IBM InfoSphere Identity Insight

Guía del usuario

Versión 9 Release 0

SC19-2870-01

IBM InfoSphere Identity Insight

Guía del usuario

Versión 9 Release 0

SC19-2870-01

Nota

Antes de utilizar esta información y el producto al cual da soporte, lea la información del apartado “Avisos” en la página 421.

Nota de edición

Esta edición se aplica a la versión 9 release 0 de IBM InfoSphere Identity Insight (número de producto 5724-L71) y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Contenido

Prefacio

IBM InfoSphere Identity Insight ayuda a las organizaciones a resolver problemas empresariales relacionados con el reconocimiento de la verdadera identidad de alguien o algo ("quién es quién") y con la determinación del valor potencial o el peligro de las relaciones ("quién conoce a quién") entre clientes, empleados, proveedores y otras fuerzas externas. Este análisis se produce en tiempo real y en el contexto de aplicación de negocio existentes. IBM InfoSphere Identity Insight proporciona información inmediata y enjuiciable para ayudar a prevenir amenazas, fraudes, abusos y connivencias en todos los sectores.

Acerca de esta publicación

IBM InfoSphere Identity Insight V8.1 es una plataforma de análisis y resolución de entidad escalable para combatir las amenazas y el fraude. Esta guía proporciona información sobre cómo utilizar y aplicar la tecnología de desambiguación de identidad y relación a la capacidad de la organización para reconocer quién es quién, quién conoce a quién y quién hace qué. Mediante la acumulación de contexto de identidad a lo largo del tiempo, InfoSphere Identity Insight V8.1 utiliza diversos orígenes de información de empresa para determinar si realmente las personas son quienes dicen ser. Puede aplicar algoritmos de entidad sofisticados junto con el análisis de nombres multiculturales patentado para determinar si una persona se ha identificado anteriormente, si una persona es nueva en la organización o si hay alguna suposición anterior que deba corregirse basándose en hechos nuevos.

Público destino

Esta guía está destinada a los administradores del sistema, desarrolladores de aplicaciones, analistas de datos y personal de IBM Professional Services para utilizar eficazmente el producto en el entorno.

Información relacionada y requisitos previos

Esta guía del usuario es un subconjunto de la información que se encuentra en el centro de información en línea (http://publib.boulder.ibm.com/infocenter/easii/v8r1m0/index.jsp). Se proporciona para comodidad del usuario. Otras fuentes de información sobre el producto incluyen:

- IBM InfoSphere Identity Insight Versión 8 Release 1 Notas del release
- Documentación de WebSphere Application Server
- Documentación de software de base de datos
- Documentación de software de IBM Cognos Business Intelligence
- Documentación de software de visualización de IBM ILOG
- En función del despliegue, la información siguiente:
  - Documentación del software de colas de mensaje
  - Documentación del software de corrección de direcciones
  - Documentación del software de la herramienta de extracción, transformación y carga

Cómo enviar comentarios

Sus comentarios son importantes y nos ayudan a proporcionar información de gran calidad. Si desea realizar algún comentario sobre esta publicación o sobre cualquier otra documentación relacionada con el producto IBM InfoSphere Identity Insight, utilice el siguiente formulario:

http://www.ibm.com/software/data/rcf/

También puede ir al Information Center y utilizar los formularios de comentarios incluidos y las opciones de comentarios relacionadas.

Cómo ponerse en contacto con el centro de soporte de software de IBM

El centro de soporte de software de IBM proporciona ayuda para los defectos del producto.

Antes de empezar

Antes de ponerse en contacto con el centro de soporte de software de IBM, la compañía debe disponer de un contrato de mantenimiento de software de IBM activo y el usuario debe estar autorizado para enviar problemas a IBM. Para obtener información acerca de los tipos de contratos de mantenimiento disponibles, consulte "Enhanced Support" en la publicación *Software Support Handbook* en techsupport.services.ibm.com/guides/services.html

Acerca de esta tarea

Complete los pasos siguientes para ponerse en contacto con el centro de soporte de software de IBM con un problema:

Procedimiento

1. Defina el problema, reúna la información de fondo, y determine la gravedad del problema. Para obtener ayuda, consulte "Contacting IBM" en la publicación *Software Support Handbook* en techsupport.services.ibm.com/guides/beforecontacting.html
2. Reúna la información de diagnóstico.
3. Cuando vaya a notificar el problema, tenga preparada la información siguiente para ayudar al centro de soporte de software de IBM:
   - Nombre y versión del producto
   - Tipo y versión de la base de datos
   - Nombre y versión del sistema operativo
4. Envíe el problema al centro de soporte de software de IBM de una de las maneras siguientes:
   - De forma electrónica: pulse **Enviar y hacer seguimiento de problemas** (Submit and track problems) en el sitio Web del centro soporte de software de IBM, situado en http://www.ibm.com/software/support/probsub.html
   - Por teléfono: para obtener el número de teléfono al que debe llamar en su país, vaya a la página Contacts de la publicación IBM Software Support Handbook en techsupport.services.ibm.com/guides/contacts.html

Qué hacer a continuación

Si envía un problema por un defecto de software o porque falta documentación, o ésta no es exacta, el centro de soporte de software de IBM crea un APAR (informe autorizado de análisis de programa). El APAR describe del problema con detalle. Siempre que es posible, el centro de soporte de software de IBM proporciona un método alternativo que se puede implementar hasta que se resuelve el APAR y se entrega un arreglo. IBM publica los APAR resueltos en el sitio web del centro de soporte diariamente, por lo que otros usuarios que experimenten el mismo problema pueden beneficiarse de la misma resolución.

Capítulo 1. Visión general de IBM InfoSphere Identity Insight

IBM® InfoSphere Identity Insight ayuda a las organizaciones a resolver problemas empresariales relacionados con el reconocimiento de la verdadera identidad de alguien o algo ("quién es quién") y a determinar el posible valor o peligro de relaciones ("quién conoce a quién") entre los clientes, empleados, proveedores y otras personas externas. IBM InfoSphere Identity Insight proporciona información inmediata y enjuiciable para ayudar a prevenir amenazas, fraudes, abusos y connivencias en todos los sectores.

En muchas organizaciones, los datos en bruto que representan identidades y relaciones ya existen. En la mayoría de sistemas el problema es que no existe una forma de gestionar, analizar y resolver el volumen de datos para obtener de él los máximos conocimientos posibles.

Con IBM InfoSphere Identity Insight, las organizaciones pueden gestionar, analizar e integrar en tiempo real datos procedentes de cualquier origen, como bases de datos de clientes, listas de proveedores, bases de datos de empleados, listas de cumplimiento legal y alimentaciones de datos en modalidad continua. IBM InfoSphere Identity Insight envía alertas en tiempo real a analistas, seguridad y otro personal para su investigación. IBM InfoSphere Identity Insight también ayuda a identificar el valor en la red de clientes o de sus segmentos de mercado, basándose en una completa visión del cliente.

Con IBM InfoSphere Identity Insight, las organizaciones pueden crear una base de datos de entidades central y dinámica que se puede utilizar como plataforma para todas sus aplicaciones basadas en conocimientos. IBM InfoSphere Identity Insight se integra con otros sistemas empresariales mediante diversos protocolos y tecnologías.

Reconocimiento de identidades

Utilizando el proceso central de la resolución de entidades, IBM InfoSphere Identity Insight resuelve registros de identidades incoherentes y ambiguos en entidades completas entre varios conjuntos de datos, a pesar de la existencia de intentos deliberados de malinterpretaciones.

Durante la resolución de entidades, IBM InfoSphere Identity Insight:

- Determina cuándo varios registros que parecen describir distintas entidades son realmente una sola entidad.
- Para cada entidad resuelta, integra los registros de identidades diferentes en una visión compuesta de la entidad, a la vez que mantiene una atribución completa para cada registro. La atribución completa asegura que nunca se pierden datos y que siempre se pueden restaurar a su origen original.
- A medida que se cargan nuevos datos en el sistema, IBM InfoSphere Identity Insight actualiza y gestiona la información en su contexto para las entidades de la base de datos de entidades. Puede abarcar por completo el significado de datos nuevos o modificados a medida que se cargan, sacando el máximo provecho de cada transacción y mejorando la visión completa de cada entidad en la base de datos de entidades.

Detección de relaciones

Basándose en el proceso de relación de entidades, IBM InfoSphere Identity Insight detecta relaciones entre entidades en la base de datos de entidades a medida que se cargan y se procesan registros procedentes de varios orígenes de datos.

Durante el proceso de resolución de entidades, IBM InfoSphere Identity Insight:

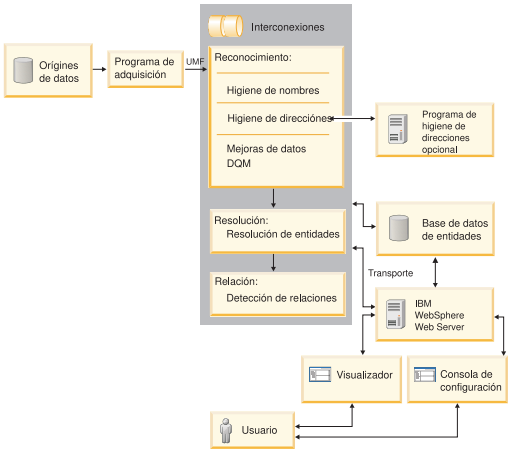
- Enlaza entidades por atributos de identidad, como números de teléfono y direcciones, para descubrir relaciones relevantes que aún no son obvias.
- Ensambla redes de asociaciones y entidades utilizando atributos de datos individuales (como números de identificación y nombres), ubicaciones (como direcciones IP), instalaciones (como almacenes, colegios, aeropuertos u hoteles), organizaciones (como clubes o asociaciones), dinero (como efectivo o transferencias) y cuentas (como cuentas bancarias, cuentas de crédito o cuentas de ahorro).
- Identifica relaciones sospechosas o interesantes, incluso las ocultas o escondidas, y envía alertas en tiempo real basadas en un conjunto de normas definidas por el usuario. IBM InfoSphere Identity Insight permite a los analistas e investigadores realizar búsquedas sofisticadas en la base de datos de entidades para explorar mejor cada entidad relacionada y cada entidad o atributo con el que están enlazadas dichas entidades.

IBM InfoSphere Identity Insight también da soporte a la creación de informes personalizados de excepciones basados en normas, de modo que las organizaciones pueden especificar qué entidades resueltas y qué relaciones detectadas activan alertas.

Arquitectura del producto

IBM InfoSphere Identity Insight es un sistema de varias capas en el que los datos procedentes de orígenes de datos se cargan en el sistema desde programas de adquisición y son procesador por las interconexiones albergadas en los nodos de interconexión. Los resultados del proceso se graban en la base de datos de entidades y se pueden direccionar a otros sistemas o a otras bases de datos.

En un despliegue típico, los datos de empresa procedentes de varios orígenes se envían a programas de adquisición, en los que los datos se transforman a UMF (Universal Messaging Format). Cada programa de adquisición utiliza un transporte para enviar los datos a una o varias interconexiones. Muchos de estos transportes son bidireccionales y el sistema se puede configurar de modo que proporcione respuestas al programa de adquisición.



En los nodos de interconexión se ejecutan uno o varios procesos de interconexión. Cada interconexión mantiene su propia conexión con la base de datos de entidades. Cuando la interconexión recibe los datos UMF de uno o varios programas de adquisición, procesa los datos registro a registro a través de sus tres procesos principales: reconocer, resolver y relacionar. A medida que se procesa cada registro, la interconexión almacena los resultados del proceso en la base de datos de entidades.

Los usuarios interactúan con el sistema mediante estas interfaces:

- Consola de configuración, que se utiliza para configurar y supervisar el sistema
- Aplicaciones de kit de herramientas de Analista, quese puede utilizar para analizar y disponer alertas, explorar relaciones, realizar búsquedas y generar informes
- Interfaces de línea de mandatos, que se utilizan para ejecutar interconexiones
- Servicios Web, que se pueden utilizar para ejecutar las interconexiones o para integrar el producto con otros sistemas de empresa, incluidas interfaces de usuario personalizadas

IBM InfoSphere Identity Insight utiliza IBM WebSphere Liberty. Este servidor de aplicaciones aloja la Consola de configuración, elementos del kit de herramientas de analista y los servicios web.

Esta potente arquitectura ofrece escalabilidad para cualquier despliegue. Las interconexiones se pueden desplegar en el número que se desee de máquinas pequeñas o grandes. El rendimiento de la interconexión se puede escalar al nivel deseado, siempre que se disponga de la suficiente capacidad de base de datos.

Programas de adquisición

Un programa de adquisición contiene las herramientas y programas que adquieren datos, los transforman al formato UMF (Universal Message Format) y luego envían los datos transformados a la interconexión para su proceso.

Puede utilizar los programas de utilidad del programa de adquisición que se proporcionan con el producto para transformar datos en UMD o puede utilizar herramientas de extracción, transformación y carga (ETL), como WebSphere QualityStage, como programas de adquisición.

Universal Message Format (UMF)

Universal Message Format (UMF) es un dialecto de XML extensible utilizado para estructurar archivos de fuente de datos. UMF contiene códigos estándar que representan partes clave de identificadores, relaciones y actividades. Para que las interconexiones puedan procesar los datos, estos se deben convertir a UMF y deben seguir la especificación UMF.

UMF consta de estos componentes jerárquicos:

Documentos UMF
Colección de segmentos UMF que estructuran los datos e indican el tipo de registro de fuente de datos.

Segmentos UMF
Parte del documento UMF que estructura los datos correspondientes a la fuente de datos.

Elementos UMF
Códigos y valores XML que definen los datos dentro de un segmento UMF de un documento UMF.

La especificación UMF lista los tipos específicos de documentos UMF, los segmentos UMF que hay dentro de cada tipo de documento UMF y los elementos UMF válidos dentro de cada segmento UMF.

Interconexiones

Las interconexiones son los componentes que realizan la estandarización de higiene de dirección y nombre, la gestión de calidad de datos y la resolución de entidades. Las interconexiones también realizan el proceso de resolución de relaciones y generan alertas, según la configuración del sistema.

Las interconexiones realizan tres procesos principales:

- Reconocer, lo que implica optimizar los datos de entrada realizando procesos de estandarización, higiene y mejora de los datos y comprobaciones de calidad.
- Resolver, lo que implica resolver entidades
- Relacionar, lo que implica detectar relaciones y generar alertas

Las interconexiones están alojadas en nodos de interconexión.

Puede configurar interconexiones para el proceso en paralelo de modo que un mandato de interconexión abarque varias hebras del proceso de interconexión en paralelo, lo que permite al sistema procesar simultáneamente varias solicitudes de datos. Esta característica puede ayudar a mejorar el rendimiento del sistema, a reducir el tiempo del proceso de datos y a mitigar las restricciones de memoria del hardware.

La característica de proceso de interconexión en paralelo es configura en dos lugares:

- El valor global de simultaneidad se controla mediante el parámetro `Simultaneidad predeterminada de conexiones` en la pestaña **Configuración del sistema** en la Consola de configuración. Este valor determina el número de hebras de proceso en paralelo que se inician desde un mandato de inicio de interconexión. El valor predeterminado para este parámetro es 1, lo que significa que, a menos que se edite este parámetro, sólo se inicia una hebra de proceso de interconexión.

- Se puede configurar un valor local de simultaneidad (por nodo de interconexión) en el archivo de configuración de interconexión. Si especifica un parámetro y un valor de simultaneidad en el archivo de configuración de interconexión por nodo de interconexión, dicho valor prevalece sobre el parámetro global del sistema. Cuando se emite un mandato de inicio de interconexión en dicho nodo de proceso, se inicia el número de hebras de proceso de interconexión simultáneas especificado en el archivo de configuración de interconexión.

Nodos de interconexión

Los nodos de interconexión son máquinas físicas que alojan uno o varios procesos de interconexión.

El nodo de interconexión es donde se instala y se inicia el ejecutable de la interconexión que ejecuta los procesos de interconexión. Debe configurar y mantener el archivo de configuración de interconexión correspondiente a todas las interconexiones alojadas en esta máquina. El sistema también graba los mensajes de interconexión en los archivos de registro de los nodos de interconexión.

Los nodos de interconexión conectan procesos de interconexión con estos componentes de la arquitectura del producto:

Programas de adquisición
Como parte del proceso de extracción, transformación y carga (ETL), los programas de adquisición utilizan transportes para enviar datos UMF a las interconexiones para su proceso. Debe utilizar el método de transporte que resulte adecuado para el tipo de programa de adquisición para conectar con las interconexiones. Por ejemplo, si utiliza el programa de utilidad de archivos UMF como un programa de adquisición, debe utilizar el transporte de archivos.

Base de datos de entidad
La base de datos de entidades contiene información sobre entidades. Las interconexiones acceder a información de entidades al procesar registros de entrada correspondientes a la resolución de entidades y de relaciones. El nodo de interconexión debe tener instalado y configurado el cliente de base de datos adecuado para que las interconexiones puedan acceder a la base de datos de entidades.

Colas Si el sistema utiliza colas como métodos de transporte para enviar datos a las interconexiones para su proceso, debe instalar y configurar el software de gestión de colas de mensajes adecuado en cada nodo de interconexión.

Servidores de higiene de dirección
Si el sistema utiliza productos de higiene de dirección de otras empresas para realizar una limpieza adicional de direcciones, cada nodo de interconexión debe estar configurado de modo que se conecte con los servidores de higiene de dirección.

Servicios web
Debe utilizar un transporte HTTP para conectar los procesos de interconexión del nodo de interconexión con los servicios web.

Supervisor de aplicaciones

La Consola de configuración incluye un supervisor de aplicaciones que puede utilizar para supervisar conexiones (su estado, estadísticas y errores) y direccionar resultados entre interconexiones y otros sistemas o bases de datos.

Para aprovechar el supervisor de aplicaciones, debe registrar en la Consola de configuración las interconexiones que desea supervisar o aquellas de las que desea redireccionar resultados.

Supervisión de interconexiones

El supervisor de aplicaciones funciona con un agente SNMP que se ejecuta en el nodo de interconexión que alberga las interconexiones que desea supervisar. El agente SNMP envía estadísticas sobre todas las interconexiones registradas en un nodo de interconexiones al supervisor de aplicaciones, el cual las publica en la Consola de configuración. El supervisor de aplicaciones renueva el estado y las estadísticas de interconexiones cada 60 segundos.

Direccionamiento de resultados de interconexiones

El supervisor de aplicaciones le permite direccionar los resultados de los datos que procesan las interconexiones a otros sistemas o bases de datos. Para direccionar los resultados del proceso de interconexiones, debe utilizar la Consola de configuración para configurar normas de direccionamiento, que especifican desde qué interconexión se realiza el direccionamiento y dónde se direccionan los resultados.

Por ejemplo, en lugar de que hacer que los analistas creen consultas de informes sobre la base de datos de entidades (lo cual puede resultar muy trabajoso), algunas organizaciones eligen direccionar un subconjunto de los resultados a una base de datos de informes. Los analistas crean y ejecutan sus consultas de informes de investigación sobre la base de datos de informes, que contiene únicamente la información sobre entidades y relaciones que interesa a los analistas.

Transportes

Los transportes mueven datos de un lugar a otro – entre programas de adquisición e interconexiones, entre interconexiones y la base de datos de entidades e incluso entre interconexiones y sistemas externos.

Para transportar datos, debe utilizar un formato de sintaxis específico del tipo de la modalidad de transporte que utilice, lo que incluye un Identificador de recursos universal (URI).

IBM InfoSphere Identity Insight soporta varios métodos de transporte:

- Bases de datos
- Archivos
- HTTP
- Colas de mensajes (IBM WebSphere MQ)

Orígenes de datos

Los orígenes de datos contienen las identidades que desea procesar para la resolución de entidades y cargar en la base de datos de entidades. Los orígenes de datos contienen datos identificativos (identificadores exclusivos y personales para una entidad) y datos no identificativos (otros atributos y puntos de datos correspondientes a una entidad). Los registros de identidad del origen de datos se deben exportar como UMF (Universal Message Format) para que los pueda procesar el sistema y se puedan cargar en la base de datos de entidades. Ejemplos de orígenes de datos incluyen, aunque sin limitarse a las mismas, listas de empleados, listas de vigilancia, listas de clientes y listas de proveedores.

Los orígenes de datos contienen información vital, como la información sobre la fuente original (porque los datos originales se han transformado en UMF) o la referencia externa correspondiente al origen de datos. Estos detalles hacen que cada origen de datos sea exclusiva en el sistema.

Durante la resolución de entidades, si dos entidades no se resuelven, el sistema utiliza la información del origen de datos para determinar qué información pertenece a cada entidad.

Ubicaciones de orígenes de datos y sistemas origen

Puede organizar los orígenes de datos de entrada creando ubicaciones origen y sistemas origen y asociándolos a sus orígenes de datos. Puede utilizar ubicaciones origen y sistemas origen para distinguir entre tipos de orígenes de datos parecidos.

Por ejemplo, si está procesando datos de reservas y datos de recursos humanos procedentes de más de una ubicación, puede utilizar la ubicación de origen de datos para distinguir qué ubicación está ofreciendo los datos:

- Datos de reservas de la propiedad X
- Datos de recursos humanos de la propiedad X
- Datos de reservas de la propiedad Y
- Datos de recursos humanos de la propiedad Y

Configuraciones por origen de datos

Para maximizar los resultados de la resolución de entidades y de la detección de relaciones, configure cada origen de datos utilizando estos valores:

Roles Puesto que los orígenes de datos son agrupaciones del mismo tipo de datos, puede asignar automáticamente el mismo rol a cada registro de identidad del mismo origen de datos de entrada. Por ejemplo, si se asocia el rol Empleado a un origen de datos de recursos humanos, a todos los registros de entrada procedentes de la lista de empleados se les asigna automáticamente el rol Empleado.

Niveles de carga
Puede determinar si se deben cargar todos los datos de un origen de datos de entrada o sólo los datos que se resuelven en una o varias entidades o que están relacionados con las mismas.

Valores de resolución de relaciones
Puede configurar el nivel de detección de relaciones por origen de datos. Por ejemplo, puede desactivar la resolución de relaciones para un origen de datos o seleccionar el número de grados de separación para detectar relaciones dentro de dicho origen de datos en concreto.

Base de datos de entidades

La base de datos de entidades es la base de datos que almacena identidades, entidades y datos que se utilizan para relaciones, resoluciones y alertas.

La base de datos de entidades es el almacén permanente de todas las entidades resueltas y sus relaciones. A medida que las interconexiones procesan registros UMF de entrada, los nuevos datos se comparan constantemente con los datos que ya están en la base de datos de entidades. Por lo tanto, la resolución de entidades y la detección de relaciones se realizan sobre entidades compuestas que contienen todos los atributos acumulados de todos los registros anteriores.

Interfaz de usuario

IBM InfoSphere Identity Insight ofrece varias interfaces de usuario para interactuar con las características del producto.

Consola de configuración

La Consola de configuración proporciona una interfaz orientada a tareas para ayudarle a realizar más fácilmente algunas de las tareas más esenciales para activarse y ejecutar con Identity Insight.

La Consola de configuración se aloja en IBM WebSphere Liberty.

Gestión de la configuración del sistema

La Consola de configuración se utiliza para configurar la mayoría de los parámetros del sistema y opciones en un conjunto de interfaces racionalizadas simplificadas. Entonces la consola graba los cambios en la base de datos de configuración. Los cambios realizados directamente en la base de datos de configuración no se soportan; lo más probable es que estos cambios hagan que el producto no funcione correctamente

Visualizador

El Visualizador es una interfaz gráfica de usuario que los analistas e investigadores utilizan para analizar los resultados de alertas, relaciones y resoluciones de entidades.

El Visualizador está alojado en una versión incorporada de IBM WebSphere Application Server. Puede configurar el Visualizador a través de la Consola de configuración y a través de la selección **Preferencias** del Visualizador en el menú **Archivo**.

Los usuarios del Visualizador pueden realizar diversas tareas de análisis:

Análisis y visualización de alertas
: Las alertas generadas por el proceso de resolución de entidades representan relaciones o resoluciones de entidades que interesan a una organización. Generalmente, los analistas revisan las alertas y deciden qué acción emprender, si deciden emprender alguna, basándose en la información de las alertas. Existen tres tipos de alertas: alertas de rol, alertas de atributo y alertas de suceso.

  El Visualizador muestra las alertas, ofreciendo a los analistas vistas textuales y gráficas de las alertas y las entidades que participan en las alertas. Los analistas pueden profundizar en los detalles y luego establecer el estado de disposición de la alerta correctamente.

Crear y gestionar generadores de alertas de atributo
: Con el Visualizador, los analistas pueden crear y gestionar búsquedas persistentes mediante la característica Generador de alertas de atributo, y gestionar cómo ven y reciben alertas de atributo. Los analistas pueden crear Generadores de alertas de atributo basándose en datos de atributos para localizar identidades que se han resuelto en entidades basadas en dichos datos de atributos. Los analistas también pueden crear un Generador de alertas de atributo para buscar de manera persistente en la base de datos de entidades en busca de una entidad determinada.

Encontrar entidades
: Los usuarios del Visualizador también pueden buscar entidades para un análisis más profundo mediante varios métodos:

- Por atributos
- Por cuenta de origen de datos
- Por ID de entidad
- Por resolución (cuánto se acercan los criterios especificados a las identidades y entidades de la base de datos de entidades, basándose en umbrales de puntuación de resolución mínima)

Adición de entidades y relaciones divulgadas

Los analistas pueden utilizar el Visualizador para añadir registros para la resolución de entidades y la detección de relaciones. Pueden añadir un solo registro de identidad o cargar un archivo UMF que contenga unos pocos miles de registros de identidades. Al igual que cuando se añaden registros de identidades a través de programas de adquisición, una interconexión procesa los registros añadidos a través del Visualizador para la resolución de entidades y la detección de relaciones. Los resultados del proceso se graban en la base de datos de entidades y las alertas, si se generan, se publican en el Visualizador.

Los analistas también pueden divulgar relaciones entre entidades (por identidad), cuando saben de la existencia de un enlace entre las identidades. Ejemplos de relaciones divulgadas serían relacionar entidades basadas en contactos de emergencia o referencias listadas en una solicitud de empleo. La entidad ha divulgado estas relaciones en la solicitud.

Generación e impresión de informes

El Visualizador también contiene varios informes que los analistas pueden ver e imprimir como ayuda para gestionar y hacer el seguimiento de su trabajo en el Visualizador.

Interfaces de línea de mandatos

El producto utiliza interfaces de línea de mandatos para ejecutar las interconexiones. Las interconexiones se inician y detienen emitiendo mandatos en una línea de mandatos.

Programa de utilidad de configuración

El programa de utilidad de configuración permite a los usuarios ver y modificar valores de instalación después de la instalación e instalar parches y arreglos dinámicos.

Puede instalar parches y arreglos dinámicos para las aplicaciones siguientes:

- Consola de configuración
- Visualizador
- Informes de visualizador
- Java™ Web Start
- Servicios Web
- Aplicación gráfica
- Aplicación EntitySearcher
- Documentación de producto

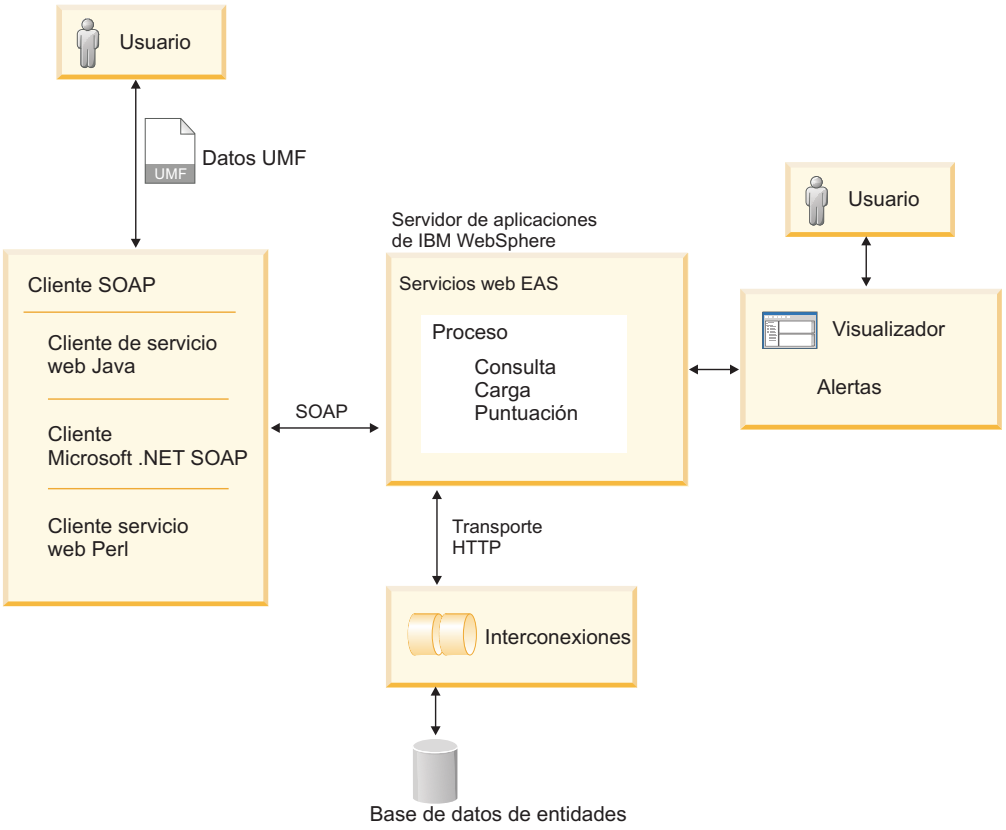
También puede modificar los valores para:

- Consola de configuración
- Configuración de WebSphere
- Conectividad de la base de datos
  - Valores de conectividad de la base de datos de entidades

- Valores de conectividad de la base de datos del supervisor de aplicaciones
- Valores de conectividad de la base de datos de la consola de configuración
- Valores de JDBC

Servicios web

IBM InfoSphere Identity Insight proporciona un conjunto de servicios Web que puede utilizar para crear aplicaciones externas que pueden cargar datos de UMF (Universal Message Format) para el proceso de interconexiones o la búsqueda de entidades en la base de datos de entidades. Puede utilizar el método de transporte HTTP (protocolo de transferencia de hipertexto) bidireccional, que es una característica estándar de la interconexión.



Los servicios Web de IBM InfoSphere Identity Insight utilizan cuatro métodos SOAP (Simple Object Access Protocol): proceso, búsqueda, carga y puntuación. El producto soporta la versión SOAP 1.1.

El producto incluye varios componentes que le ayudan a comenzar a utilizar los servicios Web.

srd.wsdl

Este archivo contiene una definición de lenguaje de descripción de servicios Web (WSDL) de los servicios Web del producto. Puede utilizar este archivo con cualquier kit de herramientas SOAP o con alguna tecnología para iniciar los servicios Web. Puede encontrarse iniciando WebSphere Liberty y cargando el archivo de http://nombrehost:puerto/easws/resources/wsdl/srd.wsdl

wsutil.jar
Este archivo es un cliente de prueba de servicios Web que se proporciona para la prueba de la instalación y configuración de servicios Web. Este programa de utilidad se puede encontrar en el directorio `ibm-home/easws`.

Conceptos principales

Para utilizar IBM InfoSphere Identity de forma eficiente, debe comprender sus conceptos clave, por ejemplo entidades, identidades y atributos.

Entidades

Una entidad es una colección de una o varias entidades que representan la misma persona, organización, lugar o elemento. Las entidades se guardan en la base de datos de entidades.

Aunque las entidades suelen identificarse con personas, también pueden ser cosas, como empresas o vehículos. De hecho, puede utilizar la configuración extensible del sistema para correlacionar los datos de la organización y crear cualquier tipo de entidad que desee resolver o relacionar.

Las entidades suelen estar compuestas de identidades que provienen de distintos sistemas origen. La resolución de entidades determina qué identidades son realmente la misma entidad y crea una entidad compuesta que contiene todas las identidades asociadas a dicha entidad compuesta. El sistema mantiene una atribución completa de registros, que identifican el origen asociado a cada identidad de la entidad compuesta.

Puede configurar el sistema de modo que resuelva y relacione entidades de forma que se ajuste a los objetivos de la organización.

Identidades

Las identidades son una colección de atributos procedentes de un origen de datos que representan una persona, organización, lugar o elemento.

Mediante la resolución de entidades, las identidades se resuelven y se crean entidades compuestas a partir de identidades individuales, cuando las identidades comparten atributos comunes con la entidad compuesta.

Anteriormente, las identidades se podían denominar cuentas.

Atributos

Los atributos son características o rasgos que describen una persona, una organización, un lugar o un elemento. Los atributos comunes incluyen información como nombres, direcciones, números de teléfono, números de tarjeta de crédito, números de identificación fiscal y números de licencia.

El sistema es compatible con las clases siguientes de atributos:

Nombres
Los atributos de nombre definen el nombre de la persona, organización, lugar o elemento, tal como está definido en el modelo de entidades y en la identidad de entrada. Los atributos de nombre suelen representar personas y empresas, pero se pueden ampliar a nombres de vehículos (como coches, camiones, barcos o aviones), grupos o cualquier otro tipo de entidad que defina la empresa en su modelo de entidades.

Direcciones
Los atributos de dirección definen una ubicación de la identidad y suelen contener información estándar de dirección: nombre y número de calle, número de unidad o de edificio, ciudad, estado, país y código postal.

Números
Los atributos de número se componen de datos que se suelen describir como un número, como por ejemplo números de tarjeta de crédito, números de teléfono y números de pasaporte. Los números no se limitan a caracteres numéricos ya que muchos números utilizan caracteres alfanuméricos.

Características
Los atributos de característica definen otros rasgos de la identidad o información que no se expresa mediante ningún otro tipo de atributo. Puede utilizar atributos de característica para personalizar el sistema a fin de definir características de identidades que desea utilizar para resolver entidades o para detectar relaciones. Los tipos de características comunes incluyen fechas de nacimiento y sexo.

Correos electrónicos
Los atributos de correo electrónico definen direcciones de correo electrónico de Internet. Las direcciones de correo electrónico tienden a ser exclusivas; algunos estudios sugieren que las personas que tienden a utilizar más de un nombre tienden a utilizar una o dos direcciones de correo electrónico.

En Universal Message Format (UMF), los diversos tipos de atributos se expresan en segmentos UMF. Cada tipo de atributo tiene su propio segmento UMF.

Resolución de entidades

La resolución de entidades es el proceso que resuelve entidades y detecta relaciones. Las interconexiones realizan la resolución de entidades a medida que procesan los registros de identidad de entrada en tres fases: reconocimiento, resolución y relación.

Reconocimiento

Durante la resolución de entidades, las interconexiones deben reconocer los datos validando, optimizando y mejorando los datos de identidades de entrada. Durante esta fase de reconocimiento del proceso de interconexión, las interconexiones limpian y estandarizan los valores de los datos y realizan comprobaciones de la calidad de los datos a fin de proteger la integridad de la base de datos de entidades.

Gestión de calidad de datos (DQM)

La Gestión de calidad de datos (DQM) es el proceso de interconexión que comprueba que los datos tengan los valores necesarios, tipos de datos válidos y códigos válidos. También puede configurar DQM de modo que corrija los datos proporcionando valores por omisión, formateando números y fechas y añadiendo nuevos códigos.

La Gestión de calidad de datos, junto con higiene y estandarización de nombres e higiene y estandarización de direcciones, está diseñada para optimizar y mejorar la calidad de los datos. Esta preparación de la calidad de los datos constituye un paso esencial en la resolución de entidades, porque aumenta la fiabilidad de las entidades resueltas resultantes y las relaciones detectadas.

Para aplicar la gestión de calidad de datos a los datos cargados en el sistema, debe configurar normas de gestión de calidad de datos (o normas DQM). Las normas DQM pueden realizar varias funciones de reparación, limpieza y estandarización sobre valores de datos de entidades de entrada, como formatear correctamente los números, identificar y corregir errores clericales y de transposición e identificar y corregir imprecisiones intencionadas incorporadas por alguien que intente ocultar sus identidades.

El producto viene preconfigurado con varias normas SQM por segmento UMF que manejan los problemas más típicos de calidad de datos correspondientes a dicho segmento UMF. Pero puede configurar normas DQM adicionales si las necesita. Sin embargo, antes de hacerlo debe estar familiarizado con la calidad de los datos original y con el proceso ETL (extracción, transformación y carga) utilizado para transformar los datos de identidades en UMF. Cuando sepa qué mejoras en los datos hay que realizar, puede seleccionar las normas DQM, funciones y valores adecuados que aplicar a cada tipo de datos de identidades que necesitan una optimización de la calidad de los datos.

Ejemplo de utilización de una norma DQM

Por ejemplo, el formato de fecha del sistema es DD/MM/AAAA. Pero en varios de sus orígenes de datos, los valores de fecha están formateados como MM-DD-AAAA. Puede añadir la norma DQM 204 al segmento UMF `<NUMBER>`, configurándolo de modo que arregle todas las fechas de entrada formateadas como MM-DD-AAAA por el formato de fecha DD/MM/AAAA.

Higiene y estandarización de nombres:

Durante el proceso de interconexiones, los nombres se limpian y estandarizan para preparar el registro de identidades para un proceso óptimo de resolución de entidades.

El proceso de interconexiones ofrece la información de nombres más precisa sobre entidades para su uso actual, futuro e histórico. A medida que entran en el sistema datos de nombres de identidades nuevos o modificados, se comparan con el diccionario de estandarización de nombres del producto, que contiene una lista de nombres raíz y sus derivados conocidos, a fin de identificar el nombre raíz. Cuando se identifica el nombre raíz, el sistema mantiene tanto el nombre raíz como el nombre original para el registro de identidades de entrada.

Por ejemplo, la tabla siguiente muestra dos ejemplos de posibles derivados del mismo nombre raíz, incluidos los distintos modos de escribir el nombre. Los nombres de la izquierda son derivados del nombre raíz de la derecha.

Tabla 1. Ejemplos de algunos posibles derivados de los nombres raíz Richard y Mohammad

Derivados	Raíz
Dick, Dickie, Ricardo Rich, Richie, Rick Rickey, Ricki, Rickie Ricky, Rikki, Ritchie	Richard
Mohamad, Mohammad Mohamed, Mohammed	Mohammad

El proceso de higiene y estandarización de nombres también corrige los errores ortográficos, si es necesario, pero de nuevo el sistema conserva tanto el original como la corrección como parte del registro. La mayoría de los otros sistemas (incluidas las herramientas ETL y de marketing de bases de datos) no lo hacen.

La higiene y la estandarización de nombres constituyen un paso importante para aumentar el nivel de fiabilidad de la resolución de entidades. Este proceso resulta especialmente importante las personas utilizan como media cinco versiones de su nombre con fines oficiales y de consumo.

Higiene de dirección y estandarización:

Higiene de dirección y estandarización es el proceso de interconexión que normaliza y estandariza información sobre direcciones a fin de corregir los posibles errores y transposiciones y de preparar el registro de identidad para un proceso óptimo de resolución de entidades.

Como parte del proceso de higiene de direcciones, las interconexiones analizan y estandarizan la información de una dirección. Por ejemplo, `Street` a `St` o `123-A Main St` a `123 Main St Apt A`.

Este proceso de interconexión verifica la información nueva o modificada frente a una base de datos de direcciones global y un software de estandarización que proporciona el producto IBM InfoSphere QualityStage o frente a otro producto de higiene de dirección, como el producto Group 1 Software CODE-1. El producto de higiene de dirección elegido determina si la información sobre direcciones está correctamente formateada, corrige y detecta errores ortográficos (como nombres de calles mal escritos) y corrige la información que falta o que es incorrecta (por ejemplo, actualiza el nombre de la ciudad para que coincida con el código postal y con la dirección).

Por ejemplo, la tabla siguiente muestra ejemplos de limpieza y estandarización de direcciones; muestra la dirección original y la dirección estandarizada corregida.

Tabla 2. Ejemplos de comparación de dos direcciones originales con la dirección estandarizada resultante

Dirección original	Dirección estandarizada
460 Oak Street Mill Valleu, CA 94914	460 South Oak Street Mill Valley, CA 94914
4737 Simeron Drive Easton, MA 02334	4737 Cimmeron Drive Easton, MA 02334

El proceso de interconexión de higiene de dirección y estandarización mantiene la dirección original y la dirección corregida y mejorada a fin de mejorar los niveles de fiabilidad de una futura resolución de entidades y detección de relaciones. El hecho de mantener esta información también ofrece una mejor información histórica.

Comprobación de la calidad de los datos:

A medida que entran datos de identidades en el sistema para su proceso, la interconexión comprueba la calidad de los datos a fin de proteger la integridad de la base de datos de entidades. Cada registro de identidad de entrada se prueba

para comprobar que la construcción UMF (Universal Message Format) sea correcta, tenga los valores necesarios, los tipos de datos sean cálidos y tenga códigos de origen de datos configurados.

Cuando el proceso comprueba la calidad de los datos, intenta corregir los problemas, si es posible y si el sistema está configurado para hacerlo. Cuando determina si se deben o no corregir problemas de calidad de los datos, el sistema utiliza las normas DQM (Gestión de calidad de datos). Las normas DQM definen qué defectos de calidad de los datos en los registros de identidades de entrada puede corregir el sistema y qué defectos se pueden dejar tal cual y seguir procesando los registros.

Para ver la calidad de los datos de una determinado origen de datos, puede ver o imprimir el informe de resumen de carga. La sección de resumen de calidad le puede ofrecer una visión útil de la calidad global de los datos correspondientes a dicho origen de datos o a un conjunto determinado de registros de identidades cargados desde dicho origen de datos. Con esta información, puede ajustar el proceso ETL, según sea necesario, correspondiente a un determinado origen de datos.

El registro estándar y el manejo de errores registran todos los errores en la calidad de los datos y las correcciones, así como los errores que el sistema no ha corregido o no ha podido corregir. Compruebe los registros del sistema con frecuencia para ver los errores en la calidad de los datos que no ha corregido el proceso de la interconexión. En la mayoría de los casos, tendrá que corregir los errores en la calidad de los datos y luego volver a cargar los registros de identidad corregidos en una interconexión para el proceso de resolución de entidades.

Ejemplos de comprobación de la calidad de los datos

El sistema puede añadir automáticamente códigos que no se reconocen como códigos nuevos, si está configurado para hacerlo. El registro UMF_EXCEPT muestra los resultados de los nuevos códigos que ha añadido el sistema o los registros rechazados y no procesados, porque el sistema no ha reconocido un código y no ha sido configurado para añadirlo como un nuevo código.

La tabla siguiente muestra dos ejemplos de códigos en registros de entrada que aún no se habían configurado en el sistema.

Tabla 3. Ejemplos de dos códigos no configurados en el sistema y el resultado del proceso del sistema

Código	Comprobación de calidad	Registro UMF_EXCEPT
Addr_Type x	Nuevo código añadido	grabar en registro
Num_Type xxx	Nuevo código rechazado	grabar en registro

- En el primer ejemplo, el sistema está configurado para añadir automáticamente el nuevo código de tipo de dirección.
- En el segundo ejemplo, el sistema no está configurado para añadir automáticamente el nuevo código ni para permitir que el registro se procese para la resolución de entidades.

En ambos casos, el sistema registra la acción en el archivo de registro adecuado.

Resolución

Durante la resolución de entidades, las interconexiones resuelven identidades en entidades. Una vez limpiados, estandarizados o mejorados los valores de datos de los registros de identidades, la interconexión utiliza sofisticados algoritmos de búsqueda para comparar los valores de los datos del registro de la identidad de entrada con las entidades existentes en la base de datos de entidades a fin de determinar si son la misma entidad.

La resolución de entidades incluye estas fases:

Generación de listas de candidatos
El sistema utiliza la información del registro de la identidad de entrada para compararla con las entidades existentes en la base de datos de entidades a fin de crear una lista de candidatos potenciales de resolución de entidades. Cada candidato comparte suficientes valores de atributos como para continuar evaluando el candidato para la resolución de entidades. Puede configurar los criterios que utiliza el sistema para generar las listas de candidatos.

Realización de la resolución de entidades
Después de generar listas de candidatos, el sistema aplica las normas de resolución a cada entidad de la lista de candidatos, utilizando un método de puntuación que calcula una puntuación de resolución para determinar si la identidad de entrada y la entidad existente se deben resolver. Puede configurar normas de resolución y establecer los umbrales para las puntuaciones de resolución para determinar cuánto se deben parecer los valores de los atributos para que la identidad de entrada y la entidad candidata se resuelvan en una entidad.

Listas de candidatos

Las listas de candidatos son las listas de entidades que tienen el potencial de coincidir con el registro de identidad de entrada. La lista de candidatos se crea recuperando aquellas entidades que comparten atributos con la identidad de entrada, según los atributos especificados en la configuración del creador de candidatos.

El proceso de resolución de entidades sólo utiliza las entidades de la lista de candidatos para resolver entidades y para resolver relaciones.

Puesto que la resolución de entidades y la detección de relaciones se determinan en función de atributos, debe examinar detenidamente los atributos de los orígenes de datos para determinar qué atributos crean los candidatos más firmes.

Una vez generada la lista de candidatos, el proceso de resolución de entidades compara la identidad de entrada con el primer candidato de la lista utilizando las reglas de resolución configuradas. El sistema utiliza las reglas de resolución, en orden, para calcular una puntuación de resolución que represente cuánto se parecen los atributos de la identidad de entrada con los de la entidad candidata. Si los atributos de la identidad de entrada se ajustan o superan la puntuación de resolución correspondiente a dicha regla, el registro de la identidad de entrada se resuelve en la entidad candidata.

Si la puntuación de resolución no se ajusta ni supera el conjunto de puntuaciones de resolución correspondiente a dicha regla de resolución, el sistema pasa a la siguiente regla de resolución hasta que se el registro de la identidad de entrada se resuelva en una entidad candidata o hasta que se agoten todas las reglas de resolución.

Si el registro de la identidad de entrada no se resuelve en una entidad existente, el sistema resuelve el registro en una nueva entidad y guarda la nueva entidad en la base de datos de entidades.

Normas de resolución

Las normas de resolución son un conjunto de criterios que utiliza el sistema para definir el modo en que se resuelven entidades comparadas (si son o no son la misma entidad) y el modo en que se relacionan (si las entidades no se resuelven en la misma entidad, cuántos atributos comparten).

Cuando se definen normas de resolución, hay que especificar umbrales que contribuyan a la puntuación total de la resolución, lo que determina si una identidad de entrada se resuelve en una entidad existente:

- Los umbrales de candidatos especifican qué valores de datos de atributos se comparan para determinar si una identidad y una entidad se resolverán en una entidad compuesta. El umbral es la puntuación mínima a la que un determinado valor de atributo coincide entre la identidad de entrada y una entidad existente para que se satisfaga la regla de resolución.
- Los umbrales de confirmación/denegación especifican el peso de puntuación (positivo o negativo) que se aplica a valores de datos de atributos coincidentes o conflictivos cuando se habilita el uso de denegaciones.

También puede especificar el modo en que valores conflictivos para los mismos atributos afectan a la puntuación de resolución. Estos valores conflictivos se denominan denegaciones. Puede configurar normas de resolución que especifiquen que la regla no se cumple si hay conflictos (denegaciones) en los valores de atributos. También puede ajustar los umbrales correspondientes a una regla de resolución para crear denegaciones automáticas, basadas en que las puntuaciones de comparación no cumplen una o más de las puntuaciones de umbral especificadas. Cuando más alta se establece una puntuación de umbral, más exacta debe ser la coincidencia para que se satisfaga la regla de resolución.

Re-resolución

El proceso de re-resolución se produce durante el proceso de resolución de entidades cuando dos entidades se resuelven como la misma entidad y se crea un registro de entidad compuesta. La resolución de entidades utiliza el nuevo registro de entidad compuesta para volver a empezar el proceso a fin de ver si la nueva entidad compuesta se puede resolver en alguna de las otras entidades de la base de datos de entidades.

AL igual que sucede con una nueva entidad de entrada, el proceso de resolución de entidades intenta generar una lista de candidatos de entidades de la base de datos de entidades. Si se puede generar una lista de candidatos, el proceso de resolución de entidades comienza la resolución de entidades, comparando cada candidato de la lista con la nueva entidad compuesta. Si no se puede generar una lista de candidatos, el proceso de resolución de entidades continúa con el proceso de detección de relaciones.

No resolución

El proceso de no resolución se produce como parte del proceso de resolución de entidades cuando los valores de atributos de la identidad de entrada proporcionan nueva información que indica que una entidad compuesta está realmente compuesta por dos entidades y el registro de la entidad compuesta se divide en dos entidades. El sistema sabe qué registros pertenecen a qué entidad por el origen de datos asociado a cada registro. Una vez finalizado el proceso de no resolución, el sistema empieza el proceso de re-resolución.

Ejemplo de no resolución

Anteriormente, el sistema resolvía un registro de identidad de entrada para Will Smith con la dirección 1234 Main Street, Anytown, USA, número de teléfono (201) 555-2244 y dirección de correo electrónico jrsmith@internetprovider.com para producir William Smith, Sr. con la misma dirección y mismo número de teléfono.

Ahora se procesa un nuevo registro de identidad de entrada para Will Smith, Jr. con la dirección de correo electrónico jrsmith@internetprovider.com y tarjeta de crédito 123-54-9999.

Según la nueva información de Junior y el número de tarjeta de crédito, el sistema puede determinar que el registro de entidad compuesta William Smith, Sr. se debe desresolver y originar William Smith, Sr. y William Smith, Jr. Después de que la entidad se divida en dos entidades, el sistema empieza el proceso de re-resolución para comprobar si la resolución de cualquier otra entidad de la base de datos ahora da como resultado William Smith, Jr, de acuerdo con la nueva información.

Relación

Durante la resolución de entidades, las interconexiones también completan el proceso de detección de relaciones, que detecta relaciones entre identidades y entidades y genera alertas para las relaciones interesantes.

El sistema utiliza roles que son la clasificación de una identidad que define el objetivo de que dicha identidad detecte y establezca relaciones entre entidades. En el sistema, el usuario define roles y luego asigna roles a identidades por origen de datos y como parte de la transformación de los datos del origen de datos original en UMF (Universal Messaging Format).

Cuando la interconexión procesa identidades de entrada para la resolución de entidades y resuelve la identidad de una entidad existente, los dos registros tienen una relación de 0 grados; es decir, la identidad de entrada y la entidad son la misma. Pero el proceso de resolución de entidades puede ir más allá de las relaciones de 0 grados, en función del modo en que esté configurado el sistema.

Cuando la interconexión agota todas las posibilidades de la fase de resolución de la resolución de entidades, el proceso de detección de relaciones evalúa las entidades que quedan en la lista de candidatos o aquellas entidades que no se han resuelto en la identidad de entrada para ver si existe una relación entre ellas. Generalmente, las entidades que no están en la lista de candidatos se enlazan con la identidad de entrada con 1 grado de separación para al menos un atributo, lo que significa que ambas entidades comparten los mismos valores de atributos al menos para un atributo (por eso la entidad está en la lista de candidatos).

Cuando el proceso detecta una relación, el sistema compara los roles asignados entre la identidad y las entidades con las normas de alerta de rol configuradas. Si el sistema encuentra que los roles asignados a la identidad y una entidad cumplen con los criterios correspondientes a dicha norma, el sistema genera una alerta que indica que ha detectado una relación interesante. La relación puede ser de 0 grados, de 1 grado o de varios grados, en función de cómo se hayan configurado el sistema y las normas de alerta de rol.

Relaciones

Las relaciones son enlaces entre dos o más entidades. Las relaciones se detectan al final del proceso de resolución de entidades, cuando dos entidades comparten varios valores de atributos de datos.

Las relaciones se pueden basar en enlaces descubiertos por el sistema, divulgados por el analista o ambos. Sin embargo, no todas las relaciones son lo suficiente interesantes como para garantizar la generación de una alerta para su futuro análisis o investigación. Puede definir relaciones interesantes configurando normas de alerta de rol que especifiquen qué combinaciones de roles asignados a entidades tienen que generar alertas.

Ejemplos de relación

Ejemplos de relaciones que se pueden detectar durante la resolución de entidades:

- Un cliente también es un proveedor. Según las políticas y procedimientos de la organización, se puede considerar una relación interesante.
- Un empleado conoce a un cliente. A no ser que las políticas y procedimientos de la organización prohíban este tipo de asociación, o quizás en función de los datos que comparten el empleado y el cliente, puede que esta no se considere una relación interesante.
- Un cliente conoce a otro cliente. Si la empresa tiene un cliente muy importante, saber a quién conoce el cliente puede ser una buena forma de utilizar la red de clientes para comercializar en la red.

Visión general de Degrees of Separation:

La característica Degrees of Separation amplía las posibilidades de coincidencia de relaciones de IBM Relationship Resolution.

El comportamiento predeterminado de IBM InfoSphere Identity Insight identifica relaciones de gran interés y establece coincidencias de entidades a un grado de separación de una entidad entrante resuelta en una entidad. Si habilita la característica Degrees of Separation se amplían estas posibilidades hasta casi un rango ilimitado de grados de separación definidos por el usuario de una entidad entrante resuelta en una entidad.

La característica Degrees of Separation utiliza configuraciones de separación, roles, reglas de alertas de rol y puntuaciones de relaciones para realizar análisis de enlaces en tiempo real respecto a grandes conjuntos de datos.

Cuando una entidad entrante se resuelve en una entidad, se crea un gráfico de entidades utilizando relaciones de un grado que detecta IBM InfoSphere Identity Insight. El gráfico de entidades utiliza las relaciones de un grado para crear cadenas de relaciones de múltiples grados que provienen de la entidad en la que quedó resuelta la entidad entrante. Se puede crear una cadena de alertas de rol enlazando dos cadenas de relaciones de múltiples grados, cada una proveniente de la entidad en la que quedó resuelta la entidad de entrada. La cadena de alertas de rol se puede utilizar para encontrar una relación entre las entidades finales e incluyendo cada cadena de relación de múltiples grados.

Degrees of Separation reduce el trabajo evaluando todas las vías de acceso que conectan dos entidades y utilizando las mejores para notificar relaciones. Se puede configurar Degrees of Separation para que informe sobre una alerta de rol para cada regla de alertas de rol configurada por entidad en la que se resolvió la entidad entrante.

La configuración de grados de separación puede establecerse en la consola utilizando la pestaña **Configuración del sistema**, valor Grados de separación.

Identificación impersonal:

La identificación impersonal es una característica de producto que amplía el proceso tradicional de resolución de relaciones para encontrar y analizar relaciones impersonales. El proceso de detección de relaciones encuentra relaciones entre entidades basándose en valores de atributos asociados a esas entidades. Algunas veces es importante encontrar relaciones entre entidades basándose en actividades u otros identificadores impersonales. Estas relaciones entre entidades basadas en actividades u otros identificadores impersonales se denominan relaciones *impersonales*, y las actividades o identificadores impersonales que establecen vínculos entre las personas se denominan *hechos relacionales.*

Las relaciones impersonales siempre existen para dos o más grados de separación, pues el propio hecho relacional es una entidad. Para habilitar la identificación impersonal y buscar relaciones impersonales, configure los orígenes de datos para utilizar la función Degrees of Separation, que puede configurarse para detectar relaciones con más de dos grados de separación.

Por ejemplo, una transacción telefónica contiene datos sobre números de teléfono: el número que realiza la llamada y el número receptor de la llamada. Aunque una persona realizó la llamada telefónica a otra persona, a partir de la transacción telefónica solamente, no se pueden atribuir datos comunes a las personas. A menudo, el hecho relacional (la llamada telefónica) se conoce antes que se conozca cualquier otra información sobre las entidades relacionadas (las dos personas que intervienen en la llamada telefónica). Puesto que estos hechos relacionales no se pueden atribuir a una persona, se deben representar como entidades separadas que no son personas, pero que están relacionadas con personas. Sin embargo, la identificación impersonal reconoce que existe una relación entre las dos personas como consecuencia de la llamada telefónica.

UMF incluye una funcionalidad de tipo de entidad, que permite definir hechos relacionales como tipos de entidad. Cuando se utiliza esta funcionalidad, los hechos relacionales pasan a ser entidades separadas en la base de datos de entidades y se pueden utilizar para detectar relaciones entre entidades Persona. Mediante la configuración de nuevos tipos de entidad, la especificación del tipo de entidad apropiado en UMF y la creación de nuevas configuraciones de resolución, estos hechos relacionales se pueden utilizar para encontrar automáticamente relaciones impersonales y conflictos entre entidades.

No se produce nunca una resolución cruzada para entidades con tipos de entidad diferentes, aunque las normas de resolución y los datos lo permitan. Por tanto, la resolución del tipo de entidad Llamada telefónica no produce nunca el tipo de entidad Persona .

El kit de herramientas de analista representa gráficos e informes de relaciones impersonales y de las alertas asociadas, al igual que lo hace con las relaciones personales y alertas asociadas.

Ejemplo de identificación impersonal

Por ejemplo, si deseara encontrar relaciones impersonales mediante llamadas telefónicas, crearía el nuevo tipo de entidad Llamada telefónica y ajustaría el nodo de adquisición para marcar correctamente cada registro de llamada telefónica con el tipo de entidad *Llamada telefónica*.

Cuando los registros telefónicos son absorbidos por el sistema, el proceso estándar de resolución de entidades y relaciones encuentra una relación de un grado entre la entidad Llamada telefónica y la entidad llamante (Persona). También encuentra una relación de grado 1 entre la persona llamada y la entidad Llamada telefónica. Por sí mismo, el sistema no encuentra una relación entre las personas.

Sin embargo, cuando se configura la función Degrees of Separation, continúa el análisis y detecta la relación impersonal de grado 2 entre el llamador y la persona llamada. Existe una relación impersonal, basada en los números de teléfono que son atributos del tipo de entidad Llamada telefónica. A continuación, la función Degrees of Separation analiza la relación impersonal y genera una alerta si se produce un conflicto.

Roles

Un rol es una clasificación de una identidad que define el objetivo de dicha identidad. Puede asociar uno o varios roles a una identidad. Cuando las identidades se resuelven en entidades, estas heredan todos los roles asociados.

