste se utilizará para efectuar la instalación silenciosa del servidor de CA EEM. Es necesario crear un archivo de respuesta nuevo por cada compilación que desee instalar.

Para crear un archivo de respuesta

1. Ejecute el paquete de instalación del servidor de CA EEM en el equipo de destino.
2. Cuando aparezca la pantalla de símbolo del sistema, introduzca el siguiente comando para crear un archivo de respuesta en el directorio especificado.

   EEMServer_[*númeroversión*].[*número_compilación*]_win32.exe -s -a /r /f1"*nombre de la ruta del archivo de respuesta*"

   Ejemplo:

   EEMServer_8.4.0.55_win32.exe -s -a /r /f1"c:\resp.iss"
3. Introduzca los valores que desee asignar a los parámetros de instalación. Tales valores quedarán almacenados en el archivo de respuesta.

Ejecución del comando especificando el archivo de respuesta

Los ejemplos siguientes muestran las opciones disponibles para realizar una instalación en modo silencioso:

- Para instalar el servidor de CA EEM en modo silencioso, escriba el siguiente comando en el símbolo del sistema:

  EEMServer_[*númeroversión*].[*número_compilación*]_win32.exe -s -a /s /f1"*nombre de la ruta del archivo de respuesta*"

  Ejemplo:

  EEMServer_8.4.0.55_win32.exe -s -a /s /f1"c:\resp.iss"

- Para crear un archivo de registro de instalación durante la instalación en modo silencioso, escriba el comando siguiente en el símbolo del sistema:

  EEMServer_[*númeroversión*].[*número_compilación*]_win32.exe -s -a /s /v"/qn /L*v <ruta para crear archivo de registro>" /f1"*nombre de la ruta del archivo de respuesta*"

  Ejemplo:

  EEMServer_8.4.0.55_win32.exe -s -a /s /v"/qn /L*v c:\install.txt" /f1"c:\resp.iss"

Con ello, el servidor de CA EEM se instalará en modo silencioso, usando, para tal fin, el archivo de respuesta especificado.

Nota: Puede proporcionar los parámetros de instalación junto con la secuencia de comandos de instalación. Para obtener más detalles acerca de los parámetros, consulte el apartado Parámetros de instalación del servidor.

Eliminación del servidor de CA EEM en modo silencioso

Para poder quitar el producto, debe utilizar un archivo de respuesta creado con un servidor de CA EEM con el mismo número de compilación. Para quitar el servidor de CA EEM en modo silencioso, escriba el siguiente comando en el símbolo del sistema:

EEMServer_[*númeroversión*].[*número_compilación*]_win32.exe -s -a /s /f1"*nombre de la ruta del archivo de respuesta*" /z"uninstall"

Ejemplo:

EEMServer_8.4.0.55_win32.exe -s -a /s /f1"c:\resp.iss" /z"uninstall"

Con ello, se quitará el servidor de CA EEM en modo silencioso.

Nota: Si hay alguna aplicación registrada en CA EEM, no podrá eliminar el servidor de CA EEM. Debe eliminar las aplicaciones del registro antes de desinstalar el servidor de CA EEM. Para obtener más información acerca de cómo eliminar una aplicación del registro, consulte la *Ayuda en línea*.

Capítulo 3: Instalación en Linux y UNIX

Esta sección contiene los siguientes temas:

Información general de la instalación

Para instalar CA EEM en los entornos operativos Linux y UNIX, se deben instalar las aplicaciones siguientes:

Servidor de CA EEM

Puede utilizar el servidor de CA EEM para definir políticas de autorización con respecto a los recursos de las aplicaciones mediante una interfaz Web. La interfaz administrativa basada en la Web le permite gestionar políticas de acceso e identidades. La infraestructura de seguridad existente se utiliza para implantar reglas en virtud de la lógica empresarial, mediante recursos y atributos del usuario, definidas en almacenes centralizados de usuarios y otros sistemas empresariales.

Kit de desarrollo de software (SDK) de CA EEM

Puede utilizar el SDK de CA EEM para integrar controles de seguridad basados en identidades en las aplicaciones. El SDK consta de bibliotecas, clases de java, archivos de encabezado y un tutorial. Puede utilizar el SDK para implementar CA EEM en cualquier aplicación. Para obtener más información acerca de cómo implementar CA EEM mediante el SDK, consulte la *Guía de programación*.

Cada una de estas aplicaciones se instala por separado y su funcionamiento es independiente del resto.

Instalación del servidor

El servidor de CA EEM para Linux y UNIX utiliza una secuencia de comandos shell autoextraíble que le guiará durante el proceso de instalación. En el proceso de instalación, la secuencia de comandos muestra la información relativa a las licencias y solicita los parámetros de instalación. Tras introducir los parámetros de instalación, ésta dará comienzo.

Para instalar el servidor de CA EEM para Linux y UNIX

1. Ejecute la secuencia de comandos de instalación EEMServer_[*númeroversión*].[*número_compilación*]_[*nombre del sistema operativo*].sh en el equipo de destino.

   Ejemplo:

   EEMServer_8.4.0.55_sunos.sh

   El archivo se descomprime y comienza el proceso de instalación.

2. Escriba Y para aceptar los términos y condiciones del contrato de licencia (o N para rechazarlos e interrumpir la instalación).

   La secuencia de comandos solicita los parámetros de instalación.

3. Introduzca los parámetros de instalación.

   Nota: Para obtener más información acerca de los parámetros de instalación disponibles, consulte el apartado Parámetros de la secuencia de comandos de instalación del servidor.

   Ejemplo:

   a. Especifique la ruta de instalación del servidor de CA EEM (o acepte el valor predeterminado).

   Se mostrará una pantalla de confirmación con los valores que haya especificado para los parámetros de instalación.

4. Introduzca Y para continuar con el proceso de instalación, siempre que la información de la pantalla de confirmación sea correcta (si introduce N, saldrá del instalador).

5. Introduzca la contraseña de EiamAdmin.

   Nota: El nombre de usuario predeterminado del Administrator es EiamAdmin.

   El procedimiento de la instalación depende de los parámetros de la línea de comandos y del tipo de paquete del servidor de CA EEM que se esté instalando.

   La secuencia de comandos del instalador completará la instalación del servidor de CA EEM en el equipo.

Actualización del servidor

Puede actualizar la instalación existente del servidor de CA EEM a la versión actual.

Para actualizar una instalación existente del servidor de CA EEM

1. Ejecute EEMServer_[*númeroversión*].[*número_compilación*]_[*nombre del sistema operativo*] en el equipo de destino.
2. En función de la versión del servidor de CA EEM que tenga instalada, tendrá lugar una de las siguientes situaciones:
   - Si la versión existente del servidor de CA EEM es anterior a la que está instalando, el asistente de instalación la actualizará automáticamente a la nueva versión.
   - Si la versión existente del servidor de CA EEM es la misma que la que está instalando, el asistente de instalación le preguntará si desea desinstalar el servidor de CA EEM. Puede desinstalar y volver a instalar el servidor de CA EEM.
   - Si la versión que está instalando es anterior a la existente, el asistente de instalación mostrará un error y finalizará el proceso.

   Para obtener más información acerca de cómo instalar el servidor de CA EEM, consulte el apartado Instalación del servidor (en la página 28).

Con la actualización del servidor de CA EEM, se actualizan los siguientes elementos:

- El servidor de CA EEM de la carpeta \\CA\SharedComponents\iTechnology
- iGateway
- CA Directory

Eliminación del servidor

Para quitar el servidor de CA EEM, ejecute la secuencia de comandos eiamuninstall.sh desde el directorio de la instalación.

Nota: Si hay alguna aplicación registrada en CA EEM, no podrá eliminar el servidor de CA EEM. Debe eliminar las aplicaciones del registro antes de desinstalar el servidor de CA EEM. Para obtener más información acerca de cómo eliminar una aplicación del registro, consulte la *Ayuda en línea*.

Instalación del SDK

El SDK de CA EEM para Linux y UNIX utiliza una secuencia de comandos shell autoextraíble que le guiará durante el proceso de instalación. En el proceso de instalación, la secuencia de comandos muestra la información sobre licencias y solicita los parámetros de instalación. Tras introducir los parámetros de instalación, ésta dará comienzo.

Para instalar el SDK de CA EEM para Linux y UNIX

1. Ejecute la secuencia de comandos de instalación EEMSDK_[*númeroversión*].[*número_compilación*]_[*nombre del sistema operativo*].sh en el equipo de destino.

   Ejemplo:

   EEM_8.4.0.55_sunos.sh

   El archivo se descomprime y comienza el proceso de instalación.

2. Escriba Y para aceptar los términos y condiciones del contrato de licencia (o N para rechazarlos e interrumpir la instalación).
3. Especifique la ruta de instalación del SDK de CA EEM (o acepte el valor predeterminado).
4. Seleccione la opción correspondiente a la instalación del producto.

   Con ello, el SDK de CA EEM se instalará en el equipo.

Inicio del SDK de CA EEM

Para iniciar el SDK de CA EEM, abra en su explorador Web /opt/CA/eIAMSDK/Doc/index.html (o la ubicación correspondiente a la instalación del SDK de CA EEM).

Eliminación del SDK

Puede eliminar el SDK de CA EEM de los sistemas operativos Linux y UNIX.

Para quitar el SDK de CA EEM

1. Ejecute la secuencia de comandos de instalación EEMSDK_[*númeroversión*].[*número_compilación*]_[*nombre del sistema operativo*].sh en el equipo de destino.

   Ejemplo:

   EEM_8.4.0.55_sunos_linux.sh

   El archivo se descomprime.

2. Seleccione la opción correspondiente a la desinstalación o eliminación del producto.

   La secuencia de comandos de instalación quitará el SDK de CA EEM de su equipo.

Parámetros de la secuencia de comandos de instalación del servidor

En el curso de la instalación de CA EEM, tendrá que recopilar información acerca de los siguientes parámetros de la línea de comandos, puesto que la secuencia de comandos la solicitará.

La secuencia de comandos acepta los siguientes parámetros de línea de comandos:

backupdir

Especifica la ubicación en la que se creará la copia de seguridad de los datos correspondientes a la instalación existente.

-capkiinstalldir

Especifica la ruta de la carpeta de instalación para el módulo de CAPKI.

Valor predeterminado: /opt/CA/SharedComponents/capki

CA EEM usa los siguientes parámetros durante la instalación de CA Directory. Podrá configurar los parámetros en función de sus necesidades.

Importante: Antes de personalizar los números de puerto predeterminados, asegúrese de que ningún otro servicio está configurado para usar los mismos puertos.

-dxadminport

Especifica el puerto en el cual DXadmind está a la escucha de solicitudes de DXmanager. Este puerto se usa para la comunicación de LDAP entre DXadmind y DXmanager. *DXadmind* es un proceso básico que se ejecuta en todos los host que contienen DSA. DXmanager utiliza DXadmind para comunicarse con los DSA.

valor predeterminado: 2123

-dsaport

Especifica el puerto que usa DSA para atender las solicitudes dirigidas a él.

Predeterminado: 509

-ssldport

Especifica el puerto que usa CA Directory para atender al servidor SSLD. El servidor SSLD constituye un proceso que se ejecuta en segundo plano, y que controla la autenticación, el cifrado y descifrado SSL y TLS para CA Directory.

Predeterminado: 21847

-routerport

Especifica el puerto que usa DSA para conectarse al DSA de enrutador. Un DSA de enrutador no cuenta con datos locales ni con almacenes de datos. Tan sólo puede enrutar el tráfico a otros DSA.

Predeterminado: 1684

-dxdbsize

Especifica el tamaño máximo del almacén de datos para CA EEM.

Predeterminado: 500 MB

-dxuser

Especifica un usuario que, sin ser DSA, puede instalar, administrar y desinstalar CA Directory. El dxuser puede ser un usuario de la red o del sistema local.

Nota: Si ha instalado CA Directory usando, para ello, un usuario del sistema local como dxuser, es posible que dicho usuario se elimine durante la desinstalación. Por lo tanto, si usa un usuario del sistema local como dxuser para instalar CA Directory, asegúrese de que el usuario en cuestión no esté configurado para ejecutar ningún otro programa.

-eiamadminpw [contraseña]

Establece el valor de [contraseña] como la contraseña de EiamAdmin.

-eiampath

Determina la ruta en la que se instalará el servidor de CA EEM. Su valor predeterminado es /opt/CA/SharedComponents/EmbeddedIAM.

-etdirpath [ruta]

Determina la ruta en la que se instalará CA Directory.

-igpath [directorio]

Establece la ruta de iGateway. Debe ser una ruta completa, como -iisystem. Su valor predeterminado es /opt/CA/SharedComponents/iTechnology.

-javahome [directorio]

Establece JAVA_HOME. De forma predeterminada, este parámetro conduce al contenido de la variable de entorno JAVA_HOME, y sólo se solicita si no se configura el valor $JAVA_HOME.

Nota: Si desea instalar CA EEM sin Java, tendrá que definir el parámetro javahome=none. Esto no es aplicable a HP-UX.

-logfile [nombrearchivo]

Hace que el instalador escriba la información de registro en [nombrearchivo]; su valor predeterminado es /tmp/eiam-install.log.

-silent

Ejecuta la instalación en modo silencioso. Si uno de los parámetros necesarios no se especifica en la línea de comandos, se anula la instalación y se genera el mensaje correspondiente. Solamente efectúa cambios en el sistema si se especifican todos los parámetros necesarios.

-tempdir [directorio]

Especifica el directorio utilizado para el almacenamiento de los archivos temporales. Su valor predeterminado es /tmp/eiam_temp. La ruta de acceso debe ser completa, y debe estar en su propio subdirectorio. La secuencia de comandos ejecuta rm -rf al final, para quitar el directorio especificado con este parámetro.

Instalación del servidor en modo silencioso

Para instalar el servidor de CA EEM en modo silencioso en Linux o UNIX, escriba el siguiente comando en el símbolo del sistema:

EEMServer_[*númeroversión*].[*número_compilación*]_[*nombre del sistema operativo*].sh -silent -eiamadminpw *contraseña -javahome directorio*

Ejemplo: el comando siguiente para los entornos operativos Sun incluye los parámetros mínimos requeridos:

EEMServer_8.4.0.55_sunos.sh -silent -eiamadminpw *contraseña -javahome directorio*

Puede determinar más parámetros de instalación. La mayoría de los parámetros de instalación tienen valores predeterminados. Si desea obtener más información acerca de los parámetros de la secuencia de comandos, consulte el apartado Parámetros de la secuencia de comandos de instalación del servidor.

El archivo se descomprime y comienza el proceso de instalación.

Eliminación del servidor de CA EEM en modo silencioso

Para quitar el servidor de CA EEM, ejecute eiamuninstall.sh -silent desde el directorio de instalación.