Se utilizan roles para configurar reglas de alerta, que definen las relaciones interesantes y generan alertas.

A cada identidad se le asigna un rol de una de estas formas:

Por origen de datos de entrada
: Cuando se configura una nuevo origen de datos, se asocia un rol a dicho origen de datos, la cual asignará dicho rol a todas las identidades que contengan dicho código de origen de datos.

Por UMF
: Cuando se transforma el origen de datos a UMF (Universal Message Format), se pueden asignar directamente roles como parte del registro UMF mediante el segmento UMF <SEP_ROLES> con el código UMF <ROLE_CODE>. Si configura por UMF, se tendrán que añadir reglas DQM y una tabla de búsqueda.

Ejemplos de roles útiles pueden incluir empleados, proveedores, clientes o lista de vigilancia.

Ejemplo de asignación de roles mediante UMF

Para asignar el rol de empleado a un registro de identidad mediante UMF, debe entrar el siguiente segmento UMF <SEP_ROLES> y el siguiente código UMF <ROLE_CODE> para el registro de la identidad:

```
<SEP_ROLES>

    <ROLE_CODE>Employee</ROLE_CODE>

</SEP_ROLES>
```

Alertas

Las alertas son mensajes u otras indicaciones que anuncian que se ha producido un suceso.

Las alertas se generan de una de estas dos formas:

- Las alertas de atributo se generan siempre que hay entidades que coinciden con un grupo especificado de atributos.

- Las alertas de rol se generan cuando una o varias entidades enlazadas a través de una relación comparten roles que el usuario ha definido como *de interés* o *conflictivos*.

Es importante definir qué alertas cumplen con los objetivos de la organización. Un buen punto de partida es preguntar qué relaciones entre entidades son de interés en la organización. Las relaciones se basan en roles configurados por el usuario, que el sistema de origen asigna a registros de datos de entrada. Cuando dos entidades comparten suficientes valores de datos de atributos sin resolver en la misma entidad, estas entidades forman una relación. Asegúrese que las normas de alerta de rol configuradas para la organización definan claramente qué roles de entidad crean una relación que los analistas desean investigar.

Ejemplos de alerta

Algunos ejemplos de relaciones de interés para las que la organización puede desea generar alertas incluyen:

- Una de las personas empleadas por la organización es también un proveedor que ofrece bienes y servicios, bajo pago, a la organización.
- Uno de los clientes comparte una dirección y un nombre similares a los de una persona que aparece en una lista de vigilancia gubernamental.
- Dos de las personas que han archivado informes sobre accidentes en la organización tienen nombres y direcciones parecidas y comparten un número de teléfono.

Alertas de atributos:

Las alertas de atributos son alertas generadas por los generadores de alertas de atributo, que crean una consulta del sistema persistente en busca de atributos o identidades específicos en la base de datos de entidades. Siempre que los atributos para entidades coinciden con los criterios del generador de alertas de atributo, el sistema crea una alerta de atributo.

Los usuarios del Visualizador crean sus propios generadores de alertas de atributo personales. Si está buscando una identidad específica o cualquier identidad o entidad que coincida con un conjunto de atributos específico, puede crear su propio generador de alertas de atributo personal que busque coincidencias hasta la fecha de caducidad especificada.

A continuación se muestran algunos ejemplos de posibles atributos de entidades sobre los que puede ser notificado:

- Nombre y número exclusivo (como un número de tarjeta de crédito)
- Nombre y número de teléfono
- Dirección
- Nombre y número no exclusivo

Los generadores de alertas de atributo se configuran y se consultan en el Visualizador. Los generadores de alertas de atributo que puede crear solo estarán disponibles para usted.

Ejemplo de una alerta de atributos de dirección

Está viendo la dirección 675 Hickory Street Las Vegas, NV. Puede configurar un generador de alertas de atributo para crear una alerta de atributo siempre que la

dirección se asocie a un registro de identidad de entrada añadido a la base de datos de entidades.

Alertas de rol:

Una alerta de rol identifica cuándo una o dos entidades están enlazadas a través de una relación que cumple o excede una regla de alerta de rol configurada. Las alertas de roles se basan en los roles configurados y en las normas de alertas de roles. Pueden indicar un aviso o un problema (como por ejemplo que un cliente conoce a un malo) o simplemente indicar relaciones interesantes (por ejemplo, un cliente conoce a un empleado).

Puede definir relaciones *interesantes* o como *conflictivas* configurando normas de alertas de rol, que identifican qué roles no deben existir en una sola entidad o no se pueden enlazar entre una o varias entidades. Utilice la Consola de configuración para configurar filtros para alertas de rol, que determinan si el sistema vuelve a alertar cuando hay información nueva (como una nueva identidad o un nuevo código de origen de datos).

Durante la resolución de entidades, la interconexión evalúa relaciones entre la identidad de entrada y entidades de la lista de candidatos. Después de determinar que existe una relación entre la identidad de entrada y una entidad candidata, el sistema evalúa si los roles asignados cumplen una regla de alerta de rol configurada. Si es así, el sistema genera una alerta de rol.

Una alerta de rol identifica datos de entidades en el momento en que se creó la alerta de rol. La pantalla de detalles de Alerta de rol muestra los datos de la entidad tal como existían en el momento en que se creó la alerta de rol. A medida que los datos de la entidad cambian con el tiempo, el resumen de la entidad contiene los últimos datos sobre la entidad. Si desea ver los datos actuales correspondientes a una entidad en particular, consulte el resumen de la entidad.

Puede ver y trabajar con alertas de rol en los componentes del kit de herramientas de analista (informes de Cognos, el plug-in de Identity Insight para i2 e Identity Insight Explorer).

Normas de alertas de rol:

Las normas de alertas de rol son normas definidas por el usuario que identifican uno o varios roles que no pueden existir en una sola entidad o que no se pueden enlazar entre varias entidades. Durante la resolución de entidades, si se cumplen los criterios correspondientes a una norma de alerta de rol, el sistema genera una alerta de rol.

Aunque la mayoría de las normas de alertas de rol especifican cuándo los roles entran en conflicto, también puede definir una norma de alerta de rol en la que una a entidad que se le asigna a un rol conoce otra entidad a la que se asigna el mismo rol. Por ejemplo, puede encontrar interesante saber cuándo los clientes se conocen entre sí y definir una norma de alerta de rol (*cliente conoce cliente*) que genere una alerta de rol siempre que una entidad de cliente se relacione con otra entidad de cliente en la base de datos de entidades.

Puesto que las entidades constan de varios registros (generalmente procedentes de distintos orígenes de datos) y puesto que los roles se suelen asignar por origen de datos, se pueden asignar varios roles a una entidad. Así que se puede definir una

norma de alerta de rol que genere un rol siempre que a una entidad se le asigne tanto el rol de cliente como el rol de malo, en función de los datos de entrada.

Nota: Recuerde que cuando un sistema se configura de modo que utilice un gran número de roles, el número de normas de alertas de rol aumenta exponencialmente.

Aunque el sistema detecta cada relación que infringe una norma de alerta de rol, por omisión sólo notifica una alerta de rol para cada entidad. Por ejemplo, si el sistema detecta que una entidad que tiene asignado un rol de empleado está relacionada con dos entidades de proveedor diferentes, y se configura una norma de alerta de rol de modo que genere una alerta de rol cuando el empleado conoce al proveedor, ambos conflictos se detectan y se graban en la base de datos pero, por omisión, sólo se notifica una alerta de rol.

Cuando configura normas de alertas de rol, puede también especificar filtros de alerta que determinan si el sistema crea una nueva alerta cuando se añaden nuevas identidades o códigos de orígenes de datos a entidades existentes que intervienen en una alerta creada previamente.

Invalidación de alerta de rol:

A medida que los datos se procesan mediante la resolución de entidad y relación, las entidades y las relaciones entre ellas cambian con el tiempo. Esos cambios, basados en el análisis perpetuo de datos nuevos y existentes, puede hacer que las alertas de rol queden no válidas. La característica de invalidación de alerta de rol de InfoSphere Identity Insight proporciona el contexto más actual a los analistas, para que los analistas no pierdan el tiempo investigando conflictos que ya no son válidos.

La invalidación de alertas de rol elimina las alertas de rol basadas en relación que aún están en estado pendiente. Normalmente, un analista aún no ha visto o procesado las alertas en estado pendiente. Si una alerta de rol tiene otro estado, como completado o asignado, aunque los datos soporten la invalidación de esa alerta de rol, la alerta no se invalida. Sólo se puede asignar un estado a una alerta por lo que si la alerta ya está en un estado de asignada o completada, no se invalida.

Las alertas de rol que se producen a 0 grados también se invalidan, cuando una identidad se suprime o no se resuelve a partir de la entidad.

Cómo funciona la invalidación de alertas de rol

Las alertas de rol basadas en relación pueden quedar no válidas por varias razones:

- Si una entidad cambia su ID de entidad como parte de los procesos de re-resolución o de eliminación de resolución durante la resolución de entidad, la relación puede desvanecerse o transferirse a un nuevo ID de entidad.
- Si una única entidad se convierte en dos entidades independientes basándose en datos nuevos, a cada una de las nuevas entidades se le asigna un nuevo ID de entidad. Mediante la atribución completa, todos los datos que pertenecen a la nueva entidad se eliminan de la entidad anterior y se añaden a la nueva entidad, incluidos los roles que crean alertas de rol basadas en relación

- Cuando los datos se suprimen de la base de datos de entidades, se puede eliminar una entidad entera o un componente clave de una relación, haciendo que una alerta de rol quede no válida.
- Cuando los datos se marcan como genéricos, su capacidad de utilizarse para detectar relaciones se reduce o elimina. Si una relación se elimina, todas las alertas de rol que dependen de esa relación quedan no válidas.

Alertas de rol de sustitución

Siempre que una alerta de rol se invalida, la interconexión vuelve a evaluar automáticamente cada conflicto a lo largo de la vía de acceso de relación, buscando datos para soportar un conflicto basado en relación alternativa.

Una *vía de acceso de relación* es la cadena de entidades y atributos que enlazan una entidad a otra entidad. La longitud de la vía de acceso de relación la determina la configuración para grados de separación. Las configuraciones de separación se establecen mediante la Consola de configuración.

Puntuación

Durante la resolución de entidades, el sistema calcula la medida en que los atributos de una identidad de entrada coinciden con los atributos de una entidad existente. Los resultados de este análisis de cálculo son puntuaciones que el sistema utiliza para resolver identidades en entidades y para detectar relaciones entre entidades.

Puntuaciones de resolución

La puntuación de resolución es el valor que se asigna durante la resolución de entidades como resultado del proceso de confirmación y denegación y que define la probabilidad de que las identidades comparadas representen la misma entidad. Esta puntuación la define el usuario y se utiliza para resolver una nueva identidad en una entidad existente.

A medida que la interconexión procesa identidades de entrada para la resolución de entidades, compara los valores de atributos compartidos correspondientes a los atributos de la identidad de entrada y de cada entidad de la lista de candidatos. Parte de la comparación incluye puntuaciones de cálculo que representan cuándo se parecen los valores de los atributos. Estas puntuaciones se pueden comparar con los umbrales configurados y la puntuación de resolución para cada norma de resolución. Después de que el proceso de resolución de entidades utilice un proceso de confirmación y denegación para evitar falsos positivos, el sistema crea una puntuación de resolución base para la identidad de entrada y la entidad en la lista de candidatos.

Si uno o varios atributos se han configurado de modo que se utilicen para la futura confirmación o denegación, el proceso evalúa dichos atributos. Los resultados afectan a las puntuaciones de resolución base de la identidad de entrada y de la entidad candidata. Si los valores de los atributos coinciden, la puntuación de resolución se puede ver afectada positivamente sumando el número configurado de puntos. Si los valores de los atributos no coinciden, la puntuación de la relación se puede ver afectada negativamente restando el número configurado de puntos. Cuando configura un atributo de modo que se utilice para confirmación o denegación, debe especificar el número de puntos al alza o a la baja para ajustar la puntuación de la resolución base.

Luego el sistema compara la puntuación de resolución resultante de la identidad de entrada y la entidad candidata con cada una de las normas de resolución. Si la puntuación de resolución se ajusta o supera la puntuación de fiabilidad de resolución configurada para la norma de resolución, el sistema resuelve la identidad de entrada en la entidad candidata, creando una entidad compuesta en la base de datos de entidades.

Puntuaciones de relaciones

La puntuación de una relación es el valor que se asigna durante la resolución de entidades como resultado de aplicar las normas de resolución y que define la relación entre dos identidades comparadas. Esta puntuación la define el usuario y se utiliza para relacionar entidades.

Durante la resolución de entidades, la interconexión compara la identidad de entrada (que es posible que no se pueda resolver en una entidad) con las entidades restantes de la lista de candidatos. Aunque puede que estas entidades candidatas no se resuelvan en la identidad de entrada, se evalúan igualmente para establecer relaciones.

Durante el proceso de detección de relaciones, las interconexiones determinan relaciones calculando una puntuación de relación para cada valor de datos de atributos que se comparte entre la identidad de entrada y las entidades de la lista de candidatos, empezando por la primera entidad:

- Si la puntuación de la relación satisface los criterios configurados para relaciones (por grados de separación), el sistema determina que dos entidades están relacionadas. La relación se graba en ambos registros de las entidades compuestas. Luego el sistema comprueba las normas de alerta de rol configuradas para determinar si la relación se considera una relación interesante. Si es así, el sistema genera una alerta. Si no es así, pasa a la siguiente entidad de la lista de candidatos.
- Si la puntuación de la relación no satisface los criterios configurados para relaciones, el proceso pasa a la siguiente entidad de la lista de candidatos, hasta que se han evaluado todas las entidades para ver si tienen relaciones.

Event Manager

Event Manager amplía las posibilidades de IBM InfoSphere Identity Insight combinando el análisis de sucesos en casi tiempo real y la supervisión de sucesos con resolución de identidad y relación. Cuando está habilitado, Event Manager proporciona a su organización la capacidad de realizar un seguimiento de sucesos empresariales y de avisarle sobre sucesos sospechosos o sucesos de interés; de este modo podrá llevar a cabo las acciones empresariales apropiadas con a fin de ayudar a su organización respecto a la lucha contra el fraude y las amenazas.

Como los casos de fraude y amenazas cambian constantemente, Event Manager le proporciona la flexibilidad de definir los tipos de sucesos a los que se realizará un seguimiento y de configurar las reglas empresariales para procesar sucesos y generar alertas de sucesos. Estas reglas son un conjunto de criterios que Event Manager utiliza para determinar cómo se procesan los sucesos y qué desencadena una alerta de sucesos. Configure las reglas empresariales, basándose en las necesidades y los escenarios empresariales.

También decide qué constituye una alerta de sucesos. Las alertas de sucesos normalmente no se desencadenan por un solo suceso, sino por una serie de sucesos complejos que se han producido en distintos momentos y en distintos

contextos. Por ejemplo, podría definir una regla empresarial que agregue transferencias de dinero por cliente en un momento específico y que genera una alerta si la cantidad total excede el límite legal. O también podría definir una regla empresarial que le avise cuando se realicen compras con dos tarjetas de crédito utilizando el mismo número de tarjeta de crédito a la misma hora y en sitios a más de 200 kilómetros de distancia.

Cómo trabaja el proceso de sucesos

La característica Event Manager de IBM InfoSphere Identity Insight funciona con el procesador de sucesos complejo de IBM Active Middleware™ Technology, que consta de dos partes: el motor de CEP y la herramienta de autor de regla basada en Eclipse™. Configure las reglas empresariales para sucesos y alertas de sucesos en la herramienta de autor de regla y, a continuación, exporte esa configuración como el archivo `CEP.XML`. Después de habilitar Event Manager, siempre que la interconexión detecte datos UMF entrantes formateados utilizando el segmento de datos EVENT, la interconexión procesa los datos para la resolución de identidad y, a continuación, pasa los datos procesados al motor de CEP. El motor de CEP procesa los datos de suceso frente a las reglas empresariales de suceso configuradas en el archivo `CEP.XML` y devuelve la información de decisión a la interconexión de IBM InfoSphere Identity Insight, donde la información de sucesos se almacena en la base de datos de entidades. Si hay alertas de sucesos asociadas a un suceso o a una combinación de sucesos, puede configurar Event Manager para que muestre estas alertas de sucesos en el Visualizador u otras herramientas de visualización a fin de realizar análisis y eliminaciones.

También puede configurar la aplicación cliente para que el motor de CEP pueda devolver decisiones inmediatas a la aplicación cliente, proporcionando a los representantes de la organización información instantánea. Por ejemplo, el motor de CEP puede indicar inmediatamente a los representantes de servicio al cliente que detengan una transacción, por ejemplo una transferencia que supere el límite legal de dólares permitido que un cliente transfiera en un periodo de tiempo 24 horas.

Sucesos

Los sucesos representan información sobre algo que ha ocurrido en el ámbito empresarial, por ejemplo "un cliente abre una cuenta" o "un cliente envía dinero". En Event Manager, los sucesos contienen atributos que están basados en sus tipos de suceso correspondientes.

Alertas de sucesos

Una alerta de suceso se produce cuando uno de los sucesos más complejos cumple los criterios establecidos en un lapso de vida especificado. Las alertas de sucesos están basadas en reglas empresariales de sucesos complejas y otras configuraciones contenidas en un archivo de reglas de sucesos (`cep.xml`). Estas alertas pueden indicar situaciones de interés, tales como "Se han producido dos o más compras de más de 10.000$ de EE.UU. en la última hora en ubicaciones separadas 200 millas entre sí".

Tipos de sucesos

Los tipos de sucesos clasifican los sucesos y definen la unidad de medida para el valor asociado con los sucesos en Event Manager. Entre los ejemplos de tipos de suceso se incluyen la transferencia de conexiones, la apertura de cuentas o la transacción de tarjetas de crédito.

Los tipos de suceso son necesarios para el proceso de sucesos, porque las reglas empresariales definidas por el usuario que el procesador de sucesos utiliza llaman a un tipo de suceso específico. Si el tipo de suceso no existe, el procesador de sucesos no puede procesar el suceso.

Reglas de suceso

Las reglas de suceso son un conjunto de reglas empresariales que determinan cómo el motor de proceso de sucesos complejos (CEP) procesa los registros de sucesos de entrada y qué tipo de respuesta de suceso (como una alerta de suceso) se devuelve a la interconexión y la aplicación cliente. Configure reglas de suceso en la herramienta de autor de reglas de proceso de sucesos complejos basados en Eclipse[tm]. Las reglas de suceso se agrupan bajo un proyecto CEP y se exportan a un archivo de reglas de suceso denominado `cep.xml`.

Configure reglas de suceso para devolver información y alertas basadas en elementos de interés a la organización o los analistas. Se pueden configurar reglas de suceso para alertar sobre los datos de un registro único de suceso de entrada. Pero la mayoría de las reglas de suceso agrupan una colección de datos de sucesos complejos y desencadenan una alerta después de que se satisfaga un determinado umbral o condición.

En la herramienta de autor de reglas, las reglas empresariales de sucesos se denominan *situaciones*. Para obtener más información, consulte "Terminología de CEP" en la página 32.

Las reglas de suceso común contienen funciones de suma o recuento. Por ejemplo, puede configurar una regla de suceso para generar una alerta de suceso cuando cualquier entidad transfiere más de 15.000 $ de EE.UU. en un periodo de tiempo de 24 horas.

Guía de inicio de Event Manager

Utilice los siguientes pasos como una lista de comprobación para configurar y utilizar Event Manager.

Procedimiento

1. Necesario: Instale la herramienta de autor de regla de CEP (procesador de sucesos complejos) basada en Eclipse. La herramienta de autor de regla basada en Eclipse[TM] no se instala automáticamente con el producto. (La funcionalidad de Event Manager y el motor de CEP se instalan automáticamente.) La herramienta de autor de reglas está incluida en un archivo ZIP en la descarga de producto.
2. Necesario: Utilice la herramienta de autor de regla para crear un proyecto CEP para agrupar todas las reglas y configuraciones de sucesos para Event Manager.
3. Necesario: En la herramienta de autor de regla, importe el archivo de reglas de suceso `cep.xml` en el proyecto de CEP y personalice el archivo creando las reglas de suceso que satisfagan los escenarios de uso de alertas y proceso de suceso empresarial. Antes de modificar un archivo de inicio original, realice una copia de seguridad o copie el archivo en otro directorio, como medida de precaución.

   Importante: Las mayúsculas y minúsculas utilizadas para denominar el archivo de reglas de suceso es muy importante, especialmente en el entorno Unix. El nombre de archivo debe estar en minúsculas solamente.

4. Necesario: Exporte el archivo de reglas de suceso `cep.xml`. El motor de CEP y Event Manager utilizan este archivo XML de reglas de suceso para procesar sucesos y determinar cuándo se deben generar alertas. El archivo XML exportado se debe denominar `cep.xml` y debe estar ubicado en el directorio siguiente: *inicio_instalación_producto*/ibm-home/gem/.
5. Necesario: Configure los parámetros de sistema de Event Manager en la Consola de configuración.

   Recuerde: Para que los cambios de la configuración del sistema entren en vigor, debe detener y reiniciar todas las interconexiones que se están ejecutando. Puede detener todas las interconexiones que están en ejecución antes de configurar los tipos de suceso y parámetros de sistema de Event Manager o puede detener y reiniciar todas las interconexiones en ejecución después de configurar los tipos de sucesos y los parámetros de sistema de Event Manager.
6. Necesario: Configure tipos de suceso en la Consola de configuración.

   Recuerde: Para que los cambios de la configuración del sistema entren en vigor, debe detener y reiniciar todas las interconexiones que se están ejecutando. Puede detener todas las interconexiones que están en ejecución antes de configurar los tipos de suceso y parámetros de sistema de Event Manager o puede detener y reiniciar todas las interconexiones en ejecución después de configurar los tipos de sucesos y los parámetros de sistema de Event Manager.
7. Para ver alertas de sucesos en las aplicaciones del kit de herramientas de analista, haga lo siguiente:
   a. Opcional: Identity Insight ya contiene códigos de actividad predeterminados para tratar las alertas de sucesos (Pendiente, Asignado y Cerrado). No obstante, si lo desea, puede crear códigos de actividad adicionales para las alertas de sucesos en la Consola de configuración. Detenga todas las interconexiones que estén en ejecución para poder crear los códigos de actividad y, a continuación, una vez creados los códigos de actividad reinicie las interconexiones.
   b. Opcional: Puede revisar alertas de sucesos, cambiar el estado de las alertas de sucesos, asignarse alertas a sí mismo o asignar alertas a otros grupos de alertas de analista.
   c. Opcional: Si desea ver los detalles completos acerca de una alerta de suceso específica, puede generar el informe de Detalle de alerta de suceso.
   d. Opcional: Puede ver el historial de alertas de sucesos para una entidad en el resumen de entidades.
   e. Opcional: Desde el resumen de entidades, puede pulsar **Mostrar sucesos** para ver todos los sucesos asociados a la entidad e incluso los sucesos que no generaron ninguna alerta de sucesos. También puede pulsar **Informe** para imprimir el informe Todos los sucesos que muestra todos los sucesos asociados a la entidad.
8. Necesario: Utilice las definiciones de segmento de datos EVENT para incluir información de proceso de suceso en los datos UMF que convierte para enviar a las interconexiones.
9. Opcional: Si desea enviar mensajes de sistema (incluyendo mensajes de Event Manager) a la aplicación cliente, asegúrese de que utiliza una interconexión HTTP, y asegúrese de que la aplicación cliente puede recibir mensajes del documento de retorno SYSTEM_MESSAGE estándar.

10. Opcional: Después de que Event Manager haya procesado los sucesos, puede revisar los archivos de registro de Event Manager y los archivos de registro de consola de configuración asociados.

Habilitación de Event Manager en la Consola de configuración

Para poder procesar sucesos utilizando Event Manager, debe habilitar y configurar Event Manager en la Consola de configuración.

Acerca de esta tarea

Procedimiento

1. En la Consola de configuración, pulse la pestaña **Configuración del sistema**.
2. Para habilitar el proceso de sucesos, modifique el valor **Habilitar proceso de sucesos**.
3. Para configurar el indicador universal de recursos (URI) para CEP, modifique el valor **URI de procesador de sucesos**. El valor predeterminado debe ser http://localhost:13510/gem
4. Para aumentar el valor de tiempo de proceso de sucesos total, modifique el valor **Tiempo de espera de procesador de sucesos**. Este valor indica en segundos la cantidad de tiempo durante el cual la interconexión espera una respuesta del procesador de sucesos externo (CEP) antes de que se supere el tiempo de espera con un error.
5. Para modificar el número de días del historial de sucesos enviados a la interconexión para utilizarlos en la evaluación de un suceso de entrada nuevo, modifique el valor **Ventana de historial de sucesos**.
6. Pulse **Guardar**.

Configuración del módulo CEP de Event Manager

En IBM InfoSphere Identity Insight, *CEP* hace referencia a las herramientas de proceso de sucesos complejos empaquetadas con el producto. Estas herramientas son los componentes contenidos en Event Manager que amplían la resolución de identidades y relaciones para procesar transacciones de sucesos y generar alertas de sucesos. En esta sección se proporciona información sobre cómo configurar las herramientas CEP para trabajar específicamente con Event Manager.

Arquitectura

El componente CEP de Event Manager consta de dos herramientas:

Herramienta de autor de reglas basada en Eclipse™
: La herramienta de autor de reglas de proceso de sucesos complejos basada en Eclipse es el componente que se utiliza para configurar y exportar reglas de sucesos en el archivo `cep.xml`. El archivo de reglas de suceso determina cómo se procesan los sucesos y qué desencadena una alerta de suceso.

  Cuando se instala IBM InfoSphere Identity Insight, también instala un archivo comprimido que contiene la herramienta de autor de reglas y su Guía del usuario. Sin embargo, primero debe descomprimir los archivos de la herramienta para poder empezar a configurar las reglas de suceso.

Motor de proceso de sucesos complejos (motor de CEP)
: El motor de proceso de sucesos complejos (motor de CEP) es el componente que procesa los datos de sucesos de entrada con las reglas de suceso configuradas en el archivo `cep.xml`.

Cuando la interconexión recibe los datos formateados utilizando el segmento de datos EVENT de un documento UMF de entrada, envía dichos datos al motor de CEP para el proceso de sucesos. Después de que el motor de CEP haya evaluado los datos de suceso en el archivo `cep.xml` configurado, devuelve los resultados a la interconexión. Si los datos de suceso cumplen o superan la regla de suceso configurada, el motor de CEP también devuelve una señal a la interconexión para generar una alerta de suceso. Tanto si se genera una alerta de suceso como si no se genera, los datos de suceso finales que la interconexión recibe se graban en la base de datos de entidad.

El motor de CEP se instala de forma predeterminada con IBM InfoSphere Identity Insight.

Estos componentes de proceso de sucesos complejos forman parte de una versión específica de IBM Active Middleware[tm] Technology que se incluye en Event Manager. Estos componentes de proceso de sucesos complejos se incluyen en la compra del producto.

Archivo cep.xml

El archivo `cep.xml` contiene las reglas de suceso y otros valores necesarios para procesar los datos de suceso y generar alertas de suceso. La funcionalidad de Event Manager en la interconexión y el motor de CEP sólo puede procesar sucesos para el archivo de reglas de suceso denominado `cep.xml`. Este archivo está en formato XML (E**x**tensible **M**arkup **L**anguage), porque los datos que entran en la interconexión están en formato UMF (**U**niversal **M**essaging **F**ormat), un formato basado en XML.

Se incluye un archivo inicial `cep.xml` con la instalación del producto que contiene muchos de los valores de configuración necesarios que Event Manager necesita para trabajar con el motor de CEP. Puede importar el archivo `cep.xml` inicial a un proyecto CEP y, a continuación, configurar las reglas empresariales de sucesos.

Nota: Antes de importar el archivo de reglas de suceso `cep.xml` y realizar los cambios o exportar ese archivo, haga una copia de seguridad del original y almacene el archivo original en otro directorio. Considere la posibilidad de utilizar un sistema de control de origen o control de versiones siempre que modifique el archivo de reglas de sucesos.

Recursos adicionales para CEP

Para obtener información de uso más detallada sobre la utilización de la herramienta de autor de regla basada en Eclipse, consulte la Guía del usuario de la herramienta. La guía, denominada `AMT3.0.UserGuide.PDF`, se encuentra en *`vía_acceso_instalación`*`/cep/`.

Instalación de la herramienta de autor de reglas de procesador de sucesos complejos basada en Eclipse

Complete los pasos siguientes para instalar la herramienta de autor de reglas basada en Eclipse[TM] en una estación de trabajo. Tanto el Gestor de sucesos como el motor de CEP se instalan con el programa de instalación del producto. Pero debe instalar la herramienta de autor de reglas desde un archivo ZIP que está incluido en la instalación.

Antes de empezar

La herramienta de autor de reglas sólo funciona en un sistema operativo Microsoft Windows y necesita Java versión 1.5 o superior.

Acerca de esta tarea

Utilice la herramienta de autor de reglas para configurar las reglas y los umbrales que se utilizan para supervisar su negocio y, a continuación, exporte esa información al archivo de reglas de suceso (`cep.xml`). Event Manager y el motor de procesador de sucesos complejos (CEP) utilizan el archivo de reglas de suceso para procesar sucesos y detectar alertas de suceso. Las alertas de sucesos se pueden asociar a un solo suceso o a una combinación de sucesos. Puede configurar Event Manager para que muestre esas alertas de sucesos en el kit de herramientas de analista u otra herramienta de visualización para un análisis adicional.

Para instalar la herramienta de autor de regla basada en Eclipse desde el archivo ZIP:

Procedimiento

1. Navegue hasta el directorio de instalación del producto.
2. Navegue hasta el subdirectorio `/cep`.
3. Copie el archivo `CEP_3.0.1.1.03.zip` en una máquina cliente de Microsoft Windows.
4. Descomprima el `archivo CEP_3.0.1.1.03` en *`letra de unidad`*`:/CEP/`

Qué hacer a continuación

Para obtener información detallada sobre el uso de la herramienta de autor de reglas, consulte la Guía del usuario que se encuentra en el archivo `cep/AMT3.0_UserGuide.PDF`.

Inicio de la herramienta de autor de reglas:

Para utilizar la herramienta de autor de reglas basada en Eclipse[tm], primero debe iniciar la herramienta. La herramienta de autor de reglas se instala e inicia independiente de los componentes de IBM InfoSphere Identity Insight.

Acerca de esta tarea

La herramienta de autor de regla sólo funciona en un cliente con un sistema operativo Microsoft Windows y necesita Java versión 1.5 o superior.

Procedimiento

1. Abra Microsoft Windows Explorer y navegue al directorio donde está instalada la herramienta de autor de regla basada en Eclipse.
2. Efectúe una doble pulsación en el script por lotes denominado `AmitIDE.cmd`. El script por lotes abre el ejecutable de herramienta de autor de regla.

Terminología de CEP

Algunos de los términos utilizados en la herramienta de autor de reglas basada en Eclipse[tm] pueden diferir ligeramente de los términos utilizados en IBM InfoSphere Identity Insight y sus componentes. Este glosario puede ayudarle a conocer los términos de proceso de sucesos complejos y el modo en que se relacionan con Event Manager y otros componentes.

Archivo cep.xml

El archivo `cep.xml` contiene todas las reglas empresariales de sucesos y los valores de configuración de proceso de sucesos sucesos complejos necesarios para Event Manager y el motor de CEP para procesar los registros de sucesos de entrada. Se debe exportar un archivo de reglas de suceso con este nombre a la ubicación *directorio_instalación_producto*`\ibm-home\gem\`.

Importante: El nombre de archivo debe estar todo en minúsculas, especialmente en entornos Unix.

Mantenga y exporte el archivo de reglas de sucesos utilizando la herramienta de autor de regla.

Se incluye un archivo de reglas de suceso `cep.xml` de inicio con la instalación del producto IBM InfoSphere Identity Insight. Este archivo de inicio ya contiene muchos de los valores y configuraciones necesarios para trabajar con Event Manager. Puede importar el archivo de reglas de suceso `cep.xml` de inicio a la herramienta de autor de reglas, haciendo primero una copia de copia de seguridad del archivo original, para añadir reglas empresariales de sucesos y para exportar el archivo a la ubicación necesaria. Considere la posibilidad de utilizar un sistema de control de versiones o de origen para almacenar el archivo antes y después de la modificación.

Motor de CEP

El motor de proceso de sucesos complejos (o motor de CEP) es el mecanismo que procesa datos de sucesos de entrada de la interconexión y evalúa los datos con las reglas definidas en un proyecto CEP. El proyecto CEP se define en el archivo `cep.xml`, que está configurado y exportado por la herramienta de autor de reglas.

El motor de CEP que Event Manager utiliza actualmente forma parte del producto IBM Active Middleware™ Technology. La versión del motor de CEP necesario para Event Manager se incluye e instala como parte de IBM InfoSphere Identity Insight. Sin embargo, debe configurar Event Manager en la Consola de configuración y las reglas de suceso en la herramienta de autor de reglas antes de poder procesar correctamente los sucesos con el motor de CEP.

Proyectos de CEP

Los proyectos son un grupo de nivel superior que el procesador de sucesos complejos utiliza para contener un grupo de sucesos, lapsos de vida y reglas. Para utilizar Event Manager, cree **un** proyecto de CEP que contenga toda la información de sucesos, incluyendo las reglas de sucesos empresariales, para los sucesos que desea supervisar. Event Manager sólo utiliza un proyecto de CEP a la vez, pero cualquier proyecto individual puede probar varios tipos de sucesos y varias reglas por cada tipo de suceso.

Puede crear y mantener el proyecto CEP dentro de la herramienta de autor de reglas.

Herramienta de autor de reglas (herramienta de autor de reglas basada en Eclipse)

Esta herramienta le permite definir proyectos, sucesos y otras configuraciones CEP que forman parte del archivo de reglas de suceso `cep.xml` que el motor de CEP utiliza para procesar sucesos y generar alertas de suceso.

Clases de sucesos

Para utilizar Event Manager, el proyecto CEP debe contener las siguientes clases de suceso, que vienen preconfiguradas en el archivo `cep.xml` de inicio:

- `EAS_START.event`: se utiliza para indicar el iniciador de lapso de vida de Event Manager.
- `EAS_STOP.event`: se utiliza para indicar el terminador de lapso de vida de Event Manager.
- `EVENT.event`: se utiliza para definir las reglas empresariales (o situaciones) de Event Manager que se utilizan para procesar datos de sucesos de entrada y generar alertas de sucesos.

EVENT.event

Esta clase de suceso CEP correlaciona los datos de entrada que se pasa de la interconexión para el motor de CEP para el proceso. La correlación corresponde directamente a la tabla `GEM_EVENT` en la base de datos de entidades. Utilice la herramienta de autor de reglas para asegurarse de que los atributos asociados con `EAS_EVENT` coinciden con las correlaciones de datos en la tabla `GEM_EVENT`.

Lapsos de vida

En CEP, los lapsos de vida son los intervalos de tiempo durante los cuales las situaciones (reglas de suceso) son pertinentes. Un lapso de vida siempre se inicia con un iniciador y siempre termina con un terminador. Los lapsos de vida s asocian con una clase de suceso.

Para Event Manager, la clase de suceso EVENT debe contener el iniciador de lapso de vida `EAS_START` y el terminador de lapso de vida `EAS_STOP`.

Situaciones

Las situaciones en el autor de reglas son equivalentes a las *reglas de suceso*. Utilice la herramienta de autor de reglas para configurar situaciones que definen las reglas empresariales para determinar qué sucesos o combinación de sucesos son significativos para la organización y qué desencadena una alerta de suceso.

Las situaciones se asocian con una clase de suceso y proyecto de CEP y están contenidas en el archivo de reglas de suceso `cep.xml` .

A medida que los datos UMF entran en la interconexión, los registros (o documentos de entrada `UMF_ENTITY`) que contienen una definición de segmento de datos `EVENT` se envían al motor de CEP. El motor de CEP evalúa estos datos de sucesos de entrada con las situaciones configuradas en el archivo de reglas de suceso cep.xml. Si un suceso cumple o supera una situación definida, el motor de CEP vuelve a enviar una alerta de suceso a la interconexión, lo que puede visualizarse en las aplicaciones del kit de herramientas de analista o una herramienta de visualización de su elección.

Condición de umbral

Defina condiciones de umbral como parte de una regla de suceso (situación). Considere las condiciones de umbral como filtros de datos o comprobaciones de datos rápidas. Durante el proceso, el motor de CEP comprueba los datos de sucesos de entrada para ver si cumplen la condición de umbral especificada antes de procesar los datos con la regla. Si los datos cumplen la condición de umbral, el motor de CEP procesa los datos de sucesos con la regla; si los datos no cumplen la condición de umbral, el motor de CEP se mueve a la siguiente regla de suceso.

Por ejemplo, para procesar sólo sucesos que se han producido en la Sucursal 102, cree una condición de umbral que especifique `EVENT_LOC='102'`.

Clave UMF_LOG_ID

`UMF_LOG_ID` es un número secuencial exclusivo asignado a cada registro a medida que se procesa. En un proyecto CEP, `UMF_LOG_ID` es una clave de agrupación que está asociada con todos los indicadores de lapso de vida y clases de sucesos de Event Manager necesarios. Esta clave de agrupación asegura que todos los registros de entrada con el mismo `UMF_LOG_ID` se procesan juntos.

Si importa el archivo `cep.xml` de inicio incluido con el producto en un proyecto CEP, la clave `UMF_LOG_ID` ya está configurada y asignada a los indicadores de lapso de vida y clases de suceso de Event Manager.

Configuración del archivo de reglas de suceso cep.xml

La información configurada en el archivo de reglas de suceso `cep.xml` determina cómo procesan los datos de sucesos de entrada Event Manager y el motor de CEP y qué respuestas se devuelven a la aplicación cliente, la interconexión, la base de datos de entidades y las aplicaciones. Las reglas de suceso son una gran parte de la información contenida en el archivo `cep.xml`, pero las reglas no son la única información necesaria. Existen otros varios elementos y valores que también deben incluirse para procesar adecuadamente sucesos a través de Event Manager.

El producto incluye un archivo de reglas de sucesos `cep.xml` de inicio que contiene los elementos y valores necesarios, ya configurados para el usuario. Si importa el archivo `cep.xml` de inicio, no necesita configurar o cambiar estos elementos o valores, pero puede centrarse en configurar las reglas empresariales de sucesos y añadiendo las reglas al archivo `cep.xml`. Puesto que las reglas de suceso son exclusivas de cada organización, el archivo `cep.xml` de inicio no incluye reglas de suceso preconfiguradas (o tipos de situación).

Elementos y valores necesarios para el archivo cep.xml

Esta información se proporciona a efectos de consulta. Si elige no importar el archivo `cep.xml` de inicio proporcionado, sino que prefiere crear su propio archivo desde cero, utilice esta información para asegurarse de que el archivo contiene todos los elementos y valores necesarios. Si el archivo de reglas de suceso `cep.xml` que exporta para utilizarlo con Event Manager no se ha completado (no incluye esta información), Event Manager no puede procesar datos de sucesos de entrada.

Clases de sucesos

Las clases de sucesos describen las diferentes estructuras de sucesos que el motor de CEP debe conocer. Para procesar sucesos, las clases de sucesos siguientes deben formar parte del archivo de reglas de sucesos `cep.xml`:

`EAS_START.event`

Esta clase de suceso se convierte en el iniciador de lapso de vida de Event Manager o la señal para que el motor de CEP empiece a procesar el suceso.

`EAS_STOP.event`

Esta clase de suceso se convierte en el terminador de lapso de vida de Event Manager o la señal para que el motor de CEP deje de procesar el suceso.

`EVENT.event`

Esta clase de suceso es la base para cada regla empresarial de

suceso que cree. Contiene la información que correlaciona los datos de registro de sucesos de entrada con la tabla de Event Manager (GEM_EVENT) y con el segmento de datos EVENT.

Lapso de vida
En CEP, un lapso de vida es un intervalo de tiempo durante el cual son relevantes determinadas reglas de sucesos. Puesto que la interconexión procesa datos casi en tiempo real, el único propósito verdadero del lapso de vida es señalar el principio y el final de un registro de sucesos.

La información de lapso de vida necesaria para el proceso de Event Manager incluye los elementos siguientes:

EAS_START
Este elemento es el iniciador de lapso de vida necesario y señala el inicio de un suceso. Establezca este elemento de lapso de vida en la tabla **Iniciadores de sucesos** en la pestaña **Lapso de vida: Iniciadores**.

EAS_STOP
Este elemento es el terminador de lapso de vida necesario y señala el final de un suceso. Elija la selección de terminador para **Terminar por suceso** en la pestaña **Lapso de vida: Terminadores y claves**.

Clave de agrupación UMF_LOG_ID
Un UMF_LOG_ID es un número secuencial exclusivo asignado a cada registro a medida que se procesa. En un proyecto CEP, la clave de agrupación UMF_LOG_ID asegura que todos los registros de entrada con el mismo UMF_LOG_ID se procesen juntos. Esta clave de agrupación se asigna a todas las clases de suceso e indicadores de lapso de vida.

Atributos EVENT.event
Los atributos necesarios para esta clase de suceso se correlacionan directamente con el segmento de datos EVENT, que son los campos de la tabla GEM_EVENT en la base de datos de entidades. Si falta alguno de estos atributos necesarios en EVENT.event, el proceso de sucesos falla. Puede que vea uno o varios mensajes de error, como errores que mencionan 'XML no válido o con formato incorrecto' o 'falta información en el archivo XML de configuración de CEP'.

Especifique estos atributos en la pestaña **Situación**: **General y suceso** de cada regla de suceso.

Creación de un proyecto CEP:

Los proyectos CEP son una agrupación de reglas de suceso, lapsos de vida y demás información de sucesos utilizada por Event Manager y el motor de CEP. Los proyectos CEP forman parte del archivo de reglas de suceso cep.xml y se crean y mantienen en la herramienta de autor de reglas de CEP basada en Eclipse™. Antes de poder configurar reglas empresariales de sucesos para Event Manager, primero debe definir un proyecto CEP.

Antes de empezar
- La herramienta de autor de reglas CEP ya debe estar instalada y sus archivos descomprimidos.
- La herramienta de autor de reglas CEP sólo funciona en un sistema operativo Microsoft Windows y necesita Java versión 1.5 o superior.

Procedimiento

1. En la herramienta de autor de reglas CEP, seleccione **Archivo** > **Nuevo** > **Proyecto**.
2. Seleccione **Proyecto de proceso de sucesos** y pulse **Siguiente**.
3. Pulse **Finalizar**. El proyecto CEP se muestra en el panel de navegación izquierdo.

Qué hacer a continuación

Importe el archivo de reglas de suceso `ibm-home\gem\cep.xml` de inicio incluido con la instalación de producto. Este archivo ya contiene los elementos y valores necesarios para trabajar con Event Manager. Después de importar estos objetos necesarios al proyecto CEP, puede configurar las reglas empresariales de sucesos, y, a continuación, exportar el archivo de reglas de sucesos `cep.xml` final para empezar a procesar sucesos a través de Event Manager.

Importación del archivo de reglas de suceso cep.xml:

El archivo de reglas de suceso `cep.xml` contiene la información que el motor CEP y Event Manager utilizan para procesar sucesos y generar alertas de suceso. Se incluye un archivo `cep.xml` de inicio que ya contiene los elementos y valores necesarios para trabajar con Event Manager con la instalación del producto. Por lo tanto, en lugar de empezar desde cero, importe el archivo `cep.xml` existente a un proyecto CEP.

Antes de empezar

- Realice una copia de seguridad del archivo de reglas de suceso `cep.xml` original, para poder devolver el archivo original, si es necesario. Considere la posibilidad de mantener el archivo en un sistema de control de origen o de versiones.
- La herramienta de autor de reglas basada en Eclipse™ debe estar instalada y los archivos comprimidos.
- Tenga en cuenta que la herramienta de autor de regla sólo funciona en un cliente con un sistema operativo Microsoft Windows y necesita Java versión 1.5 o superior.
- Ya debe haber creado un proyecto de CEP en la herramienta de autor de regla.

Procedimiento

1. En la herramienta de autor de reglas, seleccione **Archivo** > **Importar**.
2. Seleccione **Definición de proceso de sucesos** y pulse **Siguiente**.
3. Examine para seleccionar el archivo `cep.xml`. Recuerde cambiar el tipo de archivo predeterminado de `DEF` a `XML`. Normalmente, este archivo está ubicado en el directorio *`directorio_instalación_producto`*`\ibm-home\gem`.
4. Compruebe los siguientes elementos:
   - Asegúrese de que se ha seleccionado todo el contenido del archivo. (Expanda la carpeta superior para examinar el contenido del archivo, si es necesario.)
   - Asegúrese de que se visualiza el nombre de proyecto de CEP correcto. (Examine para seleccionar el proyecto, si es necesario.)
5. Pulse **Finalizar**. Pulse **Aceptar** para alterar temporalmente el archivo existente, si recibe ese mensaje. Cuando el archivo se importa satisfactoriamente, se visualizan varios signos más en el panel de navegación izquierdo de la herramienta de autor de regla.

Qué hacer a continuación

Añada reglas de suceso de negocio y, a continuación, exporte el archivo de reglas de suceso `cep.xml` al directorio *directorio_instalación_producto*`\ibm-home\gem\`.

Exportación del archivo de reglas de suceso cep.xml:

Para que Event Manager ejecute las reglas de proceso de sucesos complejos, debe exportar el archivo de reglas de suceso `cep.xml` que ha configurado en la herramienta de autor de regla basado en Eclipse[tm].

Antes de empezar

La herramienta de autor de regla sólo funciona en un cliente con un sistema operativo Microsoft Windows y necesita Java versión 1.5 o superior.

Acerca de esta tarea

- Si el motor de CEP ya está activo y en ejecución cuando se exporta el archivo de reglas de sucesos, debe volver a cargar el archivo en el servidor de IBM WebSphere para que los cambios en el nuevo archivo de reglas de suceso `cep.xml` exportado entren en vigor.

Procedimiento

1. En la herramienta de autor de regla, seleccione **Archivo** > **Exportar**.
2. Seleccione **Definición de proceso de sucesos** y pulse **Siguiente**.
3. Seleccione el proyecto de CEP.
4. Establezca el archivo de definición de proceso de suceso en el nuevo archivo de reglas de suceso `cep.xml`. El archivo normalmente se encuentra en *directorio_instalación_producto*`\ibm-home\gem\cep.xml`.
5. Pulse **Finalizar**. Si el sistema le avisa de la sobrescritura de un archivo `cep.xml` existente, pulse **Aceptar**.
6. Opcional: Si el servidor de IBM WebSphere está actualmente en ejecución, vuelva a cargar las reglas CEP. Cuando el motor de CEP se inicia en el servidor de aplicaciones de producto, CEP carga el archivo de reglas de suceso `cep.xml` actual. Si el servidor WebSphere está en ejecución cuando se exporta el archivo, los cambios no entrarán en vigor hasta que se vuelva a cargar el nuevo archivo `cep.xml`.
   a. Abra una ventana de navegador web y vaya al servidor WebSphere. Por ejemplo `http://localhost:13510/gem`.
   b. Pulse **Volver a cargar reglas**.

      Nota: El servidor WebSphere no reconoce visiblemente que las reglas se hayan vuelto a cargar.

Directrices para la configuración de resultados de regla de suceso

Las reglas de suceso definen cómo procesar sucesos y qué situaciones generan alertas de sucesos. Las reglas de suceso (denominadas *Tipos de situación* en la herramienta de autor de reglas CEP basada en Eclipse[tm]) se incluyen en el archivo de reglas de suceso `cep.xml` que Event Manager y el motor de CEP utilizan para procesar los datos de sucesos de entrada. Las reglas de suceso complejo que defina son exclusivos de la organización.

Antes de empezar a definir reglas de suceso, tenga presentes las siguientes consideraciones, para que la regla funcione con Event Manager:

- Recuerde que las reglas de suceso deben centrarse en una entidad y las transacciones que una entidad puede hacer. Las entidades suelen ser personas, pero una entidad también puede representar un lugar o un objeto. Por ejemplo, una entidad puede ser un barco.
- Las reglas de suceso deben expresarse como una sentencia declarativa (como 'Location=Texas') o como una expresión matemática (suma, recuento, promedio) expresada en el tiempo.

Atributos de situación necesarios para cada regla empresarial de suceso

Para devolver datos de suceso del procesador de sucesos complejos a la base de datos de entidad, debe añadir manualmente los atributos de situación necesarios a cada regla empresarial de sucesos que cree. Estos atributos no forman parte del archivo de reglas de suceso `cep.xml` de inicio, de modo que al importar ese archivo inicial no crea automáticamente las reglas empresariales de sucesos (situaciones) o añaden estos atributos a ninguna regla nueva o existente.

Estos atributos de situación correlacionan datos de sucesos directamente con la tabla de Event Manager `GEM_EVENT` (y coinciden con el UMF de cada registro de suceso de entrada). Sin estos atributos necesarios, ninguno de los datos procesados por el motor de CEP se devuelve a Event Manager a través de la interconexión.

Tabla 4. Atributos de situación necesarios para reglas empresariales de sucesos complejas

Nombre de atributo	Tipo de atributo	Expresión de atributo	Descripción de atributo
EVENT_SIT_STATUS	string	"PENDING"	Indica el estado de alerta de sucesos para la alerta de suceso. En el plug-in i2, Explorer y el informe Resumen de alerta Cognos, el estado de alerta de suceso se muestra como parte del resumen de alerta. Todas las alertas recién generadas normalmente reciben el estado pendiente, indicando que un analista necesita analizar y disponer dicha alerta. Tenga en cuenta que un estado de alerta de suceso puede ser cualquier cosa que tenga sentido para su organización y se configura como un estado de suceso en la Consola de configuración. Si no desea que el suceso se visualice en las interfaces de usuario de componente del kit de herramientas de analista, utilice el estado de alerta de suceso "CLOSED".

Tabla 4. Atributos de situación necesarios para reglas empresariales de sucesos complejas (continuación)

Nombre de atributo	Tipo de atributo	Expresión de atributo	Descripción de atributo
REASON_DESC	string	"<*Descripción de regla o alerta de suceso*>"	Describe la regla de suceso que ha desencadenado la alerta de suceso. Haga que esta descripción sea los más significativa posible para los analistas. Por ejemplo, si la regla de suceso genere una alerta cuando una entidad gestiona más 1500 $ en un periodo de 24 horas, puede especificar "SumOver1500" como REASON_DESC.
ALERT_GROUP	string	"<*grupo de alertas*>"	Indica qué grupo de alertas para asignar alertas de sucesos generadas desde esta regla de suceso. Normalmente, este valor es "DEFAULT", pero puede especificar cualquier grupo de alertas configurado en la Consola de configuración.

Visualización del detalle de alertas de sucesos

Normalmente, se desencadenan alertas de sucesos a partir de más de un suceso complejo. Puede visualizar alertas de sucesos en las aplicaciones de kit de herramientas de analista o una aplicación de cliente, pero de forma predeterminada, los detalles de los sucesos que han formado dicha alerta no se incluyen.

Si desea incluir los detalles de los sucesos que forman la alerta de suceso, debe incluir el atributo de situación siguiente:

Tabla 5. Valores necesarios para crear el atributo de situación EVENTS en una regla de suceso

Nombre	Tipo	Expresión	Dimensión (botón Mostrar avanzadas)
`EVENTS`	`integer`	`Event.EventID`	[] (para indicar que el EventID es una matriz] Debe editar el atributo de situación y pulsar el botón `Mostrar avanzadas` para ver y definir el valor de esta columna.

Métodos recomendados

Si visualiza las alertas de suceso en las aplicaciones de kit de herramientas de analista, mantenga el atributo de situación `REASON_DESC` como una serie de texto simple, en lugar de añadir valores del suceso al mensaje. El kit de herramientas de analista agrupa alertas comunes en un resumen de alerta que incluye un recuento del número de alertas incluidas en el resumen. Los analistas pulsan en un resumen de alerta para disponer todas las alertas contenidas en ese resumen.

Si define valores del suceso en `REASON_DESC`, cada alerta de suceso se visualiza como un resumen de alerta independiente con un recuento de 1, lo que significa que los analistas ven cada alerta de suceso en el resumen de alerta y las áreas de detalle de alerta de la ventana Resumen de alerta.

Creación de una regla de suceso para sumar sucesos complejos

Crear una regla de suceso SUM básica para sumar los totales de sucesos y crear una alerta de suceso si la suma de esos sucesos supera un umbral establecido. Por ejemplo, puede crear una regla de suceso que sume todas las transferencias monetarias enviadas por una persona en 24 horas y enviar una alerta de suceso si la suma de esas transferencias monetarias (sucesos) es superior a 15.000$.

Antes de empezar

Debe tener un proyecto CEP existente, que agrupe reglas de sucesos y toda la configuración de reglas.

Acerca de esta tarea

Estos pasos proporcionan las instrucciones básicas para crear una regla empresarial simple que resume el valor de su elección. Para algunos pasos, hay varias maneras de lograr el mismo resultado final. Para obtener más opciones, consulte la sección *Situations* de IBM Advanced Middleware™ Technology User'S Guide (guía para la herramienta de autor de reglas de CEP basada en Eclipse™), que se incluye con el producto.

Procedimiento

1. En el panel de navegación de la izquierda, pulse **Situación** y seleccione **Nuevo** > **Situación**. Asegúrese de que se visualiza el nombre de proyecto correcto en **Proyecto de proceso de sucesos**.

2. Entre un nombre de regla exclusivo en **Nombre de situación**. El nombre de situación es el nombre de regla de suceso que se muestra en la base de datos de entidades y en el componente de Visualizador, si elige visualizar alertas de sucesos allí. Asegúrese de que el nombre es significativo para quienes analizan las alertas de sucesos. Por ejemplo, si está creando una regla para sumar el valor de todos los sucesos y, a continuación, enviar una alerta si la suma de los sucesos cruza el límite de 15.000$, puede darle a esta regla el nombre de `SumOver15K`.
3. En **Seleccionar origen**, seleccione **Vacío de tipo** y, a continuación, seleccione **atleast** en la lista desplegable. La situación **atleast** puede sumar valores de sucesos, así como conservar la información de cada suceso que cumpla la regla de suceso. Para obtener más información sobre los tipos de situación, consulte *Propiedades de situación* en la Guía del usuario.
4. Pulse **Finalizar**. Cuando se visualiza la pantalla de situaciones principal, puede que observe varios errores en la sección **Problemas**. Estos errores indican valores que faltan, pero puede ignorar estos errores por ahora. Al completar estos pasos, los errores desaparecen.
5. En la sección **Sucesos**, seleccione `EVENT` como suceso base para esta regla. `EVENT` es siempre el suceso base para cada regla empresarial de suceso. Contiene la correlación necesaria con la base de datos de entidad `GEM_TABLE` y el segmento de datos `EVENT`.
6. Opcional: Puede crear una *condición de umbral* para filtrar sucesos antes de que se evalúen en esta regla para que los sucesos cumplan la condición de umbral especificada para tenerse en cuenta.
7. Para crear la expresión de suma, pulse **Mostrar avanzadas** y, a continuación, **Editar**.
8. En **Cuantificador**, seleccione `each`. Esta selección garantiza que cada registro de sucesos de entrada que satisfaga las condiciones de esta regla de suceso se incluya en la suma total.
9. En **Peso**, pulse **...** para editar el campo. Utilice el **Creador de expresiones** para seleccione el campo de suceso a sumar. Asegúrese de que la expresión se muestra en el área **Texto de creador de expresiones** y, a continuación, pulse **Aceptar**. De forma predeterminada, el peso de cada suceso es igual a 1. Cuando la regla de suceso se evalúa, la suma de todos los pesos se compara con el atributo **Cantidad** en la pestaña **Condición & Resultados**. Cuando el total es igual como mínimo a la cantidad indicada, se genera una alerta de suceso. Por ejemplo, para sumar los valores de cada suceso que satisface la regla de suceso, seleccione `EVENT.EVENT_VALUE`.
10. Opcional: Si el campo seleccionado como el peso contiene dígitos decimales (tipo doble), utilice el Generador de expresiones para crear una expresión para hacer lo siguiente:
    a. Multiplicar los resultados de cálculo por 100 para mantener los dígitos decimales al convertir los dólares a centavos.
    b. Convertir el tipo doble a un entero. Puede conseguirlo utilizando funciones.

    Por ejemplo, si está sumando los valores de sucesos (`EVENT.EVENT_VALUE`), puede especificar `EVENT.EVENT_VALUE*100` en el área **Texto de creador de expresiones**. A continuación, puede seleccionar **Funciones** > **Matemáticas** > **Redondeo** para redondear el resultado al valor entero más cercano. La expresión final se visualiza como `Round(EVENT.EVENT_VALUE*100)`.
11. En **Expresión de suma**, pulse **...** para editar el campo y seleccionar el campo de suceso a sumar. Por ejemplo, para sumar el valor de cada suceso que cumple o excede la regla de suceso, seleccione `EVENT_VALUE`.

12. Opcional: Para sumar sólo los sucesos que cumplen una condición específica, especifique la condición en **Condición de umbral** o utilice el Creador de expresiones para ayudarle. Por ejemplo, para sumar sólo los valores de los sucesos que se han producido en la bifurcación 102, especifique EVENT.EVENT_LOC="102". Este campo actúa como un filtro, saltando automáticamente sucesos que no cumplen o superan la condición.

    Consejo: Para simplificar la vista y ver **Condición de umbral** más fácilmente, pulse **Ocultar avanzadas**.
13. En la pestaña **Condición & Resultados** en **Lapso de vida**, seleccione `EASLifeSpan`. Observe que hasta que se realice la selección, este campo se muestra en rojo. El color rojo indica que este es un campo necesario y es uno de los errores listados en la sección **Problemas**. Cuando se realiza la selección de lapso de vida, el error desaparece de la sección **Problemas**.
14. En **Cantidad**, especifique la cantidad "atleast" que la regla de sucesos suma hasta antes de generar la alerta de suceso. Recuerde que debe multiplicar los importes en dólares por 100. Por ejemplo, para generar una alerta de suceso cuando la suma llega al menos a 15.000$, especifique `150000`.
15. En **Modalidad de detección**, observe que se ha seleccionado `immediate`. Conserve esta selección. La modalidad de detección determina cuándo se deben calcular y comunicar los resultados de los sucesos. La selección `immediate` genera una alerta tan pronto como la suma alcanza la cantidad.
16. En `Atributos de situación`, especifique los valores de situación necesarios para los siguientes atributos de situación:
    - `EVENT_SIT_STATUS`
    - `REASON_DESC`
    - `ALERT_GROUP`
17. Opcional: Para conservar los detalles de todos los sucesos que componen la suma, añada el atributo de situación `EVENTS`, utilizando la información siguiente:
    a. En **Nombre**, especifique `EVENTS`.
    b. En **Tipo**, escriba `integer`.
    c. En **Expresión**, escriba `EVENT_ID` (o selecciónelo en **Creador de expresiones**).
    d. Pulse **Mostrar avanzadas** para visualizar la columna **Dimensiones** y escriba `[ ]` en la columna para indicar que el tipo es una matriz de sucesos.

    Estos valores indican a CEP que devuelva el `EVENT_ID` interno de cada suceso incluido en la suma total a la interconexión junto con la alerta de suceso. La interconexión graba cada `EVENT_ID` en la base de datos de entidades y envía la información al Visualizador o la aplicación cliente utilizada para visualizar alertas de suceso. `EVENT_ID` es un número de secuencia interno (ID) creado por la interconexión cuando envía datos de suceso al motor de CEP.
18. Guarde la regla de suceso.

Creación de una regla de suceso para contar sucesos complejos

Cree una regla de suceso COUNT básica para contar sucesos y crear una alerta de suceso si el recuento total supera un umbral establecido. Por ejemplo, puede crear una regla de suceso que cuenta todas las transacciones transferencias dentro de 24 horas y envía una alerta de suceso si el recuento de transacciones es más de 500.

Antes de empezar

Debe tener un proyecto CEP existente, que agrupe reglas de sucesos y toda la configuración de reglas.

Acerca de esta tarea

Estos pasos proporcionan las instrucciones básicas para crear una regla empresarial simple que cuenta el valor de su elección. Para algunos pasos, hay varias maneras de lograr el mismo resultado final. Para obtener más opciones, consulte la sección *Situations* de IBM Advanced Middleware[tm] Technology User'S Guide (guía para la herramienta de autor de reglas de CEP basada en Eclipse[tm]), que se incluye con el producto.

Procedimiento

1. En el panel de navegación de la izquierda, pulse **Situación** y seleccione **Nuevo** > **Situación**. Asegúrese de que se visualiza el nombre de proyecto correcto en **Proyecto de proceso de sucesos**.
2. Entre un nombre de regla exclusivo en **Nombre de situación**. El nombre de situación es el nombre de regla de suceso que se muestra en la base de datos de entidades y en el componente de Visualizador, si elige visualizar alertas de sucesos allí. Asegúrese de que el nombre es significativo para quienes analizan las alertas de sucesos. Por ejemplo, si está creando una regla para contar todos los sucesos que se han producido en una ubicación de bifurcación determinada, puede denominar esta regla `CountBranch102Transactions`.
3. En **Seleccionar origen**, seleccione **Vacío de tipo** y, a continuación, seleccione uno de los valores siguientes en la lista desplegable:
   - **atleast**: Han llegado al menos *n* o más sucesos durante el lapso de vida.
   - **atmost**: Han llegado no más de *n* sucesos al final del lapso de vida.

   Ambos tipos de situación pueden contar valores de sucesos, así como conservar la información de cada suceso que ha cumplido la regla de suceso. Para obtener más información sobre los tipos de situación, consulte *Propiedades de situación* en la Guía del usuario.
4. Pulse **Finalizar**. Cuando se visualiza la pantalla de situaciones principal, puede que observe varios errores en la sección **Problemas**. Estos errores indican valores que faltan, pero puede ignorar estos errores por ahora. Al completar estos pasos, los errores desaparecen.
5. En la sección **Sucesos**, seleccione `EVENT` como suceso base para esta regla. `EVENT` es siempre el suceso base para cada regla empresarial de suceso. Contiene la correlación necesaria con la base de datos de entidad `GEM_TABLE` y el segmento de datos `EVENT`.
6. Opcional: Puede crear una *condición de umbral* para filtrar sucesos antes de que se evalúen con esta regla, de modo que los sucesos deben cumplir con la condición de umbral especificada que se debe tener en cuenta.
7. En la pestaña **Condición & Resultados** en **Lapso de vida**, seleccione `EASLifeSpan`. Observe que hasta que se realice la selección, este campo se muestra en rojo. El color rojo indica que este es un campo necesario y es uno de los errores listados en la sección **Problemas**. Cuando se realiza la selección de lapso de vida, el error desaparece de la sección **Problemas**.
8. En **Cantidad**, especifique la cantidad "atleast" o "atmost" a la que cuenta la regla de suceso antes de generar la alerta de suceso.
9. En **Modalidad de detección**, observe que se ha seleccionado `immediate`. Conserve esta selección. La modalidad de detección determina cuándo se

deben calcular y comunicar los resultados de los sucesos. La selección `immediate` genera una alerta tan pronto como el recuento alcanza la cantidad.

10. En `Atributos de situación`, especifique los nombres, tipos y expresiones de atributo de situación necesarios:
    - `EVENT_SIT_STATUS`
    - `REASON_DESC`
    - `ALERT_GROUP`
11. Para conservar los detalles de todos los sucesos que componen el recuento, añada el atributo de situación `EVENTS`, utilizando la información siguiente:
    a. En **Nombre**, especifique `EVENTS`.
    b. En **Tipo**, escriba `integer`.
    c. En **Expresión**, escriba `EVENT_ID` (o selecciónelo en **Creador de expresiones**).
    d. Pulse **Mostrar avanzadas** para visualizar la columna **Dimensiones** y escriba `[ ]` en la columna para indicar que el tipo es una matriz de sucesos.

    Estos valores indican a CEP que devuelva el `EVENT_ID` interno de cada suceso incluido en la suma total a la interconexión junto con la alerta de suceso. La interconexión graba cada `EVENT_ID` en la base de datos de entidades y envía la información al Visualizador o la aplicación cliente utilizada para visualizar alertas de suceso. `EVENT_ID` es un número de secuencia interno (ID) creado por la interconexión cuando envía datos de suceso al motor de CEP.
12. Guarde la regla de suceso.

Accesibilidad

Las características de accesibilidad ayudan a los usuarios con discapacidades físicas, como movilidad restringida o visión limitada, a utilizar correctamente productos de software.

La lista siguiente contiene las principales características de accesibilidad:

- Se puede navegar por todas las funciones de la interfaz de usuario mediante el teclado en lugar del ratón, cuando se utiliza el navegador Internet Explorer recomendado.
- El producto es compatible con tecnologías de asistencia.
- La documentación de IBM InfoSphere Identity Insight se ofrece en un formato accesible.

Acceso mediante teclado

Se puede acceder a la Consola de configuración y al Visualizador de IBM InfoSphere Identity Insight cuando se visualiza con el navegador Internet Explorer.

Puede utilizar la Consola de configuración o el Visualizador sólo con el teclado. Puede utilizar teclas o combinaciones de teclas para realizar operaciones que también se pueden realizar con un ratón. Se utilizan pulsaciones de teclas estándares del sistema operativo para operaciones estándares del sistema operativo.

En todos los sistemas operativos soportados y en todos los navegadores soportados, se resalta el área de la ventana activa en la que tendrán efecto las

pulsaciones de teclas. Los recuadros de texto y las áreas de texto muestran un cursor de punto de inserción parpadeante. Otros campos se resaltan con un borde de puntos.

Nota: Se puede navegar por la Consola de configuración utilizando el navegador Mozilla Firefox, pero existe un problema: los aceleradores y atajos del teclado en los que se utilizan las teclas **Alt** + ***número*** no reciben soporte en este navegador.

Visualización accesible

La Consola de configuración y el Visualizador tienen características que mejoran la accesibilidad para los usuarios con baja visión u otros problemas de visión. Estas mejoras en la accesibilidad incluyen soporte para propiedades de fonts que se pueden personalizar.

Puede seleccionar el color, el tamaño y el font del texto de menú y ventanas de diálogo mediante la interfaz de usuario:

- Consola de configuración: mediante los valores del navegador
- Visualizador: mediante los valores de **Configurar preferencias de pantalla**.

No es necesario que distinga los colores para poder utilizar cualquiera de las funciones de este producto.

Compatibilidad con tecnologías de asistencia

La interfaz de usuario del Visualizador da soporte a la API de accesibilidad de Java, que le permite utilizar lectores de pantalla y otras tecnologías de asistencia. En la Consola de configuración, puede habilitar lectores de pantalla en los navegadores soportados.

Documentación accesible

La documentación correspondiente a IBM InfoSphere Identity Insight se proporciona en formato XHTML 1.0, que se puede visualizar en la mayoría de los navegadores Web. XHTML le permite ver la documentación según las preferencias de visualización establecidas en el navegador. También le permite utilizar lectores de pantalla y otras tecnologías de asistencia.

Atajos de teclado y aceleradores de la Consola de configuración

La consola de configuración es completamente accesible, cuando se visualiza utilizando navegadores soportados. Esto significa que se pueden utilizar teclas o combinaciones de teclas para realizar operaciones que también se pueden realizar utilizando un ratón.

Nota: Se puede navegar en la Consola de configuración con el teclado utilizando el navegador Mozilla Firefox, pero las teclas **Alt** + ***número*** no funcionan correctamente en este navegador.

Tabla 6. Atajos de teclado y aceleradores generales

Acción	Atajo
Ir al siguiente elemento de la pantalla (campo de entrada, botón, enlace) del foco (se salta los campos de sólo lectura)	**Tabulador**

Tabla 6. Atajos de teclado y aceleradores generales (continuación)

Acción	**Atajo**
Volver al elemento anterior de la pantalla (campo de entrada, botón o enlace) del foco (se salta los campos de sólo lectura)	**Desplazamiento** + **Tabulador**
Realizar una acción (enlace o botón)	**Intro**

Tabla 7. Navegación en campos

Acción	**Tecla o atajo**
Subir o bajar en una lista desplegable Subir o bajar múltiples líneas de un campo de área de texto	Flechas arriba o abajo
Ir a la izquierda o derecha en un campo de entrada de texto	Flechas a izquierda o derecha
Ir al principio de un campo de entrada de texto Ir al principio de la línea actual en un campo grande de área de texto	**Inicio**
Ir al final de un campo de entrada Ir al final de la línea actual en un campo grande de área de texto	**Fin**
Ir al final de un campo de entrada de texto Ir a la página siguiente en un campo de área de texto	**Avance página**
Ir al principio de un campo de entrada de texto Ir a la página anterior de un campo de área de texto	**Retroceso página**
Expandir o colapsar una lista desplegable	**Alt** + flecha arriba o abajo
Ir al principio de un área de texto	**Ctrl** + **RePág**
Ir al final de un área de texto	**Ctrl** + **AvPág**

Tabla 8. Navegación en pantalla

Acción	**Atajo**
(Para utilizar con lectores de pantalla) Saltar todos los enlaces de navegación y los enlaces de acción en la cabecera de página	**Alt** + **0**
Dar el foco a las acciones del área de ubicación y la esquina superior derecha	**Alt** + **1**
Dar el foco a menús o submenús	**Alt** + **2**
Activar pestañas de nivel superior	**Alt** + **3**
Activar enlaces de nivel superior	**Alt** + **4**
(Sólo pantallas de detalles) Dar el foco a los elementos del panel de navegación izquierdo	**Alt** + **5**
(Sólo pantallas de detalles) Activar sub-paneles y botones de acción de detalles	**Alt** + **6**

Tabla 8. Navegación en pantalla (continuación)

Acción	Atajo
Activar cualquier campo de formulario del área de contenido principal	**Alt** + **7**
(Para utilizar con lectores de pantalla) Saltar el directorio hasta los campos de las pantallas de detalles	**Alt** + **8**
(Para utilizar con lectores de pantalla) Saltar hasta el pie de página de ayuda en la parte inferior de la pantalla	**Alt** + **9**

Tabla 9. Acciones de edición (dentro de campos de entrada)

Acción	Atajo
Copiar	**Ctrl** + **C**
Cortar	**Ctrl** + **X**
Pegar	**Ctrl** + **V**
Seleccionar todo	**Ctrl** + **A**
Deshacer	**Ctrl** + **Z**
Suprimir el carácter a la izquierda del cursor	**Retroceso**
Suprimir el carácter a la derecha del cursor	**Supr**

Atajos de teclado y aceleradores del Visualizador

El Visualizador es totalmente accesible. Esto significa que se pueden utilizar teclas o combinaciones de teclas para realizar operaciones que también se pueden realizar utilizando un ratón.

Tabla 10. Atajos de teclado y aceleradores generales

Acción	Atajo
Ir al siguiente elemento de la pantalla (campo de entrada, botón, enlace) del foco	**Tabulador**
Volver al elemento anterior de la pantalla (campo de entrada, botón o enlace) del foco	**Desplazamiento** + **Tabulador**
Realizar una acción (enlace o botón)	**Especifique** o pulse la barra espaciadora
Visualizar la pantalla de criterios de informes y los valores predeterminados del informe Generador de alertas de atributo	**Ctrl** + **A**
Visualizar la pantalla Carga de archivo UMF	**Ctrl** + **B**
Visualizar el diálogo Cambiar contraseña	**Ctrl** + **H**
Bloquear la aplicación - el usuario actual sigue en una sesión del Visualizador, pero la pantalla está bloqueada	**Ctrl** + **L**
Visualizar el diálogo Imprimir de las ventanas o los separadores de los que puede imprimir informes o información (por ejemplo Resumen de entidades "Entity Resume")	**Ctrl** + **P**
Finalizar la sesión del usuario actual del Visualizador y sale de la aplicación	**Ctrl** + **Q**

Tabla 10. Atajos de teclado y aceleradores generales (continuación)

Acción	**Atajo**
Visualizar el diálogo Configurar preferencias de pantalla	**Ctrl** + **R**
Visualizar el Centro de Información del producto	**F1**
Visualizar la ventana Acerca de, que incluye el número de versión del producto	**Desplazamiento** + **F1**

Tabla 11. Navegación en campos

Acción	**Tecla o atajo**
Ir al campo por encima o por debajo Subir o bajar en una lista desplegable Subir o bajar múltiples líneas de texto en un campo de entrada	Flechas arriba o abajo
Ir a la izquierda o derecha en un campo de entrada	Flechas a izquierda o derecha
Ir al principio de un campo de entrada Ir al principio de la línea actual en un campo de texto grande	**Inicio**
Ir al final de un campo de entrada Ir al final de la línea actual en un campo de texto de grande	**Fin**
Ir al final de un campo de entrada	**Avance página**
Ir al principio de un campo de entrada	**Retroceso página**
Expandir o colapsar una lista desplegable	**Alt** + flecha arriba o abajo
Expandir o colapsar un twistie (si se ha seleccionado el twistie)	Barra espaciadora
Salir de una tabla al siguiente control	**Ctrl** + **Tabulador**

Tabla 12. Acciones de edición

Acción	**Atajo**
Copiar	**Ctrl** + **C**
Cortar	**Ctrl** + **X**
Pegar	**Ctrl** + **V**
Seleccionar todo el texto de los recuadros de texto	**Ctrl** + **A**
Deshacer	**Ctrl** + **Z**
Suprimir el carácter a la izquierda del cursor	**Retroceso**
Suprimir el carácter a la derecha del cursor	**Supr**

Capítulo 2. Planificación y requisitos del sistema

Esta sección contiene información sobre plataformas, soportadas, requisitos del sistema y arquitectura del sistema.

Requisitos del sistema detallados

Estos requisitos identifican los productos de hardware y software que debe instalar y utilizar antes de abrir un informe de problema con el equipo de soporte de IBM.

Requisitos del sistema al ejecutar en IBM AIX

La lista siguiente identifica los productos soportados cuando IBM InfoSphere Identity Insight se ejecuta en el sistema operativo AIX.

Tabla 13. Requisitos del sistema al ejecutar en IBM AIX

Sistemas operativos	• IBM AIX 7.1L
Requisitos de hardware	• POWER7 (64 bits) • POWER6 • POWER5
Java	A continuación se muestras los elementos instalados en este producto: • IBM 64-bit Java Runtime Environment, Versión 8
Bases de datos	• IBM DB2 Database for Linux, UNIX y Windows 11.1 • IBM DB2 Database for Linux, UNIX y Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 o posterior)
Clientes de base de datos	• Cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1 • Cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5 • Cliente de Oracle 12c al conectarse a Oracle 12c. • Cliente de Oracle 11g Release 2 al conectarse a Oracle 11g Release 2.

Tabla 13. Requisitos del sistema al ejecutar en IBM AIX (continuación)

Clientes de **Java Database Connectivity (JDBC)**	• Controlador JDBC de cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1. • Controlador JDBC de cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5. • Controladores JDBC de Oracle 12c al conectarse a Oracle 12c. • Controladores JDBC de Oracle 11g al conectarse a Oracle 11g.
Navegadores web	• Mozilla Firefox
Software de Message Queuing	• IBM WebSphere MQ
Otros	• IBM C++ Runtime Environment Components for AIX. Para obtener más información sobre este requisito, revise esta información de soporte: http://www-01.ibm.com/support/docview.wss?uid=swg24025181

Requisitos del sistema al ejecutar en HP-UX

La siguiente lista identifica los productos soportados cuando IBM InfoSphere Identity Insight se ejecuta en el sistema operativo HP-UX.

Tabla 14. Requisitos del sistema al ejecutar en HP-UX

Sistemas operativos	• HPUX 11i v3
Requisitos de hardware	• Intel Itanium 2 (IA64)
Java	A continuación se muestras los elementos instalados en este producto: • IBM 64-bit Java Runtime Environment for HPUX, Java Technology Edition, Versión 6
Requisitos del cliente de Java	HPUX no es una plataforma de cliente soportada. Cualquier máquina de cliente de plataforma soportada que se conecta a la Consola de configuración o al Visualizar debe tener instalado SUN Java SE Runtime Environment (JRE) Versión 6.
Bases de datos	• IBM DB2 Database for Linux, UNIX y Windows 11.1 • IBM DB2 Database for Linux, UNIX y Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 o posterior)

Tabla 14. Requisitos del sistema al ejecutar en HP-UX (continuación)

Clientes de base de datos	• Cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1 • Cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5 • Cliente de Oracle 12c al conectarse a Oracle 12c. • Cliente de Oracle 11g Release 2 al conectarse a Oracle 11g Release 2.
Clientes **Java Database Connectivity (JDBC) para la consola de configuración y el visualizador**	• Controlador JDBC de cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1. • Controlador JDBC de cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5. • Controladores JDBC de Oracle 12c al conectarse a Oracle 12c. • Controladores JDBC de Oracle 11g al conectarse a Oracle 11g.
Navegadores Web	• Mozilla Firefox
Software de Message Queuing soportado	• IBM WebSphere MQ

Requisitos del sistema cuando se ejecuta en Linux x86

La siguiente lista indentifica los productos soportados cuando IBM InfoSphere Identity Insight se ejecuta en el sistema operativo Linux x86.

Tabla 15. Requisitos del sistema cuando se ejecuta en Linux x86

Sistemas operativos	• Red Hat Enterprise Linux AS, Versión 6.0 • Red Hat Enterprise Linux AS, Versión 5.0 • Novell SUSE Linux Enterprise Server, Versión 10
Requisitos de hardware	• Intel x86 (IA32)
Java	A continuación se muestras los elementos instalados en este producto: • IBM 32-bit Runtime Environment for Linux en arquitectura Intel, Java Technology Edition, Versión 6
Requisitos del cliente de Java	Cualquier máquina de cliente de plataforma soportada que se conecta a la Consola de configuración o al Visualizar debe tener instalado SUN Java SE Runtime Environment (JRE) Versión 6.

Tabla 15. Requisitos del sistema cuando se ejecuta en Linux x86 (continuación)

Bases de datos	• IBM DB2 Database for Linux, UNIX y Windows 11.1 • IBM DB2 Database for Linux, UNIX y Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 o posterior)
Clientes de base de datos	• Cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1 • Cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5 • Cliente de Oracle 12c al conectarse a Oracle 12c. • Cliente de Oracle 11g Release 2 al conectarse a Oracle 11g Release 2.
Clientes **Java Database Connectivity (JDBC) para la consola de configuración y el visualizador**	• Controlador JDBC de cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1. • Controlador JDBC de cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5. • Controladores JDBC de Oracle 12c al conectarse a Oracle 12c. • Controladores JDBC de Oracle 11g al conectarse a Oracle 11g.
Navegadores Web	• Mozilla Firefox
Software de Message Queuing soportado	• IBM WebSphere MQ

Requisitos de sistema cuando se ejecuta en Linux para System x

La lista siguiente identifica los productos soportados cuando IBM InfoSphere Identity Insight se ejecuta en el sistema operativo Linux para System x.

Tabla 16. Requisitos de sistema cuando se ejecuta en Linux para System x

Sistemas operativos	• Red Hat Enterprise Linux AS, Versión 7.0 • Red Hat Enterprise Linux AS, Versión 6.0
Requisitos de hardware	• Intel x86_64
Java	A continuación se muestras los elementos instalados en este producto: • IBM 64-bit Java Runtime Environment, Versión 8

Tabla 16. Requisitos de sistema cuando se ejecuta en Linux para System x (continuación)

Bases de datos	• IBM DB2 Database for Linux, UNIX y Windows 11.1 • IBM DB2 Database for Linux, UNIX y Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 o posterior)
Clientes de base de datos	• Cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1 • Cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5 • Cliente de Oracle 12c al conectarse a Oracle 12c. • Cliente de Oracle 11g Release 2 al conectarse a Oracle 11g Release 2.
Clientes de **Java Database Connectivity (JDBC)**	• Controlador JDBC de cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1. • Controlador JDBC de cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5. • Controladores JDBC de Oracle 12c al conectarse a Oracle 12c. • Controladores JDBC de Oracle 11g al conectarse a Oracle 11g.
Navegadores Web	• Mozilla Firefox
Software de Message Queuing soportado	• IBM WebSphere MQ

Requisitos del sistema al ejecutar en Linux para System z

La lista siguiente identifica los productos soportados cuando IBM InfoSphere Identity Insight se ejecuta en el sistema operativo Linux para System z de 64 bits.

Tabla 17. Requisitos del sistema cuando se ejecuta Linux de 64 bits en System z

Sistemas operativos	• Red Hat Enterprise Linux AS, Versión 7.0
Requisitos de hardware	• IBM System z
Java	A continuación se muestras los elementos instalados en este producto: • IBM 64-bit Java Runtime Environment, Versión 8
Bases de datos	• IBM DB2 Database for Linux, UNIX y Windows 11.1 • IBM DB2 Database for Linux, UNIX y Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 o posterior)

Tabla 17. Requisitos del sistema cuando se ejecuta Linux de 64 bits en System z (continuación)

Clientes de base de datos	• Cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1 • Cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5 • Cliente de Oracale 10g Release 2 (10.2.0.2.0) al conectarse a Oracle 11g Release 1 (11.2.0.1) o 11g Release 2 (11.2.0.2)
Clientes de **Java Database Connectivity (JDBC)**	• Controlador JDBC de cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1. • Controlador JDBC de cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5. • Cliente de Oracale 10g Release 2 (10.2.0.2.0) al conectar a Oracle 11g Release 1 (11.2.0.1) o 11g Release 2 (11.2.0.2)
Navegadores web	• Mozilla Firefox
Software de Message Queuing soportado	• IBM WebSphere MQ

Requisitos del sistema al ejecutar en Sun Solaris

La lista siguiente identifica los productos soportados cuando IBM InfoSphere Identity Insight se ejecuta en el sistema operativo Sun Solaris.

Tabla 18. Requisitos del sistema al ejecutar en Sun Solaris

Sistemas operativos	• Sun Solaris 10.0
Requisitos de hardware	• UltraSPARC T2 • UltraSPARC IV y superior
Java	A continuación se muestras los elementos instalados en este producto: • IBM 64-bit Java Runtime Environment for Solaris, Java Technology Edition, Versión 6
Requisitos de Java de cliente	Cualquier máquina de cliente de plataforma soportada que se conecta a la Consola de configuración o al Visualizar debe tener instalado SUN Java SE Runtime Environment (JRE) Versión 6.
Bases de datos	• IBM DB2 Database for Linux, UNIX y Windows 11.1 • IBM DB2 Database for Linux, UNIX y Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 o posterior)

Tabla 18. Requisitos del sistema al ejecutar en Sun Solaris (continuación)

Clientes de base de datos	• Cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1 • Cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5 • Cliente de Oracle 12c al conectarse a Oracle 12c. • Cliente de Oracle 11g Release 2 al conectarse a Oracle 11g Release 2.
Clientes **Java Database Connectivity (JDBC) para la consola de configuración y el visualizador**	• Controlador JDBC de cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1. • Controlador JDBC de cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5. • Controladores JDBC de Oracle 12c al conectarse a Oracle 12c. • Controladores JDBC de Oracle 11g al conectarse a Oracle 11g.
Navegadores web	• Mozilla Firefox
Software de Message Queuing soportado	• IBM WebSphere MQ
Otro software	• GNU Compiler Collection, paquete gcc (o gcc_small), versión 3.3.2.

Requisitos del sistema cuando se ejecuta en Microsoft Windows Server

La lista siguiente identifica los productos soportados cuando IBM InfoSphere Identity Insight se ejecuta en un sistema operativo Microsoft Windows Server de 64 bits.

Tabla 19. Requisitos del sistema cuando se ejecuta en Microsoft Windows Server

Sistemas operativos	• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 R2
Requisitos de hardware	• Intel x86_64
Java	A continuación se muestras los elementos instalados en este producto: • IBM Java Runtime Environment, Versión 8 de 64 bits
Bases de datos	• IBM DB2 Database for Linux, UNIX y Windows 11.1 • IBM DB2 Database for Linux, UNIX y Windows 10.5 • Oracle 12c • Oracle 11g Release 2 (11.2.0.1, 11.2.0.2 o posterior)

Tabla 19. Requisitos del sistema cuando se ejecuta en Microsoft Windows Server (continuación)

Clientes de base de datos	• Cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1 • Cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5 • Cliente de Oracle 12c al conectarse a Oracle 12c. • Cliente de Oracle 11g Release 2 al conectarse a Oracle 11g Release 2.
Clientes Java Database Connectivity (JDBC)	• Controlador JDBC de cliente de DB2 v11.1 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 11.1. • Controlador JDBC de cliente de DB2 v10.5 al conectarse a IBM DB2 Database for Linux, UNIX y Windows 10.5. • Controladores JDBC de Oracle 12c al conectarse a Oracle 12c. • Controladores JDBC de Oracle 11g al conectarse a Oracle 11g.
Navegadores Web	• Windows Internet Explorer 10 y posteriores • Mozilla Firefox
Software de Message Queuing soportado	• IBM WebSphere MQ

Definición de la arquitectura del sistema

Debe planificar las configuraciones de base de datos y de servidor de la instalación del producto.

Configuración de la base de datos del producto

Las instalaciones de IBM InfoSphere Identity Insight pueden contener hasta tres bases de datos separadas para las configuraciones del producto y el almacenamiento de datos de entidad.

Las bases de datos son:

Base de datos de entidad
La base de datos almacena identidades, entidades y datos que se utilizan para relaciones, resoluciones y alertas.

Base de datos de consola de configuración
La base de datos que almacena los recursos para la consola de configuración

Base de datos del supervisor de aplicaciones
La base de datos que almacena la información de direccionamiento y de supervisión de las interconexiones.

Las instalaciones nuevas pueden unificar las bases de datos, en función de qué características se hayan instalado, en una única base de datos. La opción de

unificar las bases de datos está ubicada en cada pantalla de configuración de base de datos del programa de instalación. La base de datos única es la configuración preferida.

Despliegues de interconexiones

Las interconexiones se pueden instalar en un único servidor o en múltiples servidores, en función de los requisitos del sistema y de los recursos del servidor.

Al desplegar interconexiones, tenga en cuenta los siguientes factores de rendimiento:

- Las interconexiones se pueden ejecutar en un único formulario o se puede configurar para ejecutar hebras de proceso paralelo concurrentes.
- Cada CPU puede manejar de 1,5 hasta 2 interconexiones o hebras de interconexión de proceso paralelo.
- Las interconexiones de proceso paralelo pueden recibir datos desde varios orígenes de datos a la vez, de modo que no es necesario partir los archivos manualmente para igualar el número de interconexiones únicas.

Al desplegar interconexiones, tenga también en cuenta los siguientes factores:

- las interconexiones se pueden ejecutar en cualquier hardware y configuración de sistema operativo soportado.
- aunque es posible, no ejecute las interconexiones en la máquina en la que se encuentra la base de datos.
- las interconexiones de proceso paralelo cuestan menos de configurar que las interconexiones múltiples.
- las configuraciones de servidor múltiples requieren dedicar más tiempo de trabajo y mantenimiento.
- las configuraciones de servidor único requieren un valioso hardware que incrementa exponencialmente con el número de CPU.

Creación de un usuario protegido para instalaciones que no son de Windows

Para todas las plataformas que no sean Windows, cree un usuario protegido para ejecutar el programa de instalación del producto.

Acerca de esta tarea

No ejecute el programa de instalación del producto como un usuario ROOT.

Roles y responsabilidades de usuarios

Los roles de usuarios ayudan a clasificar las tareas típicas que se deben completar para desplegar de forma eficiente y utilizar IBM InfoSphere Identity Insight. Muchos tipos diferentes de usuarios pueden utilizar IBM InfoSphere Identity Insight para varias finalidades; es decir, los usuarios adoptan las responsabilidades de uno o varios roles utilizando el producto.

Puede definir grupos de usuarios basándose en los diversos roles y responsabilidades de usuarios.

Los roles de usuario más comunes incluyen:

Analista

Analiza los datos y revisa entidades, relaciones y alertas. El analista define qué resultados son los más valiosos y se asegura de que el sistema devuelva dichos resultados. El analista trabaja junto con el operador y con el administrador de aplicaciones.

Operador

Carga datos en el sistema, ejecuta las interconexiones y verifica que el sistema se está ejecutando de forma aceptable, ofreciendo informes sobre la calidad de la carga según sea necesario. El operador también revisa los resultados, las excepciones y los sucesos. El operador trabaja junto con el analista, el administrador del origen de datos y el administrador de aplicaciones.

Administrador de fuente de datos

Prepara los datos para cargarlos en el sistema, lo que incluye convertir los datos en UMF y validar el archivo. El administrador de fuente de datos trabaja junto con los operadores, los administradores de aplicaciones y los administradores de bases de datos.

Administrador de aplicaciones

Configura la aplicación, incluida la configuración de los datos, del modelo de entidades y de las normas. El administrador de aplicaciones trabaja junto con los administradores de fuentes de datos y los operadores para definir el modelo de entidad y coordina los cambios en la configuración con el administrador de bases de datos, el administrador de fuentes de datos y los operadores. El administrador de aplicaciones también coordina y consulta con los administradores del sistema global, si existen.

Administrador de la base de datos

Asegura que la base de datos esté configurada y ajustada correctamente para su uso con la aplicación. El administrador de la base de datos trabaja junto con el operador, el administrador del origen de datos y el administrador de aplicaciones.

Arquitecto del sistema

Calcula y estima los requisitos de hardware y de software como paso de la planificación del despliegue de la aplicación. El arquitecto del sistema trabaja junto con el instalador, el administrador de la base de datos, el administrador del origen de datos y el administrador de aplicaciones para asegurar que el despliegue consigue la visión, las estrategias y los objetivos y se integra en los procesos empresariales, a la vez que ofrece los resultados esperados.

Instalador

Gestiona la instalación y la configuración inicial de la aplicación. El instalador configura los usuarios iniciales en el sistema. Generalmente los servicios profesionales de IBM suelen trabajar con el arquitecto del sistema para completar estas responsabilidades.

Programador

Diseña y desarrolla interfaces gráficas de usuario o personaliza interfaces gráficas correspondientes a varias funciones, de modo que el despliegue de la aplicación se integre en el entorno. El programador trabaja junto con el arquitecto del sistema y con el administrador de aplicaciones, a fin de distribuir alertas a las personas adecuadas de la forma más eficiente para el entorno.

Arquitecto de seguridad

Asegura que el equipo del proyecto implemente un sistema seguro. El

arquitecto de seguridad trabaja junto con el arquitecto del sistema, el instalador y el administrador de la base de datos.

Capítulo 3. Configuración de bases de datos

Antes de instalar el producto, debe configurar las bases de datos necesarias.

Cómo establecer variables de entorno

Para bases de datos DB2 u Oracle, debe establecer variables de entorno.

Variables de entorno de DB2

Establezca todas las siguientes variables de entorno necesarias para el sistema operativo de la máquina destino

Variables de entorno de AIX

Nota: Debe asegurarse de que estos valores de variable de entorno se agregan al principio de las entradas existentes de las mismas variables de entorno.

Todas las variables de entorno deben estar en mayúsculas.

Tabla 20. Variables de entorno de AIX para bases de datos DB2

Variable de entorno	Valor	Condiciones
DB2DIR	Vía de acceso de instalación de software de DB2	donde *DB2DIR* es la ubicación donde se ha instalado el software de servidor/cliente de DB2.
DB2INSTANCE	Nombre de instancia de base de datos DB2	donde *DB2INSTANCE* es el nombre de la instancia de la base de datos DB2 que ha creado.
LIBPATH	`$`*`DB2DIR`*`/lib64:` *`DIRECTORIOINSTAL`*`/lib`	donde *DB2DIR* es la ubicación en la que se ha instalado el software de servidor/cliente de DB2 e *INSTALLDIRECTORY* es la ubicación donde se instalará el producto.

Variables de entorno de Linux

Tabla 21. Variables de entorno de Linux para bases de datos DB2

Variable de entorno	Valor	Condiciones
DB2DIR	Vía de acceso de instalación de software de DB2	donde *DB2DIR* es la ubicación donde se ha instalado el software de servidor/cliente de DB2.
DB2INSTANCE	Nombre de instancia de base de datos DB2	donde *DB2INSTANCE* es el nombre de la instancia de la base de datos DB2 que ha creado.

Tabla 21. Variables de entorno de Linux para bases de datos DB2 (continuación)

Variable de entorno	Valor	Condiciones
LD_LIBRARY_PATH	$*DB2DIR*/lib64: *DIRECTORIOINSTAL*/lib	donde *DB2DIR* es la ubicación en la que se ha instalado el software de servidor/cliente de DB2 e *INSTALLDIRECTORY* es la ubicación donde se instalará el producto.

Variables de entorno de Microsoft Windows

Debe utilizar el convenido de denominación de Microsoft Windows 8.3 al configurar las variables de entorno en un entorno Microsoft Windows. Las variables de entorno no deben contener ningún espacio.

Tabla 22. Variables de entorno de Microsoft Windows para bases de datos DB2

Variable de entorno	Valor	Condiciones
DB2DIR	Vía de acceso de instalación de software de DB2	donde *DB2DIR* es la ubicación donde se ha creado la instancia de DB2. Algunas versiones de DB2 se han establecido en su lugar en *DB2_HOME* o *DB2PATH*. El instalador las buscará si no se encuentra *DB2DIR*.
DB2INSTANCE	Nombre de instancia de base de datos DB2	donde *DB2INSTANCE* es el nombre de la instancia de la base de datos DB2 que ha creado.
DB2CODEPAGE	Establézcalo igual al valor CODEPAGE de la base de datos de DB2.	Una discrepancia puede producir problemas de codificación para los datos Latin-1/UTF-8 en la carga de datos.

Variables de entorno de Oracle

Establezca todas las siguientes variables de entorno necesarias para el sistema operativo de la máquina destino

Nota: Debe asegurarse de que estos valores de variable de entorno se agregan al principio de las entradas existentes de las mismas variables de entorno.

Todas las variables de entorno deben estar en mayúsculas.

Variables de entorno de AIX

Tabla 23. Variables de entorno de AIX para bases de datos Oracle

Variable de entorno	Valor	Condiciones
ORACLE_HOME	Directorio de instalación de software del cliente de Oracle	donde *ORACLE_HOME* es la ubicación donde se ha instalado el software del cliente de Oracle.

Tabla 23. Variables de entorno de AIX para bases de datos Oracle (continuación)

Variable de entorno	Valor	Condiciones
LIBPATH	$*ORACLE_HOME*/lib:<*directorio de instalación de producto*>/lib	donde *ORACLE_HOME* es el directorio de instalación de software de cliente de Oracle y donde <*directorio_instalación_producto*> es la ubicación donde se instalará el producto.

Variables de entorno de 64 bits de Linux

Tabla 24. Variables de entorno de 64 bits de Linux para bases de datosOracle

Variable de entorno	Valor	Condiciones
ORACLE_HOME	Directorio de instalación de software del cliente de Oracle	donde *ORACLE_HOME* es la ubicación donde se ha instalado el software del cliente de Oracle.
LD_LIBRARY_PATH	$*ORACLE_HOME*/lib:<*directorio de instalación de producto*>/lib	donde *ORACLE_HOME* es el directorio de instalación de software de cliente de Oracle y donde <*directorio_instalación_producto*> es la ubicación donde se instalará el producto.

Variables de entorno de Microsoft Windows

Debe utilizar el convenido de denominación de Microsoft Windows 8.3 al configurar las variables de entorno en un entorno Microsoft Windows. Las variables de entorno no deben contener ningún espacio.

Tabla 25. Variables de entorno de Microsoft Windows para bases de datos Oracle

Variable de entorno	Valor	Condiciones
ORACLE_HOME	Directorio de instalación de software del cliente de Oracle	donde *ORACLE_HOME* es la ubicación donde se ha instalado el software del cliente de Oracle.

Variables de entorno de Microsoft SQL Server

Establezca todas las siguientes variables de entorno necesarias para el sistema operativo de la máquina destino

Variables de entorno de Microsoft Windows

Debe utilizar el convenido de denominación de Microsoft Windows 8.3 al configurar las variables de entorno en un entorno Microsoft Windows. Las variables de entorno no deben contener ningún espacio.

Tabla 26. Variables de entorno de Microsoft Windows para bases de datos de Microsoft SQL Server

Variable de entorno	Valor	Condiciones
MSSQL_JDBC	Ubicación del controlador JDBC de Microsoft.	donde *MSSQL_JDBC* es la ubicación en la que se encuentran el controlador JDBC de Microsoft y los archivos `.jar` del servidor. El instalador del producto adoptará esta vía de acceso.

Definición de valores de DSN de ODBC para Microsoft SQL Server

El DSN (data source name) de ODBC de Microsoft SQL Server debe estar establecido en el valor exacto del nombre de la base de datos de Microsoft SQL Server.

Acerca de esta tarea

El tipo de conexión de DSN debe configurarse en función del mecanismo de autenticación para el que esté configurado Microsoft SQL Server (autenticación de usuario de SO o de SQL Server).

Habilitación de transacciones XA para Microsoft SQL Server

Debe habilitar las transacciones XA para que la consola de configuración y el visualizador se ejecuten correctamente.

Procedimiento

1. Habilite las transacciones XA mediante la herramienta de administración de Servicios de componentes en Windows.
2. Ejecute el servicio coordinador de transacciones distribuidas mediante el escritorio de Microsoft SQL Server.
3. Instale los procedimientos almacenados de JTA (Java Transaction API) según se explica en la documentación adecuada de Microsoft SQL Server.
4. Establezca los permisos para que los usuarios puedan ejecutar los procedimientos almacenados JTA mediante Microsoft SQL Server Enterprise Manager.

Cómo otorgar privilegios CREATE VIEW a los usuarios de Oracle

Para que el producto se ejecute correctamente, es necesario otorgar a los usuarios de la base de datos de Oracle privilegios CREATE VIEW.

Acerca de esta tarea

Los privilegios CREATE VIEW se deben asignar al usuario directamente y no deben basarse en roles.

Creación y configuración de bases de datos

Cree una base de datos única, conocida como base de datos de entidades para todos los componentes que utiliza el producto.

Creación de una base de datos de entidades

Debe crear una base de datos para la interconexión para almacenar identidades, entidades, relaciones y alertas, así como información de configuración de la consola de configuración e información de supervisión de la aplicación.

Acerca de esta tarea

Consulte la documentación sobre la base de datos para ver como se crean bases de datos nuevas.

Utilice letras en MAYÚSCULAS para nombres de base de datos.

Configuración de la autenticación de cliente

La autenticación de cliente permite que los usuarios se conecten a la base de datos de entidades sin proporcionar credenciales de contraseña o nombre de usuario adicionales en el archivo `.ini` de la interconexión.

Acerca de esta tarea

La autenticación de cliente también se denomina autenticación de base de datos de SO de confianza. La autenticación de cliente permite que se establezca la conexión utilizando el nombre de usuario con el que se ha iniciado la sesión. Este esquema de autenticación confía en que el sistema operativo haya autenticado correctamente al usuario. Se puede utilizar la autenticación de cliente en plataformas de base de datos DB2 y Oracle. Las interconexiones y los procesos de IBM WebSphere debe ejecutarlos el usuario de sistema operativo que puede acceder a la base de datos de entidades en modalidad fiable. Si varios usuarios deben ejecutar estos procesos, póngase en contacto con el soporte de IBM para obtener más detalles.

Configuración de la autenticación de cliente para bases de datos DB2

Configure DB2 para utilizar la autenticación de cliente.

Procedimiento

1. Configure las opciones de configuración de servidor de base de datos global siguientes:
   a. Establezca **`authentication`** en el valor `client`.
   b. Establezca **`trust_allclnts`** en el valor `yes`.
   c. Establezca **`trust-clntauth`** en el valor `server`.
2. Catalogue las bases de datos del producto utilizando el parámetro **`authentication client`** del mandato **`db2 catalog database`**.
3. Sincronice los nombres de usuario de base de datos del sistema operativo y de DB2.
4. Asegúrese de que tiene el controlador de tipo 2 JDBC DB2 además del controlador de tipo 4 JDBC DB2 estándar. Debería estar en el archivo `db2java.zip`.
5. Habilite la autenticación de confianza al instalar el producto.

Configuración de la autenticación de cliente para bases de datos Oracle

Configure Oracle para utilizar la autenticación de cliente.

Procedimiento

1. Configure las opciones de configuración de servidor de base de datos global siguientes:
   a. Establezca **os_authent_prefix** en el valor OPS$.
   b. Establezca **remote_os_authent** en el valor TRUE.
2. Cree usuarios de bases de datos Oracle para que un usuario pueda utilizar métodos de autenticación de bases de datos y externos. Ejemplo de sintaxis:

```
CREATE USER OPS$<usuario> IDENTIFIED BY <contraseña_base_de_datos> DEFAULT
TABLESPACE <espacio_de_tabla> TEMPORARY TABLESPACE <espacio_de_tabla-temp>
QUOTA UNLIMITED ON <espacio_de_tabla>;
GRANT CONNECT, RESOURCE TO OPS$<usuario>;
```

3. Asegúrese de que tiene el controlador de tipo 2 JDBC Oracle además del controlador de tipo 4 JDBC Oracle estándar. Para Oracle debe estar contenido en el archivo ojdbc16.zip
4. Habilite la autenticación de confianza al instalar el producto. Proporcione un nombre de usuario con el prefijo OPS$ cuando se le soliciten las credenciales de base de datos en el instalador del producto.

Configuración de la autenticación de cliente para bases de datos Microsoft SQL Server

Configure Microsoft SQL Server para utilizar la autenticación de cliente.

Procedimiento

1. Asegúrese de que el DSN de sistema utiliza la autenticación de Windows NT y no la autenticación de SQL Server. O cree un nuevo DSN de sistema utilizando la autenticación de Windows NT.
2. Asegúrese de que el administrador de base de datos exista en Enterprise Manager de Microsoft SQL Server. Debería garantizarse que el usuario pueda acceder como mínimo a las bases de datospublic y db_owner de cada base de datos del producto. Establezca la base de datos predeterminada para la predeterminado de la entidad.
3. Asegúrese de que tiene el controlador JDBC Bridge ODBC de tipo 1.
4. Cree un usuario de base de datos (no de sistema operativo) que tenga acceso a la base de datos de entidades.
5. Habilite la autenticación de confianza al instalar el producto. Utilice el usuario de base de datos (no el de sistema operativo) cuando se le soliciten las credenciales de base de datos en el instalador del producto.

Cómo dar tamaño a la antememoria de sentencias de Oracle

Los administradores de base de datos de Oracle deben dar un tamaño adecuado a su antememoria de sentencia.

Acerca de esta tarea

El producto puede generar muchas sentencias, lo cual significa que la antememoria de sentencia de Oracle puede crecer con mucha rapidez y superar los valores de base de datos de Oracle predeterminados. Para obtener más información sobre el ajuste y tamaño de estos parámetros, consulte la documentación de Oracle.

Procedimiento

Configure los parámetros siguientes a nivel de servidor utilizando el mandato **ALTER SYSTEM SET** de Oracle:

SESSION_CACHED_CURSORS
El valor recomendado para este parámetro es de unos 20 cursores simultáneos por interconexión o hebra de interconexión de proceso paralelo.

OPEN_CURSORS
El valor recomendado para este parámetro es de unos 20 cursores simultáneos por interconexión o hebra de interconexión de proceso paralelo.

CURSOR_SHARING
Este parámetro afecta en gran medida al rendimiento. Configure este parámetro teniendo en cuenta el hecho de que el producto utiliza gran cantidad de variables de vinculación y que la aplicación se beneficiará de la compartición de cursores

Capítulo 4. Administración

La administración de tareas incluye la configuración y el mantenimiento de valores de sistema para las interfaces de usuario y la actualización de valores de configuración globales. Los administradores utilizan la Consola de configuración para realizar las tareas administrativas.

Administración de la consola

Para utilizar la Consola de forma eficaz debe configurar los navegadores, configurar las cuentas para los usuarios adecuados y gestionar el acceso a la Consola.

Consola de configuración

La Consola de configuración proporciona una interfaz orientada a tareas para ayudarle a realizar más fácilmente algunas de las tareas más esenciales para activarse y ejecutar con Identity Insight.

La Consola de configuración se aloja en IBM WebSphere Liberty.

Gestión de la configuración del sistema

La Consola de configuración se utiliza para configurar la mayoría de los parámetros del sistema y opciones en un conjunto de interfaces racionalizadas simplificadas. Entonces la consola graba los cambios en la base de datos de configuración. Los cambios realizados directamente en la base de datos de configuración no se soportan; lo más probable es que estos cambios hagan que el producto no funcione correctamente

Roles y responsabilidades de usuarios

Los roles de usuarios ayudan a clasificar las tareas típicas que se deben completar para desplegar de forma eficiente y utilizar IBM InfoSphere Identity Insight. Muchos tipos diferentes de usuarios pueden utilizar IBM InfoSphere Identity Insight para varias finalidades; es decir, los usuarios adoptan las responsabilidades de uno o varios roles utilizando el producto.

Puede definir grupos de usuarios basándose en los diversos roles y responsabilidades de usuarios.

Los roles de usuario más comunes incluyen:

Analista
Analiza los datos y revisa entidades, relaciones y alertas. El analista define qué resultados son los más valiosos y se asegura de que el sistema devuelva dichos resultados. El analista trabaja junto con el operador y con el administrador de aplicaciones.

Operador
Carga datos en el sistema, ejecuta las interconexiones y verifica que el sistema se está ejecutando de forma aceptable, ofreciendo informes sobre la calidad de la carga según sea necesario. El operador también revisa los

resultados, las excepciones y los sucesos. El operador trabaja junto con el analista, el administrador del origen de datos y el administrador de aplicaciones.

Administrador de fuente de datos
Prepara los datos para cargarlos en el sistema, lo que incluye convertir los datos en UMF y validar el archivo. El administrador de fuente de datos trabaja junto con los operadores, los administradores de aplicaciones y los administradores de bases de datos.

Administrador de aplicaciones
Configura la aplicación, incluida la configuración de los datos, del modelo de entidades y de las normas. El administrador de aplicaciones trabaja junto con los administradores de fuentes de datos y los operadores para definir el modelo de entidad y coordina los cambios en la configuración con el administrador de bases de datos, el administrador de fuentes de datos y los operadores. El administrador de aplicaciones también coordina y consulta con los administradores del sistema global, si existen.

Administrador de la base de datos
Asegura que la base de datos esté configurada y ajustada correctamente para su uso con la aplicación. El administrador de la base de datos trabaja junto con el operador, el administrador del origen de datos y el administrador de aplicaciones.

Arquitecto del sistema
Calcula y estima los requisitos de hardware y de software como paso de la planificación del despliegue de la aplicación. El arquitecto del sistema trabaja junto con el instalador, el administrador de la base de datos, el administrador del origen de datos y el administrador de aplicaciones para asegurar que el despliegue consigue la visión, las estrategias y los objetivos y se integra en los procesos empresariales, a la vez que ofrece los resultados esperados.

Instalador
Gestiona la instalación y la configuración inicial de la aplicación. El instalador configura los usuarios iniciales en el sistema. Generalmente los servicios profesionales de IBM suelen trabajar con el arquitecto del sistema para completar estas responsabilidades.

Programador
Diseña y desarrolla interfaces gráficas de usuario o personaliza interfaces gráficas correspondientes a varias funciones, de modo que el despliegue de la aplicación se integre en el entorno. El programador trabaja junto con el arquitecto del sistema y con el administrador de aplicaciones, a fin de distribuir alertas a las personas adecuadas de la forma más eficiente para el entorno.

Arquitecto de seguridad
Asegura que el equipo del proyecto implemente un sistema seguro. El arquitecto de seguridad trabaja junto con el arquitecto del sistema, el instalador y el administrador de la base de datos.

Valores óptimos del navegador para utilizar la Consola de configuración

La Consola de configuración es una aplicación basada en la web que necesita valores específicos para el navegador que se utiliza para acceder a ella.

Utilice los valores de navegador siguientes para visualizar mejor la Consola de configuración:

Tabla 27. Valores óptimos de navegador

Parámetro	Valor	Descripción
Resolución	800 x 600 como mínimo; se recomienda 1024 x 768 o superior	
Tamaño de texto	Medio	
JavaScript	Activado	
Cookies	Activado	Como mínimo, se deben activar las cookies de sesión de origen.
Seguridad - Sitio web fiable	Dirección HTTP de la Consola de configuración	Asegúrese de que la dirección HTTP de la Consola de configuración se incluye en la lista de sitios web de Internet fiables.
Seguridad - Opciones de descarga	Habilitado	Asegúrese de que están habilitadas todas las opciones de descarga para sitios web de Internet fiables.
Bloqueadores de ventanas emergentes	Permita las ventanas emergentes de la dirección HTTP de la Consola de configuración	Asegúrese de que la dirección HTTP de la Consola de configuración está en la lista de sitios web que permiten ventanas emergentes.

Inicio de sesión en la Consola de configuración

El inicio de sesión en la Consola de configuración permite ver y cambiar los valores de configuración del sistema.

Antes de empezar

El administrador del sistema debe haber creado una cuenta de usuario para que la utilice para iniciar la sesión.

Procedimiento

1. Abra la Consola de configuración:
   a. Abra el navegador en el que desee ejecutar la Consola de configuración.
   b. Escriba el URL de la Consola de configuración utilizando esta sintaxis: `http://<nombre_servidor>/console/`.
   c. Pulse la tecla **Intro**.
2. En la ventana **Inicio de sesión**, escriba el nombre de usuario y la contraseña.
3. Opcional: Si se trata del administrador del sistema y necesita editar la configuración del sistema actual, seleccione la opción **Editar configuración**. Si edita la configuración del sistema actual, normalmente deberá detener todas las interconexiones para evitar que se procesen nuevos datos hasta que se hayan completado los cambios en la configuración.
4. Pulse el botón **Inicio de sesión**.

Qué hacer a continuación

Si el nombre de usuario y contraseña coinciden con los configurados para la Consola de configuración, ésta se abrirá. De lo contrario, se producirá un error y deberá volver a iniciar la sesión después de determinar el nombre de usuario y contraseña correctos.

Finalización de la sesión de la Consola de configuración

Puede finalizar la sesión actual de la Consola de configuración sin salir de la aplicación. Si no hay actividad durante 60 minutos, la Consola de configuración finaliza automáticamente la sesión del usuario actual.

Procedimiento

Pulse **Finalizar sesión** en la esquina superior derecha de cualquier ventana de la Consola de configuración.

Qué hacer a continuación

Ha finalizado la sesión de la Consola de configuración y deberá iniciar la sesión de nuevo para continuar utilizándola.

Cuentas de usuario para la Consola de configuración

Para iniciar una sesión en la Consola de configuración, el administrador del sistema crea y le otorga una cuenta de usuario. Las cuentas de usuario incluyen un nombre de usuario y una contraseña que el usuario puede cambiar.

No puede iniciar una sesión en varias veces con la misma cuenta de usuario. Si comparte una cuenta de usuario con otras personas, no puede iniciar una sesión en la Consola de configuración a la vez. Si intenta iniciar una sesión utilizando una cuenta de usuario que alguien está utilizando, su sesión terminará y la nueva sesión comenzará.

El administrador del sistema puede crear cuentas de usuario adicionales en cualquier momento. Además, el administrador del sistema puede reiniciar la Consola de configuración para forzar un tiempo de espera excedido.

Gestión del acceso a la Consola de configuración

Se debe dar acceso a cada usuario de la Consola de configuración y debe utilizar un nombre de usuario y contraseña para iniciar la sesión en ella. Puede gestionar los nombres de usuario y contraseñas utilizando el archivo específico de la aplicación proporcionado por la Consola de configuración. O bien, si los usuarios tienen cuentas de usuarios RDBMS que les permiten acceder a la base de datos de entidades, puede utilizar estas cuentas de usuario y las herramientas de administración de bases de datos para gestionar el acceso de los usuarios a la Consola de configuración. Estos nombres de usuario y contraseñas son independientes de los configurados para acceder al Visualizador y no son necesariamente los mismos que los nombres de usuario y contraseñas del Visualizador.

Gestión del acceso a la Consola de configuración utilizando la información de inicio de sesión de la base de datos

Puede gestionar el acceso a la Consola de configuración utilizando el mismo ID de usuario y contraseña que la base de datos de entidades.

Antes de empezar

Asegúrese de que nadie ha iniciado la sesión en la Consola de configuración, para evitar conflictos de configuración

Procedimiento

1. Inicie el programa de utilidad de configuración. Para ello vaya al directorio `<ubicación de instalación>/installer/util/` y escriba uno de los mandatos siguientes:
   a. Para Windows, escriba `eacfg.bat –i –l ../logs/`.
   b. Para Unix, escriba `eacfg –i –l ../logs/`.
2. En el panel de navegación, pulse **Valores de la Consola de configuración**.
3. Pulse el recuadro de selección **Modificar autenticación de la Consola de configuración**.
4. Pulse el botón de selección **Autenticación SQL**.
5. Pulse **Aceptar**.
6. Utilice las herramientas de administración de base de datos para especificar la información de inicio de sesión de la Consola de configuración (y base de datos de entidades).

Gestión del acceso a la Consola de configuración utilizando el programa de utilidad del gestor de contraseñas

Puede gestionar el acceso a la Consola de configuración utilizando el programa de utilidad del gestor de contraseñas.

Antes de empezar

Asegúrese de que nadie ha iniciado la sesión en la Consola de configuración

Procedimiento

1. Inicie el programa de utilidad de configuración. Para ello vaya al directorio `<ubicación de instalación>/installer/util/` y escriba uno de los mandatos siguientes:
   a. Para Windows, escriba `eacfg.bat –i –l ../logs/`.
   b. Para Unix, escriba `eacfg –i –l ../logs/`.
2. En el panel de navegación, pulse **Valores de la Consola de configuración**.
3. Pulse el recuadro de selección **Modificar autenticación de la Consola de configuración**.
4. Pulse el botón de selección **Autenticación de archivo**.
5. Pulse **Aceptar**.

Resultados

Ahora puede utilizar el programa de utilidad del gestor de contraseñas (pwdmgr.jar) ubicado en el directorio srd-home/console, para añadir o suprimir usuarios o restablecer contraseñas de usuarios en el archivo console_password.properities.

Visualización de una lista de usuarios y sus estados:

Puede ver una lista de usuarios y sus estados utilizando el mandato del gestor de contraseñas.

Procedimiento

1. En una ventana de mandatos, vaya al directorio \srd-home\console.
2. Escriba el siguiente mandato. `pwdmgr console-passwords.properties console-principals.properties -l`

Ejemplo

Por ejemplo, si escribe el mandato `pwdmgr console-passwords.properties console-principals.properties -l`, es posible que se visualice la siguiente salida de ejemplo:

```
admin (super-user)
judy (super-user)
allen (super-user)
jose (super-user) *** NEVER LOGGED IN ***
```

Si acaba de restablecer una contraseña, se visualiza un mensaje que indica que el usuario todavía no ha iniciado la sesión en la Consola de configuración con la nueva contraseña.

Adición de un nuevo usuario:

Si gestiona el acceso a la Consola de configuración, en el archivo console-passwords.properties puede añadir un nuevo usuario utilizando el mandato de gestor de contraseñas.

Procedimiento

1. En una ventana de mandatos, vaya al directorio \srd-home\console.
2. Escriba el mandato siguiente, `pwdmgr console-passwords.properties console-principals.properties -a nombre_usuario` donde *nombre_usuario* es el nombre de usuario que desea añadir.

Qué hacer a continuación

Se añade un usuario con una contraseña predeterminada del nombre de usuario que ha especificado. Ahora, el nuevo usuario puede iniciar la sesión en la Consola de configuración.

Supresión de un usuario existente:

Si gestiona el acceso a la Consola de configuración, en el archivo console-passwords.properties puede suprimir un usuario existente utilizando el mandato de gestor de contraseñas.

Antes de empezar

Asegúrese de emitir el mandato desde el directorio `\srd-home\console\`. Asegúrese también de que existe el usuario que va a suprimir. Si se intenta suprimir un usuario que no existe, recibirá un mensaje de error.