Nota: Si hay alguna aplicación registrada, no podrá eliminar el servidor de CA EEM. Para poder finalizar correctamente la desinstalación, debe anular el registro de todas las aplicaciones. Para obtener más información acerca de cómo eliminar una aplicación del registro, consulte la *Ayuda en línea*.

Capítulo 4: Configuración del SDK de CA EEM

Nuevos archivos binarios necesarios para crear aplicaciones con el SDK de CA EEM

Es necesario utilizar los siguientes archivos binarios además de los DLL del SDK de CA EEM de las versiones anteriores para incrustar el SDK r8.4 SR02 de CA EEM en sus aplicaciones:

Java

- xml-apis.jar

C++

Copie los siguientes archivos de la carpeta EIAMSDK/lib/$OS de su sistema operativo:

Windows

- log4cxx.dll
- log4cxx.lib
- libexpat-2.0.1.dll
- libexpat-2.0.1.lib

HP-UX

- *log4cxx* como liblog4cxx.sl, liblog4cxx.sl.10 o liblog4cxx.sl.10.0
- libapr* como libapr-1.sl.3, libaprutil-1.sl.3, libapr-1.sl.3.3 o libaprutil-1.sl.3.4
- libexpat-2.0.1.sl

UNIX salvo HP-UX

- *log4cxx* como liblog4cxx.so, liblog4cxx.so.10 o liblog4cxx.so.10.0
- libexpat*

Cómo crear aplicaciones con los nuevos archivos binarios de Java

1. Actualice ClassPath con referencias a xml-apis.jar.
2. Actualice su instalador para empaquetar los nuevos archivos binarios y el archivo de configuración de registrador.
3. Implemente los nuevos archivos binarios y el archivo de configuración de registrador junto a los archivos binarios del SDK de CA EEM.

Los archivos necesitan ejecutarse en aplicaciones mediante C++ SDK de CA EEM

Los siguientes binarios son necesarios para incrustar y ejecutar las aplicaciones a través de C++ SDK de CA EEM:

Windows

- ipthread.dll
- libcurl_7_18_2.dll
- libexpat-2.0.1.dll
- log4cxx.dll
- msvcm80.dll
- msvcm90.dll
- msvcp71.dll
- msvcp80.dll
- msvcp90.dll
- msvcr70.dll
- msvcr71.dll
- msvcr80.dll
- msvcr90.dll
- pcre.dll
- pthread.dll
- pthreadVCE.dll
- xerces-c_2_8.dll
- zlib.dll
- Microsoft.VC80.CRT.manifest
- Microsoft.VC90.CRT.manifest

HP-UX

- liblog4cxx.sl, liblog4cxx.sl.10, liblog4cxx.sl.10.0
- libapr-1.sl.3, libapr-1.sl.3.3, libaprutil-1.sl.3.4
- libexpat-2.0.1.sl, libxerces-c.sl.28 , libcurl.sl.4, libpcre.sl.0, libexpat.sl.2 libz.sl, liblog4cxx.sl.10.0

Linux

- libxerces-c.so.28
- libcurl.so.4
- libexpat.so.2 for linux_k24 and libexpat-2.0.1.so for linux_26
- libpcre.so.0
- libz.so.1
- liblog4cxx.so.10.0.0

AIX

- libxerces-c28.a libcurl.4.so libexpat-2.0.1.a libpcre.a libz.so
- liblog4cxx.a

Sun Solaris

- libxerces-c.so.28
- libcurl.so.4 libpcre.so
- libexpat.so.2 libz.so
- liblog4cxx.so.10.0.0

Cómo crear aplicaciones con los nuevos archivos binarios de C++

1. Incluya las nuevas bibliotecas que se proporcionan con el SDK de CA EEM mediante la adición de las siguientes líneas a su makefile:

   -llog4cxx -llibexpat

2. Actualice su instalador para empaquetar los archivos binarios nuevos, el archivo eiam.config y el archivo eiam.log4cxx.config.
3. Implemente los archivos binarios nuevos, el archivo eiam.config y el archivo eiam.log4cxx.config junto a los archivos binarios del SDK de CA EEM.

Nota: No es necesario incluir los archivos de encabezado de registrador en su código de origen.

Archivos necesarios para crear y ejecutar aplicaciones que utilizan C# SDK de CA EEM

Los siguientes binarios son necesarios para insertar y ejecutar la aplicación que utiliza el C# SDK de CA EEM:

- log4net.dll
- CPoz.dll
- iclient.dll
- CsharpSDK.dll

Nota: No es necesario que CAPICOM.dll e InterOP.CAPICOM.dll creen aplicaciones mediante C# SDK. Elimine estos dlls del paquete.

Cómo empaquetar C# SDK de CA EEM con sus aplicaciones

1. Agregue los dlls de la carpeta siguiente como conjuntos de referencia cuando se crea una aplicación:

   %EIAM_SDK%\lib\csharp

2. Actualice el instalador para empaquetar los dlls de referencia, el archivo eiam.config y el archivo eiam.log4net.config.

   Nota: El archivo eiam.config y los archivos eiam.lognet.config se encuentran en la carpeta %EIAM_SDK%\bin.

3. Implemente los dlls de referencia, el archivo eiam.config, y el archivo eiam.log4net.config en los equipos de cliente.

Configuración del SDK de CA EEM

En los siguientes temas se explica cómo configurar el SDK de CA EEM con la clase Safe::Configurator.

Más información:

Acerca del archivo eiam.config (en la página 39)
Registro del SDK de CA EEM (en la página 91)
Configuración del SDK de C++ de CA EEM (en la página 46)
Configure el SDK de Java de CA EEM con SafeConfigurator (en la página 45)

Acerca del archivo eiam.config

Es necesario utilizar el archivo eiam.config para controlar los datos de configuración del SDK de CA EEM, como:

- Búfer cíclico
- Archivo de configuración del registrador
- Carpeta SAF para almacenar archivos de auditoría
- Modo de compatibilidad con FIPS

El archivo eiam.config consta de los siguientes parámetros configurables:

CyclicBuffer size

Especifica el número de mensajes de registro que se incluyen en un búfer cíclico. El búfer cíclico almacena la cantidad de mensajes más recientes especificada en la memoria. Una vez que el búfer alcanza el tamaño especificado, los mensajes de registro nuevos sustituyen a los mensajes de registro más antiguos del búfer. Si la aplicación se bloquea, puede recuperar los mensajes de registro más recientes del núcleo.

Valor predeterminado: 500

Mínimo: 0

Máximo: 1.000

enable

Especifica si el búfer cíclico está activado. Si está establecido en false, el búfer cíclico está desactivado. Por lo tanto, no es necesario especificar valores de los parámetros CyclicBuffer size, dump y file.

Valor: [*true*|*false*]

Valor predeterminado: true

Importante: El búfer cíclico está activado de forma predeterminada con independencia de si ha activado el registro o no. Si habilita el búfer cíclico, el rendimiento de CA EEM se verá afectado.

dump

Especifica si el contenido de búfer cíclico se escribe en un archivo si se actualiza o se modifica el archivo eiam.config.

Valor: [*true*|*false*]

Valor predeterminado: false

file

Especifica el nombre del archivo de volcado. Si el valor de dump es false, los mensajes de registro no se escriben en un archivo de volcado. La extensión del archivo es .log.

LoggerConfiguration file

Se especifica una ruta de archivos de configuración de registrador para los SDK de Java y C++ de CA EEM. La información de registro de CA EEM se almacena en los archivos de configuración del registrador. eiam.log4cxx.config y eiam.log4j.config son los archivos de configuración de registrador para el SDK de C++ y Java de CA EEM.

Saf directory

La carpeta SAF en la que los archivos se almacenan para su procesamiento.

Network sockettimeout

Especifica el tiempo de espera del socket de red en milisegundos.

Valor predeterminado: 120.000 segundos (2 segundos)

Más información:

Registro del SDK de CA EEM (en la página 91)

Ejemplo de un archivo eiam.config

A continuación, se encuentra un ejemplo del archivo eiam.config:

```
<EiamConfiguration>
 <!-- EIAM Internal: Configure cyclic buffer -->
 <CyclicBuffer size="500" dump="false" file="dump.log" enable="true" />
 <!-- Absolute file path for logger configuration, For Java use:-  file="eiam.log4j.config" -->
 <LoggerConfiguration file="eiam.log4cxx.config"/>
 <!-- Absolute folder path for SAF folder where audit files will be stored for processing-->
 <Saf directory="audit"/>
  <!-- Socket timeout in milli seconds. Default value is 2 mins -->
 <Network sockettimeout="120000"/>
 <SDK type="Java">
            <iTechSDK>
                        <FIPSMode>true</FIPSMode>
                        <JCEProvider>JsafeJCE</JCEProvider>
                        <Security>
                                    <digestAlgorithm>SHA1</digestAlgorithm>
                        </Security>
                        <Debug>
                                    <logLevel>trace</logLevel>
                        </Debug>
            </iTechSDK>
 </SDK>
 <SDK type="C++">
            <iTechSDK>
                        <FIPSMode></FIPSMode>
                        <Commons>
                                    <etpkiCryptoLib></etpkiCryptoLib>
                        </Commons>
                        <TransportConfig>
                                    <!--possible values are SSLV23 / SSLV3 / TLSV1-->
                                    <secureProtocol></secureProtocol>
                        </TransportConfig>
                        <Security>
                                    <!--possible values are MD5/SHA1/SHA256/SHA384/SHA512-->
                                    <digestAlgorithm></digestAlgorithm>
                        </Security>
                        <Debug>
                                    <!--possible values are ERROR/WARNING/TRACE/NOLEVEL-->
                                    <logLevel></logLevel>

                                    <!--possible values are true/false -->
                                    <logToFile></logToFile>

                                    <!--log file name-->
                                    <logFile></logFile>

                                    <!--log file size in MB(positive integer)-->
```

```
                    <maxLogSize></maxLogSize>
                </Debug>
            </iTechSDK>
        </SDK>
</EiamConfiguration>
```

Activación del registro de iTechnology SDK

Puede activar el registro de iTechnology SDK sólo para C++ SDK de CA EEM y SDK de Java de CA EEM. Para C# SDK de CA EEM, utilice el archivo de configuración del registrador.

Para activar el registro de iTechnology SDK, abra el archivo eiam.config y edite las etiquetas siguientes:

- logLevel
- logToFile
- logFile
- maxLogSize

Para SDK de Java de CA EEM, edite las etiquetas previamente mencionadas en la sección <tipo de SDK ="Java">. Para C++ SDK de CA EEM, edite las etiquetas mencionadas en la sección <tipo de SDK ="C++">.

Antes de configurar SDK de Java de CA EEM en el modo de sólo FIPS

Para configurar SDK de Java de CA EEM en el modo de sólo FIPS, haga las tareas siguientes:

1. Configure JRE para utilizar bibliotecas de Java Cryptography Extension (JCE) de terceros.
2. Agregue las bibliotecas de Crypto-J como proveedor de JCE en el archivo Java.security.

   Nota: Para obtener más información sobre cómo configurar JRE con JCE, consulte la documentación correspondiente de JCE.
3. Active el modo de sólo FIPS en el archivo eiam.config.

Configuración de SDK de Java de CA EEM en el modo de sólo FIPS

Cuando configura SDK de CA EEM en el modo de sólo FIPS, CA EEM utiliza bibliotecas criptográficas de FIPS 140-2 para cifrar y descifrar datos sensibles.

Para configurar SDK de Java de CA EEM en el modo de sólo FIPS

1. Abra el archivo eiam.config y edite la sección con las etiquetas siguientes de <tipo de SDK="Java">:
   - FIPSMode
   - JCEProvider
   - digestAlgorithm
2. Guarde y cierre el archivo eiam.config.
3. Reinicie la aplicación.

   SDK de Java de CA EEM se configura en el modo de sólo FIPS.

Configuración de C++ SDK de CA EEM en el modo de sólo FIPS

Cuando configura SDK de CA EEM en el modo de sólo FIPS, CA EEM utiliza bibliotecas criptográficas de FIPS 140-2 para cifrar y descifrar datos sensibles.

Para configurar C++ SDK de CA EEM en el modo de sólo FIPS

1. Abra el archivo eiam.config y edite las etiquetas siguientes de la sección <tipo de SDK="C++">.
   - FIPSMode
   - etpkiCryptoLib
   - secureProtocol
   - digestAlgorithm
2. Guarde y cierre el archivo eiam.config.
3. Reinicie la aplicación.

   C++ SDK de CA EEM se configura en el modo de sólo FIPS.

Configuración de C# SDK de CA EEM en el modo de sólo FIPS

Cuando se configura C# SDK de CA EEM en el modo de sólo FIPS, CA EEM utiliza bibliotecas criptográficas que cumplen con FIPS 140-2 para cifrar y descifrar datos sensibles.

Nota: C# SDK de CA EEM no es compatible con certificados de P11.

Para configurar C# SDK de CA EEM en el modo de sólo FIPS

1. Abra el archivo eiam.config y edite las etiquetas siguientes de la sección <tipo de SDK="C#">:
   - FIPSMode
   - digestAlgorithm
2. Guarde y cierre el archivo eiam.config.
3. Reinicie la aplicación.

   C# SDK de CA EEM se configura en el modo de sólo FIPS.

Configuración de la información de SafeContext

La etiqueta de <SafeContext> en el archivo eiam.config contiene la información requerida para generar un SafeContext que utiliza la clase SafeContextFactory. Cada etiqueta de SafeContext en el archivo eiam.config se identifica mediante una etiqueta única refID. Para generar un SafeContext, se debe pasar este refID a SafeContextFactory. Éstos son los beneficios de especificar la información relacionada con SafeContext en el archivo eiam.config:

Para configurar la información relacionada con SafeContext:

1. Abra el archivo eiam.config y edite la sección <SafeContext> para configurar las etiquetas siguientes:
   - refID
   - Servidor
   - Aplicación
   - Configuración regional
   - Tipo de autentificación
2. Guarde y cierre el archivo eiam.config.

Configure el SDK de Java de CA EEM con SafeConfigurator

Es necesario configurar el SDK de CA EEM con la clase Safe::Configurator. Para configurar el SDK de CA EEM, realice el siguiente proceso:

Nota: Es necesario configurar eiam.config antes que el SDK de CA EEM.

1. Incluya la siguiente API en su código para inicializar el SDK de CA EEM durante el inicio de la aplicación:

   ```
   SafeConfigurator.getInstance().init(filename);
   ```

   Dónde

   filename

   Especifica la ruta absoluta del archivo eiam.config que ha definido para la aplicación.

   Nota: Todas las operaciones del SDK de CA EEM se registran en función de los niveles de seguimiento de registro en la configuración del registrador.

2. Incluya la siguiente API en su código durante el cierre de su aplicación:

   ```
   m_config.term();
   ```

   Nota: Todas las llamadas de inicialización que realice con m_config.init(*filename*) deben finalizar con un m_config.term() correspondiente. Los métodos de inicialización y término son seguros para los subprocesos y disponen de recuento de referencias. La biblioteca de seguridad se inicializa durante la primera llamada init() y finaliza cuando el recuento de referencias llega a cero.

Más información:

Acerca del archivo eiam.config (en la página 39)
Acerca de los archivos de configuración del registrador (en la página 93)

Configuración del SDK de C++ de CA EEM

Es necesario configurar el SDK de CA EEM con la clase Safe::Configurator. Para configurar el SDK de CA EEM, realice el siguiente proceso:

Nota: Es necesario configurar eiam.config antes que el SDK de CA EEM.

1. Incluya la siguiente API en su código para inicializar el SDK de CA EEM durante el inicio de la aplicación:

   Safe::Configurator::getInstance()->init(*filename*);

   Dónde

   filename

   Especifica la ruta absoluta del archivo eiam.config que ha definido para la aplicación.

2. Incluya la siguiente API en su código durante el cierre de su aplicación:

   Safe::Configurator::getInstance()->term();

   Nota: Todas las llamadas de inicialización que realice con Safe::Configurator::getInstance()->init(filename), debe finalizarlas con un Safe::Configurator::getInstance()->term() correspondiente. Los métodos de inicialización y término son seguros para los subprocesos y disponen de recuento de referencias. La biblioteca de seguridad se inicializa durante la primera llamada init() y finaliza cuando el recuento de referencias llega a cero.

Más información:

Acerca del archivo eiam.config (en la página 39)
Acerca de los archivos de configuración del registrador (en la página 93)

Inicialice C# SDK de CA EEM

Configuración de SDK de CA EEM mediante la clase SafeConfigurator. Para configurar SDK de CA EEM, realice el proceso siguiente:

Nota: Configure el archivo eiam.config antes de configurar SDK de CA EEM. Si no configura el archivo eiam.config, SDK de CA EEM se inicializa con la configuración predeterminada siguiente:

- modo no FIPS
- El registro se configura en error y sólo se activa el registro de la consola
- Se desactiva la ubicación de SAF

Para inicializar SDK de CA EEM, realice el proceso siguiente:

1. Incluya la API siguiente en su código para inicializar SDK de CA EEM durante el inicio de la aplicación:

   SafeConfigurator.getInstance().Init(*filename*);

   Where

   filename

   Especifica la ruta absoluta del archivo eiam.config que ha definido para su aplicación.

   Nota: Si no se menciona el nombre del archivo, se inicializa SDK de CA EEM con los valores predeterminados.

2. Incluya la API siguiente en su código durante el cierre de la aplicación:

   SafeConfigurator.getInstance().term();

   Nota: Para obtener más información sobre la clase SafeConfigurator, consulte la *Guía de programación*.

Capítulo 5: Soporte de FIPS 140-2

Esta sección contiene los siguientes temas:

Información general de FIPS 140-2

La publicación de los Estándares Federales de Procesamiento de la Información (FIPS) 140-2 especifica los requisitos para el uso de algoritmos criptográficos dentro de un sistema de seguridad que protege datos sensibles y sin clasificar. El servidor de CA EEM inserta la biblioteca criptográfica v2.0 de Crypto-C ME, que se ha validado y cumple con los *requisitos de seguridad para módulos criptográficos* de FIPS 140-2. El número de certificado de validación para este módulo es 608.

SDK de Java de CA EEM utiliza una versión que cumple con el estándar FIPS de la biblioteca criptográfica de BSAFE Crypto-J 4.0 de RSA. C++ SDK de CA EEM inserta ETPKI 4.1.x, que utiliza bibliotecas de criptografía de RSA.

CA EEM puede funcionar en un modo no FIPS o en un modo de sólo FIPS. Los límites criptográficos, es decir, la forma en que CA EEM aplica el cifrado, son iguales en los dos modos, pero los algoritmos son distintos.

Los productos del equipo que utilizan módulos criptográficos acreditados de FIPS 140-2 en su modo acreditado de FIPS pueden utilizar solamente funciones de seguridad aprobadas por FIPS como AES (Algoritmo de cifrado avanzado), SHA-1 (Algoritmo hash seguro), y protocolos de nivel más alto como TLS v1.0 tal y como se permite explícitamente en las guías de implementación y estándar de FIPS 140-2.

En el modo de sólo FIPS, CA EEM utiliza los algoritmos siguientes:

- SHA1 como el algoritmo de certificación predeterminado para cifrar las contraseñas y firmar las solicitudes del servidor. Puede utilizar cualquiera de los algoritmos siguientes en el modo de sólo FIPS:
  - SHA1
  - SHA256
  - SHA384
  - SHA512
- TLS v1.0 para la comunicación con directorios de LDAP externos si la conexión de LDAP está sobre TLS.

Modos de seguridad compatibles en CA EEM

CA EEM es compatible con dos modos de funcionamiento: no FIPS y sólo FIPS. La funcionalidad de CA EEM es la misma en estos dos modos. La diferencia en estos dos modos está en los algoritmos criptográficos utilizados para el almacenamiento y la verificación de contraseñas, y la comunicación de datos sensibles entre CA EEM y otros productos como directorios de LDAP, CA SiteMinder, etc.

no FIPS

Se refiere al modo que utiliza técnicas que no cumplen con FIPS para la criptografía. En este modo MD5 es el algoritmo predeterminado utilizado para cifrar y descifrar datos sensibles. Las instalaciones nuevas o las actualizaciones se ejecutan en un modo no FIPS. En el modo no FIPS, el servidor de CA EEM es compatible con versiones anteriores de los clientes de CA EEM. Por ejemplo, puede utilizar CA EEM r8.4 SDK para conectarse a un servidor de CA EEM r8.4 SP3.

Sólo FIPS

Se refiere al modo que utiliza técnicas que cumplen con sólo FIPS para la criptografía. Este modo no es compatible con clientes que se ejecutan en el modo no FIPS. Puede utilizar solamente clientes de sólo FIPS de SDK de CA EEM r8.4 SP3 con servidores de CA EEM r8.4 SP3 que se ejecutan en el modo de sólo FIPS.

Cómo configurar el servidor de CA EEM en el modo de sólo FIPS

En el modo de sólo FIPS se debe configurar CA EEM para que utilice algoritmos que cumplen el estándar FIPS. El servidor de CA EEM y los clientes de SDK de CA EEM se pueden comunicar solamente si los dos se configuran en el modo de sólo FIPS. Similarmente, el servidor de CA EEM en un modo de sólo FIPS se puede comunicar sólo con un directorio de LDAP configurado para que utilice algoritmos que cumplen el estándar FIPS. Para configurar el entorno de CA EEM en un modo de sólo FIPS, realice lo siguiente:

- Verifique los requisitos previos para configurar el servidor de CA EEM en el modo de sólo FIPS
- Configure el servidor de CA EEM en el modo de sólo FIPS

Requisitos previos para configurar el servidor de CA EEM en el modo de sólo FIPS

Éstos son los requisitos previos para configurar el servidor de CA EEM en el modo de sólo FIPS:

- Verifique que los otros productos de CA que utilizan iGateway como por ejemplo CA ITM, CA ELM, etc., están en el modo de sólo FIPS. iGateway no se puede inicializar ni en el modo de sólo FIPS ni en el modo no FIPS. Cuando se inicializa iGateway en el modo de sólo FIPS-, todos los productos que utilizan iGateway deben estar en el modo de sólo FIPS. Abra el archivo iGateway.conf y verifique el valor para la etiqueta siguiente:

  FIPSMode

  Si el valor de esta etiqueta está establecido en Falso, significa que el producto que utiliza iGateway se encuentra en el modo no FIPS. En función de la configuración actual de iGateway se debe decidir si se va a activar CA EEM en el modo de sólo FIPS.

- Verifique las versiones de los componentes que utilizan los otros productos de CA en el archivo spin.conf y tenga en cuenta el valor que aparece para las etiquetas <Spindle Name> y <version>. Compruebe en la documentación del producto correspondiente si estas versiones son compatibles con FIPS.

  Nota: Los archivos iGateway.conf y spin.conf se almacenan en la siguiente ubicación:

  - **Windows**: %IGW_LOC%
  - **Linux y UNIX**: /opt/CA/SharedComponents/iTechnology

Pasos previos a la configuración de CA EEM en el modo de sólo FIPS

Compruebe que el entorno cumple los requisitos mínimos antes de migrar el entorno para poder utilizar el modo de sólo FIPS. Imprima los elementos siguientes para usarlos como lista de verificación:

- ☐ Actualice el servidor de CA EEM a CA EEM r8.4 SP3.
- ☐ Verifique que los productos que están integrados o conectados con CA EEM estén configurados en el modo de sólo FIPS.

Configuración del servidor de CA EEM en el modo de sólo FIPS

Cuando se configura el servidor de CA EEM en el modo de sólo FIPS, CA EEM sólo utiliza bibliotecas criptográficas que cumplan con FIPS 140-2 para cifrar y descifrar los datos sensibles.

Notas:

- En el modo de sólo FIPS, se puede utilizar IE7 (o superior) o Firefox 3.0 (o superior) para visualizar la interfaz gráfica de usuario del administrador de CA EEM. Para obtener más información sobre cómo configurar Firefox en el modo FIPS 140-2, consulte el sitio de soporte de Firefox.
- El procedimiento siguiente también es válido para cambiar el modo de seguridad del servidor de CA EEM de sólo FIPS a no FIPS o de no FIPS a sólo FIPS.

Para configurar CA EEM en el modo de sólo FIPS

1. Detenga el servicio iGateway.
2. Detenga los servicios de CA Directory mediante los comandos siguientes:

   Windows

   ```
   dxserver stop all
   ssld stop
   ```

   Linux y UNIX

   ```
   su - dsa -c "dxserver stop all"
   su - dsa -c "ssld stop"
   ```

3. Abra el archivo iGateway.conf y establezca la siguiente etiqueta en ON:

   ```
   <FIPSMode>ON<FIPSMode>
   ```

   Nota: Para modificar el modo de sólo FIPS a no FIPS, establezca la etiqueta FIPSMode en OFF.

4. Ejecute los siguientes comandos desde la línea de comandos:

   Windows

   ssld remove iTechPoz-Server
   ssld install iTechPoz-Server -certfiles "%DXHOME%/config/ssld/personalities" -ca "%DXHOME%/config/ssld/iTechPoz-trusted.pem" -port 21847 -fips

   Linux y UNIX

   su - dsa
   ssld remove iTechPoz-Server
   ssld install iTechPoz-Server -certfiles $DXHOME/config/ssld/personalities -ca $DXHOME/config/ssld/iTechPoz-trusted.pem -port 21847 -fips

   Nota: La opción -port especifica el puerto ssld. Si ha configurado un puerto ssld distinto, sustituya 21847 en los comandos anteriores con el número de puerto correcto. Por otro lado, si se modifica el modo de seguridad de sólo FIPS a no FIPS, se deben utilizar los comandos descritos en este paso sin la opción -fips.

5. Inicie los servicios de CA Directory mediante los comandos siguientes:

   Windows

   ssld start
   dxserver start all

   Linux y UNIX

   su - dsa -c "ssld start"
   su - dsa -c "dxserver start all"

6. Inicie el servicio iGateway.

   CA EEM está configurado en el modo de sólo FIPS.

Cómo comprobar que el servidor de CA EEM está en el modo de sólo FIPS

Para comprobar que el servidor de CA EEM está en el modo de sólo FIPS, haga lo siguiente:

1. En el explorador, escriba la URL https://*nombre host* o *dirección IP*:5250/spin/eiam/about.csp.

   Se abrirá la página Acerca de.

2. Compruebe que la etiqueta FIPS:está establecida en Activado.

   Si la etiqueta está establecida en Activado,ello indica que el servidor de CA EEM se encuentra en el modo de sólo FIPS.

Comunicación entre el servidor de CA EEM y los directorios de LDAP externos

La comunicación entre el servidor de CA EEM y un directorio externo depende del tipo de conexión de LDAP que existe entre ambos elementos está cifrada o no lo está. Los siguientes son los modos de cifrado admitidos por el servidor de CA EEM y el directorio externo.

El cifrado está activado en el servidor de CA EEM para la comunicación de LDAP

En los casos en que se configura el servidor de CA EEM para utilizar un canal de comunicación cifrado con un directorio de LDAP externo, si el servidor de CA EEM opera en modo FIPS, el directorio de LDAP también debe estar configurado en el modo compatible con FIPS.

Configuración de CA EEM para utilizar certificados de servidor en un dispositivo PKCS#11

Para usar dispositivos de nCipher PKCS#11 con el servidor o el SDK de CA EEM, se debe configurar el dispositivo nCipher y establecer la siguiente propiedad de la forma siguiente:

```
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=all
```

Nota: Para obtener más información sobre cómo configurar el dispositivo de nCipher con un token de hardware, consulte la documentación de nCipher.

Para configurar el servidor de CA EEM para que pueda utilizar certificados almacenados en dispositivos PKCS#11, haga lo siguiente:

1. Detenga el servicio iGateway.
2. Abra el archivo iGateway.conf y edite las etiquetas de <Connector name="defaultport"> CA Portal5250</port> y establezca los siguientes valores:

   certType

   Define el tipo de certificado que se va a utilizar. Los tipos de certificados compatibles son p12, pem y p11.

   Valor predeterminado: pem

   Tipo: Nodo secundario

Using P11 certificate

<pkcs11Lib/>: ruta a la biblioteca de PKCS11 proporcionada por el token

<token/>: ID de token

<userpin/>: PIN alterado del usuario

<Id/>: ID del certificado y de la clave privada

<sensitive/>: la clave privada es sensible. Las claves sensibles no se convierten de la misma forma en que lo hacen las claves de software, y las operaciones criptográficas se realizan mediante el hardware de PKI criptográfico (las claves no sensibles se pueden tratar como claves sensibles, pero las claves sensibles no se pueden convertir ni tratarse como claves no sensibles)

Valor predeterminado: Falso

3. Guarde y cierre el archivo iGateway.conf.
4. Inicie los servicios de iGateway.

Configuración de CA EEM para almacenar certificados de servidor en un dispositivo PKCS#11

Para almacenar los certificados de CA EEM en un dispositivo PKCS#11, haga lo siguiente:

1. Detenga el servicio iGateway.
2. Abra el archivo iGateway.conf y edite las etiquetas de <CertificateManager> para configurar los valores siguientes:

   certType

   Define el tipo de certificado que se va a utilizar. Los tipos de certificados compatibles son p12, pem y p11.