Procedimiento

1. En una ventana de mandatos, vaya al directorio \srd-home\console.
2. Escriba el siguiente mandato, `pwdmgr console-passwords.properties console-principals.properties -d nombre_usuario` donde *nombre_usuario* es el nombre de usuario que desea suprimir.

Qué hacer a continuación

El nombre de usuario que acaba de suprimir ya no podrá iniciar la sesión en la Consola de configuración.

Cambio de una contraseña:

Cuando un usuario olvida la contraseña de la cuenta Consola de configuración o necesita cambiarla por razones de seguridad, el administrador del sistema puede restablecer la contraseña utilizando el mandato del gestor de contraseñas.

Antes de empezar

Asegúrese de emitir el mandato desde el directorio `\srd-home\console\`.

Procedimiento

1. En una ventana de mandatos, cambie los directorios al directorio `\srd-home\console` .
2. Escriba el mandato siguiente, `pwdmgr console-passwords.properties console-principals.properties -r nombre_usuario` donde *nombre_usuario* es el nombre de usuario que desea restablecer.

Qué hacer a continuación

La contraseña del nombre de usuario que ha especificado se ha restablecido para que coincida con el nombre de usuario. La próxima vez que los usuarios inicien sesión en la Consola de configuración después de haber restablecido la contraseña, el sistema les solicitará que restablezcan la contraseña. Por lo tanto, tras restablecer la contraseña de un usuario puede sugerir que inicie la sesión y cambie la contraseña en cuanto sea posible para minimizar cualquier problema o asunto de seguridad.

Mandato del gestor de contraseñas:

Utilice el mandato del gestor de contraseñas para gestionar el acceso a la Consola de configuración utilizando un archivo de propiedades. Puede añadir, suprimir y listar usuarios, así como restablecer sus contraseñas.

La sintaxis para el mandato del gestor de contraseñas es:

`pwdmgr -opción parámetro`

Para utilizar un mandato del gestor de contraseñas, emita el mandato desde el directorio `\srd-home\console\`.

Opciones y parámetros

Cada opción y parámetros para el mandato del gestor de contraseñas se debe especificar como un mandatos independiente. Si no especifica una opción, se visualizará la ayuda del mandato.

-a *nombre_usuario*
Añade un usuario cada vez.

El nombre que especifique para el usuario es el valor predeterminado para la contraseña inicial. Se solicita al usuario que cambie la contraseña cuando se inicia la sesión en la Consola de configuración por primera vez.

Si añade un usuario que ya existe, obtiene un mensaje de error.

-d *nombre_usuario*
Suprime un usuario cada vez.

Si intenta suprimir un usuario que no existe, obtiene un mensaje de error. Puede visualizar una lista de usuarios utilizando la opción de lista para asegurarse de que el usuario se ha suprimido satisfactoriamente.

-l
Visualiza una lista de todos los usuarios y su estado.

-r *nombre_usuario*
Restablece la contraseña para el usuario que especifica para el ID de usuario. Por ejemplo, judy/sunflower se restablecerá en judy/judy.

Se utilizan dos archivos con el mandato del gestor de contraseñas:

- console-passwords.properties - Este archivo registra todos los nombres de usuario y el resumen del mensaje de contraseñas.
- console-principals.properties - Este archivo está reservado para utilizarlo en un futuro al crear diferentes niveles de usuarios. Actualmente, todos los usuarios de la Consola de configuración se consideran superusuarios y tienen acceso a todas las áreas de la Consola de configuración.

Estos archivos están ubicados en el directorio srd-home. Sin embargo, no se deben cambiar manualmente. El producto los utiliza para hacer un seguimiento de los inicios de sesión de los usuarios y son parámetros necesarios en algún otro mandato.

Mandatos de ejemplo del gestor de contraseñas

Para añadir un nuevo usuario cuyo nombre de inicio de sesión y contraseña sean "judy", escriba el siguiente mandato `pwdmgr -a judy`

Para suprimir un usuario existente denominado judy y la contraseña correspondiente, escriba el siguiente mandato `pwdmgr -d judy`

Para ver una lista de usuarios actuales y su estado, escriba el siguiente mandato `pwdmgr -l`

Por ejemplo, si escribe el mandato `pwdmgr -l`, es posible que se visualice la siguiente salida de ejemplo:

```
admin (super-user)
judy (super-user)
allen (super-user)
jose (super-user) *** NEVER LOGGED IN ***
```

Si acaba de restablecer una contraseña, se visualiza un mensaje que indica que el usuario todavía no ha iniciado la sesión en la Consola de configuración con la nueva contraseña.

Para restablecer la contraseña de un usuario en el ID de usuario, escriba el mandato siguiente `pwdmgr -r` *nombre_usuario*

Por ejemplo, si escribe el mandato `pwdmgr -r judy`, la contraseña del usuario existente llamado judy se restablece en la contraseña predeterminada "judy". Si el inicio de sesión/contraseña original eran judy/sunflower, ahora se restablecen en judy/judy.

Temas de ayuda

Ventana Inicio de sesión de la Consola de configuración

Utilice esta ventana para iniciar sesión en la Consola de configuración.

ID de usuario
Especifique el ID de usuario de la Consola de configuración.

Contraseña
Especifique la contraseña de la Consola de configuración.

Editar configuración
Marque este recuadro de selección para utilizar la modalidad de edición.

Inicio de sesión
Pulse esta opción para enviar el ID de usuario y la contraseña a fin de obtener acceso a la Consola de configuración.

Borrar Pulse esta opción para suprimir las entradas ID de usuario y contraseña y deseleccionar el recuadro de selección Editar configuración.

Ejecución de informes desde la Consola de configuración

Desde la Consola de configuración, puede generar informes que muestren resúmenes de estadísticas de interconexiones por origen de datos o un informe que liste los valores de configuración de sistema actuales, incluida la configuración de resolución de entidades. Los informes resultantes se visualizan en el visor de informes BIRT (Business Intelligence Reporting Tool) basado en web. Asegúrese de desactivar los bloqueadores de ventanas emergentes, ya que pueden interferir con la visualización del informe en el visor.

Visualización de informes estadísticos

Al procesar los datos, el producto realiza el seguimiento de información estadística sobre el rendimiento y los datos para los archivos de origen de datos de entrada que se han cargado. Esta información se resume en dos informes: el Informe de resumen de origen de datos y el Informe de resumen de carga.

Acerca de esta tarea

Las estadísticas de estos informes pueden ayudarle a verificar rápidamente que el producto está procesando todos los registros de datos de entrada, tomar decisiones operativas acerca del rendimiento del producto, evaluar la calidad de los datos de entrada y mostrar el número de identidades nuevas, entidades nuevas, relaciones nuevas y alertas nuevas resultantes del proceso de los archivos de datos.

Procedimiento

1. En la Consola de configuración, seleccione **Estado** > **Informes**.
2. Necesario: En la lista **Informe**, elija un informe de estadísticas:
   - **Informe de resumen de origen de datos** - Este informe proporciona un resumen estadístico rápido por origen de datos de los registros cargados y procesados. Utilice esta opción para ver el número total de registros cargados por archivo de origen de datos, el número total de registros de identidades nuevas procesados por archivo de origen de datos y el número total de entidades nuevas basadas en este archivo de origen de datos. El Informe de origen de datos se clasifica por fecha de carga, ID de carga, origen de datos y archivo de origen de datos.

- **Informe de resumen de carga** - Este informe resume las estadísticas y las características de calidad para uno o más orígenes de datos. Utilice esta opción para ver la información de rendimiento de carga, la calidad del archivo de origen de datos y los resúmenes de los valores de datos utilizados para resolver entidades, detectar relaciones y generar alertas. Este informe le ayuda a determinar la calidad de los datos cargados desde un origen de datos concreto. Los datos de calidad inferior pueden indicar que los datos de este origen de datos necesitan limpieza adicional, ya sea antes de cargarse en el producto o durante la resolución de entidades aplicando reglas DQM (gestión de calidad de datos) específicas a los datos. El Informe de resumen de carga se clasifica por ID de carga.

3. En el campo **Desde fecha**, especifique la fecha de inicio para el informe utilizando el formato `mm/dd/aaaa`. De forma predeterminada, este campo contiene los datos actuales.

   Este campo puede dejarse en blanco, lo que significa que el producto informa de todos los datos de todos los demás criterios especificados a partir de la fecha en que el producto ha quedado operativo.
4. En el campo **Hasta fecha**, especifique la fecha final para el informe utilizando el formato `mm/dd/aaaa`. De forma predeterminada, este campo contiene los datos actuales.

   Este campo puede dejarse en blanco, lo que significa que el producto informa de todos los datos de todos los demás criterios especificados hasta la fecha actual.
5. Opcional: En **Código de origen de datos**, escriba el código de una origen de datos específica sobre la que desee informar. El código de origen de datos que especifique debe coincidir exactamente con un código de origen de datos configurado.

   Este campo puede dejarse en blanco, lo que significa que el producto informa de las estadísticas para todos los orígenes de datos en todos los demás criterios especificados.
6. Necesario: Pulse **Ejecutar informe** para generar el informe seleccionado.

Resultados

El producto genera el informe estadístico seleccionado basándose en todos los criterios especificados y visualiza el informe en una ventana de navegador web independiente, titulado **Visor de informes BIRT**. Si no hay datos para informar, basándose en los criterios que ha seleccionado, la ventana **Visor de informes BIRT** muestra el nombre del informe, la fecha y hora en que se ha generado el informe y **Página 1/1** en la parte superior. La sección de datos está en blanco.

Qué hacer a continuación

Utilice la información estadística sobre este informe para ayudar a ajustar los archivos de datos o producto.

Informe Resumen de origen de datos

El informe Resumen de origen de datos proporciona un resumen rápido de estadísticas por origen de datos de los registros cargados en el sistema para proceso. Desde este informe puede ver el número total de procesados por ID de carga. De estos registros totales cargados, el informe muestra el número de registros que representan nuevas identidades o nuevas entidades y calcula el porcentaje de registros que son nuevas identidades, así como el porcentaje de registros que son entidades recién creadas.

Estadísticas por carga dentro de orígenes de datos

Fecha de la carga
Muestra la fecha en que se ha cargado este archivo de origen de datos

ID de carga
Muestra el número de ID de carga asignado por el sistema.

Origen de datos
Muestra el código de origen de datos y descripción (separados mediante un guión) para el archivo de origen de datos que se ha cargado.

Registros UMF cargados
Indica el número total de registros de identidad en este archivo de origen de datos que se han cargado.

Nuevas identidades
Indica el número total de nuevas identidades descubiertas en el archivo de datos que se ha cargado. (Este número indica una identidad que el sistema no ha procesado antes.)

% de nueva identidad
Indica el porcentaje del total de registros cargados (Nuevas identidades dividido por Registros UMF cargados) que representan nuevas identidades.

Nuevas entidades
Indica el número total de nuevas entidades creadas desde esta carga de datos.

% Entidades nuevas
Indica el porcentaje del total de registros cargados (Nuevas entidades dividido por Cargados) que representan nuevas entidades.

Gráficas de estadísticas por origen de datos

Registros cargados por origen de datos
Muestra un diagrama de barras que muestra gráficamente cuántos registros de cada origen de datos se han cargado en el sistema, basándose en los demás criterios del informe especificados. Puede ver los orígenes de datos que han proporcionado más registros o menos registros y compararlo con los números de carga estimados.

- El eje vertical muestra los orígenes de datos por código de origen de datos.
- El eje horizontal muestra el número de registros cargados.

Si hay menos registros cargados para un origen de datos determinado que los esperados, puede inspeccionar los archivos de datos para este origen de datos. (También puede tomar en consideración la ejecución del Informe de resumen de carga para ver la calidad de los datos de los archivos cargados para este origen de datos; la calidad de los datos influye directamente en el número de registros cargados.)

Nuevas entidades por origen de datos
Muestra un diagrama de barras que muestra gráficamente los orígenes de datos que han dado lugar al mayor número de nuevas entidades, basándose en los demás criterios del informe especificados.

- El eje vertical muestra los orígenes de datos por código de origen de datos.
- El eje horizontal muestra el número de nuevas entidades creadas.

Informe Resumen de carga

El informe Resumen de carga resume las estadísticas y las características de calidad por origen de datos. Contiene información acerca de los archivos de origen de datos. Utilice este informe para determinar las estadísticas de carga de rendimiento, el número de entidades y alertas creadas por la carga, información general acerca de la calidad de los datos cargados, un resumen de las acciones sobre los registros UMF por carga, y cualquier excepción de UMF generada por carga. El informe se agrupa por ID de carga.

Para cada carga, el informe divide las estadísticas en secciones:

- Resumen de carga
- Resumen de alertas de rol
- Resumen de relaciones
- Resumen de calidad
- Resumen de documentos UMF
- Resumen de excepción

Resumen de carga

Utilice esta sección como ayuda para determinar cuánto se ha tardado en procesar un archivo en particular, así como para tener una idea general de la utilidad de este archivo de origen de datos en la resolución global de entidades y la detección de relaciones.

Fecha y hora de inicio
Indica la fecha y la hora en que se inició la carga de datos.

Fecha y hora de finalización
Indica la fecha y la hora en que finalizó la carga de archivos de origen de datos.

Recuento de registros UMF
Indica el número total de registros cargados desde este archivo de origen de datos dentro del rango de **Fecha y hora de inicio** y **Fecha y hora de finalización**.

El número de **Fecha y hora de finalización** menos el número de **Fecha y hora de inicio** es el número de minutos que ha tardado la carga de este archivo de origen de datos en particular, lo que puede dar una idea del rendimiento del sistema. También puede indicar que un archivo de origen de datos mayor se debe dividir entre archivos más pequeños para un proceso más rápido.

Nuevas identidades
Indica el número total de nuevas identidades cargadas dentro del rango de **Fecha y hora de inicio** y **Fecha y hora de finalización**.

% de nueva identidad
Indica el porcentaje del total de identidades de esta carga de datos que son nuevas identidades (identidades que son nuevas para la base de datos de entidades).

Nuevas entidades
Indica el número total de identidades recién creadas dentro del rango de **Fecha y hora de inicio** y **Fecha y hora de finalización**.

% Entidades nuevas
Indica el porcentaje del total de entidades que son entidades recién creadas como resultado de esta carga de origen de datos.

El número de nuevas identidades y nuevas entidades puede proporcionar una idea general del valor de este origen de datos en la resolución global de entidades y la detección de relaciones. Si estos números son bajos y siguen bajos durante un tiempo, puede que este origen de datos no sea útil para conseguir los objetivos de resolución de entidades de su empresa.

Resumen de alertas de rol

Utilice esta sección para ver las normas de resolución y las puntuaciones de resolución comunes para las relaciones detectadas que han dado lugar a alertas de rol. Cada fila representa el número de alertas de rol que se han generado, basándose en los criterios listados.

Regla de resolución
Muestra el nombre de la regla de resolución utilizada para evaluar la identidad y entidad durante la resolución de entidades y la detección de relaciones.

Descripción de alerta
Muestra el nombre de la regla de alerta de rol que ha desencadenado la alerta de rol.

Gravedad
Muestra un indicador definido por el usuario para medir la prioridad o importancia de esta alerta de rol.

Puntuación de resolución
Muestra una puntuación de relación (0-100) para la regla de resolución dada a la identidad y entidad implicadas en la alerta de rol. Esta puntuación indica el grado de similitud entre la identidad y la entidad. Una puntuación de 100 significa que el registro de identidad se ha resuelto para la entidad.

Recuento de alertas
Indica el número total de alertas de rol generadas basándose en la descripción de regla de alerta de rol, la regla de resolución y la puntuación de resolución.

Resumen de relaciones

Utilice esta sección para ver los atributos comunes para las relaciones detectadas que no han generado una alerta de rol. Cada fila representa el número de relaciones que se han detectado, basándose en los criterios listados.

Regla de resolución
Muestra el nombre de la regla de resolución utilizada para evaluar los registros de identidad entrantes y las entidades existentes durante la resolución de entidades y la detección de relaciones.

Puntuación de resolución
Muestra una puntuación de relación (0-100) para la regla de resolución dada a la identidad y entidad durante la resolución de entidades. Esta puntuación indica el grado de similitud entre la identidad y la entidad. Una puntuación de 100 significa que el registro de identidad se ha resuelto para la entidad.

Puntuación de relación
Muestra una puntuación de relación (0-100) para la norma de resolución dada a la identidad y entidad durante la resolución de relaciones. Esta puntuación indica el grado de relación entre la identidad y la entidad.

Cuanto mayor sea la puntuación de relación, más próxima será la relación entre la identidad y la entidad, basándose en los atributos de coincidencia.

Recuento de relaciones
Indica el número total de relaciones que se detectan basándose en la regla de resolución, la puntuación de resolución y la puntuación de relación.

Resumen de calidad

Utilice la información de esta sección para evaluar la calidad de los datos de cada archivo de origen de datos. La sección indica la calidad por tipo de atributo de un segmento UMF y tipo de documento UMF. Mediante la revisión del resumen de calidad con el resumen de excepciones UMF, puede ver los archivos de origen de datos que tienen problemas de calidad o con un UMF mal formado que se deben arreglar. Normalmente, puede resolver estos temas a través de ETL o la configuración de DQM/origen de datos antes de procesar el archivo de origen de datos.

En algunos casos, esta sección puede indicar que un origen de datos tiene una calidad tan pobre que no le interesa utilizar este origen de datos para la resolución de entidades.

Tipo de documento
Muestra el nombre del tipo de documento UMF que contiene el tipo de datos listado en Tipo de datos. Normalmente, este valor es UMF_ENTITY.

Nombre de tabla
Muestra el nombre de la tabla de base de datos que almacena datos de segmentos UMF con nombres similares. Por ejemplo, los datos del segmento NUMBER se almacenan en la tabla NUMS.

Tipo de datos
Indica el tipo de datos, tal como se lista en los códigos UMF de tipo de atributo de los registros de entrada. Este tipo corresponde a un segmento UMF listado en Nombre de tabla. Por ejemplo, si el Nombre de tabla es *ADDRESS* y el Tipo de datos listado es *H*, la información de calidad evalúa el tipo de dirección de tipo *Domicilio*.

Si no reconoce un tipo de datos, puede indicar que el archivo de origen de datos no está correlacionado correctamente con la combinación adecuada de documentos, segmentos y códigos UMF. Compruebe la sección Resumen de excepción para ver si un segmento UMF y un código UMF coincidentes han causado una o varias excepciones de segmento. Si el problema es un UMF no válido, con frecuencia coinciden los números del Recuento de baja calidad de la sección Resumen de calidad con el Recuento de excepción de segmentos de la sección Excepción UMF.

Recuento de registros
Indica el número total de registros de identidad entrantes para el Tipo de documento, Nombre de tabla y Tipo de datos dados.

Recuento genérico
Indica el número total de registros de identidad entrantes con el Tipo de documento, Nombre de tabla y Tipo de datos dados que contienen valores considerados genéricos.

Recuento de baja calidad
Indica el número total de registros de identidad entrantes con el Tipo de documento, Nombre de tabla y Tipo de datos dados que están considerados como de baja calidad. Este número puede indicar un problema de entrada de datos o de transformación ETL en el archivo de origen de datos.

Porcentaje utilizable
Indica el porcentaje de registros de identidad entrantes con el Tipo de documento, Nombre de tabla (de este segmento UMF) y Tipo de datos dados que se pueden utilizar para la resolución de entidades y la detección de relaciones. (Recuento de registros menos Recuento genérico menos Recuento de baja calidad) dividido por el Recuento de registros es igual al Porcentaje utilizable.

Porcentaje de identidad
Indica el porcentaje de registros de identidad entrantes que contenían el Tipo de documento, Nombre de tabla y Tipo de datos dados.

Resumen de atributos

Utilice esta sección para ver los atributos del archivo de origen de datos que han ayudado a detectar relaciones y generar alertas de rol. Cada atributo se correlaciona con un segmento UMF específico, y esta sección muestra el número de relaciones detectadas y alertas de rol generadas, basadas en los datos del segmento UMF de entrada.

Nombre de segmento
Muestra el nombre del segmento UMF, que se correlaciona directamente con un atributo.

Tipo de datos
Lista el tipo de atributo (o tipo de datos) del segmento UMF correspondiente a la Descripción de precisión. El informe puede listar un tipo de atributo específico o listar *ALL*, que indica todos los tipos de atributo del segmento UMF.

Descripción de precisión
Describe el umbral de coincidencia entre un atributo de una identidad de entrada y un atributo de una entidad existente.

Alertas de rol
Indica el número total de alertas de rol generadas basándose en este segmento UMF, el tipo de datos y la descripción de precisión.

Relaciones
Indica el número total de relaciones detectadas basándose en este segmento UMF, el tipo de datos y la descripción de precisión.

Resumen de documentos UMF

Puede utilizar esta sección para validar el número total de registros de entrada en un archivo de origen de datos, basándose en la acción que se debe realizar en el registro. Puede conciliar estos números en el Recuento de registros de la sección Resumen de carga.

Tipo de documento
Muestra el nombre del tipo de documento UMF. Normalmente, este valor es UMF_ENTITY.

Acción

Indica el tipo de acción para el registro de identidad de entrada. He aquí una lista de las acciones utilizadas más comúnmente:

- *A* para añadir
- *C* para cambiar
- *D* para suprimir

Como parte del proceso ETL, normalmente los registros de identidad se codifican a través de UMF para indicar cómo se debe actuar en cada registro de entrada durante el proceso del sistema.

Recuento de registros UMF

Indica el número total de registros procesados para cada tipo de acción dentro del tipo de documento.

Porcentaje

Indica el porcentaje del total de registros cargados que el Recuento de registros representa. (La suma no debe exceder del 100%.)

Resumen de excepción

Utilice esta información como ayuda para señalar los registros de identidad incorrectos, como los que tienen un UMF incorrectamente formado. La excepción describe el problema, mientras que el nombre de tabla y elemento muestran el segmento y registros que son incorrectos. El recuento muestra cuántos registros del archivo contenían este UMF incorrecto.

Tipo de documento

Muestra el nombre del tipo de documento UMF. Normalmente, este valor es UMF_ENTITY.

Acción

Indica el tipo de acción para el registro de identidad de entrada:

- *A* para añadir
- *C* para cambiar
- *D* para suprimir

Como parte del proceso ETL, normalmente los registros de identidad se codifican a través de UMF para indicar cómo se debe actuar en cada registro de entrada durante el proceso del sistema.

Segmento

Muestra el nombre del segmento UMF donde se ha producido la excepción.

Código UMF

Muestra el valor del código UMF que ha causado la excepción UMF.

Excepción

Muestra el ID de mensaje u otro código de excepción para indicar el tipo de excepción UMF que se ha producido y dar información acerca de cómo resolver la excepción. Esta información también está disponible en la tabla UMF_EXCEPT.

Recuento de excepción de segmentos

Indica el número total de este tipo de excepción UMF.

Compruebe el Recuento de baja calidad en la sección Resumen de calidad para ver si se ha informado que un tipo de datos coincidente tiene baja calidad o no se puede utilizar. Si el problema es un UMF incorrecto, los

números del Recuento de baja calidad de la sección Resumen de calidad y el Recuento de excepción de segmentos en la sección Excepción UMF coinciden con frecuencia para el mismo segmento UMF y códigos UMF.

Ejecución del informe de configuración

El informe de configuración proporciona una vista unificada de todos los valores del sistema que se configuran utilizando la Consola de configuración. Vea este informe para ver los valores de configuración de sistema actuales antes de cambiar la configuración de producto actual, al resolver un problema de configuración o al comparar diferentes valores de configuración.

Procedimiento

1. En la Consola de configuración, pulse **Configuración** > **Informes**.
2. En **Informe**, seleccione **Informe de configuración**.
3. Pulse **Ejecutar informe**.

Resultados

El producto genera el informe estadístico seleccionado basándose en todos los criterios especificados y visualiza el informe en una ventana de navegador web independiente, titulado **Visor de informes BIRT**. Si no hay datos para informar, basándose en los criterios que ha seleccionado, la ventana **Visor de informes BIRT** muestra el nombre del informe, la fecha y hora en que se ha generado el informe y **Página 1/1** en la parte superior. La sección de datos está en blanco.

Informe de configuración

El informe de configuración proporciona una vista unificada de los valores del sistema que se configuran utilizando la Consola de configuración. Utilice este informe para ver o imprimir la configuración actual del sistema antes de cambiarla, cuando desee solucionar problemas de una configuración, o cuando deba comparar diferentes valores de configuración.

El informe lista los valores de configuración actuales por categoría:

Orígenes de datos
Consulte los valores de configuración para orígenes de datos, incluyendo el ID de origen de datos, el código de origen de datos, el código de rol asociado al origen de datos, la configuración de resolución de entidades asociada al origen de datos y el estado actual del código de origen de datos (activo o inactivo).

Para configurar los orígenes de datos, seleccione**Configurar** > **Orígenes** > **Orígenes de datos**.

Tipos de número
Consulte los valores de configuración para tipos de número, incluyendo el ID de tipo de número, el tipo de número, la longitud máxima y mínima para el tipo de número, cualquier máscara asociada para el tipo de número, información acerca de cómo se utiliza el tipo de número en la resolución de entidades y si el tipo de número está activo o inactivo.

Para configurar tipos de números, seleccione **Configurar** > **Orígenes** > **Números**.

Tipos de características
Consulte los valores de configuración para tipos de características, incluyendo el ID de tipo de característica, el nombre del tipo de

característica, el tipo de datos asociado para la característica (por ejemplo, carácter o fecha), la información acerca de cómo se utiliza el tipo de característica en la resolución de entidades y si el tipo de característica está activo o inactivo.

Para configurar tipos de características, seleccione **Configurar** > **Orígenes** > **Características**.

Plugin

Visualice valores de configuración para la personalización de atributos y puntuación, incluyendo ID de plugin, nombre, tipo, versión y nombre corto de biblioteca.

Para configurar plugins para la personalización de atributos y puntuación, seleccione **Configurar** > **General** > **Plugins**.

Tipos de suceso

Visualice valores de configuración para tipos de suceso, incluyendo la unidad de medida asociada con el valor del suceso. Los tipos de suceso forman parte del gestor de sucesos.

Para configurar tipos de suceso, seleccione **Configurar** > **Orígenes** > **Tipos de suceso**.

Normas de gestión de calidad de datos

Consulte la lista de normas de gestión de calidad de datos (normas DQM) y los parámetros asociados que están configurados para un código UMF específico dentro de un segmento UMF, incluyendo el segmento UMF y el nombre de código UMF que la norma DQM tiene asociados, el orden en que se utiliza la norma DQM en ese segmento y código UMF, los parámetros asociados para la norma DQM de ese segmento y código UMF, si la norma DQM corrige los datos de entrada para ese segmento y código UMF y si la norma DQM está habilitada actualmente en ese segmento y código UMF.

Para configurar un segmento UMF y un código UMF a fin de que utilicen las normas DQM, seleccione **Configurar** > **UMF** > **Normas DQM**.

Correlación de carga

Consulte la información de configuración para conocer la forma en que los datos UMF se correlacionan con las tablas y columnas de tabla correspondientes de la base de datos de entidades, incluyendo el nombre de segmento UMF, la vía de acceso de datos UMF, el nombre de la tabla de base de datos de entidades, el nombre y el tipo de campo de la tabla de base de datos de entidades, el tipo de datos para ese campo y si la correlación está habilitada.

Para correlacionar datos de un segmento UMF con una tabla de la base de datos de entidades, seleccione **Configurar** > **UMF** > **Correlación de datos**.

Normas de resolución de entidades

Consulte los valores de configuración para cada norma de resolución de entidades, incluyendo el ID de norma de resolución de entidades, el orden para la norma, las puntuaciones mínimas de resolución y relación para la norma y si la norma incorpora denegaciones.

Para configurar normas de resolución de entidades, seleccione**Configurar** > **Resolución** > **Normas de resolución**.

Confirmar/denegar resolución de entidad

Consulte los valores para las puntuaciones que contribuyen al proceso de confirmación y denegación de la resolución de entidades, incluyendo el ID

de resolución de entidades asociado y el ID de configuración, la prioridad de cada puntuación, la descripción y el nombre de atributo para cada puntuación y el valor numérico de la puntuación.

Para configurar valores para confirmaciones y denegaciones de resolución de entidades, seleccione **Configurar** > **Resolución** > **Confirmaciones y denegaciones**.

Características de resolución de entidades
Consulte los valores para los tipos de características que se han configurado con pesos de confirmación y denegación utilizados durante la resolución de entidades, incluyendo la prioridad, el peso de confirmación y el peso de denegación.

Para configurar los pesos de confirmación y denegación para tipos de características, seleccione **Configurar** > **Resolución** > **Características**.

Códigos de rol
Consulte la lista de códigos de roles configurados y sus valores asociados, incluyendo el ID de código de rol y la descripción, la clase de código de rol y el estado actual del código de rol (activo o inactivo).

Para configurar códigos de rol, seleccione**Configurar** > **Relaciones** > **Roles**.

Normas de alertas de rol
Consulte la lista de normas de alertas de rol y sus valores asociados, incluyendo el ID de alerta de rol y la descripción, la gravedad, el umbral mínimo de alerta y los ID de código de rol de los dos roles que desencadenan esta norma de alerta de rol.

Para configurar normas de alerta de rol, seleccione**Configurar** > **Relaciones** > **Normas de alertas de rol**.

Configuración del gestor de nombres
Visualice los valores configurados para la característica Gestor de nombres que amplía la precisión de nombres durante la resolución de entidades.

Para configurar los valores para el Gestor de nombres, seleccione **Configurar** > **Resolución** > **Configuración de coincidencia de gestor de nombres**.

Configuración de separación
Visualice los valores configurados para la característica Grados de separación de la interconexión que puede detectar relaciones con uno, dos o tres grados de separación.

Para configurar los valores para los grados de separación, seleccione**Configurar** > **Relaciones** > **Configuración de separación**.

Secuencias del sistema
Visualice los valores de configuración para los números de secuencia que indican cómo carga y procesa los datos el sistema. Los números de secuencia del sistema asisten al sistema en el rendimiento de carga de dos maneras. Primero, porque permiten que cada interconexión emita una consulta con un conjunto de números secuenciales y, a continuación, los conserva en la memoria caché hasta que se utilizan. Segundo, porque los números de secuencia evitan que las múltiples interconexiones que generan ID generados por el sistema utilicen el mismo número de ID para más de un registro.

Por ejemplo, cada vez que la interconexión crea una entidad nueva durante el proceso de resolución de entidades, el sistema genera un ID de entidad

exclusivo. Al utilizar secuencias del sistema, la interconexión sólo puede enviar una consulta para solicitar los 1000 siguientes números de ID de entidad disponibles. Por tanto, para las siguientes 1000 entidades recién creadas, la interconexión puede utilizar los números de ID de entidad disponibles almacenados en la memoria. El método alternativo (más lento) consiste en que cada interconexión envíe una consulta a la base de datos de entidades solicitando un nuevo ID de entidad para cada nueva entidad que se cree.

Para configurar secuencias de sistema, seleccione**Configurar** > **UMF** > **Secuencia de carga**

Umbrales genéricos
Consulte los valores de umbrales genéricos configurados por atributo, incluyendo el nombre de atributo, el tipo de atributo y el número de umbral que determina cuándo un valor específico para ese atributo se convierte en genérico.

Para configurar umbrales genéricos por tipo de atributo, seleccione**Configurar** > **UMF** > **Umbral genérico**.

Diccionario de tablas
Consulte los valores de diccionario por tabla de base de datos de entidad, incluyendo el nombre de tabla, la descripción y el tipo de tabla.

Para configurar el diccionario de tabla, seleccione**Configurar** > **UMF** > **Diccionario**.

Tablas de búsqueda
Consulte los valores para la lista de tablas que el sistema utiliza como tablas de búsqueda durante el proceso, incluyendo el nombre de tabla, el nombre de campo de clave, el nombre de campo de ID y si se debe cargar la tabla en la memoria durante el proceso.

Para configurar las tablas que el sistema utiliza como tablas de búsqueda, seleccione**Configurar** > **UMF** > **Buscar**.

Configuración de coincidencia
Consulte los valores para cada configuración de resolución configurada en el sistema, incluyendo el nombre e ID de configuración, tipo de coincidencia y nombre de segmento UMF.

Para configurar configuraciones de coincidencia, seleccione**Configurar** > **Resolución** > **Creador de candidatos**.

Tipos de documento
Consulte los valores para documentos de entrada UMF, incluyendo el tipo de documento, si se debe realizar la gestión de calidad de datos en este tipo de documento, si se deben cargar los datos procesados por este tipo de documento en la base de datos de resolución de entidades y el nivel de resolución de entidades que se debe realizar en este tipo de documento UMF de entrada.

Para configurar documentos de entrada UMF, seleccione **Configurar** > **UMF** > **Documentos de entrada**.

Formato de salida UMF
Consulte los valores de formato para el documento de salida UMF, incluyendo el ID de formato y el código, la dirección de ruta y si el valor de formato de salida está habilitado.

Para configurar formatos para documentos de salida UMF, seleccione**Configurar** > **UMF** > **Documentos de salida**.

Tipos de sucesos GEM
Visualice los valores de formato para sucesos del gestor de sucesos, incluyendo el ID de suceso, el tipo, la descripción, la categoría, la unidad de medida y la fecha y la hora creadas.

Para configurar tipos de suceso, seleccione **Configurar** > **Orígenes** > **Tipos de suceso**.

Parámetros del sistema
Consulte la lista de valores de parámetros del sistema por grupo de parámetros, incluyendo el valor y el valor predeterminado para el parámetro del sistema y el tipo de validación y valor para el parámetro

Para configurar parámetros del sistema, seleccione **Configurar** > **General** > **Parámetros del sistema**.

Códigos de actividad de aplicaciones
Consulte la lista de códigos de actividad configurados para el Visualizador por tipo de actividad (alerta de rol, alerta de atributo o alerta de suceso), incluyendo el código de actividad, estados válidos para el código de actividad y si el código de actividad está activo o inactivo.

Para configurar los códigos de actividad utilizados en el Visualizador, seleccione**Configurar** > **Visualizador** > **Códigos de actividad**.

Grupos de usuarios
Consulte los valores para los grupos de usuarios configurados para el Visualizador, incluyendo los nombres de usuarios de Visualizador asociados, la fecha y hora de creación para el grupo de usuarios, y si el grupo de usuarios está activo o inactivo.

Para configurar códigos de actividad en el Visualizador, seleccione**Configurar** > **Visualizador** > **Código**sy, a continuación, seleccione **ANALYZER_GROUP**.

Grupos de alertas de rol
Consulte los valores para los grupos de alertas de rol configurados, incluyendo el grupo de aplicaciones asignado, el ID de norma de alerta de rol asociado y la descripción, la fecha y hora de la creación para el grupo de alertas de rol y si el grupo de alertas de rol está activo o inactivo.

Para configurar grupos de alertas de rol utilizados en el Visualizador, seleccione**Configurar** > **Relaciones** > **Normas de alerta de rol** y, a continuación, el campo **Grupo de alertas**.

Usuarios
Consulte los valores para que los usuarios configurados inicien la sesión en el Visualizador, incluyendo los nombres de inicio de sesión de usuario, si se debe autenticar el usuario del Visualizador utilizando credenciales de la base de datos de entidad y si el usuario del Visualizador está activo o inactivo.

Para configurar los usuarios, seleccione **Configurar** > **Visualizador** > **Usuarios del Visualizador**.

Exportación de informes

El Visor de informes BIRT le ofrece la opción de exportar datos de informe de consola de configuración a otras aplicaciones, como Microsoft Excel, Microsoft PowerPoint, Microsoft Word o Adobe Acrobat. Puede exportar el informe entero o datos específicos desde un informe.

Exportación de informes de la Consola de configuración

Si desea exportar un informe entero (datos y formato) a otra aplicación, como por ejemplo Microsoft PowerPoint, o a otro formato, como por ejemplo PDF de Adobe Acrobat, utilice la opción **Exportar informes** en el Visor de informes BIRT. La exportación de informes completos funciona bien para informes que abarcan varias páginas y en casos donde no desea manipular los datos después de exportar el informe.

Acerca de esta tarea

La apertura de un informe de Consola de configuración exportado a un archivo *.doc de Microsoft Word necesita utilizar Microsoft Word versión 2003 o posteriores.

Si desea realizar pequeños cambios o adiciones en el informe exportado, exporte el informe a Microsoft Word o Microsoft Excel. Estas aplicaciones conservan el formato de informe, pero normalmente los datos se visualizan en columnas o tablas, permitiendo una manipulación de datos. Puesto que el informe exportado es un archivo de sólo lectura, guarde el archivo utilizando un nuevo nombre para guardar los cambios.

Procedimiento

1. Después de generar el informe, desde la ventana **Visor de informes BIRT**, pulse **Exportar informe**. El icono Exportar informe es el cuarto icono de la izquierda en la barra de herramientas de icono de Visor de informes BIRT.
2. En **Exportar informe**, seleccione el formato o la aplicación para exportar los datos:
   - **PDF**
   - **PowerPoint**
   - **Word**
   - **PostScript**
   - **Excel**
3. Seleccione las páginas o el rango de páginas a exportar.
4. Opcional: Seleccione el tamaño del informe resultante: Esta opción sólo está disponible si ha seleccionado la opción PDF, PowerPoint o PostScript.
   - **Automático**: Cada página del informe se convierte en una página independiente.
   - **Tamaño real**: Todas las páginas del informe se ajustan a una página larga.
   - **Ajustar a página completa**: Todas las páginas del informe se reducen para ajustarse a un tercio de una única página aproximadamente. Si ha seleccionado la opción PowerPoint, el informe se inserta como una imagen en la página, lo que le permite redimensionar la imagen.
5. Pulse **Aceptar**.

Resultados

Si ha exportado el informe a formato PDF o PostScript, el archivo resultante se coloca normalmente en la ubicación de carpeta donde se descargan los archivos en el cliente. Por ejemplo, C:\Documents and Settings\Administrator\My Documents\Downloads.

Si ha exportado a PowerPoint, Word o Excel, los datos se exportan a un archivo de sólo lectura que normalmente se denomina *nombre_informe.extensión_aplicación_seleccionada*.

- *nombre_informe* es el nombre del informe de Consola de configuración que ha exportado.
- *extensión_aplicación_seleccionada* es la extensión de formato de archivo adecuada para la aplicación seleccionada.

Por ejemplo, si ha exportado el informe de Resumen de carga a Word, el nombre de archivo suele denominarse LoadSummary.doc. Se visualiza un diálogo dándole la opción de abrir el archivo en la aplicación seleccionada o de guardar el archivo.

Exportación de datos de informes de la Consola de configuración

Si desea exportar datos de informes a un archivo CSV (archivo de valores separados por coma) para ver y manipular los datos en otra aplicación como Microsoft Excel, utilice la opción **Exportar datos** del visor de informes BIRT. Puede seleccionar una sección del informe, qué campos se deben exportar y el formato de datos de exportación.

Acerca de esta tarea

El Visor de informes BIRT exporta una sección de datos de un informe a la vez, lo que significa que el visor crea un conjunto de resultados independiente para cada sección en el informe. Los datos que se exportan son datos en bruto sin formato.

Si desea exportar el informe completo, utilice en su lugar la opción **Exportar informe**. Sin embargo, esa opción de exportación exporta los datos y el formato de informe, lo que le impide manipular los datos después de la exportación.

Procedimiento

1. Después de generar el informe, en el visor de informes BIRT, pulse el icono **Exportar datos**. El icono **Exportar datos** es el tercer icono de la izquierda en la barra de herramientas de icono del visor de informes BIRT.
2. Necesario: En **Conjuntos de resultados disponibles** en **Exportar datos**, seleccione la sección de un informe que desea exportar. Los nombres de las secciones de informe se visualizan por elemento, por ejemplo ELEMENT_2041. Normalmente puede indicar qué sección está seleccionando examinando los nombres de columna listados en **Columnas disponibles**.
3. Necesario: En **Columnas disponibles**, seleccione las columnas a exportar. Los nombres de columna que se aplican a la sección de informe que ha elegido en la pantalla **Conjuntos de resultados disponibles** se visualizan en **Columnas seleccionadas**. Es posible que no desee ver los datos de todas las columnas disponibles para esa sección de informe.
4. Opcional: Establezca el orden de las columnas en **Columnas seleccionadas**. Esta opción le permite reordenar los datos por columna antes de exportar los datos.

5. Opcional: En **Separador**, seleccione un separador, si desea utilizar un tipo de separador distinto de **Coma**, que es la opción predeterminada:
   - **Punto y coma**
   - **Dos puntos**
   - **Línea vertical**
   - **Tabulador**
6. Pulse **Aceptar**. En el diálogo que se visualiza, seleccione si se deben abrir los datos exportados o guardar el archivo. Microsoft Excel es la aplicación predeterminada para abrir el archivo, pero puede examinar para seleccionar cualquier aplicación que pueda exportar un archivo CSV.

Resultados

Los datos se exportan a un archivo normalmente denominado *nombre_informe*.csv, donde *nombre_informe* es el nombre del informe de la Consola de configuración desde la que ha exportado los datos.

Administración del Visualizador

Para utilizar el Visualizador eficientemente, debe configurar los navegadores, configurar las cuentas para los usuarios adecuados y gestionar el acceso al Visualizador.

Visualizador

El Visualizador es una interfaz gráfica de usuario que los analistas e investigadores utilizan para analizar los resultados de alertas, relaciones y resoluciones de entidades.

El Visualizador está alojado en una versión incorporada de IBM WebSphere Application Server. Puede configurar el Visualizador a través de la Consola de configuración y a través de la selección **Preferencias** del Visualizador en el menú **Archivo**.

Los usuarios del Visualizador pueden realizar diversas tareas de análisis:

Análisis y visualización de alertas
: Las alertas generadas por el proceso de resolución de entidades representan relaciones o resoluciones de entidades que interesan a una organización. Generalmente, los analistas revisan las alertas y deciden qué acción emprender, si deciden emprender alguna, basándose en la información de las alertas. Existen tres tipos de alertas: alertas de rol, alertas de atributo y alertas de suceso.

  El Visualizador muestra las alertas, ofreciendo a los analistas vistas textuales y gráficas de las alertas y las entidades que participan en las alertas. Los analistas pueden profundizar en los detalles y luego establecer el estado de disposición de la alerta correctamente.

Crear y gestionar generadores de alertas de atributo
: Con el Visualizador, los analistas pueden crear y gestionar búsquedas persistentes mediante la característica Generador de alertas de atributo, y gestionar cómo ven y reciben alertas de atributo. Los analistas pueden crear Generadores de alertas de atributo basándose en datos de atributos para localizar identidades que se han resuelto en entidades basadas en dichos datos de atributos. Los analistas también pueden crear un

Generador de alertas de atributo para buscar de manera persistente en la base de datos de entidades en busca de una entidad determinada.

Encontrar entidades
Los usuarios del Visualizador también pueden buscar entidades para un análisis más profundo mediante varios métodos:

- Por atributos
- Por cuenta de origen de datos
- Por ID de entidad
- Por resolución (cuánto se acercan los criterios especificados a las identidades y entidades de la base de datos de entidades, basándose en umbrales de puntuación de resolución mínima)

Adición de entidades y relaciones divulgadas
Los analistas pueden utilizar el Visualizador para añadir registros para la resolución de entidades y la detección de relaciones. Pueden añadir un solo registro de identidad o cargar un archivo UMF que contenga unos pocos miles de registros de identidades. Al igual que cuando se añaden registros de identidades a través de programas de adquisición, una interconexión procesa los registros añadidos a través del Visualizador para la resolución de entidades y la detección de relaciones. Los resultados del proceso se graban en la base de datos de entidades y las alertas, si se generan, se publican en el Visualizador.

Los analistas también pueden divulgar relaciones entre entidades (por identidad), cuando saben de la existencia de un enlace entre las identidades. Ejemplos de relaciones divulgadas serían relacionar entidades basadas en contactos de emergencia o referencias listadas en una solicitud de empleo. La entidad ha divulgado estas relaciones en la solicitud.

Generación e impresión de informes
El Visualizador también contiene varios informes que los analistas pueden ver e imprimir como ayuda para gestionar y hacer el seguimiento de su trabajo en el Visualizador.

Roles y responsabilidades de usuarios

Los roles de usuarios ayudan a clasificar las tareas típicas que se deben completar para desplegar de forma eficiente y utilizar IBM InfoSphere Identity Insight. Muchos tipos diferentes de usuarios pueden utilizar IBM InfoSphere Identity Insight para varias finalidades; es decir, los usuarios adoptan las responsabilidades de uno o varios roles utilizando el producto.

Puede definir grupos de usuarios basándose en los diversos roles y responsabilidades de usuarios.

Los roles de usuario más comunes incluyen:

Analista
Analiza los datos y revisa entidades, relaciones y alertas. El analista define qué resultados son los más valiosos y se asegura de que el sistema devuelva dichos resultados. El analista trabaja junto con el operador y con el administrador de aplicaciones.

Operador
Carga datos en el sistema, ejecuta las interconexiones y verifica que el sistema se está ejecutando de forma aceptable, ofreciendo informes sobre la calidad de la carga según sea necesario. El operador también revisa los

resultados, las excepciones y los sucesos. El operador trabaja junto con el analista, el administrador del origen de datos y el administrador de aplicaciones.

Administrador de fuente de datos
Prepara los datos para cargarlos en el sistema, lo que incluye convertir los datos en UMF y validar el archivo. El administrador de fuente de datos trabaja junto con los operadores, los administradores de aplicaciones y los administradores de bases de datos.

Administrador de aplicaciones
Configura la aplicación, incluida la configuración de los datos, del modelo de entidades y de las normas. El administrador de aplicaciones trabaja junto con los administradores de fuentes de datos y los operadores para definir el modelo de entidad y coordina los cambios en la configuración con el administrador de bases de datos, el administrador de fuentes de datos y los operadores. El administrador de aplicaciones también coordina y consulta con los administradores del sistema global, si existen.

Administrador de la base de datos
Asegura que la base de datos esté configurada y ajustada correctamente para su uso con la aplicación. El administrador de la base de datos trabaja junto con el operador, el administrador del origen de datos y el administrador de aplicaciones.

Arquitecto del sistema
Calcula y estima los requisitos de hardware y de software como paso de la planificación del despliegue de la aplicación. El arquitecto del sistema trabaja junto con el instalador, el administrador de la base de datos, el administrador del origen de datos y el administrador de aplicaciones para asegurar que el despliegue consigue la visión, las estrategias y los objetivos y se integra en los procesos empresariales, a la vez que ofrece los resultados esperados.

Instalador
Gestiona la instalación y la configuración inicial de la aplicación. El instalador configura los usuarios iniciales en el sistema. Generalmente los servicios profesionales de IBM suelen trabajar con el arquitecto del sistema para completar estas responsabilidades.

Programador
Diseña y desarrolla interfaces gráficas de usuario o personaliza interfaces gráficas correspondientes a varias funciones, de modo que el despliegue de la aplicación se integre en el entorno. El programador trabaja junto con el arquitecto del sistema y con el administrador de aplicaciones, a fin de distribuir alertas a las personas adecuadas de la forma más eficiente para el entorno.

Arquitecto de seguridad
Asegura que el equipo del proyecto implemente un sistema seguro. El arquitecto de seguridad trabaja junto con el arquitecto del sistema, el instalador y el administrador de la base de datos.

Valores óptimos del navegador para utilizar el Visualizador

El Visualizador es una aplicación basada en Java cuyo rendimiento es mejor cuando se utilizan valores específicos del navegador utilizado para acceder al Visualizador.

Para ver el Visualizador de la mejor manera, utilice los valores del navegador siguientes:

Tabla 28. Valores óptimos del navegador para el Visualizador

Parámetro	Valor	Descripción
Tamaño de texto	Medio	
JavaScript	Activado	
Cookies	Activado	Como mínimo, se deben activar las cookies de sesión de origen.
Seguridad - Sitio web fiable	Dirección HTTP del Visualizador	Asegúrese de que la dirección HTTP del Visualizador se incluye en la lista de sitios web de Internet fiables.
Seguridad - Opciones de descarga	Habilitado	Asegúrese de que están habilitadas todas las opciones de descarga para sitios web de Internet fiables.
Bloqueadores emergentes	Permita las ventanas emergentes de la dirección HTTP del Visualizador	Asegúrese de que la dirección HTTP del Visualizador esté en la lista de sitios web que permiten ventanas emergentes.

Inicio de sesión en el Visualizador

Antes de iniciar sesión en el visualizador, debe tener una cuenta de usuario del Visualizador (nombre de usuario y contraseña). El administrador del sistema puede proporcionarle información sobre la cuenta de usuario del Visualizador.

Procedimiento

1. Siga uno de los siguientes pasos:
   - Efectúe una doble pulsación en el icono del Visualizador en el escritorio.
   - O bien abra el navegador de Internet y especifique el localizador universal de recursos (URL) para el Visualizador en la línea de dirección.

   El URL para iniciar el Visualizador es:

   `http://servidor:puerto_instalación`

   Por ejemplo, `http://localhost:13510`. Cuando se ha instalado el Visualizador, el *puerto_instalación* predeterminado es 13510, pero el número de puerto puede cambiarse. Consulte al administrador del sistema si no está seguro del nombre de servidor o número de puerto correctos.
2. Inicie la sesión entrando su nombre de usuario y contraseña.

   Nota: Los campos de nombre de usuario y contraseña son sensibles a las mayúsculas y minúsculas. La primera vez que inicie la sesión, utilice la contraseña que le ha asignado el administrador del sistema. Tras el primer inicio de sesión, normalmente se cambia la contraseña del Visualizador para proteger la seguridad de la cuenta del Visualizador.
3. Pulse **Iniciar sesión**.

Cierre del Visualizador

Cuando haya terminado de utilizar el Visualizador, cierre la aplicación. Al cerrar el Visualizador, también cierra la sesión. Si se toma un descanso y desea asegurar la estación de trabajo durante unos minutos, puede bloquear el Visualizador.

Procedimiento

Para cerrar el Visualizador y cerrar la sesión:

- Seleccione **Archivo** > **Salir**.
- O bien pulse **Control** + **Q**.

Gestión del acceso al Visualizador

Los usuarios del Visualizador deben tener una cuenta registrada antes de poder iniciar la sesión en el Visualizador. Estas cuentas de usuario no son las mismas que las cuentas de usuario para la Consola de configuración sino que están autorizadas específicamente para el Visualizador.

Creación de nuevos usuarios del Visualizador

Para acceder y utilizar el Visualizador, un administrador del sistema debe crear una cuenta de usuario de Visualizador para el usuario de la Consola de configuración.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Visualizador**.
3. Pulse el separador **Usuarios del Visualizador**.
4. Pulse el botón **Nuevo**.
5. En la lista desplegable **Inicio de sesión de base de datos**, seleccione uno de los valores siguientes:
   - Seleccione **Sí** si el usuario tiene una cuenta de usuario que otorga acceso a la base de datos de entidades y desea utilizar esta información de inicio de sesión de base de datos.
   - Seleccione **No** si utiliza la información de inicio de sesión del archivo predeterminado. Esta elección significa que un administrador del sistema elige la primera contraseña que utiliza el usuario para iniciar sesión en el Visualizador y que un administrador del sistema puede restablecer las contraseñas de los usuarios del Visualizador bajo demanda.
6. En el campo **Nombre de usuario**, escriba el nombre de usuario que desea añadir. Si ha seleccionado **Sí** en la lista desplegable **Inicio de sesión de base de datos**, el nombre de usuario debe coincidir con el nombre para ese usuario de la base de datos de entidades.
7. En el campo **Contraseña**:
   a. Si ha seleccionado **Sí** en la lista desplegable **Inicio de sesión de base de datos**, este valor debe coincidir con la contraseña almacenada en la información de inicio de sesión de base de datos.
   b. Si ha seleccionado **No** en la lista desplegable **Inicio de sesión de base de datos**, escriba la contraseña inicial para el usuario.

      Nota: Por razones de seguridad, aconseje a los usuarios del Visualizador que cambien la contraseña inicial tras iniciar sesión satisfactoriamente la primera vez.

8. Opcional: En el campo **Grupo** de la lista desplegable, seleccione el grupo de analizadores al que pertenece esta persona.
9. Pulse el botón **Guardar**.

Qué hacer a continuación

Ahora el usuario puede utilizar inmediatamente este nombre de usuario y contraseña para iniciar la sesión en el Visualizador.

Desactivación de usuarios del Visualizador

Puede desactivar cuentas de usuarios del Visualizador para los usuarios que ya no necesitan acceso.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Visualizador**.
3. Pulse la pestaña **Usuarios del Visualizador**.
4. Pulse el nombre de usuario cuya cuenta de usuario desea desactivar.
5. En la lista desplegable **Estado**, elija **Inactivo**.
6. Pulse el botón **Guardar**.

Resultados

El usuario desactivado ya no puede iniciar sesión en el Visualizador.

Restablecimiento de contraseñas del Visualizador

Si un usuario del Visualizador olvida la contraseña, y la información de inicio de sesión se ha configurado mediante la Consola de configuración, no mediante la opción de inicio de sesión de la base de datos subyacente, puede restablecer la contraseña utilizando la Consola de configuración. De lo contrario, debe restablecer la contraseña utilizando la configuración de inicio de sesión de base de datos subyacente.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Visualizador**.
3. Pulse el separador **Usuarios del Visualizador**.
4. Pulse el nombre de usuario cuya contraseña desea editar.
5. En el campo **Contraseña**, escriba una nueva contraseña para el usuario.

   Nota: Por razones de seguridad, aconseje al usuario que cambie la contraseña tras iniciar sesión satisfactoriamente para que sólo la conozca él.
6. Pulse el botón **Guardar**.

Qué hacer a continuación

El usuario puede utilizar inmediatamente esta nueva contraseña para iniciar la sesión en el Visualizador. Por razones de seguridad, aconseje al usuario que cambie la contraseña tras iniciar sesión satisfactoriamente.

Creación de grupos de usuarios del Visualizador

Se asignan alertas a grupos de analistas en el Visualizador. Si añade un nuevo grupo de analistas a un proyecto, puede utilizar la Consola de configuración para crear un nuevo grupo de analistas.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Códigos**.
4. En la lista desplegable **Tipo**, pulse **ANALYZER_GROUP**.
5. Pulse el botón **Nuevo**.
6. En el campo **Código**, escriba el nombre del grupo de analistas.
7. En la lista desplegable **Estado**, seleccione **Activo**.
8. Pulse el botón **Guardar**.

Temas de ayuda

Panel General de usuarios del Visualizador:

Utilice este separador para añadir nuevos usuarios del Visualizador o para cambiar las contraseñas de los usuarios existentes.

Inicio de sesión en base de datos
Seleccione una opción para determinar si se debe utilizar la información subyacente de la base de datos de entidades (nombre de usuario y contraseña) para el acceso al Visualizador.

- Sí - Sólo utilizar este valor si el usuario del Visualizador ya tiene una cuenta de usuario que le otorgue acceso a la base de datos de entidades. Si selecciona esta opción, utilice el nombre de usuario y la contraseña de inicio de sesión de la base de datos de entidades como nombre de usuario y contraseña del Visualizador. (Si no coinciden, no se podrá iniciar sesión en el Visualizador.)
- No - Utilizar la información de inicio de sesión entrada en este separador.

Nombre de usuario
Escriba el nombre de usuario para este usuario del Visualizador. Si este usuario utiliza un inicio de sesión de una base de datos, este nombre de usuario debe coincidir exactamente con el nombre de usuario correspondiente de la base de datos.

Contraseña
Escriba la contraseña nueva para este usuario del Visualizador. Si este usuario utiliza un inicio de sesión de una base de datos, esta contraseña debe coincidir exactamente con la contraseña correspondiente de la base de datos.

Grupo Seleccione el grupo del Visualizador del que este usuario forma parte. El grupo del Visualizador determina qué alertas y notificaciones puede ver el usuario en la ventana **Resumen de alertas** del Visualizador. (Por ejemplo, si la organización tiene un grupo de seguridad del Visualizador y un grupo de reserva, es posible que los usuarios de cada grupo vean distintos tipos de alertas en el Visualizador.) .

Estado

Seleccione un estado para indicar si el usuario del Visualizador está actualmente activo (puede iniciar una sesión en el Visualizador).

Configuración de códigos de actividad para el Visualizador

El Visualizador proporciona varios códigos de actividad predeterminados para tratar las alertas. Puede añadir nuevos códigos de actividad y suprimir códigos de actividad existentes mediante la Consola de configuración.

Creación de códigos de actividad para búsquedas

El Visualizador proporciona códigos de actividad para alertas del resultado de la búsqueda. Si necesita hacer un seguimiento de actividades adicionales relacionadas con el manejo de alertas, puede añadir nuevos códigos de actividad utilizando la Consola de configuración.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Visualizador**.
3. Pulse la pestaña **Códigos de actividad**.
4. En la lista desplegable **Tipo de actividad**, pulse **SEARCH**.
5. Pulse el botón **Nuevo**.
6. En el campo **Código de actividad**, escriba el nombre del código de actividad.
7. En la lista desplegable **Código de estado de actividad**, seleccione el código de estado de actividad reconocido internamente al que corresponde el nuevo código de actividad.
8. En la lista desplegable **Estado**, seleccione **Activo**.
9. Pulse el botón **Guardar**.

Supresión de códigos de actividad para búsquedas

El Visualizador proporciona códigos de actividad para alertas del resultado de la búsqueda. Si necesita suprimir códigos de actividad relacionados con el manejo de alertas, puede suprimir los códigos de actividad existentes utilizando la Consola de configuración.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Visualizador**.
3. Pulse la pestaña **Códigos de actividad**.
4. En la lista desplegable **Tipo de actividad**, pulse **SEARCH**.
5. Marque el recuadro de selección situado junto al código de actividad que desea suprimir.
6. Pulse el botón **Suprimir**. Aparecerá una ventana de confirmación.
7. Pulse **Aceptar**.