   Valor predeterminado: pem

   Tipo: Nodo secundario

Using P11 certificate

<pkcs11Lib><pkcs11Lib/>: ruta a la biblioteca de PKCS11 proporcionada por el token

<token><token/>: ID de token

<userpin><userpin/>: PIN alterado del usuario

<id><id/>: ID del certificado y de la clave privada

<sensitive><sensitive/>: la clave privada es sensible. Las claves sensibles no se convierten de la misma forma en que lo hacen las claves de software, y las operaciones criptográficas se realizan mediante el hardware de PKI criptográfico (las claves no sensibles se pueden tratar como claves sensibles, pero las claves sensibles no se pueden convertir ni tratarse como claves no sensibles). El valor opcional predeterminado es Falso.

3. Guarde y cierre el archivo iGateway.conf.
4. Inicie los servicios de iGateway.

Configuración de la aplicación en el modo de sólo FIPS

Para configurar la aplicación en el modo de sólo FIPS, verifique que el SDK de CA EEM está en el modo de sólo FIPS, puesto que el SDK de CA EEM sólo utiliza técnicas criptográficas que cumplan con FIPS. El archivo de configuración del SDK de CA EEM, eiam.config controla el modo de funcionamiento seguro del SDK de CA EEM. Antes de configurar el SDK de CA EEM en el modo de sólo FIPS, compruebe lo siguiente:

- Verifique que la versión del SDK de CA EEM que utiliza es r8.4 SP3.
- Migre los certificados P12 utilizados por CA EEM a certificados PEM.
- Inicialice el SDK de CA EEM en modo de sólo FIPS.

Migración de los certificados P12 utilizados por la aplicación a certificados PEM

CA EEM es compatible con certificados P12, PEM, y PKCS#11, siempre y cuando se tenga en cuenta lo siguiente:

- La compatibilidad con P12 se desactiva (o no está disponible) en el modo de sólo FIPS. Como alternativa, se ha introducido la compatibilidad con los certificados PEM y PKCS#11 en el modo de sólo FIPS.

Nota: C# SDK de CA EEM sólo es compatible con certificados PEM cuando está en el modo de sólo FIPS y con certificados P12 y PEM cuando está en el modo no FIPS.

Por lo tanto, si se están utilizando certificados P12, éstos se deben migrar a uno de los formatos admitidos en el modo de sólo FIPS. Utilice la utilidad de igwCertUtil para convertir los certificados P12 en certificados pem. La utilidad igwCertUtil permite convertir, crear o suprimir certificados. La utilidad igwCertUtil se encuentra en la carpeta siguiente:

Windows

%IGW_LOC%

UNIX y Linux

$IGW_LOC

Utilidad igwcertutil: creación, copiado, conversión y supresión de certificados

Válido en Windows, UNIX y Linux

El comando create utiliza el formato siguiente:

igwCertUtil -version *version* -create -cert *inputcert*-params -issuer issuercert -params [-debug] [-silent]

El comando convert utiliza el formato siguiente:

igwCertUtil -version version -conv -cert *inputcert*-params -target newcert-params [-debug] [-silent]

El comando copy utiliza el formato siguiente:

igwCertUtil -version version -copy -cert *inputcert*-params -target newcert-params [-debug] [-silent]

El comando delete utiliza el formato siguiente:

igwCertUtil -version version -delete -cert *cert*-params [-debug] [-silent]

-version *version*

Especifica la versión de igwCertUtil que se ha utilizado para crear, convertir, copiar o suprimir certificados. La versión se utiliza para la compatibilidad con versiones anteriores. Si se modifica igwCertUtil, la etiqueta de versión sigue el comportamiento anterior.

-cert *inputcert*-parms

Especifica el certificado en forma de cadena XML al crear, convertir o copiar certificados.

-issuer *issuercert*-parms

Especifica el certificado que se utilizará para los nuevos certificados cuando éstos se generen. Si no se especifica ningún certificado, se creará un certificado autofirmado.

-target *newcert*-parms

Especifica la configuración para el nuevo certificado cuando se convierte (o se copia) un certificado existente.

-cert *cert*-parms

-debug

(Opcional) Activa la depuración de igwCertUtil.

-silent

(Opcional) Activa el modo silencioso para igwCertUtil.

igwCertUtil devuelve los siguientes códigos de error:

- CERTUTIL_ERROR_UNKNOWN (-1): se ha producido un error desconocido o indefinido
- CERTUTIL_SUCCESS (0): operación realizada correctamente
- CERTUTIL_ERROR_USAGE (1): se ha pasado un argumento incorrecto en la línea de comando
- CERTUTIL_ERROR_READCERT (2): no se puede leer el certificado
- CERTUTIL_ERROR_WRITECERT (3): no se puede escribir el certificado
- CERTUTIL_ERROR_DELETECERT (4): no se puede suprimir el certificado

Ejemplo: conversión de certificados P12 en certificados PEM

El ejemplo siguiente muestra cómo convertir un certificado P12 en certificado PEM:

```
igwCertUtil -version 4.6.0.0 -conv  -cert
"<Certificate><certType>p12</certType><certURI>testCert.p12</certURI><certPW>password</certPW></Certificate>" -target "<Certificate><certType>pem</certType>
<certURI>testCert.cer</certURI><keyURI>testCert.key</keyURI></Certificate>"
```

Ejemplo: conversión de certificados P12 en certificados PKCS#11

```
igwCertUtil -version 4.6.0.0 -conv  -cert
"<Certificate><certType>p12</certType><certURI>testCert.p12</certURI><certPW>password</certPW></Certificate>" -target "<Certificate><certType>p11</certTyp
><pkcs11Lib>pathto-pkcs11Lib</pkcs11Lib><token>pkcs11token</token><userpin>user
in</userpin><id>certid</id></Certificate>"
```

Inicialización del SDK de CA EEM en modo de sólo FIPS.

El SDK de CA EEM se puede inicializar en el modo de sólo FIPS si se configura el archivo eiam.config. Para configurar el archivo eiam.config, consulte el capítulo, Configuración del SDK de CA EEM (en la página 35).

Capítulo 6: Creación de copias de seguridad del servidor de CA EEM y su restauración

Esta sección contiene los siguientes temas:

Creación de copias de seguridad del sistema de archivos

Es recomendable crear una copia de seguridad de los servidores de CA EEM con regularidad, o siempre que se administre algún cambio en los entornos de los servidores de CA EEM. Si un servidor de CA EEM resulta dañado, se puede usar su copia de seguridad para restaurarlo.

Deberá crear una copia de seguridad de los siguientes archivos y carpetas de CA EEM:

Descripción de los datos	Nombre de los archivos en Windows	Nombre de los archivos en Linux
Archivos de configuración	■ iPoz.conf ■ Eiam.conf ■ iPoz.map ■ Spin.conf ■ iPozDsa.pem ■ iPozRouterDsa.pem ■ logDepot.conf ■ calmReporter.conf	■ iPoz.conf ■ Eiam.conf ■ iPoz.map ■ Spin.conf ■ iPozDsa.pem ■ iPozRouterDsa.pem ■ eiam-type ■ Sponsorfiles ■ logDepot.conf ■ calmReporter.conf

Descripción de los datos	Nombre de los archivos en Windows	Nombre de los archivos en Linux
Información sobre eventos	■ logdepotdb ■ Carpeta calm_catalog ■ Carpeta calm_archive	■ logdepotdb ■ Carpeta calm_catalog ■ Carpeta calm_archive
Carpetas	■ Registro del sistema ■ Carpeta iTechnology	■ Carpeta iTechnology ■ Configuración del entorno

Creación de copias de seguridad de carpetas y archivos de servidor de CA EEM

Es recomendable crear una copia de seguridad de los servidores de CA EEM con regularidad, o siempre que se administre algún cambio en los entornos de los servidores de CA EEM. Si un servidor de CA EEM resulta dañado, se puede usar su copia de seguridad para restaurarlo.

Para crear una copia de seguridad de carpetas y archivos de servidor de CA EEM

1. Detenga iGateway.
2. Cree una copia de seguridad de las carpetas, la información de los eventos y los archivos de configuración de CA EEM.
3. Cree una copia de seguridad de los datos de CA EEM almacenados en CA Directory.

   Con ello, se habrá creado una copia de seguridad de las carpetas, los eventos y los archivos de configuración del servidor de CA EEM.

Más información:

Creación de copias de seguridad del sistema de archivos (en la página 61)
Creación de una copia de seguridad de los datos de CA EEM almacenados en CA Directory (en la página 65)

Procedimientos de restauración

Deberá restaurar los datos de CA EEM si:

- desea recuperar una instalación dañada de CA EEM.
- desea recuperar un entorno de servidor de CA EEM que no funciona como debería.

Para recuperar los datos y los archivos de configuración de CA EEM

1. Detenga iGateway.
2. Cambie el nombre de todos los archivos de configuración .conf de CA EEM a .conf.merge y, a continuación, cópielos en la carpeta iTechnology. Los archivos .conf.merge son necesarios para combinar los archivos de configuración de los que se ha creado una copia de seguridad y los nuevos.
3. Restaure los datos de CA EEM.
4. Inicie iGateway.

Más información:

Creación de una copia de seguridad de los datos de CA EEM almacenados en CA Directory (en la página 65)

Inicio del servicio iGateway

Para iniciar el servicio iGateway, tendrá que introducir los siguientes comandos:

Windows

```
net start igateway
```

Linux y UNIX

```
$IGW_LOC/S99igateway start
```

Detenga el servicio iGateway.

Para detener el servicio iGateway, tendrá que introducir los siguientes comandos:

Windows

net stop igateway

Linux y UNIX

$IGW_LOC/S99igateway stop

Capítulo 7: Creación de una copia de seguridad de los datos de CA EEM almacenados en CA Directory

Esta sección contiene los siguientes temas:

Introducción a la terminología de CA Directory

En esta sección se explica la terminología de CA Directory que se usa en este documento:

DSA

Un *DSA* es un proceso que gestiona algunos, si no todos, los espacios de nombres de un directorio.

This also needs to be expanded to make it accessible to readers new to CA Directory. Al instalar un servidor de CA EEM, podrá configurar los siguientes parámetros relacionados con CA Directory:

DXmanager

DXmanager es una aplicación Web que permite crear, configurar y controlar el nodo central del directorio, así como realizar un seguimiento de él.

Consola de DSA

La *consola de DSA* permite efectuar una conexión con un DSA para enviar comandos de DXserver, recibir información de seguimiento y actuar como un agente de usuario.

DXtools

El término *DXtools* designa un conjunto de utilidades de línea de comandos que acompañan a CA Directory. Estas herramientas permiten gestionar la administración de los directorios, trabajar con datos de LDIF, cargar datos a un directorio y descargarlos de él, además de extraer esquemas y convertirlos para usarlos con CA Directory.

LDIF (del inglés LDAP Data Interchange Format, formato de intercambio de datos de LDAP)

Los *archivos LDIF* son archivos de texto que almacenan información de los directorios en LDIF. Los archivos LDIF pueden usarse para transferir información de directorios entre los servidores de directorios LDAP, o con el propósito de describir un conjunto de cambios que deberá aplicarse a uno de los directorios.

Cómo usar DXtools

Puede usar los siguientes métodos para ejecutar DXtools:

- Ejecute los comandos de DXtools en el host usando la consola de DSA.
- Ejecute los comandos de DXtools en un host remoto usando, para ello, la consola de DSA a través de una red TCP/IP.
- Incluya los comandos de DXtools en las secuencias de comandos.

Todas las herramientas devuelven el valor cero si el proceso se efectúa correctamente, y un número distinto a cero en caso de que se produzca algún error.

Variable de entorno DXHOME

Algunas herramientas requieren que se asigne la ruta de inicio de DXserver a la variable de entorno DXHOME. Esta asignación se efectúa de forma automática cuando se instala CA Directory.

Algunas herramientas buscan los archivos de configuración de DSA en la carpeta *config* correspondiente a la ruta de DXHOME.

Códigos de estado de salida para DXtools

Las herramientas de DXtools comparten códigos de salida, aunque no todos los códigos de salida se aplican a todas las herramientas. Los códigos de salida adoptan la forma siguiente:

0

Correcto

1

El DSA correspondiente está en ejecución.

2

Al menos uno de los archivos de almacén de datos ya existe.

3

No existe la ubicación de directorio especificada o no es un directorio.

4

El archivo especificado es del tipo incorrecto (como un directorio).

5

Hay un problema de permiso con este archivo.

6

El nombre de la ruta completa del archivo del almacén de datos es demasiado grande. Esto puede deberse a una longitud excesiva de la ubicación especificada para el directorio del almacén de datos.

7

Se ha producido un error al intentar eliminar los antiguos archivos de almacén de datos.

8

Se ha producido un error al intentar cambiar el nombre de los antiguos archivos de almacén de datos.

9

Se ha producido un error al intentar crear o completar uno de los archivos.

10

El tamaño del almacén de datos es inferior o igual a cero.

11

No hay suficiente espacio en el dispositivo o memoria disponible para intentar crear el archivo.

12

No se dispone de acceso suficiente para crear el archivo o establecer el acceso en el archivo (quizás debido a que los permisos eran insuficientes).

13

No se ha establecido la variable de entorno DXHOME.

14

La variable de entorno DXHOME no es válida.

15

El DSA correspondiente ya existe.

16

Error al iniciar el DSA creado. Consulte los archivos de registro para obtener más información.

17

Se suministraron parámetros de línea de comandos incorrectos o desconocidos.

18

El DSA correspondiente no existe.

Cómo crear copias de seguridad de datos de CA Directory

Lleve a cabo el siguiente proceso para realizar copias de seguridad de datos de CA Directory:

1. Conecte con un DSA local.
2. Tome una copia de instantánea del DSA predeterminado en ejecución. Este proceso recibe el nombre de volcado en línea. Use el siguiente comando para tomar la instantánea:

   dump *dxgrid-db*

   Nota: Sustituya dxgrid-db por el nombre del DSA iTechPoz-Servern para realizar la copia de seguridad de CA EEM.
3. Use la herramienta DXdumpdb para realizar la copia de seguridad del volcado en línea (archivos .ZDB), que es la copia de instantánea del almacén de datos para un archivo LDIF.

Más información:

Conecte con una consola del DSA local. (en la página 68)
Volcado de almacenes de datos en línea (en la página 69)
Comando dump dxgrid-db: toma una copia de instantánea coherente de un almacén de datos (en la página 70)

Conecte con una consola del DSA local.

Puede conectar con un DSA de forma local en UNIX o Windows si se ha establecido un puerto de la consola para dicho DSA.

Para conectar con una consola de DSA local

1. Abra un símbolo de sistema en el host en el que se ejecute el DSA.
2. Introduzca el siguiente comando:

   telnet localhost *número-puerto-local*

   número-puerto-local

   Especifica el número de puerto de la consola del DSA con el que desea conectar.

Volcado de almacenes de datos en línea

Puede tomar una copia de instantánea coherente del almacén de datos un DSA en ejecución (un volcado en línea). El DSA completa todas las actualizaciones antes de llevar a cabo el volcado en línea y no inicia más actualizaciones hasta que se haya finalizado la copia.

El archivo del almacén de datos se copia a un archivo con una extensión que comienza por .z, por lo que el archivo de la base de datos es *dxgrid-db*.zdb.

Nota: Cada volcado sobrescribe el archivo de copia de seguridad anterior. Si desea guardar el archivo de copia de seguridad, cópielo a otra ubicación antes del siguiente volcado.

Comando dump dxgrid-db: toma una copia de instantánea coherente de un almacén de datos

El comando *dump dxgrid-db* toma una copia de instantánea coherente del almacén de datos un DSA en ejecución (un volcado en línea). El DSA completa todas las actualizaciones antes de llevar a cabo el comando y no inicia más actualizaciones hasta que se haya finalizado la copia.

El archivo del almacén de datos se copia en un archivo con una extensión que comienza por .z, por lo que el archivo de la base de datos es *dxgrid-db*.zdb.

Nota: Cada volcado sobrescribe el archivo de copia de seguridad anterior. Si desea guardar el archivo de copia de seguridad, cópielo a otra ubicación antes del siguiente volcado.

La herramienta DXdumpdb puede exportar datos de un almacén de datos creado por el comando de volcado.

El comando tiene el formato siguiente:

dump *dxgrid-db* [period *inicio periodo*];

period *inicio periodo*

(Opcional) Especifica que el volcado en línea se lleva a cabo en intervalos regulares.

iniciar

Establece el número de segundos desde la hora 00:00:00 a. m. GMT del domingo.

Nota: La hora de inicio se define en horario GMT y no en su hora local.

period

Define el número de segundos entre los volcados en línea.

Ejemplo: Realizar un volcado en línea cada hora

El siguiente comando toma una copia de instantánea del almacén de datos cada hora:

dump *dxgrid-db* 0 3600

Nota: Asegúrese de crear un trabajo cron en UNIX o una tarea programada en Windows para copiar el archivo de la copia de seguridad a una ubicación segura. Cada volcado sobrescribe los archivos de copia de seguridad anteriores.

Uso de un archivo LDIF para realizar copias de seguridad y cargar datos

Los *archivos LDIF* son archivos de texto que almacenan información de los directorios en LDIF. Los archivos LDIF pueden usarse para transferir información de directorios entre los servidores de directorios LDAP, o con el propósito de describir un conjunto de cambios que deberá aplicarse a uno de los directorios.

CA Directory incluye la herramienta DXdumpdb, que le permite descargar datos de un almacén de datos en un archivo LDIF. Posteriormente, puede cargar los datos del archivo LDIF en un almacén de datos para recuperar el contenido del directorio.

Realizar copias de seguridad de un directorio en un archivo LDIF

Para realizar copias de seguridad de un directorio en un archivo LDIF

1. Inicie sesión como el *dsa* de usuario (en UNIX) o el Administrator de DXserver (en Windows).
2. Use el siguiente comando para realizar una copia de seguridad del almacén de datos en el archivo LDIF:

   dxdumpdb -f *nombre de archivo* -z *nombre de dsa*

   -f *nombre de archivo*

   Especifica la ruta de archivo y el nombre con el que se vuelcan los datos.

   -z

   Especifica que DXdumpdb realice el volcado desde la copia del almacén de datos creada mediante el comando dump dxgrid-db.

   nombre de dsa

   Especifica el nombre del DSA.

Herramienta DXdumpdb: Exportar datos de un almacén de datos a un archivo LDIF

Use la herramienta DXdumpdb para exportar datos de un almacén de datos a un archivo LDIF.

Nota: Para obtener una lista de los códigos de estado que devuelven los comandos de DXtools, incluido este comando, consulte Códigos de estado de salida para DXtools (en la página 66).

Este comando presenta el siguiente formato:

dxdumpdb *opciones DSA*

opciones

Seleccione una o más de las siguientes opciones:

-f *nombre de archivo*

Especifica el archivo que recibirá los datos exportados. Si no se especifica esta opción, los resultados se muestran como resultados estándar o en pantalla.

-v

Se ejecuta en modo detallado. Esta opción cambia en el seguimiento de errores y estado. Para que la opción -v funcione correctamente, deberá especificar también la opción -f.

-z

Especifica que DXdumpdb realice el volcado desde la copia del almacén de datos creada mediante el comando *dump dxgrid-db*.

DSA

Define el DSA. DXdumpdb busca el almacén de datos que se exportará a un archivo LDIF en los archivos de configuración del DSA.

Ejemplo: Mostrar datos de democorp en pantalla

El siguiente ejemplo muestra en pantalla los datos de formato LDIF desde el almacén de datos del DSA *democorp*:

```
dxdumpdb democorp
```

Ejemplo: Realizar una copia de seguridad de un volcado de almacén de datos en línea

En el siguiente ejemplo se exporta un volcado de almacén de datos en línea a un archivo LDIF.

```
dxdumpdb -f eembackup -z iTechPoz-Servern
```

Cómo restaurar datos de CA Directory

Siga los siguientes pasos para restaurar CA Directory:

1. Detenga el DSA.
2. Use DXloaddb para cargar un almacén de datos de un archivo LDIF.

Herramienta DXloaddb: cargar un almacén de datos de un archivo LDIF

Use DXloaddb para cargar un almacén de datos desde un archivo LDIF. El almacén de datos debe existir con anterioridad. Se eliminará toda la información anterior del almacén de datos.

Notas de uso:

- No es necesario ordenar el archivo LDIF.
- DXloaddb codifica cualquier entrada de contraseña en el archivo LDIF que sea texto no codificado.

  Si se especifica algún algoritmo hash en la configuración de DSA, será el que use DXloadbdb. De lo contrario, utilizará SHA-1.
- De forma predeterminada, DXloaddb utiliza la configuración de DSA para la gestión de atributos operativos:
  - Si *op-attrs* = *true*, se cargarán todos los atributos operativos del archivo LDIF en el almacén de datos.

    Se agregará un atributo createTimestamp en el almacén de datos a todas las entradas del archivo LDIF que no cuenten con un atributo createTimestamp.
  - Si *op-attrs* = *false*, se ignorarán los atributos operativos del archivo LDIF y DXloaddb no creará atributos operativos.

Este comando presenta el siguiente formato:

dxloaddb [*opciones*] *dsa archivo-ldif*

opciones

Seleccione una o más de las siguientes opciones:

-n

Especifica que DXloaddb no realice ninguna acción.

-O

Especifica que DXloaddb debe incluir atributos operativos estándar, como la política de contraseñas (por ejemplo, número de intentos de inicio de sesión), y los atributos de fecha y hora. Si se especifica esta opción, DXloaddb crea cualquier atributo operativo que no se haya definido en el archivo LDIF.

-s

Especifica que DXloaddb debe producir las siguientes estadísticas en relación con el almacén de datos:

- Tamaño de datos total en MB
- Número total de entradas
- Número de entradas ignoradas
- Alargamiento total en el archivo del almacén de datos en KB
- Número promedio de entradas por MB

-v

Especificar modo detallado.

ldif-file

El nombre del archivo LDIF que se cargará en el almacén de datos.

DSA

Especifica el DSA cuyo almacén de datos se debe cargar.

Ejemplo: Crear y cargar un almacén de datos

La secuencia correcta en la que crear y cargar un almacén de datos es:

```
dxnewdb
dxloaddb
```

Ejemplo: Cargar datos LDIF en el almacén de datos

En el siguiente se cargan los datos del archivo democorp.ldif al almacén de datos democorp:

```
dxloaddb democorp democorp.ldif
```

A continuación, aparece una parte posible de democorp.ldif:

```
dn: o=Democorp, c=US
oc: organization
dn: ou=Administration, o=Democorp, c=US
oc: organizationalUnit
dn: cn=Fred Jones, ou=Administration, o=Democorp, c=US
oc: organizationalPerson
postalAddress: 11 Main Street $ Newtown
surname: Jones
title: Manager
telephonenumber: +1 (123) 456 7890
telephonenumber: +1 (987) 654 3210
dn: ou=Sales, o=democorp, c=US
oc: organizationalUnit
```

El número de teléfono aparece dos veces ya que es un atributo con varios valores

Capítulo 8: Configuración de la conmutación por error

Esta sección contiene los siguientes temas:

Conmutación por error

La conmutación por error es la capacidad de asegurar el flujo ininterrumpido de datos y el funcionamiento incluso cuando los datos no están disponibles.

Para que funcione la conmutación por error de CA EEM, deberá asociar una aplicación al CA EEM instalado en un servidor para obtener información acerca de otros servidores. La información acerca de la configuración de otros servidores está disponible en el archivo iPoz.conf que se utiliza para conmutar errores.

Puede configurar CA EEM para que sea compatible con dos tipos de escenarios de conmutación por error:

- Conmutación por error del almacén de datos
- Conmutación por error del servidor (en la página 83)

Nota: En esta situación, se presupone que los nombres de host son Server1, Server2... y ServerN.

Conmutación por error del almacén de datos para las aplicaciones

El servidor de CA EEM utiliza CA Directory como almacén de datos para las aplicaciones. Este almacén de datos para las aplicaciones proporciona compatibilidad integrada para la conmutación por error y la recuperación. Sincronice los siguientes elementos en la configuración de conmutación de error para todos los servidores.

1. Hora del sistema
2. Modo de seguridad (no FIPS o sólo FIPS)
3. Almacén de datos para las aplicaciones
4. Asegure que la búsqueda de DNS se produce correctamente.

Importante: Haga una copia de seguridad del almacén de datos para las aplicaciones antes realizar la sincronización. Si desea obtener más información sobre cómo hacer una copia de seguridad del almacén de datos, consulte Creación de una copia de seguridad de los datos de CA EEM almacenados en CA Directory (en la página 65).

Configuración de la conmutación por error del almacén de datos para las aplicaciones

Nota: Ejecute los pasos descritos en el procedimiento siguiente sobre el servidor primario. Los pasos que se deben realizar en los servidores secundarios aparecen mencionados de forma explícita.

Este procedimiento presupone que el servidor CA EEM está instalado con los siguientes valores predeterminados:

- usuario de dsa: dsa
- puerto de dsa de datos: 509
- Miembro del grupo

Si se han modificado cualesquiera de estos parámetros a un valor personalizado, sustituya los valores predeterminados por los valores personalizados.

Para configurarla conmutación por error del almacén de datos para las aplicaciones

1. Durante la configuración de la conmutación por error, detenga los servicios de CA EEM en todos los servidores con los siguientes comandos:

   Windows

   net stop igateway
   dxserver stop all
   ssld stop

   Linux y UNIX

   $IGW_LOC/S99igateway stop
   su - dsa -c "dxserver stop all"
   su - dsa -c "ssld stop"

2. Copie los siguientes archivos de cada uno de los servidores secundarios de CA EEM al servidor primario (supongamos que se llama Server1), en las carpetas respectivas:

   Windows

   %DXHOME%\config\knowledge\iTechPoz-*HostnameOfServerN*.dxc
   %DXHOME%\config\knowledge\iTechPoz-*HostnameOfServerN-Router*.dxc
   %DXHOME%\config\ssld\personalities\iTechPoz-*HostnameOfServerN*.pem
   %DXHOME%\config\ssld\personalities\iTechPoz-*HostnameOfServerN*-Router.pem

   Linux y UNIX

   $DXHOME/config/knowledge/iTechPoz-*HostnameOfServerN*.dxc
   $DXHOME/config/knowledge/iTechPoz-*HostnameOfServerN-Router*.dxc
   $DXHOME/config/ssld/personalities/iTechPoz-*HostnameOfServerN*.pem
   $DXHOME/config/ssld/personalities/iTechPoz-*HostnameOfServerN*-Router.pem

3. Copie el siguiente archivo desde los servidores secundarios a una carpeta temporal en el servidor primario Server1:

   UNIX y Linux

   $DXHOME/config/ssld/iTechPoz-trusted.pem

   Windows

   %DXHOME%\config\ssld\iTechPoz-trusted.pem

4. Edite los archivos de configuración (iTechPoz-*HostnameOfServerN*.dxc) de todos los servidores en el Server1 de la manera siguiente:

   Modifique la siguiente entrada:

   address = tcp localhost port 509

   #address = tcp HostnameOfServerN port 509, tcp localhost port 509

   #dsa-flags = multi-write

   Cámbiela a:

   #address = tcp localhost port 509

   address = tcp HostnameOfServerN port 509, tcp localhost port 509

   dsa-flags = multi-write

   Notas:

   - CA EEM utiliza el número de puerto 509 como el puerto de dsa de datos predeterminado. Si se ha configurado el servidor de CA EEM para poder utilizar un puerto de dsa de datos personalizado, sustituya 509 por el número de puerto personalizado.
   - Para utilizar direcciones IP en lugar de nombres de host, sitúe la dirección IP entre comillas dobles (" ").

5. Edite el archivo iTechPoz.dxg en Server1 para que incluya las referencias a los servidores secundarios.

   Ejemplo:

   ```
   # iTechPoz - iTechnology Repozitory
   # Source the knowledge files of the iTechPozRouter and iTechPoz DSAs.
   source "iTechPoz-HostnameofServer1-Router.dxc";
   source "iTechPoz-HostnameofServer1.dxc";
   source "iTechPoz-HostnameOfServer2-Router.dxc";
   source "iTechPoz-HostnameOfServer2.dxc";
   source "iTechPoz-ServerN-Router.dxc";
   source "iTechPoz-ServerN.dxc";
   ```

6. Cree un nuevo archivo iTechPoz-trusted.pem. Para ello, concatene los contenidos del archivo iTechPoz-trusted.pem de cada uno de los servidores secundarios con Server1.

   Windows

   type <ruta absoluta de iTechPoz-trusted.pem de Server2> >> <ruta absoluta de iTechPoz-trusted.pem de Server1>

   UNIX o Linux

   cat <ruta absoluta de iTechPoz-trusted.pem de Server2> >> <ruta absoluta de iTechPoz-trusted.pem de Server1>

   Ejemplo: tipo de "C:\Archivos de programa\CA\Directory\dxserver\config\ssld\iTechPoz-trusted_2.pem" >> "C:\Archivos de programa\CA\Directory\dxserver\config\ssld\iTechPoz-trusted.pem

7. Concatene el contenido de iTechPoz-trusted.pem de cada servidor secundario con el archivo iTechPoz-trusted.pem en Server1.

8. Copie los archivos siguientes del servidor primario en las carpetas respectivas de todos los servidores secundarios:

   Nota: Haga una copia de seguridad de iTechPoz-trusted.pem, de los archivos de dsa de datos y de enrutamiento (iTechPoz*) de los servidores secundarios antes de realizar el copiado.