Creación de códigos de actividad para alertas de rol

El Visualizador proporciona códigos de actividad para alertas de rol. Si necesita hacer un seguimiento de actividades adicionales relacionadas con el manejo de alertas, puede añadir nuevos códigos de actividad utilizando la Consola de configuración.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Visualizador**.
3. Pulse la pestaña **Códigos de actividad**.
4. En la lista desplegable **Tipo de actividad**, pulse **CONFLICT**.
5. Pulse el botón **Nuevo**.
6. En el campo **Código de actividad**, escriba el nombre del código de actividad.
7. En la lista desplegable **Código de estado de actividad**, seleccione el código de estado de actividad reconocido internamente al que corresponde el nuevo código de actividad.
8. En la lista desplegable **Estado**, seleccione **Activo**.
9. Pulse el botón **Guardar**.

Supresión de códigos de actividad para alertas de rol

El Visualizador proporciona códigos de actividad para alertas de rol. Si necesita suprimir códigos de actividad relacionados con el manejo de alertas, puede suprimir los códigos de actividad existentes utilizando la Consola de configuración.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Visualizador**.
3. Pulse la pestaña **Códigos de actividad**.
4. En la lista desplegable **Tipo de actividad**, pulse **CONFLICT**.
5. Marque el recuadro de selección situado junto al código de actividad que desea suprimir.
6. Pulse el botón **Suprimir**. Aparecerá una ventana de confirmación.
7. Pulse **Aceptar**.

Creación de códigos de actividad para alertas de suceso

El Visualizador proporciona códigos de actividad para alertas de suceso generadas a través del proceso de sucesos, si el sistema tiene el gestor de sucesos habilitado. Los códigos de actividad de suceso permiten realizar un seguimiento de las actividades adicionales relacionadas con el manejo de alertas de suceso. El sistema proporciona tres códigos de actividad de suceso predefinidos, pero se pueden añadir nuevos códigos de actividad para alertas de suceso que utilicen la Consola de configuración.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Visualizador**.
3. Pulse la pestaña **Códigos de actividad**.
4. En la lista desplegable **Tipo de actividad**, seleccione **EVENT**.
5. Pulse el botón **Nuevo**.
6. En el campo **Código de actividad**, escriba un nombre exclusivo del nuevo código de actividad.
7. En la lista desplegable **Código de estado de actividad**, seleccione el código de estado de actividad reconocido internamente al que corresponde el nuevo código de actividad.

8. En la lista desplegable **Estado**, seleccione **Activo** para que el Visualizador pueda utilizar el código de actividad.
9. Pulse el botón **Guardar**.

Códigos de actividad definida previamente para alertas de suceso:

Los analistas utilizan los códigos de actividad de suceso en el Visualizador para eliminar alertas de suceso. El sistema incluye tres códigos de actividad predefinidos, después de ejecutar los scripts SQL del fixpack 1 v4.2.

Los códigos de actividad siguientes para alertas de suceso se incluyen en el conjunto predefinido de códigos de actividad de alerta de sucesos:

ASIGNADO
Cuando los analistas asignan una alerta de suceso a sí mismos o a otro grupo de analistas, el sistema utiliza el código de actividad ASSIGNED como valor predeterminado.

CERRADO
Cuando los analistas cierran una alerta de suceso, el sistema utiliza el código de actividad CERRADO como valor predeterminado.

PENDIENTE
Antes de que un analista elimine una alerta de suceso, el sistema asigna automáticamente la actividad PENDIENTE, lo cual significa que la alerta de suceso está abierta para que cualquier analista del grupo asignado la revise o elimine.

Edición de códigos de actividad para alertas de suceso

Puede utilizar los códigos de actividad existente para eliminar alertas de suceso del Visualizador. No se pueden renombrar los códigos de actividad existentes, pero se puede cambiar la descripción asociada, el código de estado de actividad o el estado.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Visualizador**.
3. Pulse la pestaña **Códigos de actividad**.
4. En la lista desplegable **Tipo de actividad**, seleccione **EVENT**.
5. Pulse el código de actividad que desea editar.
6. Desde el separador **General de códigos de actividad**, realice los cambios. Por ejemplo, si desea configurar un código de actividad pero que no aparezca en la selección del Visualizador, seleccione el estado **Inactivo**. De este modo, no será necesario suprimir el código de actividad si desea activarlo más adelante.
7. Pulse el botón **Aceptar**.

Supresión de códigos de actividad para alertas de suceso

El Visualizador proporciona códigos de actividad para la eliminación de alertas de suceso. Si necesita suprimir códigos de actividad relacionados con el manejo de alertas de suceso, puede suprimir los códigos de actividad existentes utilizando la Consola de configuración incluidos los códigos de actividad de alerta de suceso predefinidos. Al suprimir el código de actividad dejará de estar disponible en el Visualizador para utilizarlo en el manejo de alertas de suceso.

Acerca de esta tarea

Si sólo desea cambiar la información para el código de actividad, puede editar el código de actividad sin suprimirlo y volverlo a crear.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Visualizador**.
3. Pulse la pestaña **Códigos de actividad**.
4. En la lista desplegable **Tipo de actividad**, seleccione **EVENT**.
5. Marque el recuadro de selección situado junto a los códigos de actividad que desea suprimir.
6. Pulse el botón **Suprimir**. Aparecerá una ventana de confirmación.
7. Pulse el botón **Aceptar**.

Panel General de códigos de actividad del Visualizador

Los analistas utilizan los códigos de actividad en el Visualizador para eliminar alertas de rol, alertas de suceso y búsquedas.

Tipo de actividad
Lo rellena el sistema. Seleccione el tipo de actividad que desee del cual desee visualizar, añadir o suprimir códigos de actividad.

- **CONFLICT** utilizado para alertas de rol
- **EVENT** utilizado para alertas de suceso
- **SEARCH** utilizado para búsquedas en el Visualizador

Código de actividad
Escriba el nombre exclusivo de este código de actividad.

Descripción
Escriba una descripción de este código de actividad.

Código de estado de actividad
Seleccione el código de estado interno al que corresponde este código de actividad de usuario:

- **Abrir**
- **Asignado**
- **Cerrado**
- **Filtrado**

Estado
Indica si este código de actividad está actualmente activo. Por ejemplo, puede configurar un código de actividad antes de implementar el código en el Visualizador desactivando el código de actividad. Entones, cuando llegue el momento de implementar el código de actividad, edítelo para activarlo.

Administración de valores de configuración del sistema

La modificación de la configuración del sistema se puede realizar siguiendo estos procesos:

Capítulo 5. Configuración del sistema para los datos

Para utilizar IBM InfoSphere Identity Insight de forma eficaz debe configurar la base de datos de entidades, la resolución de entidades y los parámetros del sistema.

Configuración de datos en el sistema

Para utilizar IBM InfoSphere Identity Insight, primero debe configurar la base de datos de entidades para que utilice los orígenes de datos.

Configuración de tipos de características

Puede configurar tipos de características para datos que no se pueden clasificar como nombre, número, dirección o dirección de correo electrónico. Cuando se añaden datos nuevos a un origen de datos y desea clasificar esos datos como un tipo de característica que todavía no está configurada en el sistema, deberá crear una nuevo tipo de característica para los nuevos datos.

Características

Las características son rasgos o propiedades definidas por el usuario que se asocian a una identidad que no se suele expresar como un nombre, número, dirección o dirección de correo electrónico.

Este atributo permite a los usuarios ampliar el producto definiendo atributos de entidades que se pueden personalizar que resulten significativos para los orígenes de datos.

Tipos de características:

Los tipos de características organizan e identifican datos que se almacenan en la base de datos de entidades. Ejemplos de tipos de características predeterminadas que ya están configurados en la base de datos de entidades son fecha de nacimiento y sexo.

Si tiene datos que no están definidos mediante ninguno de los tipos de características predeterminadas, debe crear un nuevo tipo de características para dichos datos.

Ejemplo

Second National Banker's Trust acaba de incorporar un nuevo tipo de datos sobre sus tipos de clientes. Los datos llegan al nodo de adquisición utilizando los siguientes códigos UMF:

```
<attribute>
  <attr_type>cust_type</attr_type>
  <attr_value>merchant</attr_value>
<5/attribute>
```

En esta instancia, tiene que configurar un nuevo tipo de características llamado cust_type.

Tipos de características creados por el sistema:

Si un mensaje UMF se procesa con un tipo de característica que no está configurado, el sistema crea automáticamente un nuevo tipo de característica.

El valor del mensaje UMF se registra en la base de datos utilizando el tipo de característica recién creado y se escribe una excepción de UMF.

Cuando el sistema crea automáticamente una nueva característica, se genera un registro de base de datos incompleto que sólo contiene:

- La información del nuevo **Tipo** basada en el mensaje UMF.
- Un valor `Creado por el sistema` para **Estado**.

Visualización de tipos de características

Los tipos de características son para datos que no se pueden clasificar como tipo de nombre, número, dirección ni dirección de correo electrónico. Puede que desee ver los tipos de características existentes si está pensando en añadir una nueva.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Características**.
4. Seleccione el tipo de característica que desea ver.

Creación de un tipo de característica

Las características de entidades se organizan en el sistema por tipo.

Antes de empezar

Antes de crear un nuevo tipo de característica, consulte los datos de la característica de entrada para determinar si se puede describir con precisión utilizando cualquier tipo de característica existente.

Acerca de esta tarea

Para utilizar con eficacia nuevos datos de características, debe configurar un nuevo tipo de característica utilizando la Consola de configuración. Si crea un nuevo tipo de característica con un valor de tipo de datos DATE, tendrá la opción de crear una nueva regla DQM para validar el nuevo tipo de característica.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Características**.
4. Pulse el botón **Nuevo**.
5. En el panel **General**, especifique el tipo, la descripción, el tipo de datos, la clase, el uso de la resolución, el estado, conservar historial y el nivel de visualización para este tipo de característica.
6. Pulse el botón **Guardar**. Si crea un nuevo tipo de característica con el valor de tipo de datos DATE, y decide crear una nueva regla DQM para validar el nuevo tipo de característica, se le direccionará a la página de creación de reglas DQM con los valores llenados previamente basándose en el nuevo tipo de característica.

Resultados

Ahora, el sistema puede procesar los datos de un archivo UMF que se especifica para <CHARACTERISTIC_TYPE>.

Supresión de tipos de características

Puede suprimir un tipo de característica existente cuando la base de datos de entidades ya no la utilice.

Acerca de esta tarea

Si ha creado una regla DQM para que vaya con el tipo de característica, es posible que desee suprimir también la regla DQM correspondiente.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Características**.
4. Marque el recuadro de selección situado junto al tipo de característica que desea suprimir.
5. Pulse el botón **Suprimir**.

Temas de ayuda

Características - Panel General:

Utilice el panel **General** para especificar los detalles del tipo de característica.

Tipo Escriba el nombre del tipo de característica que desea crear.

Descripción
Escriba la descripción del tipo de característica que desea crear.

Tipo de datos
En la lista desplegable, seleccione el tipo de datos de la característica que desea crear.

CHAR
Seleccione este tipo de campo para especificar el tipo de datos del tipo de característica como caracteres.

CLOB Seleccione este tipo de campo para especificar el tipo de datos del tipo de característica como CLOB.

CLOB se debe utilizar para tipos de características que constan de grandes cantidades de datos.

Nota: El establecimiento del tipo de datos en CLOB puede afectar de forma negativa al rendimiento. Si es posible, utilice VARCHAR (LVARCHAR para Informix) para reducir el posible impacto de rendimiento.

DATE Seleccione este tipo de campo para especificar el tipo de datos del tipo de característica como una fecha.

`Crear regla DQM`
Si desea crear un nuevo tipo de característica con un valor de tipo de datos de DATE, tendrá la opción de crear una nueva regla DQM para validar el nuevo tipo de característica. Se le

redirigirá a la página de creación de regla DQM con valores ya especificados basados en el nuevo tipo de característica.

VARCHAR
Seleccione este tipo de campo para especificar el tipo de datos del tipo de característica como caracteres variables.

Clase En la lista desplegable, seleccione la clase del tipo de característica que desea crear.

LC Seleccione este tipo de campo para especificar el tipo de característica como una característica activa.

Por ejemplo, altura o peso.

SC Seleccione este tipo de campo para especificar el tipo de característica como una característica del sistema.

Por ejemplo, una preferencia de asiento en un avión o el saldo de puntos de un cliente habitual.

Uso de resolución
En la lista desplegable, seleccione si esta característica se debe utilizar para la resolución de entidades.

Ninguno
Seleccione este tipo de campo para especificar que el valor de la característica no se utilizará para la resolución de entidades.

Confirmar/denegar
Seleccione este tipo de campo para especificar que el valor de la característica se utilizará para la resolución de entidades.

Candidatos
Seleccione este tipo de campo para especificar que el valor de la característica se utilizará para crear una lista de candidatos y para incrementar la puntuación de un candidato.

Candidatos/Sin puntuación
Seleccione este tipo de campo para especificar que el valor de la característica se utilizará para crear una lista de candidatos, pero no incrementará la puntuación de un candidato.

Estado
En la lista desplegable, seleccione **Activo** para especificar que esta característica está activa. De lo contrario, seleccione **Inactiva**.

Conservar historial
En la lista desplegable, seleccione **Sí** para registrar el estado histórico del valor del tipo de característica. Sólo se debe utilizar para tipos de características cuyo valor no cambian con frecuencia. De lo contrario, seleccione **No**.

Nivel de visualización
En la lista desplegable, seleccione si esta característica se debe utilizar para gráficos e informes.

Ninguno
Seleccione este tipo de campo para excluir el valor de este tipo de característica de gráficos e informes.

Todos Seleccione este tipo de campo para incluir el valor de este tipo de característica en todos los gráficos e informes.

Configuración de tipos de números

Puede configurar tipos de números para datos que se pueden clasificar como números. Cuando se añaden nuevos datos a un origen de datos y desea clasificar esos datos como un número que aún no se ha configurado en el sistema, debe crear un nuevo tipo de número para los nuevos datos.

Números

Los números son rasgos o propiedades definidas por el usuario que se asocian a una identidad que se puede clasificar como un número.

Tipos de números

Los tipos de números organizan e identifican datos numéricos almacenados en la base de datos de entidades. Ejemplos de tipos de números predeterminados que ya están configurados en la base de datos de entidades son número de teléfono y número de seguridad social.

Si tiene datos de números que no están definidos mediante ninguno de los tipos de números predeterminados, debe crear un nuevo tipo de número para dichos datos.

Ejemplo

Second National Banker's Trust tiene datos de números que incluyen números de cuenta corriente de clientes. Desea añadir estos nuevos datos a la base de datos de entidades. Los datos llegan al nodo de adquisición utilizando los siguientes códigos UMF:

```
<number>
  <num_type>ca</num_type>
  <num_value>41510155060</num_value>
</number>
```

En este ejemplo, tiene que configurar un nuevo tipo de número denominado ca.

Visualización de tipos de números

Los tipos de números sirven para datos que se pueden clasificar como números. Puede que desee ver los tipos de números existentes cuando piense añadir un nuevo tipo de número.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **orígenes**.
3. Pulse la pestaña **Números**.
4. Seleccione el tipo de número que desea ver.

Creación de tipos de números

Deberá crear un nuevo tipo de número cuando se añadan nuevos datos a un sistema origen y desee clasificar esos datos como un tipo de número que aún no está configurado.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Números**.
4. Complete uno de los pasos siguientes:
   - Para crear un nuevo tipo de número, pulse el botón **Nuevo**.

- Para crear un tipo de número basado en un tipo de número existente, seleccione un tipo de número en la lista y, después, pulse el botón **Clonar**.

5. En el panel **General**, especifique el tipo, la descripción, la clase, si es exclusivo, el uso de la resolución, el estado, si se debe conservar el historial, el peso de confirmar ubicación, el peso de denegar ubicación y otra información de configuración para el tipo de número.
6. En el panel **Formato**, especifique la longitud mínima, la longitud máxima, la máscara, el relleno de máscara, el carácter de relleno, la longitud hash y otra información de configuración para el tipo de número.
7. Pulse el botón **Guardar**.

Supresión de tipos de números

Puede suprimir un tipo de número existente cuando el sistema ya no lo utilice.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Números**.
4. Seleccione un tipo de número en la lista y, después, pulse el botón **Suprimir**.

Temas de ayuda

Números - Panel General:

Utilice el panel **General** para especificar los detalles del tipo de número.

Tipo Escriba el nombre del tipo de número que desea crear.

Descripción
Escriba la descripción del tipo de número que desea crear.

Clase En la lista desplegable, seleccione la clase del tipo de número que desea crear.

CC Seleccione este tipo de campo para especificar el tipo de número como una tarjeta de crédito.

VARIOS
Seleccione este tipo de campo para especificar el tipo de número como de tipo variado.

Por ejemplo, un número de cliente habitual de vuelos.

OTROS
Seleccione este tipo de campo para especificar el tipo de número como de tipo otros.

Por ejemplo, un número desconocido en un origen de datos.

TELÉFONO
Seleccione este tipo de campo para especificar el tipo de número como un número de teléfono.

PID Seleccione este tipo de campo para especificar el tipo de número como un número de identificación personal.

Por ejemplo, un número de carnet de conducir o un número de seguridad social.

SYSID

Seleccione este tipo de campo para especificar el tipo de número como un número de identificación del sistema.

Por ejemplo, una dirección IP.

Uso de resolución

En la lista desplegable, seleccione si este tipo de número se debe utilizar para la resolución de entidades.

Ninguno

Seleccione este tipo de campo para especificar que el valor de número no se utilizará para la resolución de entidades.

Candidatos

Seleccione este tipo de campo para especificar que el valor de número se utilizará para crear una lista de candidatos y para incrementar la puntuación de un candidato.

Estado

En la lista desplegable, seleccione **Activo** para especificar que este número está activo. De lo contrario, seleccione **Inactiva**.

Conservar historial

En la lista desplegable, seleccione **Sí** para registrar el estado histórico del valor del tipo de número. Sólo se debe utilizar para tipos de número cuyo valor no cambian con frecuencia. De lo contrario, seleccione **No**.

Nivel de visualización

En la lista desplegable, seleccione si este número se debe utilizar para gráficos e informes.

Ninguno

Seleccione este tipo de campo para excluir el valor de este tipo de número de gráficos e informes.

Todos Seleccione este tipo de campo para incluir el valor de este tipo de número en todos los gráficos e informes.

Configuración de datos de nombre

Los datos de nombre es lo que está contenido en el segmento <NAME> de cualquier documento UMF de entrada. Durante el proceso de resolución de entidad, los datos de nombre se analizan, se comparan con los datos de nombre de entidades existentes en la base de datos de entidad y se les proporciona una puntuación basándose en el grado de rigurosidad con la que coinciden los datos de nombre.

Hashing de nombres ampliado con IBM Global Name Recognition Name Hasher

Name Hasher utiliza la tecnología de IBM Global Name Recognition para ampliar el hashing de nombres creando hashes variantes para cada nombre de entrada. Los hashes de nombre de variante permiten que la resolución de entidad utilicen la coincidencia de nombres similares durante el análisis y la puntuación de nombre.

Los escenarios siguientes muestran los beneficios de cuándo puede utilizar Name Hasher:

- Cuando la mayoría de los datos pueden ser coincidentes sólo en el segmento <NAME>

- Cuando la mayoría de los datos pueden ser coincidentes sólo en el segmento <NAME> y la mayoría de los datos no cumplen con la anotación de nombre, segundo nombre y apellido de la cultura anglosaxona.

La utilización de Name Hasher con el algoritmo de puntuación de nombres de Name Manager proporciona la posibilidad de clasificar los nombres para la cultura y comparar y puntuar de forma precisa los nombres en la lista de candidatos en un contexto culturalmente sensible.

Name Hasher no está habilitado de forma predeterminada. Utilice la consola de configuración para habilitar Name Hasher y las funciones de DQM asociadas.

Atención: Póngase en contacto con los servicios o el soporte de IBM si está actualizando desde Name Hasher de las versiones de producto 8.0 o 4.2 y si es un cliente existente que habilita Name Hasher por primera vez. En ambos casos, sin la asistencia de los servicios o soporte de IBM, la resolución de entidades de datos nuevos falla cuando se compara con los datos existentes en la base de datos de entidades.

Habilitación de la función IBM Global Name Recognition Name Hasher:

Al habilitar la característica IBM Global Name Recognition Name Hasher para el proceso de calidad de datos de segmento <NAME> de UMF, puede mejorar el análisis de nombres, la clasificación de culturas y la generación de hash de nombres.

Antes de empezar

Si está habilitando Name Hasher en una instalación existente por primera vez, póngase en contacto con los servicios o el soporte de IBM para obtener ayuda. Todos los datos existentes de todos los orígenes de datos se deben volver a cargar para evitar que la resolución de entidades de datos nuevos falle para los datos existentes en la base de datos de entidades.

Acerca de esta tarea

Estas instrucciones son resúmenes de las tareas que deben realizarse para habilitar Name Hasher. Todos los pasos se completan utilizando la Consola de configuración. Pulse el enlace para obtener las instrucciones paso a paso para cada tarea.

Procedimiento

1. Habilite la función DQM 282 para crear hashes de nombres. Esta función activa la funcionalidad Name Hasher en las interconexiones. Si ha utilizado Name Hasher antes dela versión 8.0 fixpack 2 del producto, consulte las instrucciones para migrar al Name Hasher actualizado. Puede que desee reutilizar algunos de los parámetros utilizados por DQM 282.
2. Habilite la función DQM 610, para que Name Hasher pueda crear atributos de hash de nombres compuestos.
3. Configure el compilador candidato predeterminado con sólo nombre para el hashing de nombres ampliado.
4. Configure cada origen de datos para el hashing de nombres ampliado.
5. Inhabilite el análisis de nombres completo en la función DQM 252. Name Hasher crea variantes de hash de nombres para todas las partes de nombre, no sólo el nombre completo.

6. Configure la regla DQM 255 para hashing de nombres mejorado Al completar este paso, se mantendrá la capacidad de estandarización de nombres de DQM 255, pero se inhabilitará el hashing de nombres estándar para utilizar el hashing de nombres ampliado de Name Hasher. También se asegurará de que la comprobación de validación de interconexión de verificación de que DQM 255 se ha habilitado no fallará y cerrará las interconexiones.
7. Habilite la función DQM 260 para el segmento UMF <NAME>. Esta función DQM asigna culturas de nombre a los datos de nombre de entrada. Name Hasher necesita cultura de nombres para aplicar experiencia multicultural al hashing de nombres ampliado. Asegúrese de que Name Manager está activado. (Normalmente, Name Manager está activado.) Si habilita la regla DQM 260 y Name Manager no está activado, la regla DQM 260 falla y las interconexiones se cierran.
8. Establezca los parámetros de sistema para Name Hasher. Al completar este paso, configura los parámetros de sistema necesarios para las interconexiones utilizadas durante el hashing de nombres ampliado.

Configuración de parámetros de sistema para el hashing de nombres mejorado:

Para que Name Hasher funcione correctamente durante la resolución de entidades, el valor predeterminado del parámetro de sistema HASHLESS_NAMES_ARE_GENERIC de MM debe desactivarse. Al desactivar este valor, la funcionalidad Name Hasher se aplica a todos los datos de nombre de entrada.

Inhabilitación del análisis de nombre completo para hashing de nombres ampliado:

Para que Name Hasher funcione correctamente, debe inhabilitar la regla DQM 252 existente en el segmento <NAME>.

Configuración de la regla DQM 255 para la función IBM Global Name Recognition Name Hasher:

Para que Name Hasher funcione correctamente, debe configurar el valor del parámetro **Excluir UMF** en la función DQM 255.

Acerca de esta tarea

- Inhabilite la funcionalidad de hashing de nombres y análisis de nombres estándar de la regla DQM 255 en favor del análisis y hashing mejorados proporcionados por Name Hasher
- Asegúrese de que la regla DQM 255 está habilitada, satisfaciendo la comprobación de validación de interconexión que requiere que la regla DQM 255 esté habilitada

Configuración de compiladores candidatos para el hashing de nombre ampliado:

Para que Name Hasher funcione correctamente, asegúrese de que la configuración de compilador candidato **Predeterminado con solo nombre** contiene un tipo de coincidencia de **Característica**.

Configuración de orígenes de datos para el hashing de nombres mejorado:

Si utiliza hashing de nombre mejorado, debe configurar cada origen de datos para permitir la creación de lista de candidatos de atributos de nombre, estableciendo la configuración de compilador candidato en el compilador candidato **Predeterminado con sólo nombre**.

Creación de atributos hash de nombre compuesto:

La función DQM 610 crea nuevos atributos a partir de diferentes valores más pequeños contenidos en el documento UMF de entrada. Name Hasher utiliza DQM 610 para crear hashes de nombre compuesto y almacenar esos hashes como atributos en los segmentos <NAME> y <ATTRIBUTE> de UMF.

Acerca de esta tarea

Los atributos de hash de nombre compuesto resultantes siempre contienen un <ATTR_TYPE> de GNR_HASH. Mediante la creación de estos atributos de hash de nombre, la resolución de entidades puede utilizar la coincidencia de nombres similares durante el análisis y la puntuación de nombres. La capacidad de coincidencia de nombres similares amplia el rango de posibles coincidencias de identidad y entidad en los datos de nombre.

Migración a IBM Global Name Recognition Name Hasher actualizado:

Si el producto utilizaba la función Name Hasher anterior a la versión de producto 8.0 fixpack 2, realice estas tareas además de las tareas estándares necesarias para actualizar a la última funcionalidad Name Hasher funcionalidad.

Procedimiento

1. Realice la actualización del producto estándar utilizando el programa de instalación de producto.
2. En la Consola de configuración, inhabilite la función DQM 660 en el segmento UMF `<NAME>`. Copie o escriba los valores actuales para los parámetros **`maxVariants`** y **`variantScoreThreshold`** contenidos con el parámetro de HTTP URL. Antes de la versión 8.0 fixpack 2 del producto, la funcionalidad de hashing de nombre ampliada utilizaba un servlet Name Hasher que se ejecutaba en un servidor de aplicaciones web. En la versión 8.0 fixpack 2 y posteriores del producto, la funcionalidad de Hasher está incorporada en la interconexión. Al inhabilitar la función DQM 660 en el segmento `<NAME>`, se inhabilita el servlet de Name Hasher existente.
3. En la Consola de configuración, habilite la regla DQM 282 (variantes de hash de nombres) en el segmento de UMF `<NAME>` y pegue o configure manualmente los siguientes valores de parámetros de función:

   `maxVariants`
   Establezca este valor en el mismo valor utilizado anteriormente en el parámetro **`maxVariants`** de la función DQM 660.

   `variantScoreThreshold`
   Establezca este valor en el mismo valor utilizado previamente en el parámetro **`variantScoreThreshold`** de la función DQM 660.

Nota: Si la función DQM 660 no contiene valores para estos parámetros en el URL, utilice los valores predeterminados de la función DQM 282.
Al completar este paso, puede activar la funcionalidad de Name Hasher dentro de la interconexión.

4. En la Consola de configuración, configure los parámetros de sistema para el Name Hasher. Al completar este paso, configura globalmente los parámetros necesarios que la interconexión utiliza como parte de la funcionalidad de Name Hasher.

Análisis de nombre alternativo

La creación de análisis de nombre alternativo para un nombre completo de entrada amplía las prestaciones de puntuación y coincidencia de nombres de la resolución de entidad

Analizar los nombres por partes de nombre es uno de los primeros pasos de la coincidencia de nombres. Los análisis de nombre alternativo son las variaciones posibles del nombre. Al generar análisis de nombre alternativo para los datos de nombres de entrada, puede aumentar la probabilidad de que el nombre de entrada se analice y puntúe correctamente.

Utilice la función DQM 289 para generar análisis de nombre alternativo. De forma predeterminada, esta función no está habilitada. Para generar los análisis de nombre alternativo, debe configurar la función DQM 289 en el segmento <NAME> e n la Consola de configuración.

Es posible que no haya un análisis alternativo para todos los nombres. Si existe un análisis de nombre alternativo para el nombre y si sólo ese análisis alternativo es diferente del análisis de nombre primario, la función DQM genera un segundo segmento <NAME> que incluye el análisis alternativo.

Por ejemplo, tenga en cuenta los datos de nombre de entrada siguientes:

```
<UMF_ENTITY>
 <NAME>
    <NAME_TYPE>M</NAME_TYPE>
  <FULL_NAME>ALLEN CRAIG</FULL_NAME>
  </NAME>
....
</UMF_ENTITY>
```

En este ejemplo, el nombre completo puede tener al menos dos análisis diferentes. "Allen" y "Craig" pueden ser nombres o apellidos. Al generar análisis alternativos de este nombre, el proceso de resolución de entidad puede analizar y puntuar el nombre en más entidades de la base de datos de entidades.

Si la función DQM 289 está configurada en el código UMF <FULL_NAME> del segmento <NAME>, durante el proceso de nombre, se crea un análisis de nombre alternativo que se añade al registro UMF. El registro resultante es parecido al registro siguiente:

```
<UMF_ENTITY>
 <NAME>
    <NAME_TYPE>M</NAME_TYPE>
  <FIRST_NAME>ALLEN</FIRST_NAME>
  <LAST_NAME>CRAIG</LAST_NAME>
  </NAME>
  <NAME>
  <NAME_TYPE>ALT</NAME_TYPE>
  <FIRST_NAME>CRAIG</FIRST_NAME>
```

```
  <LAST_NAME>ALLEN</LAST_NAME>
  </NAME>
....
</UMF_ENTITY>
```

El primer segmento <NAME> contiene el análisis de nombre primario y el valor de <NAME_TYPE> original. El segundo segmento <NAME> contiene el análisis alternativo generado, indicado por el valor <NAME_TYPE> de ALT. (Este ejemplo supone que el valor para el tipo de nombre de análisis alternativo es el valor predeterminado.)

Configuración de nombres para crear análisis de nombres alternativos:

Puede configurar nombres para crear análisis de nombres alternativos, que pueden utilizarse para soportar la generación de varios hashes de nombre. Si utiliza la característica IBM Global Name Recognition Name Hasher, al crear análisis de nombres alternativos se pueden mejorar las prestaciones de coincidencia de nombres similares a fin de mejorar la resolución de entidad en los datos de nombre.

Antes de empezar

- Asegúrese de que de Name Manager está activado y que la vía de acceso a los archivos de soporte está establecida en los parámetros de sistema. Si esta función DQM se habilita sin una vía de acceso válida a los archivos de soporte de Name Manager, la interconexión registra un error y concluye.
- Cuando se habilita la función DQM para la característica de análisis de nombres alternativos, se está cambiando la configuración del sistema. Al igual que con cualquier cambio de configuración, asegúrese de detener las interconexiones activas antes de cambiar la configuración. A continuación, reinicie las interconexiones para reinicializarlas con los cambios de configuración.

Acerca de esta tarea

- Para las instalaciones nuevas de productos de la V8.0 fixpack 2 o posterior, esta función DQM ya está configurada y activa.
- Para versiones actualizadas de producto a partir de la V8.0 fixpack 2 o posterior, esta función DQM está configurada pero está inactiva. Para generar análisis de nombres alternativos, cambie el estado de la función DQM existente a **Activo**.

Procedimiento

1. En la Consola de configuración, seleccione **Configurar** > **UMF** > **Reglas DQM**.
2. Seleccione NAME en la lista **Segmento**.
3. Seleccione el nombre de código UMF que lista **289 – Análisis de nombres alternativos** en **Función**.
4. En **Estado**, asegúrese de que Activo está seleccionado.
5. En la pestaña **Parámetros**, revise o establezca los valores de parámetro siguientes:
   - **Umbral de puntuación de análisis**: Establezca este valor en un número entre 0 y 100. Cuanto mayor es la puntuación, menos análisis alternativos se crean. Este valor establece el umbral para la puntuación de confianza mínima que el analizador de nombres utilizará para determinar si se debe crear un análisis alternativo para el nombre de entrada. Si no se encuentra ningún análisis alternativo con una puntuación de confianza más alta o si el análisis de entrada proporcionado originalmente ya puntúa por encima del umbral, no se creará ningún análisis alternativo.

- **Tipo de nombre alternativo**: Escriba el valor para NAME_TYPE para indicar que este nombre es un análisis alternativo. Este valor es el código UMF que se añade al segmento <NAME> para cada análisis de nombre alternativo creado. De forma predeterminada, este valor se establece en ALT. Para garantizar la atribución completa de la resolución de entidades, no establezca este valor en un NAME_TYPE de entrada existente configurado en la Consola de configuración. Concretamente, no establezca este valor en **M** o **A**.

6. Pulse **Guardar**.

Determinación de género

Al procesar los datos de nombre de entrada, a veces el género de un nombre personal puede ser el factor determinante de que dos entidades coincidan. El género añade peso de confirmación o denegación a la puntuación de resolución de entidad para determinar si dos identidades son la misma entidad.

La función DQM 258 identifica dinámicamente el género del segmento <NAME> en un registro UMF de entrada, crea una característica de género y añade la característica de género al registro UMF de entrada. La característica de género se añade utilizando el segmento <ATTRIBUTE>.

- Si el registro UMF de entrada ya contiene una característica de género en los datos, la función DQM 258 no genera otra característica de género.
- Si el registro UMF contiene más de un segmento <NAME>, la función DQM 258 crea sólo una característica de género para el registro de entrada entero. En este caso, la generación de varios atributos de género puede ser redundante o conflictiva.

Para determinar dinámicamente el género de un nombre, asegúrese de que se ha configurado al menos un código UMF en el segmento <NAME> para utilizar la función DQM 258.

- Para las instalaciones nuevas de productos de la V8.0 fixpack 2 o posterior, esta función DQM ya está configurada y activa.
- Para versiones actualizadas de producto a partir de la V8.0 fixpack 2 o posterior, esta función DQM está configurada pero está inactiva. Si desea utilizar esta funcionalidad de género mejorada, debe cambiar el estado a **Activo**. Si ha asignado anteriormente género utilizando el parámetro **Tipo de característica de género** de la función DQM 255, restablezca el valor de ese parámetro a NONE. Todavía puede utilizar DQM 255 en cualquier etiqueta UMF <NAME> para estandarizar los nombres.

Es aconsejable que también compruebe las configuraciones siguientes en la Consola de configuración:

- Asegúrese de que la característica de género se ha configurado como una confirmación o denegación en la resolución de entidades por origen de datos. Vea o configure este valor en el campo **Uso de resolución** que se encuentra seleccionando **Configurar** > **Orígenes** > **Características**.
- Asegúrese de que la característica de género se ha configurado con los valores de ajuste correctos para la resolución de entidades. Vea o configure este valor seleccionando **Configurar** > **Resolución** > **Características**. Compruebe los valores de los pesos de confirmación y denegación asignados a la característica de género para estar seguro de que se ajustan a las necesidades empresariales.

.

Examine el segmento de ejemplo <NAME> siguiente en este registro UMF de entrada:

```
<UMF_ENTITY>
 <NAME>
    <NAME_TYPE>M</NAME_TYPE>
  <LAST_NAME>RASUL</LAST_NAME>
  <FIRST_NAME>KARIM</FIRST_NAME>
  </NAME>
.....
</UMF_ENTITY>
```

Si DQM 258 se ha activado en el código UMF <FIRST_NAME> del segmento <NAME>, el registro UMF de entrada se parece al registro siguiente después de que se analice y se cree el género:

```
<UMF_ENTITY>
 <NAME>
    <NAME_TYPE>M</NAME_TYPE>
  <LAST_NAME>RASUL</LAST_NAME>
  <FIRST_NAME>KARIM</FIRST_NAME>
  </NAME>
 <ATTRIBUTE>
  <ATTR_TYPE>GENDER</ATTR_TYPE>
  <ATTR_VALUE>M</ATTR_TYPE>
 </ATTRIBUTE>
.....
</UMF_ENTITY>
```

Configuración de nombres para asignar género:

Mediante la asignación de género basándose en un nombre, puede mejorar la resolución de entidades. Puede establecer puntuaciones de confirmación y denegación basándose en si el género de las entidades comparadas es el mismo. Puede configurar nombres para asignar dinámicamente el género y añadir la característica de género a los registros UMF de entrada.

Antes de empezar

- Asegúrese de que Name Manager está activado y que la vía de acceso a los archivos de soporte de Name Manager está establecida en los parámetros de sistema. Si esta función DQM se habilita sin una vía de acceso válida a los archivos de soporte de Name Manager, la interconexión registra un error y concluye.
- Cuando se habilita la característica de género de esta función DQM, se está cambiando la configuración del sistema. Al igual que con cualquier cambio de configuración, asegúrese de detener las interconexiones activas antes de cambiar la configuración. A continuación, reinicie las interconexiones para reinicializarlas con los cambios de configuración.

Acerca de esta tarea

- Para las instalaciones nuevas de productos de la V8.0 fixpack 2 o posterior, esta función DQM ya está configurada y activa.
- Para versiones actualizadas de producto a partir de la V8.0 fixpack 2 o posterior, esta función DQM está configurada pero está inactiva. Para utilizar esta funcionalidad de género mejorada, cambie el estado de la función DQM existente a **Activa**. Si ha asignado anteriormente género utilizando el parámetro **Tipo de característica de género** de la función DQM 255, restablezca el valor de ese parámetro a NONE. Todavía puede utilizar DQM 255 en cualquier etiqueta UMF <NAME> para estandarizar los nombres.

Procedimiento

1. En la Consola de configuración, seleccione **Configurar** > **UMF** > **Reglas DQM**.
2. Seleccione **NAME** en la lista **Segmento**.
3. Seleccione el nombre de etiqueta UMF de **FIRST_NAME** que también lista **258 - Generador de género de nombres** como **Función**. Esta configuración sólo evalúa el primer nombre en el registro de entrada para nombres personales. Si la característica de categorizar nombres de Name Manager está activada, debe especificar el nombre completo en la etiqueta `LAST_NAME` UMF del segmento `NAME`.
4. En **Estado**, asegúrese de que **Activo** está seleccionado.
5. En **Filtro de norma**, asegúrese de que `NAME_TYPE=M` es el valor de campo. Este valor garantiza que sólo se evalúe el nombre principal para cada registro de entrada para asignar el género.
6. En la pestaña **Parámetros**, asegúrese de que la **Puntuación mínima de confianza de género** está establecida en un número entre 0 y 100. La puntuación predeterminada está establecida en 90, lo que significa que el género no está asignado a menos que haya un 90% de confianza en la asignación de género. Tenga cuidado con bajar esta puntuación, porque una puntuación mínima por debajo de 90 puede afectar a la resolución de entidad durante la confirmación o denegación de género.
7. Pulse **Guardar**.

Categorización de nombres

Si el parámetro de sistema de Name Manager **`NAMESIFTER`** está habilitado, el producto categoriza los nombres por tipo. Al categorizar los nombres por tipo, la resolución de entidad puede aplicar los recursos de datos de referencia y de lingüística apropiados durante el análisis, la puntuación y la coincidencia de nombres:

Los nombres se categorizan en tipos de nombres personales o de organización.

Nombres personales
: Un nombre personal no contiene indicadores que sugieran que pertenece a ninguna otra categoría. (Por ejemplo: "Linda K. Smith".) Los nombres que se categorizan como nombres personales se analizan en partes de nombre. Entonces las partes de nombre se categorizan por cultura, que añade precisión al proceso de análisis y de puntuación.

Nombres de organización
: Un nombre de empresa u organización contiene alguna forma de indicador no personal. (Por ejemplo, "Smith & Company".) A los nombres que se categorizan como nombres de organización se les asigna automáticamente una cultura de "empresa"

Nombres desconocidos
: Un nombre categorizado como "Desconocido" contiene algún elemento que parece ser un error ortográfico o alguna otra construcción que no suele aparecer en nombres personales o de empresa. (Por ejemplo "SMI".)

Categorización de nombres por tipo:

Uno de los parámetros de sistema de Name Manager (**`NAMESIFTER`**) incluye la posibilidad de categorizar nombres por tipo. Los tipos de nombre más comunes son personal y empresarial. La categorización de nombres puede hacer que la parte de análisis y evaluación de nombre del proceso de resolución de entidades sea más precisa.

Categorización de nombres personales por cultura:

La función DQM 260 se ha creado para determinar la cultura del nombre y añadir dicho valor al segmento UMF <NAME>. De forma predeterminada, la configuración de segmento <NAME> incluye una regla DQM 260 en el código UMF <LAST_NAME>. Utilice estas instrucciones para añadir la regla DQM 260 a otro código UMF en el segmento <NAME> o para actualizar la regla existente en el código UMF <LAST_NAME>

Visión general de Name Manager

Name Manager

Name Manager aumenta la precisión de los nombres en caso de problemas avanzados de confirmación de nombres, por ejemplo múltiples transliteraciones de nombres, errores ortográficos en culturas, variaciones de ortografía en culturas y entre culturas, y nombres que utilizan designaciones honoríficas o patronímicas. Utiliza las bibliotecas del componente IBM InfoSphere Global Name Recognition, que contiene una base de conocimiento de más de 1.000.000.000 nombres multiculturales e información lingüística exclusiva, que añade prestaciones de coincidencias de nombres específicas de cultura.

Nombres de puntuaciones de Name Manager que utilizan el siguiente proceso:

- Categoriza nombres por tipo de nombre (personal o empresarial)
- Analiza nombres personales en partes de nombre
- Clasifica nombres por cultura (soporta más de 20 culturas, incluidos el afgano, árabe, farsi, han, japonés, coreano, tailandés, vietnamita y yoruba)
- Normaliza nombres personales (si el nombre se clasifica como anglo, árabe, chino, francés, alemán, hispano, indio, coreano, ruso o tailandés)

Configuración de Name Manager

De forma predeterminada, la puntuación de nombre de Name Manager ya está habilitada y configurada al instalar IBM InfoSphere Identity Insight. Sin embargo, puede utilizar la Consola de configuración para revisar o cambiar los valores de configuración de Name Manager, incluidos los valores siguientes:

- Parámetros de sistema de Name Manager, incluida la vía de acceso de soporte a las bibliotecas de componente de Name Manager (parámetros globales que la interconexión utiliza para realizar la resolución de entidad)
- Umbrales de puntuación de nombres de Name Manager utilizados durante la coincidencia de nombres (confirmaciones y denegaciones)

Configuración de parámetros de sistema para Name Manager:

De forma predeterminada, los parámetros de sistema de puntuación de nombres de Name Manager se configuran al instalar el producto. Pero puede actualizar los parámetros de sistema predeterminados, cuando sea necesario. Por ejemplo, puede que necesite cambiar la ubicación de las bibliotecas de soporte de Name Manager.

Acerca de esta tarea

Establezca la vía de acceso en las bibliotecas de soporte de Name Manager y habilite la categorización de nombres por tipo mediante los parámetros de sistema de Name Manager. Establezca también el parámetro de sistema **CROSSCHECKCULTURE** para configurar el proceso de nombres entre distintas culturas de nombres.

Procedimiento

1. En la Consola de configuración, seleccione **Configurar** > **General** > **Parámetros del sistema**.
2. En la lista **Grupo de parámetros**, seleccione el grupo de parámetros **NAMEMANAGER**.
3. En el panel izquierdo, seleccione el parámetro de sistema de Name Manager que desea configurar:

parámetro del sistema de Name Manager	Descripción
SUPPORTPATH	Indica la ubicación de los archivos de soporte de Name Manager. El valor predeterminado es ./data, que es una vía de acceso relativa al directorio de producto de nivel superior. Si los archivos de soporte se mueven a una ubicación distinta durante la instalación, modifique este valor a la vía de acceso absoluta de la nueva ubicación.
NAMESIFTER	Indica si la funcionalidad de categorización de nombres por tipo de nombre (nombres personales u organización) está activada. Para habilitar la categorización de nombres de tipo (funcionalidad Tamiz de nombres), entre 1 (nuevo valor predeterminado de instalación) en **Valor actual** Para inhabilitar la categorización de nombres de tipo (funcionalidad de Tamiz de nombres), entre 0 (valor predeterminado de actualización) en **Valor actual**
CROSSCHECKCULTURE	Indica si se debe realizar la puntuación de nombres de Name Manager entre culturas de nombre cuando las culturas de nombre son diferentes. Para comprobar solo la cultura de nombre de entrada antes de puntuar ambos nombres, especifique 0 en **Valor actual**. Para comprobar los valores de cultura de nombre antes de puntuarlos (nuevo valor predeterminado de instalación), escriba 1 en **Valor actual**.

Atención: El parámetro de sistema **CROSSCHECKCULTURE** afecta a la manera en que la resolución de entidad maneja la puntuación de nombres por cultura en las interconexiones. Antes de cambiar este parámetro de sistema respecto a su valor actual, consulte los servicios o el soporte de IBM.

4. Pulse **Guardar**.

Configuración de umbrales de Name Manager para confirmaciones y denegaciones:

Puede establecer los umbrales de puntuación de nombres que Name Manager utiliza durante la resolución de entidad por regla de resolución. Después de que se haya creado la lista de candidatos, la resolución de entidades compara la puntuación de nombres de Name Manager, basándose en la parte de nombre y la

cultura determinada para cada parte de nombre, con estos umbrales. Si la puntuación de Name Manager cumple o supera la puntuación de umbral configurado para la parte de nombre, los nombres se consideran una coincidencia.

Acerca de esta tarea

Importante: De forma predeterminada, los umbrales de puntuación de partes de nombre de Name Manager están configurados para la puntuación y el rendimiento óptimos de Name Manager. El cambio de los valores predeterminados es una tarea de configuración avanzada, porque estos valores pueden afectar negativamente la resolución de entidades para reglas que incluyen la puntuación de nombres. Antes de cambiar estos valores predeterminados, consulte los servicios o el soporte de IBM.

Procedimiento

1. En la Consola de configuración, seleccione **Configurar** > **Resolución** > **Normas de resolución**
2. Seleccione la configuración de resolución en la lista **Config resolución**.
3. Seleccione la norma de resolución.
4. Pulse **Umbrales de Confirmar/Denegar**.
5. En **Name Manager**, especifique la puntuación mínima para cada umbral de parte de nombre, basándose en una puntuación de 0,0 a 1,0. Cuanto más alta es la puntuación, más exactas deben ser las partes de nombre para coincidir. Normalmente, una puntuación por debajo de 0,7 no se considera adecuada para coincidir con las partes de nombre.

Puntuación de nombre de Name Manager:

El algoritmo de Name Manager puntúa los datos de nombre de entrada basándose en la agrupación del nombre en partes de nombre y luego en la determinación de la cultura para cada parte de nombre. A continuación, el algoritmo puntúa cada parte de nombre y las puntuaciones resultantes se utilizan durante la resolución de entidades.

Mientras que el algoritmo de Name Manager es independiente de los algoritmos de comparador de nombres (NC1 y NC2), debe seleccionar de todas formas NC1 o NC2. Durante el proceso de resolución de entidades, los nombres se puntúan primero basándose en los algoritmos de comparador de nombres seleccionado. Si nombre puntúa una coincidencia exacta, la resolución de entidades se salta la puntuación de Name Manager, porque la coincidencia de nombre exacta satisface la parte de puntuación de nombre de la norma de resolución. Sin embargo, si el nombre de entrada puntúa menos de una coincidencia exacta, el proceso de resolución de entidades puntúa el nombre utilizando el algoritmo de Name Manager.

En primer lugar, el algoritmo analiza el nombre en partes de nombre (nombre, apellido y nombre completo) y, a continuación, el algoritmo determina la cultura para cada parte de nombre. Finalmente, el algoritmo asigna a cada parte de nombre una puntuación y compara las puntuaciones con los umbrales de puntuación de Name Manager configurados para determinar hasta qué punto coinciden los nombres. Cuando más alto se establece el umbral de puntuación, mayor deber la coincidencia de las partes de nombre de los datos de nombre de entrada con las partes de nombre de la entidad existente en la base de datos de entidades.

Selección de culturas para la puntuación de nombres de Name Manager:

Puede configurar los métodos de puntuación de nombres utilizados por la cultura durante el proceso de puntuación de nombres de resolución de entidad. Name Manager sólo puede determinar la cultura de nombres y puntar los nombres para las culturas configuradas para utilizar la coincidencia de nombres de Name Manager.

Acerca de esta tarea

De forma predeterminada, cada cultura soportada ya está configurada basándose en las mejores prácticas más recientes para la puntuación de nombres típica. El cambio de los valores predeterminados es una tarea avanzada que puede afectar negativamente a la resolución de entidades para reglas que incluyen la puntuación de nombres. Consulte el soporte o los servicios de IBM antes de cambiar los valores de configuración predeterminados.

Procedimiento

1. En la Consola de configuración, seleccione **Configurar** > **Resolución** > **Configurar coincidencia de Name Manager**.
2. Seleccione una cultura de Name Manager.
3. En **Utilizar coincidencia de nombres de Name Manager**, seleccione Sí
4. Pulse **Guardar**.

Configuración de reglas DQM

Puede configurar reglas DQM para reparar o limpiar datos que no satisfacen los estándares mínimos de calidad de datos. Las reglas DQM se aplican a un código UMF específico en un segmento UMF específico.

Acerca de esta tarea

Las reglas DQM pueden verse y modificarse utilizando la consola en la pestaña **Reglas DQM**.

Reglas DQM

Las reglas DQM son funciones de reparación, limpieza y estandarización configuradas y definidas por el sistema que se aplican a los valores de datos de identidades de entrada en un orden específico.

Las reglas DQM definen el modo en que el sistema procesa los datos de entrada y están diseñadas para formatear correctamente números, identificar y corregir errores clericales o de transposición e identificar las imprecisiones intencionadas incorporadas por aquellos que intentan ocultar sus identidades. Las reglas DQM pueden realizar diversas funciones de reparación, limpieza y estandarización sobre valores de datos de identidades de entrada.

Para configurar una regla DQM, debe seleccionar un segmento UMF específico (como por ejemplo UMF) y un código UMF (como NAME_TYPE), luego debe seleccionar una función DQM definida por el sistema para aplicar a loa datos de entrada y finalmente debe especificar los parámetros asociados correspondientes a dicha función, incluidos los valores predeterminados que debe aplicar el sistema. Debe elegir el orden en el que se debe aplicar esta regla DQM en el segmento UMD seleccionado, puesto que el producto da soporte a varias reglas DQM para cada segmento UMF.

Visualización de reglas DQM

Las reglas DQM reparan o limpian datos que no satisfacen los estándares mínimos de calidad de datos.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Reglas DQM**.
4. En la lista desplegable **Segmento**, seleccione el segmento UMF que contiene las reglas DQM que se deben visualizar.

Creación de reglas DQM

Las reglas DQM se crean para reparar o limpiar datos que no satisfacen los estándares mínimos de calidad de datos.

Acerca de esta tarea

Las reglas DQM se aplican a un código UMF específico en un segmento UMF específico. Las reglas DQM también se pueden clonar para crear la base para una nueva regla.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Reglas DQM**.
4. En la lista desplegable **Segmento**, seleccione el segmento UMF para el que se debe crear una regla DQM.
5. Complete uno de los pasos siguientes:
   - Para crear una nueva regla DQM, pulse el botón **Nuevo**.
   - Para crear una regla DQM basándose en una regla DQM existente, seleccione una regla DQM en la lista y, después, pulse el botón **Clonar**.
6. En el panel **General**, especifique el orden, el nombre de código UMF, la función, el filtro de regla, la exclusión de UMF, si es corregible, el estado y otra información de configuración para la regla DQM.
7. En el panel **Parámetros**, especifique los parámetros para la regla DQM.
8. Pulse el botón **Guardar**.
9. Valide la regla DQM.

Supresión de reglas DQM

Cuando ya no necesite la regla DQM, debe suprimirla.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Reglas DQM**.
4. En la lista desplegable **Segmento**, seleccione el segmento UMF para el que desea suprimir una regla DQM.
5. Marque el recuadro o recuadros de selección situados junto a la regla o reglas DQM que desea suprimir.
6. Pulse el botón **Suprimir**.

Validación de reglas DQM

Cuando añada o edite una regla DQM, debe validarla antes de aplicar la regla DQM a los datos de origen.

Acerca de esta tarea

La función de validación se utiliza para validar todas las reglas, en relación las unas con las otras, para todo un segmento. La validación que se puede realizar en una sola regla, se efectúa automáticamente cuando se guarda la regla.

Al iniciar la sesión en la Consola de configuración, se realiza una validación automática para ver si las reglas DQM son válidas. Si se encuentra un error, se visualizará un mensaje de cabecera en la parte superior de la pantalla de la Consola de configuración. Pulse el enlace **Revisar los errores** para abrir una nueva ventana que describa los errores.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Reglas DQM**.
4. En la lista desplegable **Segmento**, seleccione el segmento UMF para el que se debe validar una regla DQM. Si no se selecciona ningún segmento, la validación se realizará en todos los segmentos.
5. Pulse el botón **Validar**.

Desactivación de reglas DQM

Puede desactivar una regla DQM que ya no se necesite.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Reglas DQM**.
4. En la lista desplegable **Segmento**, seleccione el segmento UMF deseado que contenga la regla DQM que se debe desactivar.
5. Pulse la regla DQM que se debe desactivar.
6. En el panel **General**, establezca el campo de estado en **Inactivo**.
7. Pulse el botón **Guardar**.

Temas de ayuda

Reglas DQM - Panel General:

Utilice el panel **General** para especificar los detalles de la regla DQM.

Segmento
Escriba el nombre del segmento UMF en el que se va a aplicar la regla DQM. Generalmente este campo será de solo lectura. Sólo se puede editar si la lista desplegable **Segmento** se ha dejado en blanco al crear una nueva regla DQM. El nombre del segmento se debe especificar en mayúsculas.

Orden Escriba el número de orden en el que se aplicará la regla DQM.

Nombre de código UMF
Escriba el nombre del código UMF que se aplicará a la regla DQM. El nombre del código UMF se debe especificar en mayúsculas.

Función
En la lista desplegable, seleccione la función DQM en la que desea basar la regla DQM.

Descripción de la función
El campo de descripción de la función es un campo de sólo lectura que describe lo que hace la regla DQM.

Filtro de regla
Si desea que la regla DQM sólo se aplique si el código UMF contiene un valor específico, especifique una ecuación que incluya el nombre del código UMF y el valor necesario para ejecutar la regla DQM.

Por ejemplo: `NAME_TYPE=m`
Este valor de ejemplo sólo aplica la regla DQM si el valor del código `NAME_TYPE` es `m`.

Excluir UMF
Si desea que la regla DQM no se aplique a determinados documentos de entrada UMF, especifique una lista delimitada por comas de documentos de entrada UMF para los que no se deba ejecutar esta regla.

Por ejemplo: `UMF_QUERY, UMF_DISCLOSED RELATION`
El valor de ejemplo no aplicará la regla DQM únicamente a los documentos de entrada UMF `UMF_QUERY` o `UMF_DISCLOSED_RELATION`.

Corregible
En la lista desplegable, seleccione **Sí** para ajustar valores no válidos o subestándar. De lo contrario, seleccione **No**.

Los parámetros de cada regla DQM determinan cómo se ajustan los valores de datos subestándar.

Estado
En la lista desplegable, seleccione **Activo** para especificar que esta regla DQM está activa. De lo contrario, seleccione **Inactiva**.

Configuración de códigos de búsqueda

Los códigos de búsqueda son valores predeterminados utilizados por diversas funciones de la aplicación.

Los códigos de búsqueda se clasifican por tipos de códigos. Se puede utilizar la regla DQM 190 para validar que los códigos de búsqueda de entrada forman parte de un tipo de código definido o para añadirlos a dicho tipo de código si falta.

Visualización de códigos de búsqueda

Los códigos de búsqueda son valores predeterminados utilizados por diversas funciones de la aplicación.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Códigos**.
4. En la lista desplegable **Tipo**, seleccione el tipo de valores de código de búsqueda que desea visualizar.

Creación de códigos de búsqueda

Los códigos de búsqueda son valores predeterminados utilizados por diversas funciones de la aplicación.

Acerca de esta tarea

Puede crear un código de búsqueda nuevo, o puede crear un código de búsqueda basado en un código de búsqueda existente.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Códigos**.
4. En la lista desplegable **Tipo**, seleccione el tipo de valores de código de búsqueda que desea crear. Para crear un tipo de código completamente nuevo, deje el valor tal cual.
5. Complete uno de los pasos siguientes:
   - Para crear un nuevo código de búsqueda, pulse el botón **Nuevo**.
   - Para crear un código de búsqueda basado en un código de búsqueda existente, seleccione un código de búsqueda en la lista y, después, pulse el botón **Clonar**.
6. En el panel **General**, especifique el tipo (será un campo de sólo lectura si ya se ha especificado en la lista desplegable **Tipo**), el código, la descripción, el estado y otra información de configuración para este código de búsqueda.

Supresión de códigos de búsqueda

Puede suprimir los códigos de búsqueda creados por el usuario que ya no se utilicen.

Acerca de esta tarea

No debe suprimir los códigos de búsqueda predeterminados del sistema ya que son necesarios para varios componentes del producto.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Códigos**.
4. En la lista desplegable **Tipo**, seleccione el tipo de valores de código de búsqueda que desea suprimir.
5. Seleccione un código de búsqueda en la lista y, después, pulse el botón **Suprimir**.

Desactivación de códigos de búsqueda

Puede desactivar un código de búsqueda que ya no se necesite.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Códigos**.
4. En la lista desplegable **Tipo**, seleccione el tipo de valores de códigos de búsqueda que desea desactivar.
5. Seleccione un código de búsqueda en la lista.
6. En el panel **General**, establezca el campo de estado en **Inactivo**.
7. Pulse el botón **Guardar**.

Temas de ayuda

Códigos de búsqueda - Panel General:

Utilice el panel **General** para especificar los detalles del código de búsqueda.

Tipo Escriba el tipo de código de búsqueda bajo el que agrupar el código de búsqueda. Este campo será de solo lectura una vez especificado. Sólo se puede editar si el desplegable **Tipo** se ha dejado sin especificar al crear un nuevo código de búsqueda.

Código
Escriba el valor que estará disponible como valor predeterminado del código de búsqueda. Suele ser un valor que se utiliza realmente en códigos UMF y que se almacena en tablas de base de datos. Cuando se editan códigos de búsqueda existentes, este campo es de sólo lectura.

Descripción
Escriba la descripción del código de búsqueda.

Estado
En la lista desplegable, seleccione **Activo** para especificar que este código de búsqueda está activo. De lo contrario, seleccione **Inactiva**.

Códigos de búsqueda - Campo Tipo:

Utilice el campo **Tipo** para especificar el tipo bajo el que agrupar el código de búsqueda.

ADDR_STAT
Este tipo de código de búsqueda se utiliza para valores de estado de direcciones. Estos valores se pueden utilizar para marcar direcciones particulares con información, como por ejemplo si es una dirección en la que se pueden realizar entregas.

ADDR_TYPE
Clasificaciones de direcciones que puede definir el usuario. Son los valores válidos correspondientes al código UMF `ADDR_TYPE`.

ANALYZER_GROUP
Este tipo de código de búsqueda lo utilizan las reglas de alerta de rol y el Visualizador. Cualquier nuevo código de búsqueda con el tipo ANALYZER_GROUP constituye una opción disponible en el menú desplegable **Grupo de alertas** del panel **Configuración** > **Relaciones** > **Reglas de alerta de rol** > **General** y en el menú desplegable **Grupo** del panel **Configuración** > **Visualizador** > **Usuarios del Visualizador** > **General**.

ATTR_CLASS
Clasificaciones de tipos de características que puede definir el usuario. Los valores aquí especificados aparecen como opciones en el menú desplegable **Clase** del panel **Configuración** > **Orígenes** > **Características** > **General**. Las características que utilizan el código de búsqueda LINK para su clase de atributo se pueden mostrar como un enlace HTML en el Visualizador si el valor de la característica sigue este formato:

Link Display Text=URL

ATTR_MATCH_LEVEL
Este tipo de código de búsqueda ha quedado obsoleto.

CONF_LEVEL
Este tipo de código de búsqueda ha quedado obsoleto.

DENSITY_LOG_LEVEL
Este tipo de código de búsqueda ha quedado obsoleto.

DOC_TYPE
Este tipo de código de búsqueda ha quedado obsoleto.

DSRC_ACTION
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

EX_CLASS
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

EX_SEVERITY
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

LOG_LEVEL
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

ER_LEVEL
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

ER_LOG_LEVEL
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

LDR_MESSAGE_TYPE
Este tipo de código de búsqueda ha quedado obsoleto.

MM_STAT
Este tipo de código de búsqueda ha quedado obsoleto.

NAME_TYPE
Este tipo de código de búsqueda se utiliza para almacenar clasificaciones de nombres que puede definir el usuario. Estos son los valores válidos para el código UMF `NAME_TYPE`.

NS-FGEN
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

NS-LGEN
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

NS-PREFIX
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

NS-SUFFIX
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

NUM_CLASS
Este tipo de código de búsqueda se utiliza para almacenar clasificaciones de tipos de números de que puede definir el usuario. Los valores aquí

especificados aparecen como opciones en el menú desplegable **Clase** del panel **Configuración** > **Orígenes** > **Números** > **General**.

REC_STAT
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

SEARCH_REASON
Este tipo de código de búsqueda lo utiliza el Visualizador para una lista de opciones desplegables para el campo de razón de búsqueda de la alerta de atributo. Los usuarios pueden añadir aquí su propia lista de razones válidas para una alerta de atributo.

SYS_DELETE_STAT
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

UNIQUE_FLAG
Este tipo de código de búsqueda ha quedado obsoleto.

USABILITY_LOG_LEVEL
Este tipo de código de búsqueda lo utiliza el sistema y no se debe modificar.

Configuración de valores de datos genéricos

Puede configurar valores de datos para que sean genéricos si exceden de un número de ocurrencias configurado en la base de datos de entidades.

Valores genéricos

Los valores genéricos describen valores de datos que aparecen repetidamente en la base de datos de entidades y, como resultado, el sistema ya no los utiliza para resolver entidades.

Los valores de datos se consideran genéricos después de superar un determinado umbral. El umbral es un número máximo de apariciones de entidades en la base de datos de entidades que pueden compartir el valor de datos.

Los valores genéricos se organizan y se configuran mediante un atributo y un tipo de atributo. El valor de datos genérico de un tipo de atributo específico prevalece sobre el valor de datos genéricos del atributo padre. Los elementos de datos estándar cuyos valores se consideran genéricos son:

- Dirección
- Característica
- Correo electrónico
- Nombre
- Número

Ejemplo

Si el umbral genérico correspondiente a números de teléfono se establece en 25, cuando un valor de número de teléfono (por ejemplo, 555-555-5555) es el valor de número de teléfono de más de 25 entidades, a partir de este momento dicho valor específico se deja de utilizar para resolver entidades.

Nota: Cuando vaya a decidir el valor que se debe atribuir a umbrales genéricos, tenga en cuenta que un valor demasiado alto puede dar lugar a que el rendimiento del sistema se vea desbordado por un exceso de datos que deberían ser genéricos.

Por el contrario, si el valor del umbral genérico es demasiado bajo, es posible que no se generen alertas importantes porque criterios clave se consideren genéricos.

Visualización de valores de datos genéricos

Los valores de datos genéricos son umbrales genéricos para cada elemento de datos que desee considerar genérico. Puede que desee ver los genéricos existentes cuando añada un nuevo origen de datos.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Umbral genérico**.

Configuración de valores de datos genéricos

Para que se pasen por alto los valores genéricos durante la resolución de entidades, debe configurar el umbral genérico para el elemento de datos.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Umbral genérico**.
4. Complete uno de los pasos siguientes:
   - Para crear un nuevo valor de datos genérico, pulse el botón **Nuevo**.
   - Para crear un valor de datos genérico basado en un valor de datos genérico existente, seleccione un valor de datos genérico en la lista y, a continuación, pulse el botón **Clonar**.
5. En el panel **General**, especifique el atributo, el tipo de atributo y el valor de umbral del valor genérico.
6. Pulse el botón **Guardar**.

Supresión de valores de datos genéricos

Los valores de datos genéricos son umbrales genéricos para cada elemento de datos que desee considerar genérico. Es posible que desee suprimir los genéricos existentes cuando ya no sean importantes para los datos de entrada.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Umbral genérico**.
4. Marque el recuadro de selección situado junto a cualquier nombre de elemento existente que desee suprimir.
5. Pulse el botón **Suprimir**.

Temas de ayuda

Umbral genérico - Panel General:

Utilice el panel **General** para especificar los detalles del valor de los datos genéricos.

Nombre de atributo

En la lista desplegable, seleccione el atributo al que desea aplicar el valor de datos genéricos.

Tipo de atributo
En la lista desplegable, seleccione el tipo de atributo al que desea aplicar el valor de datos genéricos.

Esta lista desplegable sólo tendrá varias opciones si el campo **Nombre de atributo** está establecido en Nombre o Característica.

Umbral
Escriba el número de entidades que pueden compartir un valor UMF del tipo configurado para que se considere genérico.

Configuración de roles

Puede configurar roles para clasificar entidades en la base de datos de entidades. Los roles se pueden asignar a orígenes de datos o entidades. Los roles en conflicto generan alertas.

Acerca de esta tarea

Los roles pueden verse y modificarse utilizando la consola, en la pestaña **Orígenes de datos**.

Roles

Un rol es una clasificación de una identidad que define el objetivo de dicha identidad. Puede asociar uno o varios roles a una identidad. Cuando las identidades se resuelven en entidades, estas heredan todos los roles asociados.

Se utilizan roles para configurar reglas de alerta, que definen las relaciones interesantes y generan alertas.

A cada identidad se le asigna un rol de una de estas formas:

Por origen de datos de entrada
Cuando se configura una nuevo origen de datos, se asocia un rol a dicho origen de datos, la cual asignará dicho rol a todas las identidades que contengan dicho código de origen de datos.

Por UMF
Cuando se transforma el origen de datos a UMF (Universal Message Format), se pueden asignar directamente roles como parte del registro UMF mediante el segmento UMF <SEP_ROLES> con el código UMF <ROLE_CODE>. Si configura por UMF, se tendrán que añadir reglas DQM y una tabla de búsqueda.

Ejemplos de roles útiles pueden incluir empleados, proveedores, clientes o lista de vigilancia.

Ejemplo de asignación de roles mediante UMF

Para asignar el rol de empleado a un registro de identidad mediante UMF, debe entrar el siguiente segmento UMF <SEP_ROLES> y el siguiente código UMF <ROLE_CODE> para el registro de la identidad:

```
<SEP_ROLES>

    <ROLE_CODE>Employee</ROLE_CODE>

</SEP_ROLES>
```

Visualización de roles

Un rol define cómo se clasifica o conoce una entidad en el sistema. Puede que desee ver los roles existentes si piensa añadir un nuevo rol.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Relaciones**.
3. Pulse la pestaña **Códigos de rol**.
4. Seleccione el rol que desea visualizar.

Creación de roles

Para definir cómo las entidades se relacionan con otras entidades, cree roles en el sistema.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Relaciones**.
3. Pulse la pestaña **Códigos de rol**.
4. Complete uno de los pasos siguientes:
   - Para crear un nuevo rol, pulse el botón **Nuevo**.
   - Para crear un rol basándose en un rol existente, seleccione un rol en la lista y, después, pulse el botón **Clonar**.
5. En el panel **General**, especifique el código de rol, la descripción, la clase, el estado y otra información de configuración para el nuevo rol.
6. Pulse el botón **Guardar**.

Qué hacer a continuación

Puede utilizar este rol al definir las reglas de alertas de rol.

Supresión de roles

Un rol define cómo se clasifica o conoce una entidad en el sistema. Es posible que desee suprimir un rol existente si ya no es válido.

Acerca de esta tarea

No puede suprimir un rol que una regla de alertas de rol o un origen de datos esté utilizando.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Relaciones**.
3. Pulse la pestaña **Códigos de rol**.
4. Marque el recuadro de selección situado junto a cualquier rol existente que desee suprimir.
5. Pulse el botón **Suprimir**.

Temas de ayuda

Roles - Panel General:

Utilice el panel **General** para especificar los detalles del rol.

ID Escriba un entero exclusivo que identifique el ID del rol.

El valor del ID se llena automáticamente con el siguiente número secuencial no utilizado.

Código de rol
Escriba un valor exclusivo para identificar este rol.

Descripción
Escriba una descripción para este rol.

Clase de rol
Escriba una clase para este rol.

Estado
En la lista desplegable, seleccione **Activo** para especificar que el rol está activo. De lo contrario, seleccione **Inactiva**.

Configuración de reglas de alertas de rol

Puede configurar reglas de alertas de rol para definir una combinación de roles que, cuando se detectan, generan alertas.

Acerca de esta tarea

Las reglas de alerta de rol pueden verse y modificarse utilizando la Consola, en la pestaña **Reglas de alerta de rol**.

Alerta de rol

Una alerta de rol se define en el sistema mediante una regla de alerta de rol que representa relaciones que se utilizan para generar alertas.

Las reglas de alerta de rol definen una combinación de roles que, cuando se detectan en una relación o entidad, indican alguna forma de conflicto. Por ejemplo, una regla de alerta de rol puede indicar que cada vez que una entidad con el rol Empleado conoce una entidad con el rol Proveedor, existe una alerta de rol. Esta regla de alerta de rol se puede describir como "Empleado conoce Proveedor". Cuando el sistema encuentra alertas de rol en entidades o relaciones, se crean alertas que se pueden publicar en la empresa y ver en las aplicaciones del kit de herramientas de analista.

Aunque la mayoría de las reglas de alerta de rol especifican una combinación de dos roles diferentes que indican un conflicto, también es válido tener una regla de alerta de rol en la que una entidad de un rol conoce a otro entidad del mismo rol. Por ejemplo, es posible que desee conocer cualquier relación entre sus clientes y crear una regla de alerta de rol que genere una alerta de rol cada vez que la entidad de un cliente se relacione con la entidad de otro cliente. Esta regla de alerta de rol se puede describir como "cliente conoce cliente".

Las reglas de alerta de rol se basan en códigos de rol existentes. Se deben definir roles para poder crear reglas de conflicto basadas en esos roles.

Visualización de reglas de alertas de rol

Las reglas de alertas de rol se utilizan para generar alertas cuando se detecta una relación entre dos roles definidos. Puede que desee ver las reglas de alertas de rol existentes cuando piense añadir una nueva regla de alertas de rol.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Relaciones**.
3. Pulse la pestaña **Reglas de alertas de rol**.
4. Seleccione la regla de alertas de rol que desea ver.

Configuración de reglas de alertas de rol

Configure reglas de alertas de rol para generar alertas de rol o relaciones entre dos roles o identidades.

Antes de empezar

Antes de definir una regla de alertas de rol, configure los roles que desee utilizar en la regla de alertas de rol. Por ejemplo, si desea configurar una regla de alerta de rol donde un empleado no pueda ser proveedor, el sistema debe contener los roles "Empleado" y "Proveedor".

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **Relaciones**.
3. Pulse la pestaña **Reglas de alertas de rol**.
4. Complete uno de los pasos siguientes:
   - Para crear una nueva regla de alertas de rol, pulse el botón **Nuevo**.
   - Para crear una regla de alertas de rol basándose en una regla de alertas de rol existente, seleccione una regla de alertas de rol en la lista y, después, pulse el botón **Clonar**.

   El campo **ID de regla de alertas de rol** se llena automáticamente con el siguiente ID exclusivo. Puede cambiarlo por cualquier número de ID exclusivo.
5. Pulse el botón **Nuevo**.
6. En el panel **General**, especifique el ID, la descripción, la gravedad, los códigos de rol, el grupo de alertas y el umbral mínimo de alerta para esta regla de alertas de rol.
7. En el panel **Filtros**, especifique opcionalmente el filtro de identidad, el filtro de cambio de datos y el ajuste de resistencia de vía de acceso (sólo aparece si el campo de filtro de cambio de datos se establece en Ajuste de resistencia de vía de acceso). Si se establecen ambos filtros, sólo se tiene que satisfacer uno para generar una alerta de rol.
8. Pulse el botón **Guardar**.

Supresión de reglas de alertas de rol

Una regla de alertas de rol se debe suprimir cuando se suprime un rol definido en la regla de alertas de rol, o cuando la combinación de roles de la regla de alertas de rol ya no tiene interés.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Relaciones**.
3. Pulse la pestaña **Reglas de alertas de rol**.
4. Marque el recuadro de selección situado junto a la regla de alerta de rol existente que desea suprimir.
5. Pulse el botón **Suprimir**.

Temas de ayuda

Reglas de alertas de rol - Panel General:

Utilice la pestaña **General** de la ventana **Reglas de alerta de rol** para configurar los detalles de las reglas de alerta de rol. Los roles se asocian con orígenes de datos. En función de la configuración del origen de datos, se asigna un rol a todas las entidades que se introducen en el sistema procedentes de un origen de datos. Las reglas de alerta de rol definen cuando se debe generar una alerta de rol, basándose en un conflicto entre los roles asignados a las entidades entrantes y las entidades asociadas con entidades de la base de datos de entidades.

ID de regla de alerta de rol
El valor del ID se llena automáticamente con el siguiente número secuencial no utilizado.

Descripción
Escriba una descripción para esta regla de alerta de rol. Este texto se muestra en el Visualizador siempre que se genera una alerta de rol basándose en esta regla de alerta de rol.

Gravedad
Un código de un solo carácter definido por el usuario que se utiliza para clasificar la prioridad de las alertas generadas a partir de esta regla.

La gravedad de la alerta de rol debe coincidir con su importancia. Este código se muestra con las alertas de rol generadas desde la regla de alerta de rol en el Visualizador. Los analistas utilizan esta opción para priorizar las alertas que se deben revisar en primer lugar, de modo que los códigos de un sólo carácter son significativos para los usuarios del Visualizador. Por ejemplo, puede ser más importante revisar una regla de alertas de rol que genere una alerta siempre que un pasajero coincida con alguien que no esté en la lista de vuelo que una regla de alertas de rol diseñada para generar una alerta cuando un empleado conozca a un cliente.

Ejemplos de códigos de gravedad: C es grave, N es neutro, I es interesante, H es alto y L es bajo.

Rol 1 En la lista desplegable, seleccione el primer rol que se debe comparar en esta regla de alerta de rol.

Las opciones de rol que se mostrarán son los roles existentes y configurados. Si no encuentra el rol que desea seleccionar, configúrelo primero en la pestaña **Roles**.

Rol 2 En la lista desplegable, seleccione el segundo rol que se debe comparar en esta regla de alerta de rol.

Las opciones de rol que se mostrarán son los roles existentes y configurados. Si no encuentra el rol que desea seleccionar, configúrelo primero en la pestaña **Roles**.

Grupo de alertas
En la lista desplegable, seleccione el grupo de analizadores del Visualizador que analizarán las alertas de rol generadas desde la regla de alertas de rol. Por ejemplo, puede direccionar todas las alertas de rol de la lista de pasajeros que no estén en la lista de vuelo a un escritorio de seguridad y todas las alertas de rol empleado-proveedor a recursos humanos.

Las opciones de grupo que se muestran son los grupos de analizadores del Visualizador con el tipo de código `ANALYZER_GROUP`. Si no encuentra el

grupo que desea seleccionar, configure primero un código ANALYZER_GROUP nuevo en la pestaña **Configuración - General - Códigos**.

Este campo es necesario y debe configurarse y seleccionarse un código de grupo de alertas aunque su empresa no utilice el Visualizador.

Pestaña Reglas de alerta de rol:

Si ambos filtros están establecidos, sólo se tiene que cumplir con un filtro para que se genere una alerta de rol.

Filtro de identidad

En la lista desplegable, seleccione un filtro para restringir la generación de alertas de rol cuando se añaden nuevas identidades a las entidades involucradas en la alerta de rol.

Este filtro sólo afecta al comportamiento de re-alerta. La primera vez que se satisface una regla de alerta de rol correspondiente a un determinado conjunto de entidades, siempre se genera una alerta de rol. Este filtro puede impedir la futura generación de la misma alerta de rol cuando se realizan cambios en las entidades involucradas.

Desactivado

Seleccione este tipo de campo para desactivar la restricción de alerta de rol cuando se añaden nuevas identidades a las entidades involucradas en la alerta de rol.

Nueva identidad

Seleccione este tipo de campo para realertar únicamente cuando se incorpora un nuevo código de origen de datos entre las identidades en las entidades involucradas en la alerta de rol.

Nuevo código de origen de datos

Seleccione este tipo de campo para alertar cuando se incorpora un nuevo código de origen de datos entre las identidades.

Filtro de cambio de datos

En la lista desplegable, seleccione un filtro para restringir la generación de alertas de rol cuando se añaden nuevos datos de atributo a las entidades involucradas en la alerta de rol.

Este filtro sólo afecta al comportamiento de re-alerta. La primera vez que se satisface una regla de alerta de rol correspondiente a un determinado conjunto de entidades, siempre se genera una alerta de rol. Este filtro puede impedir la futura generación de la misma alerta de rol cuando se realizan cambios en las entidades involucradas.

Desactivado

Seleccione este tipo de campo para desactivar la restricción de alerta de rol cuando se añaden nuevos datos de atributo a las entidades involucradas en la alerta de rol.

Nuevos datos de atributo

Seleccione este tipo de campo para realertar únicamente cuando se añaden nuevos datos de atributo a las entidades involucradas en la alerta de rol.

Ajuste de resistencia de la vía de acceso

Seleccione este tipo de campo para realertar únicamente cuando se añaden nuevos datos de atributo que generan un cambio en la

resistencia de la vía de acceso igual o mayor que el valor de **Ajuste de la resistencia de la vía de acceso**.

Ajuste de resistencia de la vía de acceso
Este campo sólo muestra si el menú desplegable **Filtro de cambio de datos** está establecido en Ajuste de la resistencia de la vía de acceso. Escriba un valor de ajuste (entre -100 y 100) que se utilizará cuando **Filtro de cambio de datos** esté establecido en Ajuste de la resistencia de la vía de acceso. Esto permite la regeneración de alertas de rol sólo cuando se añaden nuevos datos de atributo que hacen que un cambio en la resistencia de la vía de acceso sea igual o mayor que el valor de Ajuste de la resistencia de la vía de acceso. Especificar cero equivale a desactivar el filtro.

Configuración de tipos de entidad

Puede configurar tipos de entidad para definir la naturaleza exacta de la entidad.

Acerca de esta tarea

Cuando se añaden datos de entidad nuevos a un origen de datos y desea clasificar esos datos como un tipo de entidad que todavía no está configurado en el sistema, debe crear un nuevo tipo de entidad para los nuevos datos.

Los tipos de entidad se pueden ver y modificar utilizando la consola, en la pestaña **Tipos de entidad**.

Tipos de entidad

Los tipos de entidad son características o propiedades definidas por el usuario que se asocian a una entidad para definir la naturaleza exacta de la entidad.

La identificación impersonal utiliza tipos de entidad para enlazar entidades que en otro caso no tendrían una relación de grado 1.

Por ejemplo, si deseara encontrar relaciones impersonales mediante llamadas telefónicas, crearía el nuevo tipo de entidad *Llamada telefónica* y ajustaría el nodo de adquisición para marcar correctamente cada registro de llamada telefónica con el tipo de entidad *Llamada telefónica*.

Cuando los registros telefónicos son absorbidos por las interconexiones, el proceso de resolución de entidades y relaciones encuentra una relación de un grado entre la entidad *Llamada telefónica* y la entidad llamante (*Persona*). También encuentra una relación de grado 1 entre la persona llamada y la entidad *Llamada telefónica*. Por sí mismo, el sistema no encuentra una relación de grado 1 entre las personas.

```
<UMF_ENTITY>
<DSRC_CODE>100</DSRC_CODE>
<DSRC_ACCT>123abc</DSRC_ACCT>
<DSRC_REF>1</DSRC_REF>
<ENTITY_TYPE>PHONE</ENTITY_TYPE>
<NUMBER>
<NUM_TYPE>PH</NUM_TYPE>
<NUM_VALUE>702-555-1212</NUM_VALUE>
</NUMBER>
</UMF_ENTITY>
```

Identificación impersonal

La identificación impersonal es una característica de producto que amplía el proceso tradicional de resolución de relaciones para encontrar y analizar relaciones impersonales. El proceso de detección de relaciones encuentra relaciones entre

entidades basándose en valores de atributos asociados a esas entidades. Algunas veces es importante encontrar relaciones entre entidades basándose en actividades u otros identificadores impersonales. Estas relaciones entre entidades basadas en actividades u otros identificadores impersonales se denominan relaciones *impersonales*, y las actividades o identificadores impersonales que establecen vínculos entre las personas se denominan *hechos relacionales.*

Las relaciones impersonales siempre existen para dos o más grados de separación, pues el propio hecho relacional es una entidad. Para habilitar la identificación impersonal y buscar relaciones impersonales, configure los orígenes de datos para utilizar la función Degrees of Separation, que puede configurarse para detectar relaciones con más de dos grados de separación.

Por ejemplo, una transacción telefónica contiene datos sobre números de teléfono: el número que realiza la llamada y el número receptor de la llamada. Aunque una persona realizó la llamada telefónica a otra persona, a partir de la transacción telefónica solamente, no se pueden atribuir datos comunes a las personas. A menudo, el hecho relacional (la llamada telefónica) se conoce antes que se conozca cualquier otra información sobre las entidades relacionadas (las dos personas que intervienen en la llamada telefónica). Puesto que estos hechos relacionales no se pueden atribuir a una persona, se deben representar como entidades separadas que no son personas, pero que están relacionadas con personas. Sin embargo, la identificación impersonal reconoce que existe una relación entre las dos personas como consecuencia de la llamada telefónica.

UMF incluye una funcionalidad de tipo de entidad, que permite definir hechos relacionales como tipos de entidad. Cuando se utiliza esta funcionalidad, los hechos relacionales pasan a ser entidades separadas en la base de datos de entidades y se pueden utilizar para detectar relaciones entre entidades Persona. Mediante la configuración de nuevos tipos de entidad, la especificación del tipo de entidad apropiado en UMF y la creación de nuevas configuraciones de resolución, estos hechos relacionales se pueden utilizar para encontrar automáticamente relaciones impersonales y conflictos entre entidades.

No se produce nunca una resolución cruzada para entidades con tipos de entidad diferentes, aunque las normas de resolución y los datos lo permitan. Por tanto, la resolución del tipo de entidad Llamada telefónica no produce nunca el tipo de entidad Persona .

El kit de herramientas de analista representa gráficos e informes de relaciones impersonales y de las alertas asociadas, al igual que lo hace con las relaciones personales y alertas asociadas.

Ejemplo de identificación impersonal

Por ejemplo, si deseara encontrar relaciones impersonales mediante llamadas telefónicas, crearía el nuevo tipo de entidad Llamada telefónica y ajustaría el nodo de adquisición para marcar correctamente cada registro de llamada telefónica con el tipo de entidad *Llamada telefónica*.

Cuando los registros telefónicos son absorbidos por el sistema, el proceso estándar de resolución de entidades y relaciones encuentra una relación de un grado entre la entidad Llamada telefónica y la entidad llamante (Persona). También encuentra una relación de grado 1 entre la persona llamada y la entidad Llamada telefónica. Por sí mismo, el sistema no encuentra una relación entre las personas.

Sin embargo, cuando se configura la función Degrees of Separation, continúa el análisis y detecta la relación impersonal de grado 2 entre el llamador y la persona llamada. Existe una relación impersonal, basada en los números de teléfono que son atributos del tipo de entidad Llamada telefónica. A continuación, la función Degrees of Separation analiza la relación impersonal y genera una alerta si se produce un conflicto.

Visualización de tipos de entidad

Los tipos de entidad son características o propiedades definidas por el usuario que se asocian a una entidad para definir la naturaleza exacta de la entidad. Puede ser conveniente ver los tipos de entidad existentes si está pensando en añadir uno nuevo.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Tipos de entidad**.
4. Seleccione el tipo de entidad que desee ver.

Creación de tipos de entidad

Los tipos de entidad son características o propiedades definidas por el usuario que se asocian a una entidad para definir la naturaleza exacta de la entidad. Puede añadir un nuevo tipo de entidad al sistema si piensa añadir un nuevo tipo de datos al sistema.

Antes de empezar

Antes de crear un nuevo tipo de entidad, consulte los datos de entidad de entrada para determinar si se puede describir con precisión utilizando cualquier tipo de entidad existente.

Acerca de esta tarea

La identificación impersonal utiliza tipos de entidad para enlazar entidades que en otro caso no tendrían una relación de grado 1.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Tipos de entidad**.
4. Pulse el botón **Nuevo**.
5. En el panel **General**, especifique el ID, el tipo, la descripción, la configuración de resolución de entidades, el colaborador genérico, el colaborador de alertas de rol, el tipo de búsqueda y permitir la resolución para este tipo de entidad.
6. Pulse el botón **Guardar**.

Resultados

El sistema puede ahora asignar tipos de entidad a datos y utilizar la identificación impersonal para enlazar entidades que en otro caso no tendrían una relación de grado 1.

Supresión de tipos de entidad

Puede suprimir un tipo de entidad existente cuando la base de datos de entidades ya no lo utilice.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Tipos de entidad**.
4. Marque el recuadro de selección situado junto al tipo de característica que desea suprimir.
5. Pulse el botón **Suprimir**.

Temas de ayuda

Panel Tipos de entidad - General:

Utilice la pestaña **Tipos de entidad** para especificar los detalles del tipo de entidad.

ID Escriba el número de ID del tipo de entidad que desee crear.

El ID es un código numérico que se incrementa automáticamente. Dado que el producto suministra el número siguiente disponible en secuencia, puede establecer el código para que sea un valor numérico exclusivo escribiendo dicho valor en el campo ID.

Tipo Escriba el nombre del tipo de entidad que desee crear.

Por ejemplo, utilizaría el tipo de entidad Llamada telefónica para describir entidades que son registros de llamadas telefónicas realizadas entre dos entidades.

Descripción
Escriba la descripción del tipo de entidad que desee crear.

Configuración de la resolución de entidades
En la lista desplegable, seleccione la configuración de resolución que el tipo de entidad utilizará durante la carga.

Las configuraciones de resolución se definen en la pantalla **Configuración** > **Resolución** > **Configuraciones de resolución**.

Colaborador genérico
En la lista desplegable, seleccione **Sí** para permitir que los datos del tipo de entidad sean genéricos. De lo contrario, seleccione **No**.

Colaborador de alertas de rol
En la lista desplegable, seleccione **Sí** para permitir que los datos del tipo de entidad generen alertas de rol. De lo contrario, seleccione **No**.

Tipo de búsqueda
En la lista desplegable, seleccione **Sí** para permitir que los datos del tipo de entidad se utilicen para realizar búsquedas. De lo contrario, seleccione **No**.

Permitir resolución
En la lista desplegable, seleccione **Sí** para permitir que los datos del tipo de entidad se utilicen para resolver entidades. De lo contrario, seleccione **No**.

Visión general de Degrees of Separation

La característica Degrees of Separation amplía las posibilidades de coincidencia de relaciones de IBM Relationship Resolution.

El comportamiento predeterminado de IBM InfoSphere Identity Insight identifica relaciones de gran interés y establece coincidencias de entidades a un grado de separación de una entidad entrante resuelta en una entidad. Si habilita la característica Degrees of Separation se amplían estas posibilidades hasta casi un rango ilimitado de grados de separación definidos por el usuario de una entidad entrante resuelta en una entidad.

La característica Degrees of Separation utiliza configuraciones de separación, roles, reglas de alertas de rol y puntuaciones de relaciones para realizar análisis de enlaces en tiempo real respecto a grandes conjuntos de datos.

Cuando una entidad entrante se resuelve en una entidad, se crea un gráfico de entidades utilizando relaciones de un grado que detecta IBM InfoSphere Identity Insight. El gráfico de entidades utiliza las relaciones de un grado para crear cadenas de relaciones de múltiples grados que provienen de la entidad en la que quedó resuelta la entidad entrante. Se puede crear una cadena de alertas de rol enlazando dos cadenas de relaciones de múltiples grados, cada una proveniente de la entidad en la que quedó resuelta la entidad de entrada. La cadena de alertas de rol se puede utilizar para encontrar una relación entre las entidades finales e incluyendo cada cadena de relación de múltiples grados.

Degrees of Separation reduce el trabajo evaluando todas las vías de acceso que conectan dos entidades y utilizando las mejores para notificar relaciones. Se puede configurar Degrees of Separation para que informe sobre una alerta de rol para cada regla de alertas de rol configurada por entidad en la que se resolvió la entidad entrante.

La configuración de grados de separación puede establecerse en la consola utilizando la pestaña **Configuración del sistema**, valor Grados de separación.

Ejemplo de grados de separación

Este ejemplo le guía a lo largo de una vía de acceso de relación y muestra cómo la configuración de grados de separación influye en la determinación de las alertas de rol.

Ejemplo de grados de separación

Después de procesar los datos de entrada, Identity Insight informa sobre la vía de acceso de relación siguiente:

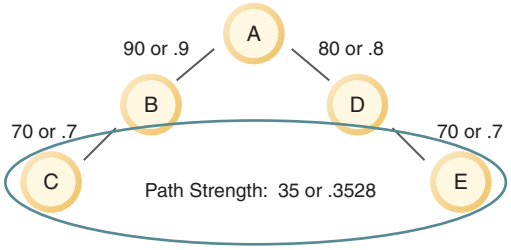
- La entidad A conoce a la entidad B.
- La entidad B conoce a la entidad C.
- La entidad A conoce a la entidad D.
- La entidad B conoce a la entidad E.

Una *vía de acceso de relación* es la cadena de entidades y atributos que enlazan una entidad a otra entidad.

Como parte del proceso de alerta de rol y relación, Identity Insight determina la resistencia de la vía de acceso de relación. La resistencia de la vía de acceso es el producto de las conversiones de decimales de puntuación de relación de cada entidad de la cadena, convertido en un entero.

Mediante nuestro ejemplo, el producto calcula las puntuaciones de relación y convierte las puntuaciones en decimales:

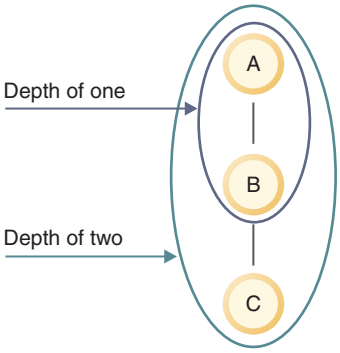
- La puntuación de relación la entidad A sabe que la entidad B es 90. 90 se convierte al decimal 0,9
- La puntuación de relación para la entidad B sabe que la entidad C es 70. 70 se convierte al decimal 0,7
- La puntuación de relación para la entidad A sabe que la entidad D es 80. 80 se convierte al decimal 0,8
- La puntuación de relación para la entidad D que conoce a la entidad E es 70. 70 se convierte al decimal 0,7



Las puntuaciones de relación en la vía de acceso de relación se multiplican. El resultado del cálculo es una resistencia de vía de acceso de relación de 0,3528, que se convierte en el entero 35.

Entonces el producto compara la resistencia de vía de acceso calculada con el parámetro de grados de separación de **umbral de resistencia de vía de acceso** configurado. Si la resistencia de vía de acceso de relación cumple o excede el umbral de vía de acceso configurado, el rol generado por el producto produce una alerta. Si la resistencia de vía de acceso de relación está por debajo del umbral de resistencia de vía de acceso configurado, el producto no genera alertas de rol.

El producto utiliza entonces el parámetro de grados de separación **max depth** configurado para calcular los grados de separación entre las entidades de la cadena de relaciones. El valor de profundidad máxima determina el número máximo de grados de separación en una vía de acceso de relación de varios grados que puede considerarse como parte de la detección de alertas de rol.



Normalmente, el parámetro **max depth** se establece en dos.

En este ejemplo, el parámetro **max depth** se establece en 6. La entidad C y la entidad E tienen roles conflictivos y están separadas por 6 grados, por lo tanto se genera una alerta de rol.

Visualización de las configuraciones de separación

Debido a que el producto permite varias configuraciones de separación, utilice estas instrucciones para ver los valores de una configuración de separación específica.

Procedimiento

1. En la consola de configuración, pulse **Configurar** > **Relaciones** > **Configuración de separación**.
2. Seleccione la configuración de separación.

Creación de configuraciones de separación nuevas

Defina configuraciones de separación para determinar si la resolución de relación detecta una, dos o varios grados de separación entre entidades.

Procedimiento

1. En la consola de configuración, pulse **Configurar** > **Relaciones** > **Configuración de separación**.
2. Pulse **Nuevo**.
3. En la pestaña **General**, especifique los valores para esta configuración de separación.
4. Pulse **Guardar**.

Edición de configuraciones de separación

Edite una configuración de separación para cambiar los valores que determinan cuántos grados pueden separar dos entidades y que todavía se pueda considerar una relación.

Procedimiento

1. En la consola de configuración, pulse **Configurar** > **Relaciones** > **Configuración de separación**.
2. Seleccione la **configuración de separación** a editar y realice los cambios.
3. Pulse **Guardar**.

Temas de ayuda

Configuración de separación - Pestaña General:

Utilice el separador **General** para especificar los detalles de la configuración de separación.

ID Escriba un entero exclusivo que identifique la configuración de separación.

El valor del ID se llena automáticamente con el siguiente número secuencial no utilizado.

Código
Escriba un valor exclusivo para identificar este rol.

Descripción
Escriba una descripción para esta configuración de separación.

Profundidad máxima
Número máximo de grados de separación de una cadena de relaciones de varios grados en un gráfico de entidades que se tiene en cuenta para la detección de alertas de rol.

Umbral de resistencia de vía de acceso

Umbral de resistencia de vía de acceso de una cadena de alertas de rol. Cuando una cadena de alerta de rol cuya vía de acceso es inferior a este umbral no generará alertas de rol.

La resistencia de la vía de acceso es el producto, convertido a entero, de las conversiones decimales de la puntuación de relación de cada entidad en la cadena de alerta de rol. El valor predeterminado para este parámetro es 15.

Grados de separación evalúa todas las vías de acceso que conectan dos entidades y utiliza la resistencia de la vía de acceso más fuerte en las relaciones de informes.

Configuración de documentos UMF

Para utilizar satisfactoriamente documentos UMF (Unified Messaging Format), se deben conocer y estar configurados.

Visualización de documentos de entrada UMF predeterminados

Los documentos de entrada UMF son la colección de segmentos UMF que estructuran los datos de entrada para cargar, modificar o consultar datos en la base de datos de entidades.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Documentos de entrada**.

Configuración de documentos de salida

Debe configurar el estado habilitado de un código de formato de documento de salida si se utiliza.

Acerca de esta tarea

Los documentos de salida UMF formatean los datos de resultados UMF.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Documentos de salida**.
4. Pulse en cualquier enlace de la fila que contiene el código de formato de documento de salida UMF que desee editar.
5. En la lista desplegable **Habilitado**, seleccione el estado adecuado del código de formato de documento de salida UMF.
6. Pulse el botón **Guardar**.

Configuración del origen de datos

Debe configurar un origen de datos cuando haya un nuevo origen de datos que desee cargar en la base de datos de entidades.

Antes de empezar

Para configurar un origen de datos, primero debe configurar roles.

Acerca de esta tarea

Los orígenes de datos pueden verse y modificarse utilizando la Consola, en la pestaña **Orígenes de datos**.

Orígenes de datos

Los orígenes de datos contienen las identidades que desea procesar para la resolución de entidades y cargar en la base de datos de entidades. Los orígenes de datos contienen datos identificativos (identificadores exclusivos y personales para una entidad) y datos no identificativos (otros atributos y puntos de datos correspondientes a una entidad). Los registros de identidad del origen de datos se deben exportar como UMF (Universal Message Format) para que los pueda procesar el sistema y se puedan cargar en la base de datos de entidades. Ejemplos de orígenes de datos incluyen, aunque sin limitarse a las mismas, listas de empleados, listas de vigilancia, listas de clientes y listas de proveedores.

Los orígenes de datos contienen información vital, como la información sobre la fuente original (porque los datos originales se han transformado en UMF) o la referencia externa correspondiente al origen de datos. Estos detalles hacen que cada origen de datos sea exclusiva en el sistema.

Durante la resolución de entidades, si dos entidades no se resuelven, el sistema utiliza la información del origen de datos para determinar qué información pertenece a cada entidad.

Ubicaciones de orígenes de datos y sistemas origen

Puede organizar los orígenes de datos de entrada creando ubicaciones origen y sistemas origen y asociándolos a sus orígenes de datos. Puede utilizar ubicaciones origen y sistemas origen para distinguir entre tipos de orígenes de datos parecidos.

Por ejemplo, si está procesando datos de reservas y datos de recursos humanos procedentes de más de una ubicación, puede utilizar la ubicación de origen de datos para distinguir qué ubicación está ofreciendo los datos:

- Datos de reservas de la propiedad X
- Datos de recursos humanos de la propiedad X
- Datos de reservas de la propiedad Y
- Datos de recursos humanos de la propiedad Y

Configuraciones por origen de datos

Para maximizar los resultados de la resolución de entidades y de la detección de relaciones, configure cada origen de datos utilizando estos valores:

Roles Puesto que los orígenes de datos son agrupaciones del mismo tipo de datos, puede asignar automáticamente el mismo rol a cada registro de identidad del mismo origen de datos de entrada. Por ejemplo, si se asocia el rol Empleado a un origen de datos de recursos humanos, a todos los registros de entrada procedentes de la lista de empleados se les asigna automáticamente el rol Empleado.

Niveles de carga
Puede determinar si se deben cargar todos los datos de un origen de datos de entrada o sólo los datos que se resuelven en una o varias entidades o que están relacionados con las mismas.

Valores de resolución de relaciones

Puede configurar el nivel de detección de relaciones por origen de datos. Por ejemplo, puede desactivar la resolución de relaciones para un origen de datos o seleccionar el número de grados de separación para detectar relaciones dentro de dicho origen de datos en concreto.

Visualización de orígenes de datos

Un origen de datos contiene los datos cargados en la base de datos de entidades. Puede que desee ver los orígenes de datos existentes si tiene previsto añadir un nuevo origen de datos.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Orígenes de datos**.
4. Seleccione el origen de datos que desea visualizar.

Configuración de un origen de datos

Para cargar satisfactoriamente datos en la base de datos de entidades, debe configurar el sistema para que reconozca cada origen de datos.

Antes de empezar

Antes de poder cargar datos en el sistema, el origen de datos debe utilizar el estándar UMF.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Orígenes de datos**.
4. Pulse el botón **Nuevo**.
5. En el panel **General**, especifique el ID, la descripción y otra información de configuración para el origen de datos.
6. Pulse la pestaña **Resolución de entidad**.
7. En el panel **Resolución de entidad**, especifique la información de configuración de resolución para el origen de datos.
8. Pulse la pestaña **Relaciones**.
9. En el panel **Relaciones**, especifique la información de configuración de relaciones para el origen de datos.
10. Pulse el botón **Guardar**.

Configuración del nivel de coincidencia de nombres de Name Manager

Configure el nivel de coincidencia de Name Manager por origen de datos, porque los datos de nombre pueden variar por origen. El nivel de coincidencia que seleccione es un parámetro de comparación que determina hasta qué punto es estricta la coincidencia de los nombres de entrada de este origen de datos.

Procedimiento

1. En la Consola de configuración, seleccione **Configurar** > **Orígenes** > **Orígenes de datos**.
2. Seleccione el origen de datos.

3. Pulse **Resolución de entidad**.
4. En **Nivel de coincidencia de Name Manager**, seleccione el nivel de coincidencia. En la mayoría de situaciones, utilice el valor **Predeterminado**, que es suficientemente estricto para producir buenas coincidencias de nombre.

Configuración de orígenes de datos para el hashing de nombres mejorado

Si utiliza hashing de nombre mejorado, debe configurar cada origen de datos para permitir la creación de lista de candidatos de atributos de nombre, estableciendo la configuración de compilador candidato en el compilador candidato **Predeterminado con sólo nombre**.

Supresión de orígenes de datos

Un origen de datos contiene los datos cargados en la base de datos de entidades. Es posible que desee suprimir un origen de datos existente si ya no existe el origen de datos, o si ya no es importante para la base de datos de entidades.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Orígenes**.
3. Pulse la pestaña **Orígenes de datos**.
4. Marque el recuadro de selección situado junto al origen de datos que desee suprimir.
5. Pulse el botón **Suprimir**.

Creación de una ubicación de origen de datos

Para seleccionar una ubicación a fin de clasificar un origen de datos, esa ubicación debe estar configurada en el sistema.

Acerca de esta tarea

Las ubicaciones de orígenes de datos se crean utilizando la Consola de configuración. Se trata de una opción que se utiliza principalmente si el origen de datos reúne datos de múltiples ubicaciones físicas. Por ejemplo, una base de datos del sistema de un hotel reúne datos de múltiples ubicaciones físicas del hotel.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Ubicaciones**.
4. Pulse el botón **Nuevo**.
5. En el panel **General**, especifique el código de ubicación, el nombre de ubicación, el distrito, la compañía, la latitud, la longitud, el estado y otra información de configuración para la ubicación del origen de datos.
6. Pulse el botón **Guardar**.

Qué hacer a continuación

Ahora puede aplicar la ubicación que acaba de configurar a los orígenes de datos del sistema.

Temas de ayuda

Orígenes de datos - Panel Resolución de entidades:

Utilice el panel **Resolución de entidades** para especificar los detalles de resolución de entidades del origen de datos.

Configuración de la resolución de entidades
En la lista, seleccione la configuración de resolución que este origen de datos utiliza al cargar datos.

Configuración del creador de candidatos
En la lista, seleccione la configuración de creador de candidatos adecuado utilizada durante el proceso de resolución de entidad al cargar datos para este origen de datos.

Valor predeterminado
Seleccione este valor para utilizar la configuración de creador de candidatos predeterminada.

Predeterminado con sólo nombre
Seleccione este valor para utilizar la configuración predeterminada del creador de candidatos con la adición de coincidencia de sólo nombre.

Para utilizar Name Hasher para procesar datos de nombre para este origen de datos, seleccione esta configuración de creador de candidatos. (Asegúrese de que los parámetros del sistema para Name Hasher se han establecido.)

Confirmación de la característica
En la lista, seleccione **Sí** para especificar que las confirmaciones de característica se procesan cuando se cargan datos de este origen de datos. De lo contrario, seleccione **No**.

Realizar desconexión
Este valor se utiliza normalmente sólo para sistemas de hotel.

En la lista, seleccione **Sí** para especificar que la interconexión puede coincidir con datos sin la cuenta de origen de datos. Si la coincidencia no resulta satisfactoria, la fecha de supresión se establece en datos anteriores. De lo contrario, seleccione **No**.

Nivel de coincidencia de Name Manager
En la lista, seleccione el valor para el nivel de comparación que se debe utilizar al puntuar datos de nombres de entrada de este origen de datos.

Valor predeterminado
Seleccione este valor para utilizar el nivel de comparación de coincidencias de nombre más común.

Inexacto
Seleccione este valor si desea producir más coincidencias de nombre desde este origen de datos. Este valor reduce el nivel de coincidencia de comparación de nombres, para que la comparación sea menos estricta que el valor predeterminado.

Ajustado
Seleccione este valor si desea producir menos coincidencias de de este origen de datos. Este valor ajusta el nivel de coincidencia de comparación de nombre, para que la comparación sea más estricta que el valor predeterminado.

Permitir no resolver

La característica de eliminación de resolución es el proceso de separación de identidades resueltas en dos entidades independientes, basándose en la información nueva de los datos de entrada. En la lista, realice la selección adecuada para este origen de datos:

- Seleccione **Sí** para permitir que la resolución de entidad separe identidades en entidades independientes, si están garantizadas, al cargar cuentas para este origen de datos.
- Seleccione **No** para impedir que la resolución de entidad separe identidades en entidades independientes al cargar las cuentas para este origen de datos.

Orígenes de datos - Panel General:

Utilice el panel **General** para especificar los detalles del origen de datos.

ID Escriba el número de ID del origen de datos que desea crear.

El ID es un código numérico que se incrementa automáticamente. Dado que el producto suministra el número siguiente disponible en secuencia, puede establecer el código para que sea un valor numérico exclusivo escribiendo dicho valor en el campo ID.

Código

Escriba el código del origen de datos que desea crear.

Es el valor del código UMF `DSRC_CODE`. El valor del código del origen de datos puede ser alfanumérico y se utiliza para identificar mejor un origen de datos. Este valor puede ser exclusivo y no se puede cambiar una vez que se ha guardado el registro.

Descripción

Escriba la descripción del origen de datos que desea crear.

Ubicación

En la lista desplegable, seleccione el código de ubicación del origen de datos que desea crear.

Este campo sólo se utiliza como referencia.

Sistema origen

En la lista desplegable, seleccione el código del sistema origen del origen de datos que desea crear.

Este campo sólo se utiliza como referencia.

Estado

En la lista desplegable, seleccione **Activo** para especificar que este origen de datos está activa. De lo contrario, seleccione **Inactiva**.

Confiar en la acción

En la lista desplegable, seleccione **Sí** para especificar que puede confiar en la precisión del código UMF `ACTION` del origen de datos. De lo contrario, seleccione **No** para determinar la acción examinando la base de datos de entidades. Si se selecciona **No** se incorpora un acierto de rendimiento.

Para búsqueda

En la lista desplegable, seleccione **Sí** para especificar que este origen de datos se utiliza para cargar búsquedas. De lo contrario, seleccione **No**.

Transliterar

En la lista desplegable, seleccione **Sí** para especificar que se debe producir

transliteración para este origen de datos. Esto permite trabajar con el juego de caracteres Latin 1. De lo contrario, seleccione **No**.

Nota: Si habilita el valor de transliteración para cualquier origen de datos, debe también habilitar el valor de configuración de transliteración para el ID de origen de datos 1589 (Buscar). El origen de datos 1589 es utilizado por el producto para especificar búsquedas en la interconexión y, de forma predeterminada, para recibir caracteres ASCII. Habilite esta configuración para asegurar que los nombres que forman parte de una búsqueda también se transliteren debidamente para proporcionar unos resultados de búsqueda lo más exactos posible.

Panel Orígenes de datos - Relaciones:

Utilice el panel **Relaciones** para especificar los detalles de relación del origen de datos.

Rol Seleccione el código de rol que se asignará a este origen de datos.

Clase de origen de datos
Seleccione el origen de datos apropiado para este origen de datos.

Carga completa
Seleccione este tipo de campo para cargar los datos en la base de datos.

Este valor también resolverá las identidades que se puedan resolver, actualizará la entidad, detectará cualquier posible relación y generará alertas de rol definidas por el usuario.

Totalmente pasivo
Seleccione este tipo de campo para no cargar los datos en la base de datos.

Si realiza una carga totalmente pasiva no se almacenarán datos. El Visualizador no puede mostrar la alerta.

Cargar si resolución/relación
Seleccione este tipo de campo para cargar los datos en la base de datos si se resuelven o se relacionan con los registros existentes en la base de datos de entidades.

Este valor también resolverá las identidades que se puedan resolver, actualizará la entidad, detectará cualquier posible relación y generará alertas de rol definidas por el usuario.

Cargar si resolución/relación selectiva
Seleccione este tipo de campo para cargar los datos en la base de datos si se resuelven o se relacionan con los registros existentes en la base de datos de entidades, sólo si este origen de datos está configurada en la tabla SELECTIVE_PASSIVE_CONFIG.

Este valor también resolverá las identidades que se puedan resolver, actualizará la entidad, detectará cualquier posible relación y generará alertas de rol definidas por el usuario.

Cargar si resolución selectiva
Seleccione este tipo de campo para cargar los datos en la base de datos si se relacionan con los registros existentes en la base de datos de entidades, sólo si este origen de datos está configurada en la tabla SELECTIVE_PASSIVE_CONFIG.

Este valor también resolverá las identidades que se puedan resolver, actualizará la entidad, detectará cualquier posible relación y generará alertas de rol definidas por el usuario.

Nivel de separación
En la lista desplegable, seleccione el nivel de separación adecuado para este origen de datos.

Cargar datos
Seleccione siempre este tipo de campo. Actualmente es la única opción.

Configuración de DoS
En la lista desplegable, seleccione la configuración de grados de separación adecuada para este origen de datos.

Las configuraciones de separación se establecen en la pantalla **Configuración** > **Relaciones** > **Configuración de separación**.

Ubicaciones - Panel General:

Utilice el panel **Ubicaciones** para especificar los detalles de la ubicación del origen de datos.

Código de ubicación
Escriba el código de ubicación que se asignará a esta ubicación de origen de datos.

Un valor alfanumérico no se puede modificar una vez guardado el registro.

Este valor es obligatorio.

Nombre de ubicación
Escriba el nombre de ubicación que se asignará a esta ubicación de origen de datos.

Distrito
Escriba el distrito que se asignará a esta ubicación de origen de datos.

Este valor es obligatorio.

Empresa
Escriba el nombre de empresa que se asignará a esta ubicación de origen de datos.

Latitud
Escriba la latitud de esta ubicación de origen de datos en el siguiente formato:

DD:MM:SS

Longitud
Escriba la longitud de esta ubicación de origen de datos en el siguiente formato:

DD:MM:SS

Estado
En la lista desplegable, seleccione **Activo** para especificar que esta ubicación de origen de datos está activa. De lo contrario, seleccione **Inactiva**.

Desactivación de la detección de relaciones

Si los requisitos de la empresa especifican que sólo necesita saber quién es quién y no quién conoce a quién, puede reducir la cantidad de proceso necesario para cada nuevo registro y acelerar el rendimiento global del sistema configurando la resolución de entidades para que sólo realice la resolución de entidades y no detecte las relaciones entre entidades.

Antes de empezar

Asegúrese de que ha seleccionado **Editar configuración** al iniciar la sesión actual de la Consola de configuración.

Procedimiento

1. Desactive las asignaciones de roles para cada origen de datos.
   a. Pulse **Configuración**.
   b. Pulse **Orígenes**.
   c. En el panel **Orígenes de datos**, pulse el origen de datos que desea editar.
   d. Pulse la pestaña **Relaciones**.
   e. En la lista desplegable **Rol**, elija **— Seleccionar uno —**.
   f. En la lista desplegable **Nivel de separación**, elija **Sólo alertas**.
   g. Pulse **Guardar**.
2. Inhabilite la regla de gestión de calidad de datos de asignaciones de roles predeterminados.
   a. Pulse **Configuración**.
   b. Pulse **UMF**.
   c. En la lista desplegable **Segmento** del panel **Reglas DQM**, elija **ROOT**.
   d. Pulse un enlace de la fila que contiene la función DQM 551, Asignación de roles predeterminados.
   e. En la lista desplegable **Estado** del panel **General**, elija **Inactivo**.
   f. Pulse **Guardar**.
3. Suprima todas las normas de resolución que no estén establecidas para resolver entidades.
   a. Pulse **Configuración**.
   b. Pulse **Resolución**.
   c. Pulse la pestaña **Normas de resolución**.
   d. En la lista desplegable **Config resolución**, elija **DEFAULT**.
   e. Pulse el recuadro de selección situado junto a cualquier regla de resolución que muestre un valor **No** en la columna **Resolver desencadenantes**.
   f. Pulse **Suprimir**.
   g. Pulse **Aceptar** para confirmar que desea suprimir las normas de resolución seleccionadas.
4. Por último, suprima todas las reglas de conflicto.
   a. Pulse **Configuración**.
   b. Pulse **Relaciones**.
   c. Pulse la pestaña **Reglas de conflicto**.
   d. Pulse el recuadro de selección situado junto a cada regla de conflicto.
   e. Pulse **Suprimir**.

f. Pulse **Aceptar** para confirmar que desea suprimir las reglas de conflicto seleccionadas.

Qué hacer a continuación

Ahora, el sistema está configurado para resolver entidades sin detectar relaciones.

Configuración de tipos de suceso

Puede configurar tipos de suceso para definir y clasificar sucesos que procesa Event Manager. Sin embargo, antes de que el sistema procese datos entrantes que contengan tipos de eventos, se debe habilitar el proceso de sucesos en los parámetros del sistema deEvent Manager, configurar las reglas empresariales en la herramienta de procesador de sucesos compleja basada en Eclipse y formatear los datos de sucesos utilizando las definiciones de segmentos de datos UMF EVENT.

Los tipos de suceso se pueden ver y modificar utilizando la consola, en la pestaña **Tipos de sucesos**.

Tipos de sucesos

Los tipos de sucesos clasifican los sucesos y definen la unidad de medida para el valor asociado con los sucesos en Event Manager. Entre los ejemplos de tipos de suceso se incluyen la transferencia de conexiones, la apertura de cuentas o la transacción de tarjetas de crédito.

Los tipos de suceso son necesarios para el proceso de sucesos, porque las reglas empresariales definidas por el usuario que el procesador de sucesos utiliza llaman a un tipo de suceso específico. Si el tipo de suceso no existe, el procesador de sucesos no puede procesar el suceso.

Creación de tipos de suceso

Si desea añadir un caso de ejemplo de suceso nuevo para procesar sucesos, es necesario que cree un nuevo tipo de suceso para definir los tipos de transacciones o actividades incluidos en dicho caso de ejemplo de suceso, así como la unidad de medida asociada con esta categoría de suceso.

Antes de empezar

Event Manager debe estar habilitado para el sistema IBM InfoSphere Identity Insight.

Acerca de esta tarea

El procesador de sucesos complejos llama a los tipos de suceso, mientras procesa sucesos de acuerdo con las reglas empresariales definidas por el usuario. Para poder utilizar un tipo de suceso, se debe crear al menos una regla empresarial que utilice el tipo de suceso.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Orígenes**.
3. Pulse el botón **Tipo de suceso**.
4. Pulse el botón **Nuevo**.

5. Necesario: En el panel **General**, especifique el nombre y la descripción del tipo de suceso, la unidad de medida asociada con el tipo de suceso y el estado del tipo de suceso (activo o inactivo).
6. Opcional: También puede especificar información adicional, como la categoría, la subcategoría y notas sobre el tipo de suceso.
7. Pulse el botón **Guardar**.

Edición de tipos de suceso

Puede editar un tipo de suceso cuando desee cambiar la descripción, la unidad de medida o la información adicional asociada con el tipo de suceso. También puede editar un tipo de suceso para inactivarlo, de manera que no se pueda utilizar más. No se puede editar el nombre de tipo de suceso.

Acerca de esta tarea

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Orígenes**.
3. Pulse el botón **Tipo de suceso**.
4. Seleccione el tipo de suceso que desee editar.
5. Realice los cambios en la pestaña **General**.
6. Pulse el botón **Guardar**.

Qué hacer a continuación

Supresión de tipos de suceso

Es posible que desee suprimir un tipo de suceso cuando ya no se utiliza para el proceso de sucesos. Si desea conservar el tipo de suceso, pero mantenerlo inactivo, puede editar el estado del tipo de suceso en lugar de suprimirlo.

Antes de empezar

Acerca de esta tarea

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Orígenes**.
3. Pulse el botón **Tipo de suceso**.
4. Marque el recuadro de selección situado junto a los tipos de sucesos que desee suprimir.
5. Pulse el botón **Suprimir**.

Qué hacer a continuación

Temas de ayuda

Tipos de sucesos - Panel general:

Utilice este panel para definir o editar un tipo de suceso. Los tipos de suceso definen y clasifican sucesos y se utilizan durante el proceso de sucesos si Event Manager está habilitado para el sistema.

Tipo Escriba un nombre exclusivo para este tipo de suceso. Por ejemplo, es posible que desee crear un tipo de suceso llamado `Transferencia de conexiones`.

Descripción
Escriba una descripción del tipo de suceso.

Unidad de medida
Escriba una abreviatura de la unidad de medida para el valor asociado con el tipo de suceso. Por ejemplo, es posible que desee introducir `USD` para los dólares estadounidenses.

Estado
En la lista desplegable, seleccione el estado para el tipo de suceso, ya sea **Activo** o **Inactivo**. (Puede utilizar el estado **Inactivo** para eliminar el tipo de suceso del proceso de sucesos, pero conservando la configuración para el tipo de suceso.)

Categoría
Escriba un nombre de categoría opcional para el tipo de suceso.

Subcategoría
Escriba un nombre de subcategoría opcional para el tipo de suceso.