   UNIX y Linux

   $DXHOME/config/ssld/iTechPoz-trusted.pem
   $DXHOME/config/ssld/personalities/iTechPoz-*.pem
   $DXHOME/config/knowledge/iTechPoz*

   Windows

   %DXHOME%\config\ssld\iTechPoz-trusted.pem
   %DXHOME%\config\ssld\personalities\iTechPoz-*.pem
   %DXHOME%\config\knowledge\iTechPoz*

9. Edite el archivo iTechPoz.dxg en cada uno de los servidores secundarios. El archivo iTechPoz.dxg debe contener:

   # iTechPoz - iTechnology Repozitory
   # Source the knowledge files of the iTechPozRouter and iTechPoz DSAs.
   source "iTechPoz-HostnameOfServerN-Router.dxc";
   source "iTechPoz-HostnameOfServerN.dxc";
   source "iTechPoz-HostnameOfServer1-Router.dxc";
   source "iTechPoz-HostnameOfServer1.dxc";
   source "iTechPoz-HostnameOfServer2-Router.dxc";
   source "iTechPoz-HostnameOfServer2.dxc";
   source "iTechPoz-ServerKRouter.dxc";
   source "iTechPoz-ServerK.dxc";

   Nota: Las entradas para el host local deben aparecer antes que las entradas para otros servidores.

10. Modifique la propiedad y pertenencia a grupo de los archivos siguientes a dsa y etrdir, respectivamente, para todos los servidores de CA EEM que se ejecuten en UNIX o Linux. Ejecute los siguientes comandos:

    chown dsa:etrdir /opt/CA/Directory/dxserver/config/ssld/iTechPoz-trusted.pem
    chown dsa:etrdir /opt/CA/Directory/dxserver/config/knowledge/iTechPoz*

11. Inicie el servicios de CA EEM en todos los servidores mediante los siguientes comandos:

    Windows

    ssld start
    dxserver start all
    net start igateway

    Linux y UNIX

    su - dsa -c "ssld start"
    su - dsa -c "dxserver start all"
    $IGW_LOC/S99igateway start

    Se guardará la configuración de la conmutación por error del almacén de datos para las aplicaciones.

Conmutación por error del servidor de CA EEM

Nota: Asegúrese de que instala la misma versión de servidor de CA EEM en todos los servidores de la instalación de conmutación por error (Server1, Server2... y ServerN) y de que sincroniza la hora del sistema.

Puede configurar Server1 para que confíe en las sesiones y certificados de todos los demás servidores de la instalación de conmutación por error. Repita el procedimiento siguiente con todos los servidores de la instalación de conmutación por error.

Para configurar la conmutación por error en Server1

1. Introduzca la URL https://server1:5250/spin.
2. Seleccione iTech Administrator y haga clic en Ir.

   Aparecerá la pantalla Iniciar sesión.
3. Escriba las credenciales de inicio de sesión de la siguiente forma en función de su selección de la opción Tipo en la pantalla de inicio de sesión:

   Host

   Inicie sesión como root o Administrator.
4. Haga clic en la ficha de configuración, añada ServerN como nombre de host en el panel de host iAuthority de confianza y haga clic en Trust.

   Se añade una entrada en el archivo iControl.conf y Server1 comienza a confiar en las sesiones de ServerN.

   Nota: Agregue todos los demás servidores de la instalación de conmutación por error al panel de host iAuthority de confianza.
5. Haga clic en la ficha iAuthority, introduzca Label como ServerN, desplácese a la ubicación del archivo de certificado PEM en el panel de adición de raíz de confianza y haga clic en Add Trusted Root.

   Nota: El archivo de certificado PEM (rootcert.pem) está ubicado en el directorio iTechnology de ServerN.

   Se añade una entrada en iAuthority.conf, y Server1 comienza a confiar en los certificados de ServerN.

   Nota: Agregue entradas de certificado a todos los demás servidores de la instalación de conmutación por error.

Configuración de archivos de CA EEM

Debe configurar Server1 de CA EEM para recibir la lista de servidores disponibles de apoyo, que son versiones replicadas.

Para configurar el Server1 de CA EEM

1. Abra el directorio iTechnology de Server1.
   - **Windows**: %IGW_LOC%
   - **Linux y UNIX**: /opt/CA/SharedComponents/iTechnology (predeterminado)
2. Abra el archivo iPoz.conf y añada la siguiente etiqueta:

   <BackboneMember>Server2</BackboneMember>
3. Detenga e inicie iGateway.

   Windows

   net stop igateway
   net start igateway

   Linux y UNIX

   /opt/CA/SharedComponents/iTechnology/S99igateway stop
   /opt/CA/SharedComponents/iTechnology/S99igateway start

Asimismo, debe configurar Server2 de CA EEM para recibir la lista de servidores disponibles de apoyo, que son versiones replicadas.

Para configurar el Server2 de CA EEM

1. Abra el directorio iTechnology de Server2.
   - **Windows**: %IGW_LOC%
   - **Linux y UNIX**: /opt/CA/SharedComponents/iTechnology (predeterminado)
2. Abra el archivo iPoz.conf y añada la siguiente etiqueta:

   ```
   <BackboneMember>Server1</BackboneMember>
   ```

3. Detenga e inicie iGateway.

   Windows

   ```
   net stop igateway
   net start igateway
   ```

   Linux y UNIX

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

Nota: Repita el procedimiento anterior en todos los servidores de CA EEM configurados en la instalación de conmutación por error.

Capítulo 9: Federación de artefactos

Habilitar la federación de artefactos

Si desea utilizar la federación de artefactos, realice el siguiente procedimiento en todos los servidores de CA EEM durante una instalación de conmutador por error.

Habilitar la federación de artefactos

1. Detenga el servicio iGateway.
2. Busque y abra el archivo iPoz.conf.
3. Edite la siguiente etiqueta:

   <ArtifactManager SessionTimeout="10"
   RequestTimeout="30"ArtifactStore="local/federated"></ArtifactManager>

   Dónde

   SessionTimeOut

   Especifica el tiempo de caducidad en minutos durante una sesión exportada.

   Valor predeterminado: 10 minutos

   Intervalo:

   RequestTimeOut

   Especifica el tiempo de caducidad en minutos para una solicitud de ejecución.

   Valor predeterminado: 30 minutos

   Intervalo:

   Store

   Especifica la ubicación de almacenamiento de los artefactos. Si el valor se menciona como local, los artefactos de un servidor de CA EEM no están disponibles en otros servidores de CA EEM en la instalación de conmutación por error. Para que los artefactos estén disponibles en todos los servidores de CA EEM, establezca el valor de este parámetro en federated.

   Valor: [local|federated]

   Valor predeterminado: local

Nota: Los parámetros SessionTimeOut y RequestTimeOut también se encuentran presentes en el archivo eiam.conf. Si especifica estos parámetros en el archivo eiam.conf, los valores del archivo eiam.conf prevalecen.

4. Guarde y cierre el archivo.
5. Reinicie el servicio iGateway.

   La federación de artefactos está habilitada.

Capítulo 10: Integración con CA SiteMinder

Esta sección contiene los siguientes temas:

Cómo integrar CA SiteMinder con CA EEM

Para integrar CA SiteMinder con CA EEM, realice los siguientes pasos en el Administrator de CA SiteMinder:

- Cree un agente en CA SiteMinder para la comunicación entre el servidor de políticas de CA EEM y CA SiteMinder. Asegúrese de que el agente es compatible con agentes 4.x.
- Cree un Administrator o utilice el Administrator existente predeterminado de SiteMinder con el ámbito de nivel del sistema.
- Crear un directorio de usuarios de CA SiteMinder para obtener una autorización, que usará CA EEM para recuperar los atributos de LDAP.
- Establezca el campo ID universal para que identifique a un usuario del directorio, como sAMAccountName o UID. Puede establecer el campo ID universal desde la IU de SiteMinder, los directorios de usuario, Propiedades y la ficha Atributo de usuario.
- En la ficha Atributo de usuario, establezca el atributo de contraseña (RW) en userPassword.
- Cree un almacén de datos de CA SiteMinder para la autenticación, que usará CA EEM para autenticar usuarios.

  Nota: Si el almacén de usuarios de autorización y autenticación es el mismo, utilice el almacén de usuarios existente que se ha creado para la autorización.
- Cree un territorio con el filtro Recurso como /iamt.html.
- Cree un dominio de CA SiteMinder y agregue los directorios de usuario, el Administrator y el territorio al dominio.

Para obtener más información acerca de CA SiteMinder, consulte la documentación de CA SiteMinder.

Configuración del registro del servidor de CA EEM para los módulos de CA SiteMinder

Para configurar el nivel de registro para la integración de CA SiteMinder

1. Cree un archivo con los siguientes contenidos, y guarde el archivo con el nombre sm_log.properties:

   ```
   #filename: sm_log.properties
   #set the default logging level for the root logger
   .level = INFO
   #set the default logging level for the logger name com.ca.eiam
   com.ca.eiam.level = ALL
   ```

2. Modifique el nivel de registro del registrador de com.ca.eiam en el archivo sm.properties a cualquiera de los siguientes valores.

   SEVERO

   Especifica un nivel para mensajes que indican errores severos.

   ADVERTENCIA

   Especifica un nivel para advertencias.

   INFO

   Especifica un nivel para mensajes informativos.

   CONFIGURACIÓN

   Especifica un nivel para mensajes de configuración estáticos.

   AGUDO

   Especifica un nivel para la información de rastreo.

   ALL

   Especifica que se registran todos los niveles de mensajes.

3. Guarde el archivo en la ubicación siguiente:

   Windows

   %IGW_LOC%

   Linux y UNIX

   /opt/CA/SharedComponents/iTechnology

4. Detenga el servicio iGateway.

5. Abra el archivo iGateway.conf desde la ubicación especificada en el Paso 3, y agregue las etiquetas siguientes entre las etiquetas <JVMSettings></JVMSettings>:

   ```
   <Properties name="eiam.sm">
   <system-properties>java.util.logging.config.file=sm_log.properties</system-properties>
   </Properties>
   ```

6. Guarde y cierre el archivo.
7. Inicie el servicio iGateway.

Capítulo 11: Registro del SDK de CA EEM

Para los SDK de Java y C++, el nuevo proceso de registro de CA EEM utiliza log4j y log4cxx, respectivamente, como marcos de registrador. El proceso de registro anterior utilizaba un registrador de utilidad safe::util. Esta nueva característica le proporciona las siguientes ventajas.

- No es necesario reiniciar la aplicación si actualiza o modifica los niveles de registro.
- Puede gestionar las propiedades de registro (como el nombre de archivo, el tamaño del archivo, el número de archivos de registro de copia de seguridad, etc.) mediante la edición de los parámetros en el archivo de configuración del registrador.
- Puede clasificar los mensajes de registro del SDK de CA EEM en llamadas de red y estadísticas de rendimiento.

Nota: No se actualiza el registro en el SDK C# de CA EEM. Debe seguir utilizando safe::util para registrar los mensajes en el SDK de C# de CA EEM.

El registro le permite guardar mensajes, errores e información generada por el SDK de CA EEM. En el SDK de CA EEM, los siguientes archivos se encargan de controlar el registro:

- eiam.log4cxx.config
- eiam.log4j.config

Estos tres archivos son parte del paquete del SDK de CA EEM y se encuentran de forma predeterminada en la carpeta Bin del siguiente modo.

UNIX

/opt/CA/eIAMSDK/bin

Windows

C:\Archivos de programa\CA\Embedded IAM SDK\bin

Acerca de los archivos de configuración del registrador

Los archivos de configuración del registrador, eiam.log4cxx.config y eiam.log4j.config, se utilizan para configurar el registro del SDK de CA EEM. Estos archivos contienen los siguientes componentes principales:

- Salidas de destino
- Registradores
- Registrador raíz

Estos componentes contienen parámetros configurables que le permiten personalizar el proceso de registro según las necesidades de su negocio.

Salida de destino (appender)

Las salidas de destino contienen parámetros que controlan el registro de cada registrador. De forma predeterminada, los archivos de configuración del registrador contienen las siguientes salidas de destino:

SDK

Registra los mensajes del SDK en un archivo de registro. Especifica la ruta que incluye el nombre de archivo del archivo de registro.

Valor predeterminado: eiam.cppsdk.log

Nota: Si va a implementar su aplicación en un servidor Tomcat en Windows, asegúrese de utilizar una barra diagonal '/' en lugar de la antibarra '\'. Si utiliza una antibarra, el archivo de registro no se crea en la ruta que ha especificado. En su lugar, se crea el archivo de registro en la carpeta Apache Tomcat.

Red

Registra la llamada de red relacionada con los mensajes en un archivo de registro.

Valor predeterminado: eiam.network.cpp.log

Rendimiento

Registra la llamada de rendimiento relacionada con los mensajes en un archivo de registro.

Valor predeterminado: eiam.performance.cpp.log

Consola

Muestra los mensajes de registro en la consola.

La salida de destino del SDK está habilitada de forma predeterminada. Para habilitar otros parámetros, elimine las cadenas de comentarios (<!-- y -->) de su código respectivo.

Las salidas de destino constan de los siguientes parámetros configurables:

file

Especifica el nombre de archivo de registro de la salida de destino.

append

Especifica si se anexa un conjunto de mensajes de registro se encuentra anexado al archivo de registro. Si el valor es true, se anexa un conjunto de mensajes de registros al último mensaje de registro del archivo de registro.

BufferedIO

Especifica si se almacena en búfer el mensaje de registro más reciente. Si el valor es true, los mensajes de registro más recientes guardan en la memoria antes de escribir en el archivo de registro. De esta forma, se minimizan las operaciones de E/S y es beneficioso si el nivel de registro es elevado.

Valor: [*true*|*false*]

Valor predeterminado*:* false

Nota: El valor predeterminado de BufferedIO es 8 KB.

maxFileSize

Especifica el tamaño máximo del archivo de registro. Si un archivo de registro supera el tamaño máximo, se crea un archivo de registro nuevo con el nombre log.1 y se transfiere el contenido del archivo de registro al archivo log.1. El archivo de registro ahora contiene los mensajes de registro más recientes. Si este archivo supera el tamaño máximo, se crea un archivo de registro nuevo con el nombre log.2, el contenido de log.1 se transfiere al archivo de registro log.2 y el contenido del archivo de registro se transfiere al archivo log.1.

Valor predeterminado: 10 MB

Mínimo: 10 KB

Máximo: 2 GB

Nota: El tamaño mínimo de maxFileSize debe ser superior o igual que el tamaño de BufferedIO.

maxBackupIndex

Especifica el número máximo de archivos de registro de copia de seguridad que se utilizan para conservar los registros antiguos. Si el número de archivos de registro supera el valor de índice de copia de seguridad máximo, se elimina el archivo que tenga los mensajes de registro más antiguos.