Cabecera de memoria 1
Escriba una cabecera de memoria 1 opcional para el tipo de suceso.

Cabecera de memoria 2
Escriba una cabecera de memoria 2 opcional para el tipo de suceso.

Configuración de la resolución de entidades

La resolución de entidades es el proceso que busca relaciones en los datos. Los valores de configuración de la resolución de entidades se organizan en agrupaciones denominadas configuraciones de resolución. Cinco componentes forman la configuración de resolución: las normas de resolución, las confirmaciones y denegaciones, los atributos, las configuraciones de coincidencias de Name Manager y el creador de candidatos.

Resolución de entidades

La resolución de entidades es el proceso que resuelve entidades y detecta relaciones. Las interconexiones realizan la resolución de entidades a medida que procesan los registros de identidad de entrada en tres fases: reconocimiento, resolución y relación.

Configuración de configuraciones de resolución

Todos los valores de resolución de entidades se conservan en una configuración de resolución, dos de las cuales se proporcionan de forma predeterminada.

Configuraciones de resolución

Los valores de resolución de entidad se organizan por un grupo de configuraciones de resolución que se definen utilizando el valor de regla de resolución de carga de sistema de la pestaña **Configuración del sistema** de la Consola de configuración.

La instalación predeterminada de Relationship Resolution incluye dos configuraciones de resolución.

- **DEFAULT** - los valores predeterminados de resolución que se utilizan cuando entran datos nuevos en el sistema procedentes de un origen de datos definida.

- **SEARCH** - valores de resolución utilizados por el proceso de búsqueda resuelta siempre que un usuario envía una solicitud de búsqueda completamente resuelta.

Puede crear su propio conjunto de valores de resolución e identificarlos utilizando una configuración de resolución recién creada. Este proceso debe comenzar clonando la configuración de resolución **DEFAULT** y utilizándola como punto de partida de la nueva configuración de resolución.

Se pueden asignar distintas configuraciones de resolución a orígenes de datos específicas. Si elige aplicar varias configuraciones de resolución en varios orígenes de datos, debe tener en cuenta que la resolución de entidades siempre utiliza la configuración de resolución asignada a la identidad de entrada cuando se generan alertas. Esto puede dar lugar a resultados de alerta distintos basados en cuál de las identidades comparadas es la identidad de entrada y cuál de las identidades ya existe en la base de datos de entidades. Por ejemplo, a la Identidad 123 del origen de datos Cliente se le asigna la configuración de resolución DEFAULT, que contiene una regla de resolución para nombre y dirección con un umbral de nombre de 80 y un umbral de dirección de 5. La Identidad 456 procedente del origen de datos Proveedor utiliza la configuración de resolución NEW que tiene la misma regla de resolución, pero el umbral de nombre se ha establecido en 95 y el umbral de dirección se ha establecido en 7. Cuando Cliente 123 es la identidad de entrada y se compara con el Proveedor 456 existente, la puntuación de nombre entre ellos se calcula a 85 y la puntuación de dirección es 5, lo que da lugar a que se genere una alerta. Si el orden del proceso se invierte con Cliente 123 ya en el sistema y el Proveedor 456 entrando en el sistema, se seguirán generando las mismas puntuaciones de resolución de 85 para nombre y de 5 para dirección. Sin embargo, en este caso no se generará ninguna alerta porque las puntuaciones de resolución no cumplen con los umbrales de resolución de la configuración de resolución NEW, en la que el nombre está establecido en 95 y la dirección en 7.

Nota:

El uso de una configuración de resolución distinta de la configuración de resolución de entidades predeterminadas debe hacerse con mucho cuidado y planificación. Los valores de resolución de entidades predeterminadas, como normas de resolución y valores de puntuación, son el resultando de cientos de personas y años de análisis y estudios de datos reales. Generalmente sólo es necesario cambiar estos valores predeterminados cuando los datos o las reglas de la empresa requieren comportamientos específicos y no estándares del sistema.

Visualización de configuraciones de resolución

Las configuraciones de resolución se utilizan para especificar una colección de valores de resolución de entidades. Puede que desee ver las configuraciones de resolución existentes cuando piense realizar cambios en los valores de resolución de entidades o si desea crear un nuevo conjunto de valores de resolución de entidades.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Resolución**.

Clonación y personalización de la configuración de resolución predeterminada

La manera ideal de crear una nueva configuración de resolución de entidades es clonar (hacer una copia de) la configuración de resolución predeterminada y

utilizarla como punto de inicio para la nueva configuración de resolución. Si mantiene la configuración predeterminada en estado no modificado, siempre podrá volver a ella si lo necesita, sin tener que volver a instalar el producto.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Resolución**.
3. En el panel **Configuraciones de resolución**, seleccione el recuadro de selección situado junto a la configuración de resolución DEFAULT.
4. Pulse el botón **Clonar**.
5. En el campo **Código** del panel **General**, escriba el nuevo nombre para la configuración de resolución.
6. En el campo **Descripción**, escriba una nueva descripción de la configuración de resolución clonada.
7. Pulse el botón **Guardar**.

Qué hacer a continuación

Cuando realice cambios en los valores de resolución de entidades como, por ejemplo, al configurar normas de resolución, confirmaciones y denegaciones, o el creador de candidatos, puede seleccionar la nueva configuración de resolución.

Supresión de configuraciones de resolución personalizadas

Si ya no utiliza una configuración de resolución personalizada, puede suprimirla. No suprima la configuración de resolución DEFAULT; si mantiene la configuración predeterminada en estado no modificado, siempre podrá volver a ella si lo necesita, sin tener que volver a instalar el producto.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Resolución**.
3. En el panel **Configuraciones de resolución**, seleccione el recuadro de selección situado junto a la configuración de resolución que desea suprimir.
4. Pulse el botón **Suprimir**.
5. En la ventana de confirmación, pulse **Aceptar** para suprimir la configuración de resolución.

Qué hacer a continuación

Ya no podrá seleccionar esta configuración de resolución cuando realice cambios en los valores de resolución predeterminados. Además, los valores de resolución de entidades relacionados con esta configuración de resolución ya no se pueden aplicar al proceso de resolución de entidades.

Temas de ayuda

Ventana Configuraciones de resolución:

Utilice esta ventana para ver una lista de las configuraciones de resolución de entidades disponibles. Los valores de resolución de entidades se organizan en grupos llamados configuraciones de resolución. Se pueden asignar distintas configuraciones de resolución a orígenes de datos individuales. Cada origen de datos sólo puede tener una configuración de resolución aplicada a la vez.

Código
Nombre de la configuración de resolución.

Descripción
Descripción de la configuración de resolución.

Configuración de normas de resolución

Para definir la forma en que las entidades comparadas se resuelven y relacionan, debe configurar normas de resolución, incluyendo umbrales candidatos y umbrales de confirmación/denegación.

Acerca de esta tarea

Las normas de resolución se pueden ver y modificar utilizando la Consola, en la pestaña **Normas de resolución** .

Normas de resolución

Las normas de resolución son un conjunto de criterios que utiliza el sistema para definir el modo en que se resuelven entidades comparadas (si son o no son la misma entidad) y el modo en que se relacionan (si las entidades no se resuelven en la misma entidad, cuántos atributos comparten).

Cuando se definen normas de resolución, hay que especificar umbrales que contribuyan a la puntuación total de la resolución, lo que determina si una identidad de entrada se resuelve en una entidad existente:

- Los umbrales de candidatos especifican qué valores de datos de atributos se comparan para determinar si una identidad y una entidad se resolverán en una entidad compuesta. El umbral es la puntuación mínima a la que un determinado valor de atributo coincide entre la identidad de entrada y una entidad existente para que se satisfaga la regla de resolución.
- Los umbrales de confirmación/denegación especifican el peso de puntuación (positivo o negativo) que se aplica a valores de datos de atributos coincidentes o conflictivos cuando se habilita el uso de denegaciones.

También puede especificar el modo en que valores conflictivos para los mismos atributos afectan a la puntuación de resolución. Estos valores conflictivos se denominan denegaciones. Puede configurar normas de resolución que especifiquen que la regla no se cumple si hay conflictos (denegaciones) en los valores de atributos. También puede ajustar los umbrales correspondientes a una regla de resolución para crear denegaciones automáticas, basadas en que las puntuaciones de comparación no cumplen una o más de las puntuaciones de umbral especificadas. Cuando más alta se establece una puntuación de umbral, más exacta debe ser la coincidencia para que se satisfaga la regla de resolución.

Umbrales de candidatos

Los umbrales de candidatos son las primeras partes de una regla de resolución utilizada para determinar si una identidad de entrada realmente representa una entidad existente o representa una entidad completamente nueva.

Los umbrales de candidatos se configuran utilizando la Consola y son una parte integral de una regla de resolución. Por ejemplo, si una regla de resolución tiene un umbral de candidatos de número exclusivo, dicha regla de resolución se puede describir como una que necesita un número exclusivo coincidente.

Los umbrales de candidatos sólo se aplican a entidades existentes para colocar dicha entidad en la lista de candidatos como parte del proceso de resolución de

entidades. El umbral real es el nivel mínimo al que debe coincidir un tipo de datos en particular entre una identidad de entrada y una entidad existente para que el proceso de resolución de entidades añada la entidad existente a la lista de candidatos.

Precisión de la dirección:

La precisión de la dirección es el proceso de puntuación que utiliza el sistema de resolución de entidades para determinar si dos direcciones comparadas representan la misma dirección.

La precisión de la dirección se ha dividido en nueve niveles (1-9). La mayoría de las direcciones contienen componentes fundamentales que se pueden comparar, como calle (incluido número), ciudad, estado, código postal, postal+4. Cuando se comparan estos componentes, la precisión de la dirección empieza por un componente de calle coincidente y asigna el nivel de precisión 5. Luego este nivel de precisión se ajusta al alza o a la baja en función de si los componentes adicionales coinciden o difieren. Cada componente coincidente aumenta el nivel de previsión en 1 y cada componente no coincidente reduce el nivel de precisión en 1. Si el valor de un componente está presente en una dirección pero no hay ningún valor presente para el mismo componente en la otra dirección, no se realiza ningún ajuste de precisión.

De forma predeterminada, la resolución de entidades considera todas las direcciones comparadas con el nivel de previsión cinco o mayor como candidatos para direcciones coincidentes.

Tabla 29. Niveles de precisión de dirección

Nivel	Descripción
1	Calle coincide con todas las partes, postal+4 diferente. Esto significa que debe existir una dirección que coincide con todas las partes, pero los 4 dígitos adicionales del código postal son diferentes. Por ejemplo, 123 N Water St. Las Vegas, NV 89123-1234 y 123 S Water St. Las Vegas, NV 89123-5433.
2	Calle coincide y todas las demás partes difieren. Esto significa que solamente coincide la calle, y la Ciudad, el Estado, el Código postal y el País son todos diferentes o faltan. Por ejemplo, 123 Main St. Orlando, FL 32555 y 123 Main St. Las Vegas, NV
3	Calle coincide con modificador de diferencia -2. Esto significa que la dirección de calle coincide, pero el cálculo ascendió a -2. Por ejemplo, 123 Main St. Las Vegas, NV 89111 y 123 Main St. Las Cruces, NM.
4	Calle coincide con modificador de diferencia -1. Esto significa que la dirección de calle coincide, pero el cálculo ascendió a -1. Por ejemplo, 123 Main St. Las Vegas, NV 89111 y 123 Main St. Las Vegas, NM 54633.
5	Calle coincide con modificador 0 (valor de referencia). Esto significa que la dirección de calle coincide, pero el cálculo ascendió a 0. Por ejemplo, 123 Main St. Las Vegas, NV 89111 y 123 Main St.123 Main St.
6	Calle coincide con el modificador coincidente +1. Esto significa que la dirección de calle coincide, pero el cálculo ascendió a +1. Por ejemplo, 123 Main St. Las Vegas, NV 89111 y 123 Main St. Las Vegas

Tabla 29. Niveles de precisión de dirección (continuación)

7	Calle coincide con el modificador coincidente +2. Esto significa que la dirección de calle coincide, pero el cálculo ascendió a +2. Por ejemplo, 123 Main St. Las Vegas, NV 89111 y 123 Main St. Las Vegas, NV.
8	Calle coincide con todas las partes, falta postal+4. Esto significa que coinciden todas las partes de la dirección, pero falta el código postal junto con los 4 dígitos adicionales. Por ejemplo, 123 Main St. Las Vegas, NV 89111 y 123 Main St. Las Vegas, NV 89111
9	Coincidencia exacta (calle con todas las partes). Esta selección significa que coinciden todas las partes de la dirección, incluido el código postal con los 4 dígitos adicionales. Por ejemplo, 123 Main St. Las Vegas, NV 89111-1234 y 123 Main St. Las Vegas, NV 89111-1234 **Nota:** Esto no es aplicable a los códigos postales internacionales donde no se utilizan los 4 dígitos adicionales.

Nivel de precisión 1

Cada uno de los niveles de precisión, del uno al nueve, representa un nivel mayor de precisión con la excepción del nivel 1. El nivel 1 representa un caso especial, en el que la información de dirección puede ser la misma con la excepción de una designación de calle North/SouthEast/West, como por ejemplo, 456 North Main Street Sometown, Nevada y 456 South Main Street Sometown, Nevada. En este caso, las direcciones pueden ser las mismas, pero postal+4 es definitivamente diferente. A simple vista, puede parecer que estas direcciones requieren una resolución. Sin embargo, no se han podido resolver entre sí porque en realidad son diferentes. Debido a que este caso aparentemente tan claro de resolución de direcciones es de hecho un caso muy claro para no resolver las direcciones entre sí, el valor asignado al nivel de precisión de de este caso de ejemplo está al final de la escala (nivel 1) para impedir que se produzca este hecho.

El nivel 1 también puede indicar un error de dirección intencionado. Algunos clientes tienen interés en que se produzcan patrones intencionales de errores de dirección, personas que deliberadamente alteran una dirección para que se produzca un error. Por este motivo, el orden de las reglas de resolución se puede configurar de modo que considere un nivel de precisión de dirección más bajo, como por ejemplo, el nivel 1.

Nota: Si el nivel 1 es de interés para resolver entidades; por ejemplo, si desea saber si alguien da una información de dirección conflictiva en el nivel postal+4, debe crear una regla de resolución distinta. Dicha regla debe preceder a la regla de resolución predeterminada que considera que todos los niveles de precisión son de cinco y más. Debido a la complejidad que implica crear correctamente nuevas reglas de resolución, sólo debe hacerlo si dispone de la suficiente experiencia o con la ayuda de IBM.

Ejemplos detallados de precisión de la dirección:

En los siguientes ejemplos, se representan los datos comparados junto con las puntuaciones de precisión de dirección resultantes.

La primera dirección representa la dirección existente en la base de datos de entidades y la segunda es la dirección de entrada.

Nivel de precisión 1 - Calle coincide con todas las partes, postal+4 diferente.

Este caso muestra dos direcciones que están en la misma calle, pero que son direcciones diferentes. Una dirección está en el extremo norte de la calle y la otra en el extremo sur. Las únicas diferencias entre estas dos direcciones son los valores Código Postal+4.

CALLE	CIUDAD	ESTADO	CÓDIGO POSTAL
123 N Main St	Fairmount	IN	46928-1655
123 S Main St	Fairmount	IN	46928-1924

Nota: El nivel de precisión 1 representa un caso especial en el que la información de dirección puede ser la misma, salvo la excepción de la designación North/South o East/West de la calle. A simple vista, puede parecer que estas direcciones requieren una resolución. Sin embargo, no se deben resolver entre sí porque en realidad son direcciones distintas. Debido a que este caso aparentemente tan claro de resolución de direcciones es de hecho un caso muy importante para no resolver las direcciones entre sí, se ha colocado el valor de este escenario al final de la escala (nivel 1) para impedir que se resuelvan las direcciones.

Nivel de precisión 2 - Calle coincide con todas las partes que difieren.

Este ejemplo muestra dos direcciones con la misma información de calle, pero diferente ciudad, información de estado y de código postal. La segunda dirección es obviamente un error (quizás intencional) porque los códigos postales en Nevada empiecen todos por 89.

CALLE	CIUDAD	ESTADO	CÓDIGO POSTAL
123 E Main St	Fairmount	IN	46928
123 S Main St	Las Vegas	NV	46999

Nivel de precisión 3 - Calle coincide con modificador de diferencia -2.

En este ejemplo, sólo la información de calle coincide. No se proporciona ninguna información de estado en la dirección de entrada y la información de ciudad y código postal están en conflicto.

CALLE	CIUDAD	ESTADO	CÓDIGO POSTAL
123 E Main St	Delphi	IN	46923-1522
123 E Main St	Fairmount		46928

Nivel de precisión 4 - Calle coincide con modificador de diferencia -1.

Este ejemplo muestra dos direcciones con la misma información de calle y estado, pero diferente información de ciudad y código postal.

CALLE	CIUDAD	ESTADO	CÓDIGO POSTAL
123 E Main St	Delphi	IN	46923-1522
123 E Main St	Fairmount	IN	46928-1924

Nivel de precisión 5 - Calle coincide con modificador 0 (línea base)

En este ejemplo, sólo se proporciona la información de calle en la dirección de entrada. Aunque no contenga ninguna información de ciudad, estado o código postal, la coincidencia recibe la puntuación de precisión de dirección de línea base (5). La puntuación de decisión refleja las partes que faltan (a no confundir con las partes en conflicto ya que las partes que faltan no se puntúan).

CALLE	CIUDAD	ESTADO	CÓDIGO POSTAL
220 JEFFERSON	BUFFALO	IA	
220 Jefferson St.			

Nivel de precisión 6 - Calle coincide con el modificador coincidente +1.

Este ejemplo muestra una dirección de calle de entrada sin información de estado o de código postal, pero la misma información de calle y ciudad. La dirección de entrada es probablemente la dirección correcta, pero faltan datos.

CALLE	CIUDAD	ESTADO	CÓDIGO POSTAL
220 Washington	Syracuse	NY	
220 Washington Sq.	Syracuse		

Nivel de precisión 7 - Calle coincide con el modificador coincidente +2.

Este ejemplo muestra información de calle, ciudad y código postal coincidente, pero no se proporciona ninguna información de estado en la dirección de entrada.

CALLE	CIUDAD	ESTADO	CÓDIGO POSTAL
220 JEFFERSON	BUFFALO	IA	52728
220 Jefferson St.	Buffalo		52728

Nivel de precisión 8 - Calle coincide con todas las partes, falta postal+4.

Las dos direcciones siguientes son iguales, pero la higiene de dirección no ha podido validar las direcciones, por lo que no han recibido un código postal+4.

CALLE	CIUDAD	ESTADO	CÓDIGO POSTAL
220 JEFFERSON	BUFFALO	IA	52728
220 Jefferson St.	Buffalo	IA	52728

Nivel de precisión 9 - Coincidencia exacta (calle con todas las partes). Esta selección significa que coinciden todas las partes de la dirección, incluido el código postal con los 4 dígitos adicionales.

En este ejemplo, dos direcciones comparten la misma dirección de calle, ciudad, estado y Código Postal+4. Como resultado, las direcciones comparadas reciben la puntuación de dirección más alta.

Nota: Esto no es aplicable a los códigos postales internacionales donde no se utilizan los 4 dígitos adicionales.

CALLE	CIUDAD	ESTADO	CÓDIGO POSTAL
123 W Main St	Camden	IN	46917-9997
123 W Main	Camden	IN	46917-9997

Precisión de nombre:

La precisión de nombres es el proceso de puntuación que utiliza el sistema de resolución de entidades para determinar si dos nombres comparados representan el mismo nombre.

La puntuación de la precisión de nombres se basa en el uso de uno de estos dos posibles algoritmos.

- Name Comparator 1.0
- Name Comparator 2.0

Cada algoritmo tiene su propio conjunto de criterios de coincidencia de nombres que están disponibles para su configuración como parte de la configuración de reglas de resolución.

Cualquiera de estos dos algoritmos funciona con la característica Name Manager. Name Manager es una característica que se adquiere por separado que amplía la coincidencia de nombres a fin de incluir funciones adicionales de coincidencia basadas en consideraciones culturales exclusivas.

Consideraciones sobre la comparación

Name Comparator 1.0 es el valor predeterminado para instalaciones actualizadas de la versión 3.9.0 y anteriores. Name Comparator 2.0 es el valor predeterminado para instalaciones actualizadas de la versión 3.9.1 y posteriores y para instalaciones nuevas.

Cuando considere qué algoritmo se ajusta mejor a sus requisitos, tenga en cuenta las ventajas que ofrece cada uno de ellos.

Name Comparator 1.0:

- Necesita menos uso de CPU, lo que aumenta su rendimiento
- Permite una comprensión más precisa de por qué los nombres coinciden

Name Comparator 2.0:

- Maneja mejor los nombres que tienen más de tres palabras
- Compara mejor las frases con un orden incorrecto
- Realiza una mejor coincidencia de similares
- Compara mejor nombres de organizaciones
- Maneja mejor las iniciales

Name Comparator 1.0:

Este algoritmo de coincidencia de nombres está diseñado para que funcione principalmente con nombres consistentes en dos o tres palabras. Es el valor predeterminado de coincidencia de nombres para actualizaciones de la versión 3.9.0 o anteriores.

Name Comparator 1.0 compara dos nombres y luego clasifica su similitud según 15 niveles de similitud.

Tabla 30. Name Comparator 1.0 - Niveles de precisión

Nivel	Descripción
1	Sólo coincidencia parcial de Nombre o Primer apellido EJEMPLO: John Jacob Smith = Joe Smithson
2	Sólo coincidencia exacta de Nombre o Primer apellido EJEMPLO: John Jacob Smith = Jonathan Henry Smith
3	Coincidencia aleatoria ajustada EJEMPLO: Joe Smith = Joe Snith
4	Sólo los Primeros apellidos son distintos, pero sin orden EJEMPLO: Bob Jacob Smith = Jacob Bob Jones
5	Sólo los Primeros apellidos son distintos EJEMPLO: Bob Jacob Smith = Bob Jacob Jones
6	Los nombres estandarizados coinciden con algunas diferencias EJEMPLO: John Jacob Smith = Jonathan Henry Smith
7	Coincidencia de nombres estandarizados EJEMPLO: Joe W Anderson = Joseph Andersen
8	Coincidencia estandarizada con coincidencia exacta de Primeros apellidos, Inicio segundos apellidos, pero sin orden EJEMPLO: J Bob Smith = Robert J Smith
9	Coincidencia estandarizada con coincidencia exacta de Primeros apellidos, Inicio segundos apellidos EJEMPLO: Joe W Anderson = Joseph W Anderson
10	Coincidencia estandarizada con coincidencia exacta de Primeros apellidos, pero sin orden EJEMPLO: Bob Smith = Robert Smith
11	Coincidencia estandarizada con coincidencia exacta de Primeros apellidos EJEMPLO: John Jacob Smith = Johnny Jake Smith
12	Coincidencia de nombres en bruto con coincidencia de inicio segundos apellidos, pero sin orden EJEMPLO: Joe W. Brown = Will Joe Brown
13	Coincidencia de nombres en bruto con coincidencia de inicio segundos apellidos EJEMPLO: Joe W Anderson = Joe W Anderson
14	Coincidencia de nombres en bruto, pero sin orden EJEMPLO: John Bob Smith = Bob John Smith
15	Coincidencia de nombres en bruto EJEMPLO: Joe William Anderson = Joe William Anderson

Name Comparator 2.0:

Este algoritmo de coincidencia de nombres está diseñado para señalizar nombres comparados - divide el grupo de palabras de la serie del nombre en nombres individuales, o señales. Luego el algoritmo compara las señales y crea una puntuación para cada una de ellas. Es el valor predeterminado de coincidencia de nombres para instalaciones actualizadas de la versión 3.9.1 y posteriores y para instalaciones nuevas.

Name Comparator 2.0 agrupa los nombres en tres categorías, que luego compara y puntúa:

- Nombre de pila (nombre y segundo apellido – o todas las palabras excepto el primer apellido)
- Apellidos
- Nombre completo (nombre y apellidos)

Estas tres categorías de puntuación le permiten ajustar la coincidencia de nombres para reglas de resolución específicas de modo que se ajusten a sus requisitos de coincidencia de nombres. Las puntuaciones son números enteros, comprendidos entre 0 y 100, donde 0 es la puntuación más baja y 100 es la puntuación más alta. Cuanto más alta sea la puntuación de una categoría, mayor es la coincidencia entre los nombres de la categoría.

Consideraciones sobre la configuración - directrices para la puntuación

Siempre que edite o cambie valores de coincidencia de nombres para Name Comparator dos, utilice estas directrices para la puntuación como ayuda para configurar los umbrales de nombres de reglas de resolución. Estas directrices también resultan útiles para interpretar los resultados de la puntuación de estas categorías de puntuación del algoritmo.

Puntuación de nombre completo

De acuerdo con una escala de puntuación del 0 al 100, estas son las directrices para ayudarle a determinar el nivel de coincidencia para la puntuación de nombre completo:

- 100 = coincidencia exacta
- 90 = coincidencia muy buena (apropiado para la resolución del nombre y la fecha de nacimiento)
- 80 = coincidencia buena (apropiado para la mayoría de las reglas de resolución)
- 70 = coincidencia media (apropiado cuando también intervienen números exclusivos)
- Por debajo de 70 = no apropiado para establecer una coincidencia

Puntuación de nombre de pila

De acuerdo con una escala de puntuación del 0 al 100, estas son las directrices para ayudarle a determinar el nivel de coincidencia para la puntuación de Nombre de pila:

- 100 = coincidencia exacta
- 90 = coincidencia muy buena (puede denotar un intercambio de nombre y apellido)
- 85 = coincidencia aceptable mínima

- Por debajo de 85 = no apropiado para establecer una coincidencia; puede ser útil cuando se utiliza en combinación con Nombre de pila o Nombre completo para asegurar un cierto grado de similitud

Puntuación de apellido

De acuerdo con una escala de puntuación del 0 al 100, estas son las directrices para ayudarle a determinar el nivel de coincidencia para la puntuación de apellido:

- 100 = coincidencia exacta
- 90 = coincidencia muy buena (puede denotar un intercambio de nombre y apellido)
- 85 = coincidencia aceptable mínima
- Por debajo de 85 = no apropiado para establecer una coincidencia; puede ser útil cuando se utiliza en combinación con Nombre de pila o Nombre completo para asegurar un cierto grado de similitud

Puntuación de nombre de Name Manager:

El algoritmo de Name Manager puntúa los datos de nombre de entrada basándose en la agrupación del nombre en partes de nombre y luego en la determinación de la cultura para cada parte de nombre. A continuación, el algoritmo puntúa cada parte de nombre y las puntuaciones resultantes se utilizan durante la resolución de entidades.

Mientras que el algoritmo de Name Manager es independiente de los algoritmos de comparador de nombres (NC1 y NC2), debe seleccionar de todas formas NC1 o NC2. Durante el proceso de resolución de entidades, los nombres se puntúan primero basándose en los algoritmos de comparador de nombres seleccionado. Si nombre puntúa una coincidencia exacta, la resolución de entidades se salta la puntuación de Name Manager, porque la coincidencia de nombre exacta satisface la parte de puntuación de nombre de la norma de resolución. Sin embargo, si el nombre de entrada puntúa menos de una coincidencia exacta, el proceso de resolución de entidades puntúa el nombre utilizando el algoritmo de Name Manager.

En primer lugar, el algoritmo analiza el nombre en partes de nombre (nombre, apellido y nombre completo) y, a continuación, el algoritmo determina la cultura para cada parte de nombre. Finalmente, el algoritmo asigna a cada parte de nombre una puntuación y compara las puntuaciones con los umbrales de puntuación de Name Manager configurados para determinar hasta qué punto coinciden los nombres. Cuando más alto se establece el umbral de puntuación, mayor deber la coincidencia de las partes de nombre de los datos de nombre de entrada con las partes de nombre de la entidad existente en la base de datos de entidades.

Precisión de la fecha de nacimiento:

La precisión de la fecha de nacimiento es el proceso de puntuación que utiliza el sistema de resolución de entidades para determinar si dos fechas de nacimiento comparadas representan la misma fecha.

Esta comparación tiene en cuenta las diversas medidas de similitud de la series de fecha de nacimiento, entre ellas: las posiciones de enteros, transposiciones, deltas del día y valores de año. Las medidas se analizan para determinar una puntuación de similitud comprendida entre 2 y 100. Puede configurar los valores de precisión de fecha de nacimiento según cuatro categorías de similitud:

- Exacto - coincidencia de 100 puntos
- Ajustado - coincidencia >= 90 puntos
- Medio - coincidencia >= 85 puntos
- Inexacto - coincidencia >= 80 puntos

Consideraciones sobre la configuración

El sistema ofrece un valor preconfigurado de Ajustado como nivel mínimo de similitud para que una regla de resolución considere que dos fechas de nacimiento comparadas son la misma. El hecho de cambiar este valor afectará al número de coincidencias y puede afectar al número de resoluciones de entidades que realiza el sistema. Considere detenidamente si se debe modificar este valor y asegúrese de probar cualquier cambio antes de implementarlo en un entorno de producción.

Ejemplos detallados de precisión de la fecha de nacimiento:
Los siguientes ejemplos representan los datos comparados junto con las puntuaciones de precisión de fecha de nacimiento resultantes. La primera fecha de nacimiento representa la fecha de nacimiento existente para una entidad en la base de datos de entidades y la segunda fecha de nacimiento es para una entidad de fecha de nacimiento de entrada.

Nivel de precisión: Exacto (100 puntos)

Este caso muestra dos fechas exactas. El algoritmo generará una coincidencia de 100 puntos.

FECHA DE NACIMIENTO	ESTADO
1963/12/01	Existente
1963/12/01	Entrante

Nivel de precisión: Ajustado (90 puntos)

En este caso se muestran dos fechas cuya precisión es mayor o igual que 90 puntos. En el ejemplo se muestran dos valores de fecha de nacimiento con el mismo valor de año y día, pero el valor de mes difiere de un mes.

FECHA DE NACIMIENTO	ESTADO
1963/12/01	Existente
1963/11/01	Entrante

Nivel de precisión: Medio (85 puntos)

En este caso se muestran dos fechas cuya puntuación de precisión es mayor o igual que 85 puntos. En el ejemplo, se muestran dos valores de fecha de nacimiento con el mismo valor de mes y día, pero los dos últimos dígitos del valor de año se transfieren.

FECHA DE NACIMIENTO	ESTADO
1963/12/01	Existente
1936/12/01	Entrante

Nivel de precisión: Inexacto (80 puntos)

En este caso se muestran dos fechas cuya puntuación de precisión es mayor o igual que 80 puntos. El ejemplo muestra dos valores de fecha de nacimiento con el mismo valor de mes y día, y valor del tercer dígito del año incorrecto (pero sigue siendo un valor racional para una fecha de nacimiento).

FECHA DE NACIMIENTO	ESTADO
1963/12/01	Existente
1933/12/01	Entrante

Visualización de normas de resolución

Antes de añadir o suprimir normas de resolución, puede ver el conjunto actual de normas de resolución.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Resolución**.
3. Pulse la pestaña **Normas de resolución**.
4. En la lista desplegable **Config resolución**, seleccione una configuración de resolución.
5. Para ver los detalles de normas de resolución específicas, pulse en el enlace de la fila que contiene la regla de resolución que desea ver.

Creación de normas de resolución

Después de considerar detenidamente los requisitos de la empresa y revisar las normas de resolución existentes, puede decidir crear nuevas normas de resolución para los datos.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Resolución**.
3. Pulse la pestaña **Normas de resolución**.
4. En la lista desplegable **Config resolución**, seleccione una configuración de resolución.
5. Pulse el botón **Nuevo**.
6. En el panel **General**, especifique los valores que se deben utilizar al comparar datos de dos entidades
7. Pulse la pestaña **Umbrales de candidato**.
8. En el panel **Umbrales de candidato**, especifique los valores de umbral para los datos.
9. Pulse la pestaña **Umbrales de Confirmar/Denegar**.
10. En el panel **Umbrales de Confirmar/Denegar**, especifique los valores de umbral para los datos.
11. Pulse el botón **Guardar**.

Supresión de normas de resolución

Para eliminar una regla de resolución y no tomarla en consideración durante el proceso de resolución de entidades, suprima la regla.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Resolución**.
3. Pulse la pestaña **Normas de resolución**.
4. En la lista desplegable **Config resolución**, seleccione una configuración de resolución.
5. Marque el recuadro de selección situado junto a las normas de resolución que desea suprimir.
6. Pulse el botón **Suprimir**.
7. En la ventana de confirmación, pulse **Aceptar** para suprimir la configuración de resolución.

Temas de ayuda

Ventana Reglas de resolución:

Utilice esta ventana para ver las reglas de resolución contenidas dentro de una configuración de resolución. Las reglas de resolución se procesan en el orden listado. Una vez satisfecha una regla de resolución, las puntuaciones de resolución asignadas se aplican i, si la regla está configurada para desencadenar una resolución, la entidad de entrada se resuelve en la entidad existente y no se tiene en cuenta ninguna otra regla de resolución de entidades para dicha comparación en particular.

Orden Orden en el que se aplican las reglas de resolución a la identidad de entrada comparada y a la entidad existente

Descripción
Descripción de la regla de resolución

Confianza de resolución
Puntuación de resolución que se aplica a la comparación si se satisface la regla

Confianza de relación
Puntuación de relación que se aplica a la comparación si se satisface la regla

Resolver desencadenantes
Si la regla resuelve automáticamente la identidad de entrada en la entidad existe en el caso de que se satisfaga la regla

Reglas de resolución - Panel General:

Utilice este panel para configurar una nueva regla de resolución o para ver los detalles de una regla de resolución existente.

Orden Especifique un número exclusivo que indique el orden en el que se debe procesar la regla.

Descripción
Especifique la descripción de la regla.

Confianza de resolución
Especifique un porcentaje de confianza de resolución si la regla tiene éxito. Sólo se tiene en cuenta 100% para la resolución.

Confianza de relación
Especifique un porcentaje de confianza de relación si la regla tiene éxito. Sólo se tiene en cuenta 100% para la resolución.

Resolver desencadenantes
Seleccione "Sí" para resolver la identidad de entrada y la entidad existente si la confianza de resolución y la de relación son 100%.

Denegaciones habilitadas
Seleccione "Sí" para habilitar el proceso de confirmaciones/denegaciones. De lo contrario, no se producirá ningún proceso de denegación.

Denegaciones de característica habilitadas
Seleccione "Sí" para habilitar el proceso de confirmaciones/denegaciones de característica. De lo contrario, no se producirá ningún proceso de denegación de característica.

Reglas de resolución - Panel Umbrales de candidato:

Utilice este panel para especificar los valores de los umbrales de candidato de una nueva regla de resolución o para ver los detalles de los umbrales de candidato de una regla de resolución existente. Estos valores definen la regla de resolución **descripción** especificada en el panel **General** de Resolución.

Umbral de precisión de dirección
Seleccione la puntuación mínima de dirección necesaria para que se considere que se satisface la regla.

Umbral de dirección aproximada
Seleccione el número mínimo de coincidencias necesarias en el valor de dirección aproximada para que se considere que se satisface la regla.

Umbral de proximidad
Seleccione el número mínimo de direcciones necesarias dentro del área definida en la regla de calidad para que se considere que se satisface la regla.

Umbral de número exclusivo
Seleccione el número mínimo de coincidencias de número exclusivo para que se considere que se satisface la regla.

Umbral de número no exclusivo
Seleccione el número mínimo de coincidencias de número no exclusivo para que se considere que se satisface la regla.

Umbral de característica
Seleccione el número mínimo de coincidencias de característica para que se considere que se satisface la regla.

Umbral de correo electrónico
Seleccione el número mínimo de coincidencias de correo electrónico para que se considere que se satisface la regla.

Umbral de datos de resumen
Seleccione el número mínimo de coincidencias de número exclusivo, otro número, dirección, característica y correo electrónico para que se considere que se satisface la regla.

Umbral de resumen
Seleccione el número mínimo de coincidencias de proximidad de dirección, dirección aproximada, número ajustado y DOB para que se considere que se satisface la regla.

Normas de resolución - Panel Umbrales de confirmación/denegación:

Utilice esta pestaña para especificar los valores de umbral de confirmación y denegación de una nueva regla de resolución o para ver los detalles de umbral de confirmación y denegación de una regla de resolución existente.

Umbral de número ajustado
Seleccione el número mínimo de coincidencias de número ajustado para que se considere que se satisface la regla.

Umbral de fecha de nacimiento
Seleccione la puntuación mínima de coincidencias de fecha de nacimiento para que la regla se considere satisfecha.

Valores de Name Comparator
Estos valores determinan los requisitos de precisión de nombres para la resolución de entidades. Estos valores de trabajo funcionan solos o con el valores de Name Manager.

Umbral de puntuación de nombre de pila
Especifique el umbral de puntuación para el nombre de pila de 0 a 100.

Umbral de puntuación de apellido
Especifique el umbral de puntuación para el apellido de 0 a 100.

Umbral de puntuación de nombre completo
Especifique el umbral de puntuación para el nombre completo de 0 a 100.

Valores de Name Manager
Name Manager amplía la precisión estándar de nombres para incluir consideraciones culturales importantes. Estos valores sólo se aplican si se ha configurado Name Manager.

Umbral de puntuación de nombre de pila
Especifique la puntuación mínima de nombre de pila para que la regla se considere satisfecha.

El umbral debe ser un valor entero entre 0 y 100. Cuanto más alta es la puntuación, más exacta es la coincidencia. Normalmente, una puntuación por debajo de 70 no es adecuada para la coincidencia, pero puede ser útil al combinarse con Apellido o Nombre completo para asegurar alguna similitud.

Umbral de puntuación de apellido
Especifique la puntuación mínima de apellido para que se considere que se ha satisfecho la regla.

El umbral debe ser un valor entero entre 0 y 100. Cuanto más alta es la puntuación, más exacta es la coincidencia. Normalmente, una puntuación por debajo de 70 no es adecuada para la coincidencia, pero puede ser útil al combinarse con Nombre de pila o Nombre completo para asegurar alguna similitud.

Umbral de puntuación de nombre completo
Especifique la puntuación de nombre completo mínima para que se considere que se satisface la regla.

El umbral debe ser un valor entero entre 0 y 100. Cuanto más alta es la puntuación, más exacta es la coincidencia. Normalmente, una puntuación por debajo de 70 no es adecuada para la coincidencia.

Personalización del creador de candidatos

Puede cambiar los valores del creador de candidatos utilizando configuraciones del creador de candidatos. Los cambios en el creador de candidatos se realizan mediante la Consola de configuración.

Creador de candidatos

La característica creador de candidatos define criterios que el sistema utiliza para añadir una entidad existente a la lista de candidatos como parte del proceso de resolución de entidades.

Los valores típicos del creador de candidatos incluyen dirección, números exclusivos y otros números. Estos son los tipos de datos que el sistema compara para determinar qué entidades existentes se pueden resolver en una identidad de entrada. Cuando un nuevo registro de entidad entra en el sistema, si una entidad existente tiene un valor coincidente para cualquiera de los tipos de datos identificados por el creador de candidatos, dicha entidad se añade a la lista de candidatos.

Configuraciones del creador de candidatos

Los valores del creador de candidatos se organizan por grupos llamados configuraciones del creador de candidatos. Sólo se puede utilizar una configuración del creador de candidatos dentro de una configuración de resolución.

Las configuraciones del creador de candidatos que se incluyen con el producto son:

- **Predeterminado** - este valor incluye dirección, número exclusivo, otro número como criterios para incluir una entidad en la lista de candidatos.
- **Predeterminado sólo con nombre** - este valor incluye nombres como un criterio para incluir una entidad en la lista de candidatos. Este valor está diseñado para que se utilice cuando los datos de la entidad sólo pueden contener nombres o nombres y muy pocos de los otros tipos de datos.

Consideraciones sobre la configuración

Los genéricos afectan directamente a si un valor se considera parte del proceso del creador de candidatos. Después de que un valor se considere un valor genérico, se deja de utilizar para generar listas de candidatos.

Los valores del creador de candidatos afectan directamente al rendimiento del sistema. Cuando el sistema utiliza búsquedas de índice para comparar una entidad de entrada con cada una de las entidades de la base de datos de entidades, sólo compara tipos de datos que están configurados en la característica creador de candidatos. Esto permite generar listas de candidatos con gran rapidez. A medida que la base de datos de entidades crece e incluye más entidades, hay más material de comparación para el creador de candidatos. Por ejemplo, si la base de datos de entidades contiene 100.000 entidades y el creador de candidatos está definido de modo que compare tres tipos de datos al cuando cree la lista de candidatos, siempre que entra una nueva identidad en el sistema, el sistema puede realizar hasta 300.000 comparaciones sólo para generar la lista de candidatos. SI la base de datos de entidades contiene 1.000.000 de entidades y el creador de candidatos está definido de modo que compare tres tipos de datos cuando cree la lista de candidatos, siempre que una nueva identidad entra en el sistema, el sistema puede realizar hasta 3.000.000 de comparaciones sólo para generar la lista de candidatos. Si añade un solo criterio del creador de candidatos, el sistema puede realizar

1.000.000 de comparaciones adicionales sólo para generar una lista de candidatos. Esto forma un total de 1.000.000 de comparaciones adicionales por registro de identidad cargado en el sistema. Si las listas de candidatos son demasiado largas porque tienen en cuenta demasiados tipos de datos, la ejecución del proceso de resolución de entidades será mucho más lenta que si los valores del creador de candidatos sólo contuvieran los tipos de datos necesarios para crear listas de candidatos efectivas.

Cuando considere si se debe utilizar el valor de configuración **Predeterminado** o **Predeterminado sólo con nombre**, recuerde que si elige **Predeterminado sólo con nombre**, está añadiendo comparaciones en un orden de magnitud superior que las que necesita la configuración **Predeterminado**.

Listas de candidatos

Las listas de candidatos son las listas de entidades que tienen el potencial de coincidir con el registro de identidad de entrada. La lista de candidatos se crea recuperando aquellas entidades que comparten atributos con la identidad de entrada, según los atributos especificados en la configuración del creador de candidatos.

El proceso de resolución de entidades sólo utiliza las entidades de la lista de candidatos para resolver entidades y para resolver relaciones.

Puesto que la resolución de entidades y la detección de relaciones se determinan en función de atributos, debe examinar detenidamente los atributos de los orígenes de datos para determinar qué atributos crean los candidatos más firmes.

Una vez generada la lista de candidatos, el proceso de resolución de entidades compara la identidad de entrada con el primer candidato de la lista utilizando las reglas de resolución configuradas. El sistema utiliza las reglas de resolución, en orden, para calcular una puntuación de resolución que represente cuánto se parecen los atributos de la identidad de entrada con los de la entidad candidata. Si los atributos de la identidad de entrada se ajustan o superan la puntuación de resolución correspondiente a dicha regla, el registro de la identidad de entrada se resuelve en la entidad candidata.

Si la puntuación de resolución no se ajusta ni supera el conjunto de puntuaciones de resolución correspondiente a dicha regla de resolución, el sistema pasa a la siguiente regla de resolución hasta que se el registro de la identidad de entrada se resuelva en una entidad candidata o hasta que se agoten todas las reglas de resolución.

Si el registro de la identidad de entrada no se resuelve en una entidad existente, el sistema resuelve el registro en una nueva entidad y guarda la nueva entidad en la base de datos de entidades.

Creación de configuraciones del creador de candidatos

Puede utilizar la Consola de configuración para crear nuevos grupos de valores del creador de candidatos. Estas configuraciones del creador de candidatos son útiles porque es una forma fácil de aplicar diversos valores configurados del creador de candidatos cambiando solamente un único valor.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Resolución**.

3. Pulse la pestaña **Creador de candidatos**.
4. Asegúrese de que la lista desplegable **Configuración del creador de candidatos** visualiza **- - - Seleccionar uno - - -**, después pulse el botón **Nuevo**.
5. En el campo **Configuración del creador de candidatos**, escriba el nombre de la nueva configuración del creador de candidatos.
6. En el campo **Tipo de coincidencia**, elija el primer tipo de datos que desea utilizar como criterio de candidato para la resolución.
7. En el campo **Nombre de segmento**, escriba el nombre del segmento UMF donde se pueden encontrar los datos de tipo de coincidencia.
8. Pulse el botón **Guardar**.

Qué hacer a continuación

Ahora, la configuración del creador de candidatos que acaba de crear se visualiza en la lista desplegable **Configuración del creador de candidatos**, lo que permite añadir criterios a esta configuración nueva.

Adición de criterios a configuraciones del creador de candidatos

Puede utilizar la Consola de configuración para añadir tipos de datos a configuraciones del creador de candidatos existentes que especifican determinados tipos de datos como criterios para añadir una entidad existente a la lista de candidatos como parte del proceso de resolución de entidades.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Resolución**.
3. Pulse la pestaña **Creador de candidatos**.
4. Elija una configuración en la lista desplegable **Configuración del creador de candidatos**.
5. Pulse el botón **Nuevo**.
6. Elija un tipo de datos en la lista desplegable **Tipo de coincidencia**.
7. En el campo **Nombre de segmento**, escriba el nombre del segmento UMF donde se pueden encontrar los datos de tipo de coincidencia.
8. Pulse el botón **Guardar**.

Qué hacer a continuación

Ahora, el sistema tendrá en cuenta el tipo de datos que acaba de especificar al construir listas de candidatos como parte del proceso de resolución de entidades.

Supresión de configuraciones del creador de candidatos

Puede suprimir una configuración del creador de candidatos utilizando la Consola de configuración. Puede que desee suprimir una configuración del creador de candidatos que haya creado que ya no desee utilizar.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Resolución**.
3. Pulse la pestaña **Creador de candidatos**.
4. Seleccione una configuración en la lista desplegable **Configuración del creador de candidatos**.

5. Seleccione la casilla situada junto a cualquier tipo de coincidencia que desee suprimir.
6. Pulse el botón **Suprimir**. Aparece una ventana de confirmación que indica `Los registros seleccionados se suprimirán.`
7. Pulse **Aceptar** para confirmar la supresión de la configuración del creador de candidatos.

Qué hacer a continuación

La colección de valores del creador de candidatos que acaba de suprimir ya no se podrá utilizar para generar listas de candidatos como parte del proceso de resolución de entidades.

Temas de ayuda

Ventana Creador de candidatos:

Utilice esta ventana para ver una lista de valores del creador de candidatos. Los valores del creador de candidatos están agrupados por configuraciones del creador de candidatos.

Configuración del creador de candidatos: campo
Seleccione la configuración del creador de candidatos cuyos valores desea ver.

Tipo de coincidencia
Escriba los datos que deben coincidir entre una identidad de entrada y una entidad existente para que dicha entidad existente se añada a la lista de candidatos para la resolución de entidades.

Nombre de segmento
Nombre del segmento UMF en el que se encuentran los datos del tipo de coincidencia.

Secuencia de coincidencia
Número de grupo del orden en el que se comparan los criterios de la lista de candidatos.

Creador de candidatos - Panel General:

Utilice este panel para definir un nuevo criterio del creador de candidatos o para ver los detalles de un criterio del creador de candidatos existente.

Configuración del creador de candidatos
Configuración del creador de candidatos a la que pertenece este criterio

Tipo de coincidencia
Seleccione el tipo de datos que desea comparar para que la entidad existente se tenga en cuenta como un candidato para la resolución.

Nombre de segmento
Escriba el nombre del segmento UMF en el que se pueden encontrar los datos del tipo de coincidencia: Unique & Other Number = NUMBER; Address = ADDRESS; Characteristic = ATTRIBUTE; Name = NAME; Email = EMAIL_ADDR

Configuración de confirmaciones y denegaciones

Puede ajustar los valores de confirmación y denegación para cambiar las puntuaciones de resolución de entidades comparadas.

Acerca de esta tarea

Las confirmaciones y denegaciones pueden verse y modificarse utilizando la consola, en la pestaña **Normas de resolución**.

Confirmaciones y denegaciones

Después de que se cree una lista de candidatos y de que se comparen los criterios de resolución básicos, la resolución de entidades compara criterios adicionales para reforzar o debilitar una puntuación de resolución. Estos criterios adicionales son confirmaciones y denegaciones.

Las confirmaciones y denegaciones comparan los siguientes tipos de datos:

- Fecha de nacimiento
- Número exclusivo
- Generación
- Características
  - Puede especificar cualquier característica para que se utilice como parte de las confirmaciones y denegaciones.

El peso de la confirmación es un valor que se utiliza para aplicar más peso a la puntuación de resolución base de dos entidades comparadas. El peso de la denegación es el valor (generalmente un valor negativo) que se utiliza para aplicar menos peso a la puntuación de resolución base de dos entidades comparadas.

Ejemplo

Una configuración de resolución puede tener un valor de confirmación de fecha de nacimiento de +10 y un valor de denegación de -20. Si el registro entrante comparte una fecha común de nacimiento con una entidad candidata, se añadirá un valor de 10 a la puntuación de la resolución. Si tienen fechas de nacimiento distintas, se restará un valor de 20 de la puntuación de la resolución.

Nota: Los pesos de confirmación y de denegación de la fecha de nacimiento se aplican a la puntuación de resolución asignada por una regla de resolución específica. No es lo mismo que el parámetro **DOBConfThreshold** que se configura en el archivo de configuración de la interconexión.

Visualización de confirmaciones y denegaciones de características

Antes de crear nuevas confirmaciones y denegaciones, puede consultar la lista actual de tipos de características que se utilizan durante la resolución de entidades.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **Resolución**.
3. Pulse la pestaña **Características**.
4. En la lista desplegable **Config resolución**, seleccione una configuración de resolución.

Creación de confirmaciones y denegaciones de características

Puede especificar cualquier tipo de característica como criterio para la resolución de entidades añadiéndola a la lista de confirmaciones y denegaciones de características.

Antes de empezar

Debe haber configurado el uso de la resolución del tipo de característica que se debe confirmar/denegar al configurar los valores de resolución del tipo de característica.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Resolución**.
3. Pulse la pestaña **Características**.
4. En la lista desplegable **Config resolución**, seleccione una configuración de resolución.
5. Pulse el botón **Nuevo**.
6. En el campo **Número de grupo** del panel **General**, escriba el número del grupo que desea aplicar a esta característica.
7. En el campo **Descripción**, escriba una descripción del tipo de característica que se configura.
8. En la lista desplegable **Tipo de característica**, seleccione el tipo de característica que desea configurar.
9. En el campo **Peso de confirmar**, escriba el valor (en una escala de 1-100) que se debe añadir a la puntuación de similitud (si las entidades comparadas satisfacen los requisitos de confirmación).
10. En el campo **Peso de denegar**, escriba utilizando un signo menos (-) el valor negativo (en una escala de 1-100) que se debe restar a la puntuación de similitud (si las entidades comparadas satisfacen los requisitos de denegación).
11. Pulse el botón **Guardar**.

Supresión de confirmaciones y denegaciones de características

Para eliminar un tipo de característica de la consideración de criterio para la resolución de entidades, elimínela de la lista de confirmaciones y denegaciones de características.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **Resolución**.
3. Pulse la pestaña **Características**.
4. En la lista desplegable **Config resolución**, seleccione una configuración de resolución.
5. Marque el recuadro de selección situado junto a los tipos de características que desea suprimir.
6. Pulse el botón **Suprimir**.
7. En la ventana de confirmación, pulse **Aceptar** para suprimir la configuración de resolución.

Temas de ayuda

Ventana Confirmaciones y denegaciones:

Utilice esta ventana para configurar el proceso de configuración y denegación de resolución de entidades. Puede especificar puntuaciones de confirmación y denegación para que se añadan a la puntuación de resolución, así como el orden en el que se procesarán las confirmaciones y denegaciones. Después de que

satisfaga una confirmación o denegación, se aplica la puntuación correspondiente y el resto de confirmaciones y denegaciones no se procesan. Las conformaciones aplican una puntuación positiva y las denegaciones aplican una puntuación negativa.

Orden Orden del proceso actual

Descripción
Descripción de la confirmación o denegación

Puntuación
Especifique un modificador de puntuación positivo o negativo para la confirmación/denegación dada.

Reordenar
Pulse las flechas (hacia arriba o hacia abajo) para mover la confirmación o la denegación una posición en la dirección correspondiente. Puesto que el proceso se detiene cuando se satisface la primera confirmación o denegación, el hecho de seleccionar el orden adecuado es importante puesto que puede tener un impacto significativo sobre los resultados del proceso de resolución de entidades.

Ventana Características:

Utilice esta ventana para ver una lista de características de entidad cuyas comparaciones están configuradas de modo que afecten a la puntuación de la resolución de entidades. Esto sólo afecta a la puntuación de la resolución de entidades si el valor de **Denegaciones de características habilitadas** en el panel **Reglas de resolución - General** está establecido en Sí.

Descripción
Nombre de la característica que se va a comparar

Tipo de característica
Nombre del sistema del tipo de característica que se va a comparar

Peso de confirmar
Valor que se añade al proceso de puntuación de la resolución de entidades si los valores comparados de la característica coinciden

Peso de denegar
Valor que se añade al proceso de puntuación de la resolución de entidades si los valores comparados de la característica no coinciden

Resolución - Características - Panel General:

Utilice este panel para configurar una nueva confirmación/denegación de característica o para ver los detalles de una confirmación/denegación de característica existente.

Grupo Especifique un número que indique el orden en el que se debe procesar la confirmación/denegación de característica.

Descripción
Especifique la descripción de la confirmación/denegación.

Tipo de característica
Seleccione el tipo de característica correspondiente a la confirmación/denegación.

Peso de confirmar
Especifique la puntuación que se va a añadir a la puntuación de la resolución de entidades si los valores comparados de la característica coinciden.

Peso de denegar
Especifique la puntuación negativa que se va a añadir a la puntuación de la resolución de entidades si los valores comparados de la característica no coinciden.

Configuración de parámetros del sistema

Puede configurar determinadas características del sistema Identity Insight.

Configuración de parámetros del sistema para la puntuación de nombre

Puede configurar el algoritmo de puntuación de nombres que desee utilizar al generar una lista de candidatos como parte del proceso de resolución de entidades.

Procedimiento

1. En la Consola de configuración, seleccione **Configurar** > **General** > **Parámetros del sistema**.
2. En la lista **Grupo de parámetros**, seleccione el grupo de parámetros **NAME_MATCHING**.
3. Seleccione el parámetro de sistema **ALGORITHM**.
4. En **Valor actual**, especifique el valor entero del algoritmo de comparador de nombres a utilizar. Para devolver este parámetro de sistema al valor predeterminado, escriba el valor que se visualiza en **Valor predeterminado**, en el campo **Valor actual**.

   Nota: El comparador de nombres 2 es el algoritmo de puntuación de nombre predeterminado para las versiones de producto 3.9.1 y posteriores.
5. Pulse **Guardar**.

Configuración de parámetros de sistema para Name Manager

De forma predeterminada, los parámetros de sistema de puntuación de nombres de Name Manager se configuran al instalar el producto. Pero puede actualizar los parámetros de sistema predeterminados, cuando sea necesario. Por ejemplo, puede que necesite cambiar la ubicación de las bibliotecas de soporte de Name Manager.

Acerca de esta tarea

Establezca la vía de acceso en las bibliotecas de soporte de Name Manager y habilite la categorización de nombres por tipo mediante los parámetros de sistema de Name Manager. Establezca también el parámetro de sistema **CROSSCHECKCULTURE** para configurar el proceso de nombres entre distintas culturas de nombres.

Procedimiento

1. En la Consola de configuración, seleccione **Configurar** > **General** > **Parámetros del sistema**.
2. En la lista **Grupo de parámetros**, seleccione el grupo de parámetros **NAMEMANAGER**.

3. En el panel izquierdo, seleccione el parámetro de sistema de Name Manager que desea configurar:

parámetro del sistema de Name Manager	Descripción
SUPPORTPATH	Indica la ubicación de los archivos de soporte de Name Manager. El valor predeterminado es ./data, que es una vía de acceso relativa al directorio de producto de nivel superior. Si los archivos de soporte se mueven a una ubicación distinta durante la instalación, modifique este valor a la vía de acceso absoluta de la nueva ubicación.
NAMESIFTER	Indica si la funcionalidad de categorización de nombres por tipo de nombre (nombres personales u organización) está activada. Para habilitar la categorización de nombres de tipo (funcionalidad Tamiz de nombres), entre 1 (nuevo valor predeterminado de instalación) en **Valor actual** Para inhabilitar la categorización de nombres de tipo (funcionalidad de Tamiz de nombres), entre 0 (valor predeterminado de actualización) en **Valor actual**
CROSSCHECKCULTURE	Indica si se debe realizar la puntuación de nombres de Name Manager entre culturas de nombre cuando las culturas de nombre son diferentes. Para comprobar solo la cultura de nombre de entrada antes de puntuar ambos nombres, especifique 0 en **Valor actual**. Para comprobar los valores de cultura de nombre antes de puntuarlos (nuevo valor predeterminado de instalación), escriba 1 en **Valor actual**.

Atención: El parámetro de sistema **CROSSCHECKCULTURE** afecta a la manera en que la resolución de entidad maneja la puntuación de nombres por cultura en las interconexiones. Antes de cambiar este parámetro de sistema respecto a su valor actual, consulte los servicios o el soporte de IBM.

4. Pulse **Guardar**.

Configuración de parámetros del sistema para la base de datos

Puede configurar el tamaño máximo de cualquier cláusula IN de lista de candidatos creada por la interconexión durante la resolución de entidades.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Parámetros del sistema**.
4. En la lista desplegable **Grupo de parámetros**, seleccione el grupo de parámetros **DB_CONFIG**.

5. Pulse el parámetro del sistema **MAX_IN_CLAUSE**.
6. En el campo **Valor actual**, escriba el número máximo de caracteres que desea incluir en una cláusula IN al generar una lista de candidatos como parte del proceso de resolución de entidades. Los valores válidos son cualquier entero de 0 a 1000. Para devolver este parámetro a su valor predeterminado, escriba el valor que se visualiza en el campo **Valor predeterminado**, en este campo.

   Nota: Este valor afecta al rendimiento de la base de datos. Basándose en el tamaño de la base de datos y las posibilidades del hardware del sistema, considere detenidamente el valor que especifica para este parámetro.
7. Pulse **Guardar**.