Valor predeterminado: 1

Mínimo: 1

Máximo: 12

ConversionPattern

Especifica el formato de un mensaje de registro. Configura los modificadores de formato y los caracteres de conversión que definen el patrón de conversión.

Nota: Para obtener más información acerca de los patrones de conversión, consulte el tema log4j en www.apache.org.

Ejemplo: Salida de destino del SDK

```
<appender name="SDK" class="org.apache.log4j.RollingFileAppender">
```

```
        <!-- The active sdk log file -->
        <param name="file" value="eiam.cppsdk.log" />
        <param name="append" value="true" />
        <param name="BufferedIO" value="false"/>
        <param name="maxFileSize" value="10000KB" />
        <param name="maxBackupIndex" value="1" />
        <layout class="org.apache.log4j.PatternLayout">
        <!-- The log message pattern -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
</appender>
```

Anexos en eiam.log4net.config

Los anexos contienen parámetros que controlan el registro de cada registrador. De forma predeterminada, los archivos de configuración del registrador contienen los siguientes anexos:

SDK

Registra los mensajes del SDK en un archivo de registro. Especifica la ruta en incluye el nombre del archivo de registro.

Predeterminado: EIAM.C#SDK.log

Nota: Si está implementando su aplicación en el servidor de Tomcat en Windows, asegúrese de que utiliza la barra diagonal '/' en la ruta en lugar de la barra invertida '\'. Si utiliza la barra invertida, el archivo de registro no se creará en la ruta que ha especificado; en cambio, el archivo de registro se creará en la carpeta Apache Tomcat.

Red

Registra los mensajes relacionados con la llamada de red en un archivo de registro.

Predeterminado:EIAM.NETWORK.C#SDK.log

Rendimiento

Registra los mensajes relacionados con la llamada de rendimiento en un archivo de registro.

Predeterminado: EIAM.PERFORMANCE.C#SDK.log

Consola

Muestra los mensajes de registro sobre la consola.

Se activa el adicionador de SDK de forma predeterminada. Para activar otros adicionadores, elimine las cadenas de comentarios (<!-- y -->) de su código respectivo.

Un adicionador está formado por los parámetros configurables siguientes:

archivo

Especifica el nombre de archivo de registro del adicionador.

appendToFile

Especifica si un conjunto de mensajes de registro se añaden al archivo de registro. Si el valor es verdadero, el conjunto de mensajes de registro se añade en el último mensaje de registro en el archivo de registro.

maxSizeRollBackups

Especifica el número máximo de archivos de registro de copia de seguridad utilizado para mantener registros antiguos. Si el número de archivos de registro supera el valor máximo del índice de copia de seguridad, el archivo con los mensajes de registro más antiguos se suprimirá.

Predeterminado: 1

Mínimo: 1

Máximo: 12

rollingStyle

Especifica si el último mensaje de registro se almacena en búfer. Si el valor es verdadero, los últimos mensajes de registro se guardan en la memoria antes de escribir en el archivo de registro. Esto minimiza la operación de E/S y es beneficioso si el nivel de registro es más alto.

Valor: [*verdadero*|*falso*]

Valor predeterminado*:* falso

Nota: El tamaño predeterminado de BufferedIO es 8 KB.

maximumFileSize

Especifica el tamaño máximo del archivo de registro. Si un archivo de registro supera el tamaño máximo, un nuevo nombre de archivo de registro log.1 se crea y los contenidos del archivo de registro se transfieren al archivo log.1. El archivo de registro contiene los últimos mensajes de registro. Si este archivo también supera el tamaño máximo, un nuevo nombre de archivo de registro log.2 se crea, los contenidos de log.1 se transfieren al archivo log.2, y los contenidos del archivo de registro se transfieren al archivo log.1.

Predeterminado: 10 MB

Mínimo:10 KB

Máximo: 2 GB

Nota: El tamaño mínimo de maxFileSize debe ser mayor que o igual al tamaño de rollingStyle.

ConversionPattern

Especifica el formato de un mensaje de registro. Configure los modificadores de formato y los caracteres de conversión para definir el patrón de conversión.

Nota: Para obtener más información sobre los patrones de conversión, consulte el tema log4net en www.apache.org.

Registrador (logger)

Los registradores le permiten controlar el funcionamiento de la red, los mensajes de registro de rendimiento se clasifican en función de los niveles y se muestran en tiempo de ejecución. De forma predeterminada, los registradores Red y Rendimiento están desactivados. Para activar un registrador, elimine las cadenas de comentarios de sus códigos respectivos.

Los registradores contienen los siguientes parámetros:

logger name

Especifica el nombre de un registrador.

additivity

Especifica si los mensajes de registro de rendimiento o la red están duplicados en el archivo de registro del SDK.

Valor: [*true*|*false*]

Valor predeterminado: false

level value

Especifica el nivel de registro de un registrador.

Valor: [*Trace*|*Debug*|*Info*|*Warn*|*Error*|*Fatal*|*Off*]

A continuación, puede encontrar los niveles de registro en orden de prioridad:

Nota: Cuanto mayor sea el nivel de registro, menor será el rendimiento de CA EEM.

Realizar seguimiento

Indica un nivel de depuración bajo. Contiene flujos de control y transfiere argumentos.

Depurar

Indica los mensajes que se usan para el diagnóstico de problemas. Contiene información contextual.

Información

Indica información contextual que realiza un seguimiento de la ejecución a nivel general en un entorno de producción.

Advertencia

Indica un posible problema en el sistema. Por ejemplo, si la categoría del mensaje se corresponde con la seguridad, debe aparecer un mensaje de advertencia al detectar ataques de diccionario.

Error

Indica un problema grave en el sistema. El problema no se puede recuperar y es necesario intervenir manualmente.

Grave

Indica una excepción de aplicación severa.

Desactivado

Indica la ausencia de registros.

Nota: El nivel de registro de la salida de destino del SDK debe ser Error.

Ejemplo: Registrador de rendimiento

```
<logger name="Perform" additivity="false">
    <level value="trace"/>
    <appender-ref ref="Performance" />
</logger>
```

Registrador raíz

El registrador raíz controla el nivel de registro de todas las salidas de destino. Sin embargo, si el nivel de registro de la salida de destino a la que se hace referencia en el registrador raíz difiere del nivel de registro especificado en la salida de destino principal, el nivel de registro de prioridad más elevado reemplazará al nivel de prioridad más baja.

Por ejemplo, si el nivel de registro del registrador raíz es Error y el nivel de registro de la salida de destino de red es Trace, el nivel de registro Trace reemplaza a Error y el sistema tiene en cuenta los mensajes de registro del nivel Trace en tiempo de ejecución.

Ejemplo: Registrador raíz

```
<root>
    <priority value="error" />
    <appender-ref ref="SDK" />
    <appender-ref ref="Console" />
</root>
```

Configuración de los archivos de registro

CA EEM le permite configurar los mensajes de registro relacionados con la red, el rendimiento, la consola y las clases del SDK.

Para configurar los archivos de registrador

1. Abra el archivo de configuración de registrador, eiam.log4cxx.config o eiam.log4j.config, en un editor de texto.
2. Habilite los registradores y las salidas de destino.
3. Actualice los parámetros de las salidas de destino.
4. Guarde el archivo de configuración de registrador.

Ejemplo de un archivo eiam.log4cxx.config

A continuación, se encuentra un ejemplo del archivo eiam.log4cxx.config:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE log4j:configuration SYSTEM "log4j.dtd">
<!-- Note that this file is read by the sdk every 60 seconds -->

<log4j:configuration xmlns:log4j="http://jakarta.apache.org/log4j/">

    <appender name="SDK" class="org.apache.log4j.RollingFileAppender">
        <!-- The active sdk log file -->
        <param name="file" value="eiam.cppsdk.log" />
        <param name="append" value="true" />
        <param name="BufferedIO" value="false"/>
        <param name="maxFileSize" value="10000KB" />
        <param name="maxBackupIndex" value="1" />
        <layout class="org.apache.log4j.PatternLayout">
        <!-- The log message pattern -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
    </appender>

    <appender name="Network" class="org.apache.log4j.RollingFileAppender">
        <!-- The file to log Network calls -->
        <param name="file" value="eiam.network.cpp.log" />
        <param name="append" value="true" />
        <param name="BufferedIO" value="true"/>
        <param name="maxFileSize" value="10000KB" />
        <param name="maxBackupIndex" value="1" />
        <layout class="org.apache.log4j.PatternLayout">
        <!-- The log message pattern -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
    </appender>

    <appender name="Performance" class="org.apache.log4j.RollingFileAppender">
        <!-- The file to log Performance calls -->
        <param name="file" value="eiam.performance.cpp.log" />
        <param name="append" value="true" />
        <param name="BufferedIO" value="true"/>
        <param name="maxFileSize" value="10000KB" />
        <param name="maxBackupIndex" value="1" />
        <layout class="org.apache.log4j.PatternLayout">
        <!-- The log message pattern -->
        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
        </layout>
    </appender>

    <appender name="Console" class="org.apache.log4j.ConsoleAppender">
        <!-- Logs to Console -->
        <layout class="org.apache.log4j.PatternLayout">
```

```
            <!-- The log message pattern -->
            <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c] %m%n"/>
            </layout>
        </appender>

        <!-- Remove comment to enable Performance Logging -->
        <!--
        <logger name="Perform" additivity="false">
            <level value="trace"/>
            <appender-ref ref="Performance" />
        </logger>
        -->

        <!-- Remove comment to enable Network Logging -->
        <!--
        <logger name="Network" additivity="false">
            <level value="trace"/>
            <appender-ref ref="Network" />
        </logger>
        -->

        <root>
            <priority value="error" />
            <appender-ref ref="SDK" />
            <!-- <appender-ref ref="Console" /> -->
        </root>
</log4j:configuration>
```

Ejemplo de un archivo eiam.log4net.config

El siguiente es un ejemplo de un archivo eiam.log4net.config:

```
<?xml version="1.0" encoding="utf-8" ?>

<log4net>
	<appender name="SDK" type="log4net.Appender.RollingFileAppender">
		<file value="EIAM.C#SDK.log" />
		<appendToFile value="true" />
		<maxSizeRollBackups value="1" />
		<maximumFileSize value="10000KB" />
		<rollingStyle value="Size" />
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>

	<appender name="Network" type="log4net.Appender.RollingFileAppender">
		<file value="EIAM.NETWORK.C#SDK.log" />
		<appendToFile value="true" />
		<maxSizeRollBackups value="1" />
		<maximumFileSize value="10000KB" />
		<rollingStyle value="Size" />
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>

	<appender name="Performance" type="log4net.Appender.RollingFileAppender">
		<file value="EIAM.PERFORMANCE.C#SDK.log" />
		<appendToFile value="true" />
		<maxSizeRollBackups value="1" />
		<maximumFileSize value="10000KB" />
		<rollingStyle value="Size" />
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>

	<appender name="ConsoleAppender" type="log4net.Appender.ConsoleAppender">
		<layout type="log4net.Layout.PatternLayout">
			<conversionPattern value="%date [%thread] %-5level %logger -
%message%newline" />
		</layout>
	</appender>
```

```
        <!-- Uncomment to enable Performance Logging -->
        <!--
        <logger name="Perform" additivity="false">
                <level value="ERROR"/>
                <appender-ref ref="Performance" />
        </logger>-->

        <!-- Uncomment to enable Network Logging -->
        <!--<logger name="Network" additivity="false">
                <level value="ERROR"/>
                <appender-ref ref="Network" />
        </logger>-->

        <root>
                <level value="ERROR" />
                <appender-ref ref="SDK" />
                <!--        <appender-ref ref="ConsoleAppender" />      -->
        </root>
</log4net>
```

Ejemplo de un archivo eiam.lo4j.config

El siguiente es un ejemplo de un archivo eiam.log4cxx.config:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE log4j:configuration SYSTEM "log4j.dtd">

<!-- Note that this file is read by the sdk every 60 seconds -->

<log4j:configuration xmlns:log4j="http://jakarta.apache.org/log4j/">

        <appender name="SDK" class="com.ca.eiam.log4j.RollingFileAppender">
                <!-- The active sdk log file -->
                <param name="file" value="eiam.javasdk.log" />
                <param name="append" value="true" />
                <param name="BufferedIO" value="false"/>
                <param name="maxFileSize" value="10000KB" />
                <param name="maxBackupIndex" value="1" />
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
                </layout>
        </appender>

        <appender name="Network" class="com.ca.eiam.log4j.RollingFileAppender">
                <!-- The file to log Network calls -->
                <param name="file" value="eiam.network.java.log" />
                <param name="append" value="true" />
                <param name="BufferedIO" value="false"/>
                <param name="maxFileSize" value="10000KB" />
                <param name="maxBackupIndex" value="1" />
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
                </layout>
        </appender>

        <appender name="Performance" class="com.ca.eiam.log4j.RollingFileAppender">
                <!-- The file to log Performance calls -->
                <param name="file" value="eiam.performance.java.log" />
                <param name="append" value="true" />
                <param name="BufferedIO" value="false"/>
                <param name="maxFileSize" value="10000KB" />
                <param name="maxBackupIndex" value="1" />
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
```

```
                </layout>
        </appender>

        <appender name="Console" class="com.ca.eiam.log4j.ConsoleAppender">
                <!-- Logs to Console -->
                <layout class="com.ca.eiam.log4j.PatternLayout">
                        <!-- The log message pattern -->
                        <param name="ConversionPattern" value="%5p %d{ISO8601} [%t] [%c]
%m%n"/>
                </layout>
        </appender>

        <!-- Uncomment to enable Performance Logging -->
        <!--
        <logger name="Perform" additivity="false">
                <level value="trace"/>
                <appender-ref ref="Performance" />
        </logger>
        -->

        <!-- Uncomment to enable Network Logging -->
        <!--
        <logger name="Network" additivity="false">
                <level value="trace"/>
                <appender-ref ref="Network" />
        </logger>
        -->

        <root>
                <priority value="error" />
                <appender-ref ref="SDK" />
                <!-- <appender-ref ref="Console" /> -->
        </root>

</log4j:configuration>
```

Capítulo 12: Configuración de asistencia del servidor de directorio externo

Esta sección contiene los siguientes temas:

Configuración de un directorio externo con CA EEM

Si está utilizando almacenes de directorio externos diferentes para la autenticación y autorización, configure CA EEM de la siguiente manera:

- Utilice el archivo iPoz.conf para configurar el directorio de autenticación externo con CA EEM
- Utilice la interfaz gráfica de usuario de administrador de CA EEM para configurar el servidor de CA EEM con el directorio de autorización externo.

  Nota: Para obtener más información sobre cómo configurar referencias al directorio externo, consulte la Ayuda en línea.

Para configurar el servidor de CA EEM para usar un directorio externo para la autenticación, configure las opciones siguientes en el archivo iPoz.conf que se encuentra en la carpeta /CA/SharedComponents/iTechnology después de la instalación.

Nota: Detenga iGateway antes de modificar el archivo iPoz.conf y reinícielo después.

UseExternalAuthDirectory

Especifica si desea usar un directorio externo distinto para la autenticación. Introduzca True para utilizar un directorio externo distinto. La opción predeterminada es False.

ExternalAuthDirType:

Especifica el tipo del directorio externo. Los tipos admitidos actualmente incluyen CA Identity Manager, Custom Mapped Directory, Microsoft Active Directory, Novell eDirectory, Novell eDirectory-CN y Sun One Directory.

ExternalAuthDirUserDn

Especifica el UserDn del tipo de directorio externo especificado.

ExternalAuthDirPassword

Especifica la contraseña de usuario en formato codificado.

Nota: Debe modificar la contraseña mediante el siguiente comando y pegarla en el archivo ipoz.conf.

/iTechnology/safex -munge *<contraseña en texto no cifrado>*

ExternalAuthDirHost

Especifica el nombre de host en el que se ha configurado el directorio externo.

ExternalAuthDirPort

Especifica el número de puerto que utiliza el directorio externo.

ExternalAuthDirUserSearchPreFilter

Especifica el filtro previo a la búsqueda en función del directorio externo. Puede buscar cualquier clase de objeto, como por ejemplo usuarios.

ExternalAuthDirUserSearchPostFilter

Especifica el filtro posterior a la búsqueda en función del directorio externo. Puede buscar cualquier clase de objeto, como por ejemplo usuarios.

ExternalDirCacheFolder

Especifica si el servidor de CA EEM debe guardar en la memoria caché las carpetas de directorio externas. Si esta etiqueta se configura en Verdadero, el servidor de CA EEM guarda en la memoria caché las carpetas externas a las que se puede acceder a través de la interfaz gráfica de usuario del administrador de CA EEM. Si esta etiqueta se configura en Falso, CA EEM no muestra las carpetas de directorio externas en la interfaz gráfica de usuario del administrador de CA EEM.

Valor: [verdadero|falso]

Valor predeterminado: **Verdadero**

Configuración del servidor de CA EEM para escapar barras diagonales en DN devuelto por directorios externos

Para configurar el servidor de CA EEM para usar un directorio externo para la autenticación, configure las opciones siguientes en el archivo iPoz.conf que se encuentra en la carpeta /CA/SharedComponents/iTechnology después de la instalación.

Nota: Detenga iGateway antes de modificar el archivo iPoz.conf y reinícielo después.

ExternalDirEscapeSlash

Especifica si CA EEM debe escapar la barra diagonal '/' en el DN devuelto por directorios externos. Configure esta etiqueta en Verdadero si CA EEM debe escapar la barra diagonal.

Nota: Se debe configurar CA EEM para escapar la barra diagonal en los DNS, de lo contrario CA EEM podría no recuperar bien los objetos.

Valor: [verdadero|falso]

Valor predeterminado: **Falso**

Configuración de asistencia de conmutación por error del directorio externo

Puede ampliar la capacidad de CA EEM para utilizar como apoyo otro servidor de directorio externo que sea una versión replicada del servidor.

Para ello, proporcione la asignación de iPoz.conf.

Nota: Debe detener iGateway antes de realizar cambios en el archivo iPoz.conf y reiniciarlo acto seguido.

ExternalDirHostBackup

Especifica el nombre de host del servidor de directorio externo replicado.

ExternalAuthDirHostBackup

Especifica el nombre de host del servidor de directorio externo distinto que se va a utilizar en la autenticación de usuarios.

Conexión con servidores de LDAP a través de TLS

Para establecer una conexión de TLS con el servidor de LDAP, debe configurar el servidor de LDAP para que acepte certificados anónimos. Para configurar EEM para conectarse a LDAP a través de TLS, haga lo siguiente:

Para configurar CA EEM para conectarse a LDAP a través de TLS

1. Inicie sesión en la interfaz gráfica de usuario de CA EEM.
2. Haga clic en Configurar, servidor de EEM.
3. Haga clic en Usuarios globales/Grupos globales.

   Aparecerá el panel Configuración del servidor de EEM.
4. Seleccione la referencia desde una opción de directorio externo.
5. Introduzca los detalles de configuración.

   Nota: Para obtener más información sobre los detalles de configuración, consulte la ayuda en línea.
6. Seleccione la opción Utilizar Transport Layer Security (TLS).
7. Haga clic en Guardar.

Conexión con servidores de LDAP a través de SSL

Para establecer una conexión SSL con servidores LDAP debe disponer de los siguientes certificados:

Certificado de una entidad emisora de certificados

Puede obtener este certificado a través de una entidad emisora de certificados, por ejemplo, Verisign o Thwate. Este certificado indica que los certificados emitidos por esta entidad emisora de certificados son válidos y de confianza.

Certificado de servidor LDAP

Debe obtener este certificado a través de una entidad emisora de certificados. Este certificado incluye información relacionada con el servidor LDAP y lo identifica con el cliente.

Nota: CA EEM es compatible solamente con certificados .pem para conexiones SSL.

Cómo se conecta CA EEM con el servidor LDAP a través de SSL

En el siguiente proceso se explica cómo el servidor de CA EEM y el servidor LDAP se comunican a través de SSL.

1. El servidor de CA EEM conecta con el servidor LDAP mediante un certificado de una entidad emisora de certificados.
2. El servidor LDAP comprueba el certificado de la entidad emisora de certificados y, si el certificado es válido, establece un protocolo de enlace con el servidor de CA EEM.
3. El servidor LDAP envía su clave pública al servidor de CA EEM durante el protocolo de enlace. La clave pública se usa para cifrar datos enviados al servidor LDAP.
4. El servidor de CA EEM utiliza la clave pública para cifrar los datos y los envía al servidor LDAP.
5. El servidor de CA EEM envía el nombre de usuario y la contraseña para autenticarla con el servidor LDAP.

Configuración de conexiones SSL

Debe llevar a cabo los siguientes pasos para configurar la comunicación SSL entre el servidor LDAP y el servidor de CA EEM:

1. Configure el servidor LDAP para el uso de certificados
2. Configure el servidor de CA EEM para la comunicación a través de SSL

Configure el servidor LDAP para el uso de certificados SSL

Para configurar el servidor de LDAP con el fin de usar SSL, debe realizar los siguientes pasos:

1. Obtenga un certificado de una entidad emisora de certificados e instale el certificado en el almacén de certificados de confianza en su servidor LDAP.
2. Obtenga un certificado de servidor de una entidad emisora de certificados e instale el certificado en el almacén de certificados de servidor en su servidor de LDAP.
3. Habilite el servidor LDAP para que acepte conexiones SSL.

Habilite SSL en el servidor de CA EEM

Para habilitar SSL en el servidor

1. Copie el certificado de la entidad emisora de certificados del servidor LDAP y guárdelo en el equipo en el que se esté ejecutando CA EEM.
2. Abra el archivo iPoz.conf y edite las siguientes etiquetas:

   <ExternalDirSSL>

   Especifica si la comunicación SSL está habilitada o no. Debe establecer esta etiqueta en "true" para habilitar la comunicación SSL.

   <ExternalDirCACertPath>

   Especifica la ruta donde se almacenará el certificado de autoridad en el equipo en que se ejecute el servidor de CA EEM.
3. Reinicie igateway.

Capítulo 13: Configurar compatibilidad con grandes cantidades de políticas

Esta sección contiene los siguientes temas:

Compatibilidad con grandes cantidades de políticas

Nota: CA EEM ofrece compatibilidad con grandes cifras de políticas en el entorno de cliente habilitado del SDK de C++.

Es necesario configurar el servidor de CA EEM y los clientes antes de registrar las aplicaciones que usarán una gran cantidad de políticas.

Nota: CA EEM admite hasta 20.000 políticas en la plataforma HP-UX.

Configurar otros parámetros para el servidor de CA EEM en AIX

Debe llevar a cabo los siguientes pasos adicionales para configurar el servidor de CA EEM con el fin de que admita el uso de una gran cantidad de políticas en AIX.

Para configurar el servidor de CA EEM en AIX

1. Modifique la configuración de red mediante el siguiente comando en el símbolo del sistema AIX:

   ```
   no -o tcp_nodelayack=1
   ```

2. Aumente el límite de procesamiento mediante el siguiente comando en el símbolo del sistema AIX:

   ```
   ulimit -d unlimited
   ulimit -f unlimited
   ```

Configuración de cliente

Debe configurar el cliente para que admita el uso de un gran número de políticas.

Configure el cliente para todos los sistemas operativos

Con el fin de admitir la distribución de un gran número de políticas, debe configurar los clientes para todos los sistemas operativos:

- Aumente el tiempo de actualización de caché de la aplicación para evitar las actualizaciones de caché durante el registro de aplicaciones con Safex.

  Para obtener más información acerca de la actualización de caché, consulte la *Guía de programación.*

  Nota: Es recomendable establecer el tiempo de actualización de caché a 3.600 segundos durante el registro para evitar que se lleven a cabo actualizaciones de caché durante el registro. Una vez haya finalizado el registro, cambie el tiempo de actualización de caché a 30 segundos, que es la configuración predeterminada.

- Habilite la entrega de eventos fiable.

  Para obtener más información acerca de la entrega de eventos fiable, consulte la *Guía de programación*.

Capítulo 14: Archivado de eventos

Esta sección contiene los siguientes temas:

Información general

CA EEM le permite generar y gestionar informes para eventos generados por el servidor de CA EEM. El sistema de archivado organiza los archivos archivados en los tres estados siguientes:

Archivos de base de datos disponibles

Hace referencia a los archivos archivados creados una vez que el número de eventos supera el máximo de filas en una base de datos de eventos. Se puede acceder a los archivos de base de datos disponibles para realizar consultas e informes desde el servidor de CA EEM. No se pueden introducir datos en los archivos de base de datos disponibles. Sólo se puede acceder a los archivos de base de datos disponibles en el servidor de CA EEM durante el número de días especificado como días de archivado máximos en la configuración del registro de eventos.

Archivos de base de datos no disponibles

Hace referencia a los archivos en estado disponible de los que se ha realizado una copia de seguridad manual en otra ubicación. No se puede realizar consultas ni crear informes a partir de un archivo de base de datos no disponible. Es necesario restaurar la disponibilidad de los archivos de base de datos no disponibles para realizar consultas o informes.

Archivos de base de datos restaurados para estar disponibles

Hace referencia a los archivos archivados en estado no disponible que han restaurado con el fin de que los usuarios puedan realizar consultas o generar informes a partir de un servidor de CA EEM. Sólo se podrá acceder a los archivos de base de datos restaurados para estar disponibles en el directorio de archivado durante el número de horas especificado como política de evento en la configuración del registro de eventos.

Para cambiar la configuración del registro de eventos

1. Inicie sesión en CA EEM.

   Aparecerá la página inicial de CA EEM.

2. Haga clic en Gestionar informes, Configuración, Servicios, Configuración del registro de eventos.

Aparecerá la configuración del registro de eventos.

Nota: Para obtener más información acerca de la configuración de servicios para la gestión de informes, consulte la *Ayuda en línea*.

Utilidad para restaurar la disponibilidad de archivos de base de datos no disponibles

CA EEM proporciona una utilidad para restaurar la disponibilidad de archivos de base de datos no disponibles. Debe restaurar los archivos y su disponibilidad antes de poder ejecutar consultas en los archivos y ver informes actuales. La herramienta SEM proporciona esta funcionalidad. Puede descargar la herramienta SEM en la sección Soporte en http://ca.com/support.

Para configurar la herramienta SEM

1. Extraiga los archivos comprimidos de la herramienta SEM.
2. Establezca las variables de entorno en función de su sistema operativo:

   Linux o Solaris

   Export LD_LIBRARY_PATH = <*sem_Extraction_Folder*>:$LD_LIBRARY_PATH

   AIX

   Export LIBPATH = <*sem_Extraction_Folder*> :$LIBPATH

   HP-UX

   Export SHLIB_PATH= <*sem_Extraction_Folder*> :$SHLIB_PATH

Nota: En el caso de Windows, para configurar la herramienta SEM, debe desplazarse desde la línea de comandos a la carpeta extraída y ejecutar sem.exe.

Sintaxis de la herramienta SEM

La herramienta SEM presenta la siguiente sintaxis:

sem -h <nombre de host> -u <usuario> -p <contraseña> -listcolddb | -defrost <archivo>

-h

Especifica el nombre de host del equipo en que se almacenen los archivos de base de datos no disponibles.

-u

Especifica el nombre de usuario utilizado para la autenticación con el servidor de CA EEM.

-p

Especifica la contraseña para un nombre de usuario usado para la autenticación con el servidor de CA EEM.

-listcolddb

Enumera todos los archivos de base de datos no disponibles almacenados en el equipo host.

-defrost <archivo>

Restaura la disponibilidad del archivo de archivado especificado.

-fips

Especifica que la utilidad de sem utilice algoritmos que cumplen con el estándar FIPS.

Nota: La utilidad de sem se debe utilizar con la opción de -fips si el servidor de CA EEM está configurado en un modo de sólo FIPS.

En la siguiente tabla se explican los valores devueltos de la herramienta SEM:

Valor de devolución	Descripción
0	Correcto
1	Argumentos no válidos
2	Nombre de usuario no válido
3	Error durante la autenticación
4	Error al enumerar los archivos de base de datos no disponibles
5	Error al restaurar un archivo de base de datos no disponible
6	Error de inicialización

Restauración de disponibilidad de archivos de base de datos no disponibles

Debe restaurar los archivos y su disponibilidad antes de poder ejecutar consultas en los archivos y ver informes actuales.

Nota: Antes de restaurar la disponibilidad, se deben copiar los archivos de base de datos no disponibles al directorio de archivado iTechnology\calm_archive.

Para restaurar archivos de base de datos no disponibles y su disponibilidad

1. Copie la carpeta con copia de seguridad calm_archive en la carpeta actual calm_archive.
2. Ejecute la herramienta SEM desde la línea de comandos para recuperar una lista de todos los archivos de base de datos no disponibles.

   sem -h <*nombre de host*> -u <*nombre de usuario*> -p <*contraseña*> -listcolddb

   Servidor de CA EEM en el modo de sólo FIPS

   sem -h <*nombre de host*> -u <*nombre de usuario*> -p <*contraseña*> -fips -listcolddb
3. Ejecute la herramienta SEM para restaurar la disponibilidad de archivos de base de datos no disponibles.

   sem -h <*nombre de host*> -u <*nombre de usuario*> -p <*contraseña*> -defrost <*archivo*>

   Servidor de CA EEM en el modo de sólo FIPS

   sem -h <*nombre de host*> -u <*nombre de usuario*> -p <*contraseña*> -fips -defrost <*archivo*>

   Se restaurarán los archivos de base de datos no disponibles y su disponibilidad.