Configuración de parámetros del sistema para los registros

Puede configurar el nivel de registro que desea utilizar para tablas de resolución de entidades específicas en la base de datos.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configurar**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Parámetros del sistema**.
4. En el menú desplegable **Grupo de parámetros**, seleccione el parámetro del sistema **LOG_LEVEL**.
5. Pulse el nombre del parámetro que desea configurar.
6. En el campo **Valor actual**, escriba el nivel de registro que desea aplicar a este código de parámetro. Los valores válidos se listan y describen en el campo **Descripción de parámetro**. Para devolver este parámetro a su valor predeterminado, escriba el valor que se visualiza en el campo **Valor predeterminado**, en este campo.

   Nota: Este valor afecta al rendimiento de la base de datos y los componentes tales como el Visualizador. Basándose en el tamaño de la base de datos y las posibilidades del hardware del sistema, considere detenidamente el valor que especifica para este parámetro. Por ejemplo, si se establece LOG_LEVEL por debajo de 4 para algunas tablas, el Visualizador puede dejar de funcionar, incluyendo:
   - ER_DETAIL
   - ER_ENTITY_SCORE
   - ER_ENTITY_STATE
   - ER_RELOCATION
7. Pulse **Guardar**.

Configuración de parámetros del sistema para confirmación y denegación

Puede especificar si desea realizar todas las comparaciones de confirmación y denegación que están configuradas. O puede especificar que estas comparaciones se realicen en el orden configurado hasta que se satisfaga una de las confirmaciones o denegaciones. Si se utiliza la segunda opción, los tiempos de proceso pueden ser más rápidos.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Parámetros del sistema**.
4. En el menú desplegable **Grupo de parámetros**, seleccione el grupo de parámetros **MM**.
5. Pulse el parámetro del sistema **MULTICONFIRMATION**.
6. En el campo **Valor actual**, escriba `1` para que se procesen todas las confirmaciones y denegaciones, y para todas aquellas cuya condición se satisfaga, se aplique la suma de cambios en su puntuación para la regla de resolución que se está procesando. O bien, escriba `0` para que se procesen todas las confirmaciones y denegaciones en el orden especificado, deteniéndose en la primera cuya condición se satisfaga y aplicando el cambio en su puntuación a la regla de resolución que se está procesando. Para devolver este parámetro a su valor predeterminado, escriba el valor que se visualiza en el campo **Valor predeterminado**, en este campo.
7. Pulse **Guardar**.

Configuración de parámetros del sistema para alertas de rol

Puede configurar si desea informar de todas las alertas de rol generadas por una regla de resolución de entidades para una entidad de entrada o si desea informar sólo de la alerta de rol más importante generada por una regla de resolución de entidades para una entidad de entrada.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Parámetros del sistema**.
4. En el menú desplegable **Grupo de parámetros**, seleccione el grupo de parámetros **MM**.
5. Pulse el parámetro del sistema **REPORT_SAME_CONFLICTS**.
6. En el campo **Valor actual**, escriba `1` para informar de todas las alertas de rol generadas por cada regla de resolución para una entidad de entrada. O bien escriba `0` para informar sólo de la alerta de rol más importante generada por cada regla de resolución para una entidad de entrada. Para devolver este parámetro a su valor predeterminado, escriba el valor que se visualiza en el campo **Valor predeterminado**, en este campo.
7. Pulse **Guardar**.

Configuración de parámetros del sistema para generadores de alertas de atributo

Puede configurar el número inicial de días que estará activo un nuevo generador de alertas de atributo antes de que caduque.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Parámetros del sistema**.
4. En el menú desplegable **Grupo de parámetros**, seleccione **PERSISTENT_SEARCH**.

5. Pulse el parámetro del sistema **SEARCH_EXPIRATION_TIME**.
6. En el campo **Valor actual**, escriba el número inicial de días que desea que esté activo un nuevo generador de alertas de atributo antes de que caduque. Los usuarios del Visualizador pueden especificar otra fecha de caducidad, pero este valor proporciona el número inicial de días de actividad para un nuevo generador de alertas de atributo.
7. Pulse **Guardar**.

Configuración de parámetros del sistema para el proceso simultáneo

Si sus interconexiones están configuradas para el proceso de interconexiones paralelo, puede definir el número inicial de hebras de interconexión paralelas (número predeterminado) que se inician cuando inicia una interconexión.

Antes de empezar

Compruebe que seleccionó la casilla **Editar configuración** cuando inició la sesión en la Consola de configuración. Esta opción le permite añadir, cambiar y suprimir parámetros de configuración del sistema.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Parámetros del sistema**.
4. En el menú desplegable **Grupo de parámetros**, seleccione el grupo de parámetros **CONCURRENCY**.
5. Seleccione el parámetro del sistema **DEFAULT_CONCURRENCY**.
6. En Valor actual, escriba el número inicial de hebras de proceso de interconexiones que se deben iniciar cada vez que se inicie una hebra.

Configuración de parámetros del sistema para la gestión de la calidad de datos

Puede configurar el delimitador de fechas predeterminado que la Consola de configuración utiliza al formatear las fechas.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Parámetros del sistema**.
4. En el menú desplegable **Grupo de parámetros**, seleccione el grupo de parámetros **DQM**.
5. Pulse el parámetro del sistema **SYSTEM_DATE_DELIMITER**.
6. En el campo **Valor actual**, escriba / o - para especificar el delimitador que desea que el sistema utilice al formatear fechas. Para devolver este parámetro a su valor predeterminado, escriba el valor que se visualiza en el campo **Valor predeterminado**, en este campo.
7. Pulse **Guardar**.

Configuración de parámetros del sistema para opciones del producto

Puede configurar las opciones adicionales del producto que desea habilitar.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Parámetros del sistema**.
4. En el menú desplegable **Grupo de parámetros**, seleccione el grupo de parámetros **CONSOLE_CONFIG**.
5. Pulse el parámetro del sistema **PRODUCT_OPTIONS**.
6. En el campo **Valor actual**, escriba el código proporcionado por IBM que corresponde a la característica del producto que desea habilitar. Debe especificar todas las letras en mayúsculas. Puede escribir una lista de todas las características delimitadas por espacios que desea que el sistema habilite. Para devolver este parámetro a su valor predeterminado, escriba el valor que se visualiza en el campo **Valor predeterminado**, en este campo.
7. Pulse **Guardar**.

Configuración de parámetros del sistema para Event Manager

Puede habilitar el proceso de sucesos de Event Manager y configurar los parámetros del sistema para el proceso de sucesos, incluido el indicador de recurso universal (URI) del procesador de sucesos.

Procedimiento

1. En la Consola de configuración, pulse la pestaña **Configuración del sistema**.
2. En el panel izquierdo, seleccione el parámetro del sistema de Event Manager que desea configurar:
   a. **Habilitar proceso de sucesos** indica si el proceso de sucesos a través de Event Manager está habilitado o inhabilitado.
   b. **Tiempo de espera de procesador de sucesos** indica el número de segundos durante los cuales la interconexión espera una respuesta del procesador de sucesos externo antes de exceder el tiempo de espera con un error. El valor predeterminado es de 60 segundos.
   c. **URI de procesador de sucesos** indica el indicador de recurso universal (URI) para conectarse al procesador de sucesos externo. En **Valor actual**, introduzca el URI, incluido el número de puerto, incluso si es el número de puerto predeterminado. Por ejemplo: `http://localhost:13510/gem`
   d. La **Ventana de historial de sucesos** indica el número de días del historial de sucesos que la interconexión envía al procesador de sucesos externo al evaluar un suceso de entrada nuevo. (El numero de días predeterminado es 180.)
3. Pulse el botón **Guardar**.

Configuración de parámetros del sistema para el Visualizador

El parámetro del sistema para el Visualizador permite que los usuarios del Visualizador individuales consulten todas las alertas, incluidas las que no alcanzan el valor **Umbral de alerta mínimo** definido en cada regla de alerta de rol. Puede cambiar este valor para dar más flexibilidad a los usuarios del Visualizador a la hora de consultar alertas.

Procedimiento

1. En la Consola de configuración, pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Parámetros del sistema**.
4. En la lista desplegable **Grupo de parámetros**, seleccione el grupo de parámetros **VISUALIZER**.
5. Pulse el parámetro del sistema **ALLOW_ALERT_THRESHOLD_OVERRIDE**.
6. Elija una de las opciones siguientes:
   - Para permitir que los usuarios del Visualizador sustituyan el umbral de alertas definido en la pestaña **Reglas de alerta de rol - Filtros** de la Consola de configuración, escriba 1 en el campo **Valor actual**.
   - Para evitar que los usuarios del Visualizador sustituyan el umbral de alertas definido por el sistema en la pestaña **Reglas de alerta de rol - Filtros** en la Consola de configuración, escriba 0 .
   - Para devolver este parámetro a su valor predeterminado, escriba el valor que se visualiza en el campo **Valor predeterminado** en el campo **Valor actual**.
7. Pulse el botón **Guardar**.

Establecimiento de la vía de acceso predeterminada para Centrifuge

Si utiliza el Centrifuge Desktop opcional de Centrifuge Systems para visualizar y mostrar gráficos de entidad, debe especificar la vía de acceso al archivo de Centrifuge Desktop en las preferencias del Visualizador.

Acerca de esta tarea

Los valores de la vía de acceso predeterminada se configuran para cada cliente del Visualizador. Al especificar una vía de acceso predeterminada mediante esta tarea, solamente establece la vía de acceso en el Visualizador al que está conectado actualmente.

Procedimiento

1. En el Visualizador, pulse **Archivo** > **Preferencias** > **Preferencias del sistema**.
2. Bajo la sección **Vías de acceso a archivo** en **Vía de acceso de Centrifuge**:
   - Especifique la vía de acceso a archivo o el URL (localizador universal de recursos) a la aplicación Centrifuge Desktop en el campo.
   - O bien vaya a la aplicación Centrifuge Desktop y ábrala.
3. Pulse **Enviar**. Un mensaje de confirmación le informa de que debe reiniciar el Visualizador para que los cambios surtan efecto.
4. En el mensaje de confirmación, pulse **Aceptar**.
5. Cierre el Visualizador, vuelva a abrir el Visualizador y vuelva a iniciar la sesión.

Resultados

Una vez se ha configurado la vía de acceso, aparece el botón **Centrifuge** en las pantallas **Detalle de alerta de rol** y **Resumen de entidad** en la ventana **Investigación**. Pulse el botón para lanzar la aplicación Centrifuge Desktop directamente desde el Visualizador.

Establecimiento de la vía de acceso predeterminada para archivos UMF

Si carga registros de identidad de forma regular en archivos de datos UMF para procesarlos mediante el Visualizador, establecer la vía de acceso predeterminada puede ahorrarle un paso.

Acerca de esta tarea

Los valores de la vía de acceso predeterminada se configuran para cada cliente del Visualizador. Al especificar una vía de acceso predeterminada mediante esta tarea, solamente establece la vía de acceso en el Visualizador al que está conectado actualmente.

Procedimiento

1. En el Visualizador, seleccione **Archivo** > **Preferencias** > **Preferencias del sistema**.
2. En **Vía de acceso predeterminada para Carga de archivo**, realice una de las acciones siguientes:
   - Entre la vía de acceso completa del directorio a utilizar.
   - O bien examine para seleccionar el directorio.
3. Pulse **Enviar**. Un mensaje de confirmación le informa de que debe reiniciar el Visualizador para que los cambios surtan efecto.
4. En el mensaje de confirmación, pulse **Aceptar**.
5. Cierre el Visualizador, reinicie el Visualizador y vuelva a iniciar la sesión.

Resultados

Siempre que cargue un archivo UMF, la vía de acceso predeterminada es el directorio que ha especificado.

Personalización de atributos y puntuación

IBM InfoSphere Identity Insight proporciona mejoras funcionales para configurar datos de atributo e integrar algoritmos de puntuación. Estos cambios amplían el tamaño y los tipos de datos de identidad que se pueden comparar y puntuar y permiten la adición de nuevos algoritmos de puntuación en el proceso de resolución de entidad. A dichas capacidades generalmente se les denomina personalización de atributos y puntuación.

La tecnología de resolución de entidad permite utilizar la comparación de entidades y los algoritmos de puntuación para comparar y resolver datos de identidad comunes como nombres, direcciones, números de teléfono, números de tarjeta de crédito, números de identificación fiscal y números de licencia y así indicar las coincidencias potenciales. Los elementos de datos que describen una cuenta o entidad se denominan atributos. Los atributos son características o rasgos que describen una persona, una organización, un lugar o un elemento. Añadiendo la personalización de atributos y puntuación, puede añadir nuevos tipos de datos de identificación y asociar algoritmos de puntuación desarrollados como plugins de puntuación de producto. Por ejemplo, puede añadir datos de identidad derivados de huellas dactilares, de escáneres de retina o de pruebas de ADN para compararlos y puntuarlos utilizando un plugin de puntuación que incluya un algoritmo de comparación apropiado.

Estas mejoras de atributo y de puntuación mejoran el proceso de resolución de entidades permitiéndole:

- Almacenar y comparar datos de atributo de gran tamaño utilizando ATTR_VALUE (ampliado hasta 8 KB) y ATTR_LARGE_DATA para almacenar datos incluso mayores.
- Aplicar los algoritmos de puntuación proporcionados a un rango más amplio de tipos de atributo y configurar fácilmente dichos atributos con un control mayor.
- Integrar los resultados de la comparación y puntuación de atributos personalizados utilizando las funciones de informe y de alerta del Visualizador.
- Aplicar un modelo de plugin para añadir algoritmos de puntuación creados por el usuario.
- Integrar plugins de puntuación personalizados utilizando la Consola de configuración.

Almacenamiento de datos de atributos grandes

Para que el sistema almacene y procese datos de atributos grandes con plugins de puntuación, los metadatos se deben convertir a UMF (Universal Message Format) y se deben almacenar en las columnas apropiadas.

Acerca de esta tarea

Procedimiento

1. Con el modelo de entidad que ha creado para el sistema, analice los datos de entrada para ver cómo encajan con el estándar UMF. Tener una idea clara de los segmentos y códigos UMF existentes antes de continuar con el siguiente paso.
2. Configure la herramienta ETL para producir registros UMF que coincidan con el modelo de entidad.
3. Ejecute la herramienta ETL.

Qué hacer a continuación

Tras convertir los datos a UMF, puede enviar los registros UMF a la interconexión para proceso.

Parámetros de almacenamiento de datos de atributo grandes

Para que el sistema almacene y procese datos de atributos grandes para a puntuación, los metadatos se deben convertir a UMF (Universal Message Format) y se deben almacenar en las columnas apropiadas.

Utilice las columnas ATTR_VALUE y ATTR_LARGE_DATA para almacenar datos de atributo grandes y desestructurados para atributos personalizados y aplicaciones de puntuación.

Nombre de columna y código UMF	Tipo y tamaño de datos	Necesario	Explicación

ATTR_VALUE	varchar(255) (predeterminado) redimensionable hasta 8 k	**Sí**	Datos utilizados como uno de los atributos en un proceso ETL con plugins de puntuación base. En los casos en que los datos superan los 8 k y están en formato binario, almacene los datos en la columna ATTR_LARGE_DATA y cree un identificador exclusivo para los datos en la columna ATTR_VALUE. El identificador ATTR_VALUE se utiliza para comparar y puntuar. Por ejemplo, puede crear un hash unidireccional MD5 (algoritmo 5 Message-Digest) que se pueda comparar y mostrar en el Visualizador y en los informes. El tamaño máximo de la columna depende de la base de datos. Para los datos binarios que superen 255/3 y deban almacenarse en ATTR_VALUE, deberá redimensionarse la columna. Por motivos de rendimiento, debe considerar el reajuste de la memoria caché de la base de datos porque es probable que quepan menos filas en la memoria caché.

ATTR_LARGE_DATA	Objeto de caracteres largos (CLOB), utilizado para datos que superen los 8 k.	**No**	Almacénelo como datos de carácter. Por ejemplo, utilice la codificación Base64 de datos binarios. Utilice esta columna para almacenar los datos de atributo que sean demasiado grandes para la columna ATTR_VALUE. ATTR_LARGE_DATA es una columna de tipo CLOB (objeto de carácter largo) que puede manejar datos de tamaño ilimitado. Estos datos están disponibles para la resolución de entidades. El autor del plugin de comparación personalizado debe conocer la estructura de los datos. El Visualizador no mostrará los datos porque no tienen un formato estándar y serán distintos según el tipo de sistema. El rendimiento de CLOB no será tan bueno como el de una columna varchar porque un CLOB no puede almacenarse en la memoria caché y necesita lectura de disco, lo cual hace preferible ATTR_VALUE. Aumentar el tamaño de ATTR_VALUE provocará que se almacenen pocos datos de atributo en la memoria caché; por tanto, es mejor utilizar ATTR_LARGE_DATA sólo para datos inferiores a 8 k para asegurar que otros atributos de menor tamaño como los de género y DOB se almacenen correctamente en la memoria caché. Esta cuestión depende del arquitecto. Póngase en contacto con el administrador de la base de datos. Cuando se utiliza ATTR_LARGE_DATA, ATTR_VALUE debe llenarse con algún valor. Si existe alguna manera de crear una clave de búsqueda significativa desde los datos que se ajuste en ATTR_VALUE, se debe crear y poner en ATTR_VALUE. Si no hay ningún modo de crear una clave de búsqueda significativa, se debe poner algo más exclusivo para el valor en ATTR_VALUE o la interconexión no funcionará correctamente y probablemente fallará con errores DQM. Se puede generar automáticamente una clave exclusiva configurando una regla DQM para crear un hash MD5 de los datos (regla 600) o un hash personalizado basado en reglas configuradas (regla 615). Es importante que este valor sea aceptablemente exclusivo especialmente si el tipo de atributo se va a configurar para búsquedas persistentes porque ATTR_VALUE se utiliza en la determinación de valores genéricos. **Nota:** El plug-in 'binaryAttributeScoring' enviado no compara ATTR_VALUE en absoluto. Sólo examina y puntúa el segmento ATTR_LARGE_DATA.

Ejemplo

A continuación se muestra un ejemplo de una salida hash MD5 de datos binarios grandes:

```
<ATTRIBUTE><ATTR_TYPE>BIOMETRIC-1</ATTR_TYPE>
<ATTR_VALUE>214b21fc3e040f844a07710b1bb451a0
</ATTR_VALUE><ATTR_LARGE_DATA>
<![H4sICBRTqkgAA2Zvby50eHQAK0ktLuHlAgDkTqoPBgAAAA==]>
</ATTR_LARGE_DATA></ATTRIBUTE>
```

Los valores ATTR_LARGE_DATA reales son mayores que los mostrados en el ejemplo anterior.

Configuración de características de origen para datos de atributos grandes

Utilice la Consola de configuración para configurar características de origen para datos de atributos grandes.

Acerca de esta tarea

La Consola de configuración permite configurar nuevos tipos de datos de atributo para plugins de puntuación personalizados del mismo modo en que se configuran datos para los plugins base.

Procedimiento

1. En la pestaña Plugins de la Consola de configuración, pulse el recuadro de selección del plugin personalizado.
2. Pulse la pestaña Características.
3. Pulse la pestaña General y rellene los campos según convenga.
4. Seleccione el tipo de datos apropiado. El tipo de datos puede ser uno de los siguientes: CHAR, DATE o CLOB. Tenga en cuenta los requisitos del tipo de datos que se encuentran en “Parámetros de almacenamiento de datos de atributo grandes” en la página 188.
5. Seleccione una clase apropiada.
6. Seleccione un valor para Uso de resolución.
7. Seleccione el nombre del plugin de puntuación que esté configurando.
8. Seleccione un valor apropiado en el campo Nivel de visualización. Elija "Sólo el tipo sin valor" para impedir que el visualizador muestre el contenido de las columnas ATTRIBUTE.ATTR_VALUE o ATTRIBUTE.ATTR_LARGE_DATA. La columna ATTR_VALUE no se suele utilizar cuando se usa la columna de objeto grande (CLOB). Además, la columna ATTR_LARGE_DATA (CLOB) contiene normalmente datos codificados en Base 64 que no serán relevantes o útiles para mostrarse en el Visualizador.
9. Pulse Guardar.

Resultados

La pestaña Características bajo Orígenes muestra el tipo nuevo y la información relacionada.

Configuración de características de resolución para datos grandes

Utilice la Consola de configuración para configurar características de resolución para datos de atributo grandes y personalizar plugins de puntuación.

Acerca de esta tarea

Información de confirmación o denegación para un tipo de característica nueva configurada recientemente.

Procedimiento

1. En la Consola de configuración, pulse el botón Configuración.
2. Pulse el botón Resolución.
3. Pulse la pestaña Características.
4. Seleccione una configuración de resolución apropiada como, por ejemplo, PREDETERMINADA en el menú desplegable y pulse el botón Nueva.
5. Seleccione el panel general e introduzca los valores en los campos mostrados. Consulte “Características y opciones de resolución” para obtener descripciones de las opciones de campo y recomendaciones.
6. Pulse Guardar.

Resultados

La pantalla Visión general muestra una tabla de resumen con los valores creados para la configuración de resolución.

Características y opciones de resolución

Utilice la vista de la pestaña General de Características de resolución para configurar acciones y opciones para tipos de datos grandes y plugins de puntuación personalizados.

Si se está configurando un tipo de carácter que tiene un campo Uso de resolución y se selecciona el valor "Confirmar/Denegar", los campos adicionales aparecerán dinámicamente.

Campo	Necesario	Selecciones de campo y descripciones
Grupo	**Sí**	Escriba el nombre del grupo que desee utilizar para identificar esta característica.
Descripción	**Sí**	Introduzca una descripción breve de la configuración de resolución predeterminada. Si deja este campo en blanco, se puede producir un error.
Tipo de característica	**Sí**	Seleccione el tipo con el que esté trabajando. La lista incluirá todos los tipos configurados para Orígenes.
Peso de confirmar	**Sí**	Cualquier valor de 0 a 100. Afecta a la puntuación de similitud.

Umbral de confirmación de plugin	**No**	Campo de texto sin formato. Este campo se muestra cuando se especifica un tipo de característica cuyo campo Uso de resolución se establece en “Confirmar/Denegar," como cuando se trata de un tipo para un plugin personalizado. Si un plugin de puntuación puntúa el tipo de característica durante la parte de confirmación y denegación del proceso de resolución de entidades, especifique un valor de umbral de confirmación. Cuando la puntuación asignada por el plugin es igual o superior a este valor, la coincidencia se considera una confirmación y esto hace que se añada el valor del campo Confirmar peso a la puntuación Confianza de resolución.
Peso de denegar	**Sí**	Cualquier valor de 0 a 100. Afecta a la puntuación de similitud.
Umbral de denegación de plugin	**No**	Campo de texto sin formato. Este campo sólo se muestra cuando se especifica un tipo de característica cuyo campo Uso de resolución se establece en “Confirmar/Denegar," como cuando se trata de un tipo para un plugin personalizado. Si un plugin de puntuación puntúa el tipo de característica durante la parte de confirmación y denegación del proceso de resolución de entidades, especifique un valor de umbral de denegación (que pueda interpretar el plugin). Cuando la puntuación asignada por el plugin es igual o superior a este valor, la coincidencia se considera una denegación y esto hace que se añada el valor del campo Denegar peso a la puntuación Confianza de resolución.

Configuración de informes para la personalización de atributos y puntuación

El informe de configuración en la Consola de configuración también incluye elementos para la personalización de atributos y puntuación.

Entre las adiciones al informe de configuración se incluye:

- La sección "Tipos de características" del informe tiene una columna nueva llamada "Plugin de puntuación", que muestra el valor del tipo de característica de plugin respectivo.
- Una sección de informe de plugin nueva que muestra los registros configurados. Las etiquetas de cabecera de columna incluyen: ID, Nombre, Tipo, Versión y Nombre corto de biblioteca.
- La sección “Características de la resolución de entidades” tiene dos columnas nuevas añadidas para mostrar los valores “Umbral de confirmación de plugins” y “Umbral de denegación de plugins”.

Configuración de plugins de puntuación personalizados

Utilice la Consola de configuración para configurar plugins de puntuación personalizados.

Antes de empezar

Asegúrese de que el nuevo plug-in se ha adaptado correctamente para IBM InfoSphere Identity Insight. Consulte Desarrollo de plug-ins de puntuación personalizados para IBM InfoSphere Identity Insight.

Acerca de esta tarea

La Consola de configuración permite configurar los plugins de puntuación que se han añadido al sistema.

Procedimiento

1. En la Consola de configuración, pulse el botón Configuración.
2. Pulse la petaña General.
3. Pulse la pestaña Plugins.
4. Para configurar un plugin nuevo, pulse el botón Nuevo.
5. Para editar un plugin existente, seleccione el plugin que desee configurar en la lista de la columna Plugins. Sólo los plugins del cliente son editables.
6. En la pestaña General, rellene los campos según convenga:

Nombre de campo	Necesario	Descripción
Plugin	**Sí**	Nombre del plugin que se mostrará en las opciones del menú "Plugin de puntuación".
Nombre corto de biblioteca	**Sí**	El nombre de este campo se utiliza en la columna LIBRARY_NAME de la tabla Plugin. El campo Nombre corto de biblioteca se utiliza para construir el nombre del archivo de biblioteca de software llamado por el código de la conexión. Se recomienda que coincida con el caso del archivo de biblioteca actual utilizado por la interconexión. Es necesario porque algunos sistemas son sensibles a las mayúsculas y minúsculas. Este nombre incluye el prefijo o sufijo EAS según el SO.
Versión	**Sí**	Este campo se utiliza para realizar un seguimiento del número de versión de la biblioteca de software.

7. Pulse Guardar.

Resultados

La pestaña Plugin muestra el nombre del plugin actualizado y la información relacionada.

Desarrollo de plugins de puntuación personalizados para IBM InfoSphere Identity Insight

IBM InfoSphere Identity Insight permite crear plugins de puntuación personalizados e incluir tipos de datos de atributo adicionales en el proceso de resolución de entidades.

Para crear un plugin de puntuación para IBM InfoSphere Identity Insight, se deben incluir varios elementos básicos y crear una biblioteca compartida. Los plugins personalizados se debe instalar en un directorio especificado en la vía de acceso de carga de la biblioteca.

Interfaz de desarrollo de plugins de puntuación

La personalización de plugins de puntuación necesita una interfaz estándar.

Utilice objetos primitivos para eliminar una dependencia de versiones de biblioteca y opciones de compilador. Así permitirá que los plugins se utilicen con múltiples

versiones de interconexión sin tener que recrear el plugin cuando la interconexión cambie la biblioteca, las versiones de compilador u otras opciones. Se deben incluir los prototipos de interfaz C o C++ siguientes:

```
#ifdef _WIN32
#define _DLEXPORT __declspec(dllexport)
#else
#define _DLEXPORT
#endif

extern "C"
{
  _DLEXPORT const int initPlugin(const char *configInfo,
                                 const uint configSize,
                                 char *errorStr,
                                 const uint maxStrSize);
  _DLEXPORT const char *getVersion();
  _DLEXPORT const int score(const char *thresholdStr,
                            const uint thresholdSize,
                            const char *inboundStr,
                            const uint inboundSize,
                            const char *candidateStr,
                            const uint candidateSize,
                            char *result,
                            const uint resultSize);
};
```

getVersion

La personalización de plugins de puntuación necesita una función getVersion.

Ejemplo

Debe incluir lo siguiente:

```
const char *getVersion();
```

return char * contiene una serie terminada nula que describe la versión del plugin.

Implemente esta función almacenando el número de versión de plugin en una serie estática y devuelva un puntero al puntero base de la serie.

myPlugin.h includes the following:

```
class MyPlugin
{
public:
  static const std::string mVersion;

};

myPlugin.cpp includes the following
const std::string MyPlugin::mVersion = std::string("1.0");

const char *getVersion ()
{
  return MyPlugin::mVersion.c_str();
}
```

initPlugin

La personalización de plugins de puntuación necesita una función initPlugin.

Ejemplo

initPlugin permite que el plugin cargue y guarde la información de configuración que se necesitará para la puntuación. La serie de conexión de la base de datos y el nombre del archivo .ini se proporcionan en la serie **configInfo**. Se llamará a initPlugin una vez para cada tipo de atributo que utilice un plugin. Estos son objetos compartidos. Para poder utilizar el plugin para más de un tipo de atributo, la información de configuración se debe guardar para cada tipo de atributo. Así, cuando se llama a la puntuación, se puede buscar la información de configuración para el tipo de atributo adecuado.

```
const int initPlugin(const char *configInfo,
                     const uint configSize,
                     char *errorStr,
                     const uint maxStrSize);
```

configSize
es la longitud de la serie contenida en configInfo. El error debe estar en el formato siguiente.

errorStr
es una memoria de almacenamiento intermedio asignada previamente para copiar una serie terminada nula. La serie contiene XML que describe los errores de inicialización. El error debe estar en el formato siguiente:

```
<ERROR>texto de error</ERROR>
```

maxStrSize
es el tamaño de la memoria de almacenamiento intermedio asignada previamente a la que apunta errorStr. El tamaño de la serie de error no puede superar este valor.

A continuación se muestra un ejemplo de pseudocódigo de una función de puntuación:

```
const int initPlugin(const char *configInfo, const uint configSize, char *errorStr
, const uint maxStrSize)
{
  //create string out of configInfo
  //parse string with XML parser
  //extract DB_CONNECTION and CONFIG_FILE
  //connect to database
  //select config info from database
  //open CONFIG_FILE
  //read config info from .ini file

  //if there was an error create null terminated error string and
  //strcpy into errorStr. Return -1.
  //if no error, return 0.
}
```

initPlugin debe devolver -1 si se produce un error.

puntuación

La personalización de plugins de puntuación necesita una función de puntuación.

score contiene los parámetros siguientes:

```
const int score(const char *thresholdStr,
                const uint thresholdSize,
                const char *inboundStr,
                const uint inboundSize,
```

```
                const char *candidateStr,
                const uint candidateSize,
                char *result,
                const uint resultSize);
```

thresholdStr
contiene los umbrales de confirmación y denegación. Dichos umbrales no son necesarios.

thresholdSize
es el tamaño de la serie contenida en thresholdStr.

inboundStr
contiene el atributo de la entidad de entrada que se puntúa.

inboundSize
es el tamaño de la serie contenida en inboundStr.

candidateStr
es un puntero a una serie que contiene el atributo de la entidad candidata que se puntúa.

candidateSize
es el tamaño de la serie contenida en candidateStr.

result es una memoria de almacenamiento intermedio asignada previamente para copiar una serie terminada nula que contiene un archivo xml que describe los resultados de la puntuación. En caso de error, los resultados serán una descripción del error. El formato de la serie devuelta se define de la manera siguiente:

```
<SCORE_RESULT>
  <MATCH_SCORE>integer 0-100</MATCH_SCORE>
  <CONFIRMATION>TRUE/FALSE</CONFIRMATION>
</SCORE_RESULT>
```

En caso de error, el formato resultante es el siguiente:

```
<ERROR>texto de error</ERROR>
```

resultSize
es el tamaño de la memoria de almacenamiento intermedio asignada previamente a la que apunta el resultado. La serie resultante no puede superar este tamaño. El documento resultante es bastante reducido, así que esta cuestión no será un problema excepto si se trata de mensajes de error extremadamente largos.

A continuación se muestra un ejemplo de pseudocódigo de una función de puntuación:

```
const int score(const char *thresholdStr,
       const uint thresholdSize,
                const char *inboundStr,
       const uint inboundSize,
             const char *candidateStr,
       const uint candidateSize,
       char *result,
              const uint resultSize)
{
  //create strings out of thresholdStr, inboundStr, and candidateStr
  //create XML documents out of thresholdStr, inboundStr, and candidateStr
  //parse thresholds out of threshold xml doc if thresholds are used
  //parse values out of inbound xml doc
  //parse values out of candidate xml doc

  //check for any errors such as attr type mismatches, bad data, etc.
```

```
  //un-encode attr_value and attr_large_data data fields if necessary
  //apply scoring algorithm to attribute data
  //scale score into 0-100 range
  //determine confirmation or denial (possibly using thresholds)

  //if there was an error, create null terminated error string and
  //strcpy into result. Return -1.
  //if no error, create null terminated result document and strcpy into
  //result.  Return 0.
}
```

La función de puntuación debe devolver -1 si se produce un error.

Formatos de fecha

La personalización de plugins de puntuación necesita un formato de datos específico.

Ejemplo

Formato de datos de umbral

```
<THRESHOLDS>
  <CONFIRMATION_THRESHOLD>string</CONFIRMATION_THRESHOLD>
  <DENY_THRESHOLD>string</DENY_THRESHOLD>
</THRESHOLDS>
```

Los umbrales son series sin formato. Se cargan desde la tabla MATCH_MERGE_ATTR y deben adaptarse al formato que espera el plugin. El autor del plugin define el formato y puede variar entre un plugin y otro.

Formato de datos de atributo

```
<ATTRIBUTE>
  <ATTR_TYPE_ID>unsigned int</ATTR_TYPE_ID>
  <ATTR_VALUE>string</ATTR_VALUE>
  <ATTR_LARGE_DATA>string</ATTR_LARGE_DATA>
</ATTRIBUTE>
```

ATTR_LARGE_DATA puede ser una serie vacía en función del tipo de atributo y del proceso ETL. ATTR_LARGE_DATA es opcional y sólo debe utilizarse cuando los datos del atributo son demasiado largos para la columna ATTR_VALUE. Esto se debe determinar durante la configuración del sistema para poder crear correctamente UMF y para poder grabar los plugins para utilizar los campos correctos.

ATTR_LARGE_DATA pueden codificarse para formar conjuntos de caracteres válidos de XML. Se recomienda la codificación Base64, pero esta acción se realiza en el proceso ETL. Es posible que el plugin necesite descodificar los datos de ATTR_LARGE_DATA. La serie también debe codificarse en UTF-8. Si la codificación de la serie en ETL era base64, la serie UTF-8 será idéntica a la serie ASCII7.

A continuación se muestra un ejemplo de pseudocódigo de una función de puntuación:

```
const int score(const char *thresholdStr,
       const uint thresholdSize,
                const char *inboundStr,
       const uint inboundSize,
              const char *candidateStr,
       const uint candidateSize,
       char *result,
              const uint resultSize)
{
```

```
  //create strings out of thresholdStr, inboundStr, and candidateStr
  //create XML documents out of thresholdStr, inboundStr, and candidateStr
  //parse thresholds out of threshold xml doc if thresholds are used
  //parse values out of inbound xml doc
  //parse values out of candidate xml doc

  //check for any errors such as attr type mismatches, bad data, etc.
  //un-encode attr_value and attr_large_data data fields if necessary
  //apply scoring algorithm to attribute data
  //scale score into 0-100 range
  //determine confirmation or denial (possibly using thresholds)

  //if there was an error, create null terminated error string and
  //strcpy into result. Return -1.
  //if no error, create null terminated result document and strcpy into
  //result.  Return 0.
}
```

La función de puntuación debe devolver -1 si se produce un error.

Creación del objeto de plugin

El objeto de plugin debe crearse en una biblioteca compartida.

Acerca de esta tarea

Cree el objeto en una biblioteca compartida (.dll en windows, .so en linux/unix). Todas las bibliotecas deben estar enlazadas estáticamente. De esta manera se evitarán posibles errores de coincidencia de versión de biblioteca y símbolos sin resolver.

Capítulo 6. Gestión de interconexiones

Las interconexiones constituyen el corazón del sistema. Son el punto donde tiene el lugar el proceso: donde se resuelven las entidades, donde se detectan las relaciones y donde se generan las alertas. Las interconexiones son el principal método de cargar datos en la base de datos de entidades. La gestión de interconexiones es una tarea operativa continua que implica la configuración de interconexiones, el inicio y detención de interconexiones, la supervisión de interconexiones y el direccionamiento de mensajes procedentes de interconexiones a otras interconexiones, nodos o sistemas externos.

Interconexiones

Las interconexiones son los componentes que realizan la estandarización de higiene de dirección y nombre, la gestión de calidad de datos y la resolución de entidades. Las interconexiones también realizan el proceso de resolución de relaciones y generan alertas, según la configuración del sistema.

Las interconexiones realizan tres procesos principales:

- Reconocer, lo que implica optimizar los datos de entrada realizando procesos de estandarización, higiene y mejora de los datos y comprobaciones de calidad.
- Resolver, lo que implica resolver entidades
- Relacionar, lo que implica detectar relaciones y generar alertas

Las interconexiones están alojadas en nodos de interconexión.

Puede configurar interconexiones para el proceso en paralelo de modo que un mandato de interconexión abarque varias hebras del proceso de interconexión en paralelo, lo que permite al sistema procesar simultáneamente varias solicitudes de datos. Esta característica puede ayudar a mejorar el rendimiento del sistema, a reducir el tiempo del proceso de datos y a mitigar las restricciones de memoria del hardware.

La característica de proceso de interconexión en paralelo es configura en dos lugares:

- El valor global de simultaneidad se controla mediante el parámetro `Simultaneidad predeterminada de conexiones` en la pestaña **Configuración del sistema** en la Consola de configuración. Este valor determina el número de hebras de proceso en paralelo que se inician desde un mandato de inicio de interconexión. El valor predeterminado para este parámetro es 1, lo que significa que, a menos que se edite este parámetro, sólo se inicia una hebra de proceso de interconexión.
- Se puede configurar un valor local de simultaneidad (por nodo de interconexión) en el archivo de configuración de interconexión. Si especifica un parámetro y un valor de simultaneidad en el archivo de configuración de interconexión por nodo de interconexión, dicho valor prevalece sobre el parámetro global del sistema. Cuando se emite un mandato de inicio de interconexión en dicho nodo de proceso, se inicia el número de hebras de proceso de interconexión simultáneas especificado en el archivo de configuración de interconexión.

Comprobación de la configuración de la interconexión

El sistema realiza una comprobación de configuración de interconexión antes de iniciar un nuevo proceso de interconexión y a intervalos frecuentes para cada interconexión en ejecución para garantizar que la configuración de la interconexión sea válida.

Durante la comprobación de configuración de interconexión, el sistema comprueba si la interconexión tiene una configuración válida:

- ¿Es la configuración para esta interconexión igual que la configuración de la Consola de configuración?
- ¿Hay un número razonable de registros para cada tabla de configuración que utiliza esta interconexión?
- ¿Hay valores estándar en tablas de configuración específicas?
- ¿Se han establecido identificadores y valores de configuración en tablas de configuración específicas?

Si no se pasan estas comprobaciones de configuración, según la gravedad de la discrepancia, el sistema registra un aviso en los archivos de registro o concluye automáticamente la interconexión (o no inicia la interconexión) y registra un error.

Nodos de interconexión

Los nodos de interconexión son máquinas físicas que alojan uno o varios procesos de interconexión.

El nodo de interconexión es donde se instala y se inicia el ejecutable de la interconexión que ejecuta los procesos de interconexión. Debe configurar y mantener el archivo de configuración de interconexión correspondiente a todas las interconexiones alojadas en esta máquina. El sistema también graba los mensajes de interconexión en los archivos de registro de los nodos de interconexión.

Los nodos de interconexión conectan procesos de interconexión con estos componentes de la arquitectura del producto:

Programas de adquisición
Como parte del proceso de extracción, transformación y carga (ETL), los programas de adquisición utilizan transportes para enviar datos UMF a las interconexiones para su proceso. Debe utilizar el método de transporte que resulte adecuado para el tipo de programa de adquisición para conectar con las interconexiones. Por ejemplo, si utiliza el programa de utilidad de archivos UMF como un programa de adquisición, debe utilizar el transporte de archivos.

Base de datos de entidad
La base de datos de entidades contiene información sobre entidades. Las interconexiones acceder a información de entidades al procesar registros de entrada correspondientes a la resolución de entidades y de relaciones. El nodo de interconexión debe tener instalado y configurado el cliente de base de datos adecuado para que las interconexiones puedan acceder a la base de datos de entidades.

Colas Si el sistema utiliza colas como métodos de transporte para enviar datos a las interconexiones para su proceso, debe instalar y configurar el software de gestión de colas de mensajes adecuado en cada nodo de interconexión.

Servidores de higiene de dirección
Si el sistema utiliza productos de higiene de dirección de otras empresas para realizar una limpieza adicional de direcciones, cada nodo de interconexión debe estar configurado de modo que se conecte con los servidores de higiene de dirección.

Servicios web
Debe utilizar un transporte HTTP para conectar los procesos de interconexión del nodo de interconexión con los servicios web.

Inicio de interconexiones

Antes de que una interconexión pueda recibir y procesar datos, se debe iniciar. Es normal ejecutar múltiples interconexiones para incrementar el rendimiento de los datos o procesar diferentes tipos de datos de origen. Siga estos pasos para iniciar una interconexión o reiniciar una interconexión que está inactiva.

Antes de empezar

- El nodo de interconexión que aloja esta interconexión debe tener instalado el ejecutable de interconexión.
- Se debe haber configurado como mínimo un archivo de configuración de interconexiones para utilizarlo con la interconexión que desea iniciar. Puede especificar el archivo de configuración de interconexiones que se debe utilizar como parte del mandato para iniciar la interconexión. Si no especifica el nombre de archivo de configuración como parte del mandato de interconexión, el archivo de configuración de interconexiones debe estar ubicado en el nodo de interconexión, y debe coincidir con el nombre del ejecutable (nombre de interconexión especificado). Por ejemplo, pipeline.ini.
- Las variables de entorno de base de datos debe establecerse. Consulte Establecimiento de las variables de entorno.
- Si utiliza un script para iniciar las interconexiones, asegúrese de que el script está ubicado en el mismo directorio en el que inicia la interconexión.
- Si el valor del parámetro del sistema *DEFAULT_CONCURRENCY* se ha establecido en mayor que 1 o si ha configurado el parámetro de *simultaneidad* en el archivo de configuración de interconexiones para el nodo de interconexión, puede iniciar múltiples hebras de proceso de interconexiones paralelas utilizando un solo mandato de inicio de interconexión.

Acerca de esta tarea

Existen tres pasos para iniciar una interconexión:

Procedimiento

1. Cada interconexión debe tener un nombre exclusivo para el nodo de interconexión, por lo que debe asegurarse de que no hay otras interconexiones en ejecución con el mismo nombre que la interconexión que desea iniciar. (El nombre de interconexión predeterminado es `pipeline`.) Para verificarlo, escriba el mandato siguiente en un indicador de mandatos: `pipeline -n` *`nombre_interconexión`* `-l`

   donde *`nombre_interconexión`* es el nombre que desea utilizar para iniciar la nueva interconexión. Asegúrese de que este nombre coincide con el nombre registrado en la consola de configuración para esta interconexión.

2. En un indicador de mandatos, inicie una o varias interconexiones especificando el tipo de opciones y parámetros del mandato de interconexión adecuados utilizando este formato:

   `pipeline -opción parámetro`

3. Verifique que el mandato ha funcionado y que la interconexión se ha iniciado y está activa.
   a. Si el sistema se ejecuta en una plataforma Microsoft Windows y utiliza la opción de interconexión de servicios, puede ver el estado de la interconexión en el panel de control de los servicios de Microsoft Windows.
   b. Si el sistema se ejecuta en una plataforma UNIX y utiliza la opción de interconexión de daemons, puede escribir el mandato siguiente para comprobar si hay procesos en ejecución:

      `ps -fu id_usuario`

      donde *id_usuario* es la identificación del usuario que inicia la interconexión.
   c. O bien, en un indicador de mandatos, escriba el siguiente mandato:

   `pipeline -nnombre_interconexión -l`

   donde *nombre_interconexión* es el nombre de la interconexión que acaba de iniciar. Si la interconexión está activa, el indicador de mandatos devuelve `Running`.

Detención de interconexiones

La detención de una interconexión significa cambiar su estado de activo y abierto para el proceso de datos a inactivo y cerrado para los datos de entrada. Puede detener manualmente una interconexión cada vez. Siga estas instrucciones para detener una interconexión después de realizar cambios en la configuración del sistema (después reinicie la interconexión para que los cambios de configuración surtan efecto), si instala un arreglo en caliente o una actualización del release, o si realiza cambios de configuración en el nodo de interconexión que aloja la interconexión.

Procedimiento

1. Verifique que la interconexión que desea detener esté en ejecución actualmente. Para verificar esto: `pipeline -n nombre_interconexión -l` donde *nombre_interconexión* es el nombre de la interconexión que desea detener. El indicador de mandatos devuelve `Running` si la interconexión está activa.
2. En una línea de mandatos, escriba el mandato de detención de interconexión: `pipeline -e -n nombre_interconexión` donde *nombre_interconexión* es el nombre de la interconexión que desea detener.

   Nota: Si ha iniciado la interconexión utilizando la opción de depuración del mandato de interconexión, puede detener la interconexión pulsando **Ctrl** + **C** en una línea de mandatos.
3. Verifique que el mandato ha funcionado y la interconexión se ha detenido: `pipeline -nnombre_interconexión -l` donde *nombre_interconexión* es el nombre de la interconexión que acaba de detener. El indicador de mandatos devuelve `Stopped` si la interconexión se ha detenido.

Configuración de interconexiones

Cuando se inicia una interconexión, se comprueba un archivo de configuración de interconexiones para obtener las variables de arranque inicial y la información de configuración necesaria para procesar los datos de entrada. Por omisión, cuando se instala una interconexión en el nodo de interconexión, el sistema también instala un archivo de configuración de interconexiones por omisión, denominado pipeline.ini, que todas las interconexiones de ese nodo de interconexión pueden utilizar. Pero algunas secciones de este archivo predeterminado deben configurarse específicamente para las interconexiones que se ejecutan en el nodo de interconexión para que la interconexión tenga las conexiones adecuadas y acceso a la base de datos de entidades. Utilice esas instrucciones para configurar el archivo de configuración de interconexiones.

Antes de empezar

- Debe conocer el nombre exacto de la base de datos de entidades y las credenciales de inicio de sesión necesarias para acceder a la base de datos de entidades.
- Si el sistema se conecta a software externo de corrección de direcciones, debe conocer el nombre de la máquina del sistema principal de software de corrección de direcciones y poder seleccionar los valores adecuados para este software.
- Para que los cambios del archivo de configuración surtan efecto, debe detener cualquier interconexión en ejecución en este nodo de interconexión y reiniciar las interconexiones después de completar los cambios.

Acerca de esta tarea

El archivo de configuración pipeline.ini es un archivo de texto ASCII estándar. Puede utilizar cualquier editor de texto ASCII para editar el archivo.

Procedimiento

1. Haga una copia del archivo de configuración pipeline.ini por omisión y guarde el archivo original en una ubicación segura. Si guarda una copia del archivo original, puede revertir a ese archivo, si es necesario.
2. Abra la copia del archivo de configuración pipeline.ini en el editor de texto que prefiera.
3. Actualice el archivo para que refleje la configuración adecuada para las interconexiones que se ejecutan en ese nodo de interconexión. Generalmente, los valores por omisión del archivo de configuración de interconexiones por omisión son adecuados; normalmente, sólo es necesario especificar o actualizar la información de conexión de base de datos bajo la cabecera [SQL] y cualquier información de corrección de direcciones bajo la sección [OAC], si el sistema utiliza software externo de corrección de direcciones.
4. Guarde el archivo de configuración de interconexiones actualizado. El archivo se debe guardar en el directorio donde reside el mandato ejecutable de interconexiones. (De lo contrario, deberá especificar el nombre de archivo de configuración de interconexiones y la ubicación de vía de acceso completa cada vez que inicie una interconexión en este nodo de interconexión.)

Qué hacer a continuación

Si ha detenido todas las interconexiones en ejecución de este nodo de interconexión antes de realizar los cambios, puede reiniciar las interconexiones. Si no ha detenido todas las interconexiones que se ejecutan cuando se realizan estos cambios, debe

detenerlas y reiniciarlas ahora. Las interconexiones en ejecución no aplican los cambios del archivo de configuración de interconexiones hasta que se han reiniciado. Si se cambia la información de configuración de interconexiones sin detener las interconexiones puede causar errores de interconexión, incluyendo el cierre de interconexiones, debido a valores incorrectos del archivo de configuración de interconexiones.

Registro de interconexiones

Para poder supervisar el estado o los resultados del direccionamiento de interconexiones, primero debe registrar las interconexiones en la Consola de configuración. El registro de interconexiones no es lo mismo que la instalación o configuración de una interconexión; significa añadir la interconexión al panel **Interconexiones** en la Consola de configuración.

El sistema utiliza la información registrada en el panel **Interconexiones** para identificar de forma exclusiva la interconexión. El supervisor de aplicaciones utiliza esta información para notificar el estado y estadísticas de interconexiones supervisadas o para direccionar comunicaciones y resultados entre las interconexiones y otros sistemas. El nombre que registre para una interconexión es el mismo, exactamente (incluidas mayúsculas y minúsculas), que debe utilizar cuando inicie la interconexión. Si utiliza otro nombre o no coinciden las mayúsculas y minúsculas de la interconexión registrada, el supervisor de aplicaciones no reconoce la interconexión y no la direccionará ni la supervisará.

Una vez registrada una interconexión en el panel **Interconexiones**, puede configurar normas de direccionamiento para la interconexión en el panel **Direccionamiento**, supervisar el estado y las estadísticas de la interconexión mediante el panel **Estado de la interconexión**, o ambos. Para supervisar el estado y las estadísticas de una interconexión, cuando la registre debe indicar que desea que el sistema supervise la interconexión.

Una vez se ha registrado una interconexión, no puede editar el nombre de la misma, pero puede actualizar el resto de la información sobre la interconexión. Por ejemplo, si el nombre del nodo de la interconexión cambia o si desea iniciar la supervisión del estado y de las estadísticas de la interconexión, puede editar dicha información.

Registro de interconexiones

Hay tres razones para registrar una interconexión: para utilizar el supervisor de aplicaciones a fin de supervisar el estado y las estadísticas de la interconexión, para configurar las normas de direccionamiento de la interconexión, o ambas. Puede añadir un nuevo registro de interconexión o basar el registro en una interconexión registrada existente.

Antes de empezar

Debe conocer el nombre exclusivo de la interconexión y el nombre del nodo de interconexión que aloja la interconexión. La interconexión no tiene que estar ya instalada y configurada en el nodo de interconexión antes de registrarla. (Pero se debe instalar y configurar antes de que el sistema pueda supervisarla o direccionar a la interconexión.)

Acerca de esta tarea

Sugerencia: si añade múltiples interconexiones que se ejecutan en el mismo nodo de interconexión, puede registrar la primera interconexión y después clonar las demás a partir de la primera que ha añadido.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Interconexiones**.
4. Complete uno de los pasos siguientes:
   - Para registrar una nueva interconexión, pulse el botón **Nuevo**.
   - Para registrar una nueva interconexión basada en otra existente, pulse el botón **Clonar**.
5. En el panel **General**, especifique un nombre de interconexión exclusivo, la descripción, el nombre de nodo de interconexión y si se debe supervisar el estado y las estadísticas de la interconexión.

   Nota:
   - El nombre de interconexión que especifique es el mismo nombre que debe utilizar cuando inicie esta interconexión. Este nombre es sensible a las mayúsculas y minúsculas, por lo que cuando inicie la interconexión, deberá especificar una coincidencia exacta del nombre de interconexión registrado. Si no especifica una coincidencia exacta (o coincidencia de mayúsculas y minúsculas), ninguna de las normas de direccionamiento configuradas para esta interconexión ni la aplicación que supervisa esta interconexión funcionarán.
   - Si desea supervisar el estado y las estadísticas para esta interconexión en el panel **Estado de interconexión** de la Consola de configuración, seleccione **Sí** en el campo **Supervisado**.
6. Pulse el botón **Guardar**.

Qué hacer a continuación

Si la interconexión se ha añadido satisfactoriamente, se visualizará en la lista de la izquierda de la pantalla. Ahora puede configurar normas de direccionamiento para esta interconexión o utilizar el sistema para supervisar la interconexión. Sin embargo, recuerde que para direccionar satisfactoriamente o supervisar la interconexión, se debe iniciar utilizando el mismo nombre exactamente, incluyendo las mayúsculas y minúsculas, tal como se ha registrado en el campo **Nombre de interconexión**.

Visualización de detalles de una interconexión registrada

Puede ver los detalles de una interconexión registrada en la Consola de configuración para asegurarse de que la información de registro está actualizada. Las interconexiones se registran para permitir que el sistema supervise el rendimiento y las estadísticas de la interconexión, para direccionar a interconexiones, o para ambas acciones.

Antes de empezar

- La interconexión debe estar registrada en la Consola de configuración.

Procedimiento

1. Pulse el botón **Estado**.
2. Pulse el botón **Estado**.
3. Pulse la pestaña **Visión general**.
4. Pulse el nombre registrado de la interconexión.

Resultados

En la ventana **Detalle**, revise los detalles de la interconexión seleccionada.

Edición de registros de interconexión

Edite la información acerca de una interconexión registrada cuando un componente clave del registro de la interconexión haya cambiado como, por ejemplo, el nombre del nodo de interconexión. El nombre registrado de una interconexión es la única información que no se puede cambiar. Si debe cambiar el nombre registrado de una interconexión, suprima el registro de interconexión y vuelva a añadirlo con la información correcta o añada otro registro de interconexión.

Acerca de esta tarea

Si la interconexión que desea editar está activa (en ejecución actualmente), es aconsejable detener la interconexión antes de editar el registro, especialmente si cambia el estado de supervisión.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Interconexiones**.
4. Seleccione la interconexión o interconexiones que desea editar y después pulse el botón **Editar**.
5. Cambie la información.

   Nota: Recuerde que para supervisar el estado y las estadísticas de la interconexión en el panel **Estado de interconexión**, el campo **Supervisado** se debe establecer en **Sí**.
6. Pulse el botón **Guardar**.

Resultados

Puede ver los cambios en el panel **Interconexiones**.

Qué hacer a continuación

Si ha detenido la interconexión, vuelva a iniciarla.

Supresión de registros de interconexión

La supresión de un registro de interconexión en la Consola de configuración no suprime físicamente la interconexión del sistema, elimina la interconexión en los paneles **Interconexiones**, **Normas de direccionamiento** y **Estado de interconexión**. Estos registros suprimidos ya no podrán direccionar información utilizando normas de direccionamiento ni proporcionar información de estado y de supervisión de estadísticas. No se puede editar un nombre de interconexión

registrado. Si necesita cambiar el nombre de una interconexión registrada, suprima el registro de interconexión y después vuelva a añadirlo con la información correcta o añada otro registro de interconexión.

Acerca de esta tarea

Si la interconexión que desea suprimir está activa (en ejecución actualmente) y el sistema la está supervisando en el panel **Estado de interconexión**, es aconsejable detener la interconexión antes de suprimirla. También es aconsejable comprobar el panel **Normas de direccionamiento** para ver si hay normas de direccionamiento asociadas a esta interconexión; si las hay, puede redireccionar estas normas de direccionamiento a otra interconexión o añadir una nueva interconexión que utilice esas normas de direccionamiento antes de suprimir esta interconexión.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **General**.
3. Pulse la pestaña **Nodos**.
4. Seleccione la interconexión o interconexiones que desee suprimir y pulse el botón **Suprimir**.

Qué hacer a continuación

La interconexión que ha suprimido ya no se visualizará en los paneles **Nodos** y **Normas de direccionamiento**. La interconexión suprimida ya no informará del estado en el panel **Estado de interconexión**. El sistema ya no direccionará ninguna de las normas de direccionamiento asignadas a la interconexión suprimida en el panel **Normas de direccionamiento**.

Temas de ayuda

Panel Interconexiones

Utilice el panel **Interconexiones** para registrar una interconexión o para editar, suprimir o ver las interconexiones registradas. Si hay interconexiones registradas en este panel y se ha instalado y configurado un agente SNMP en el nodo de interconexión que ejecuta la interconexión registrada, puede ver el estado, las estadísticas y el rendimiento de la interconexión en el panel **Estado**. También puede utilizar el panel **Normas de direccionamiento** para configurar y dirigir resultados procedentes de una interconexión registrada a otras bases de datos y sistemas externos.

Nombre de interconexión
Lista los nombres de cada nodo registrado para la supervisión de aplicaciones en la Consola de configuración, en orden alfabético.

Descripción
Ofrece texto adicional que puede ayudar a describir mejor y a distinguir este nodo de otros nodos del sistema.

Nombre de sistema principal
Muestra el nombre del nodo de interconexión donde reside esta interconexión. (Si piensa supervisar esta interconexión, esto también es el servidor donde se debe instalar y ejecutar un agente SNMP).

Supervisada
Muestra si el estado y las estadísticas de esta interconexión se van a

supervisar y a notificar en el panel **Estado**. (No es lo mismo que el estado actual de la interconexión; esta columna indica cómo está registrada actualmente esta interconexión.)

- Sí indica que el supervisor de aplicaciones está supervisando la interconexión registrada.
- No indica que esta interconexión no está configurada para la supervisión de aplicaciones, pero puede estar configurada para el direccionamiento.

Interconexiones - Panel Detalles

Utilice este panel para registrar una interconexión o para ver los detalles de una interconexión registrada existente. Debe registrar una interconexión antes de configurar normas de direccionamiento para la misma en el panel **Direccionamiento** o de supervisar sus estadísticas y su estado en el panel **Estado**.

Todos los campos de este panel son obligatorios para registrar correctamente una interconexión. Una vez se ha registrado una interconexión, puede cambiar cualquier valor excepto el nombre de la misma. Por ejemplo, si tiene que cambiar el nombre del nodo de interconexión (campo **Nombre de sistema principal**, edite dicho nombre. Sin embargo, si desea cambiar el nombre de la interconexión, primero debe suprimir el nombre de interconexión incorrecto registrado aquí y luego volver a añadir la interconexión con la información correcta.

Nombre de interconexión
Especifique un nombre exclusivo para la interconexión que no supere los 15 caracteres. Si desea supervisar o direccionar desde o hacia la interconexión, el nombre debe coincidir exactamente con este nombre de interconexión registrada al iniciar la interconexión, incluidas mayúsculas y minúsculas.

La lista de la izquierda muestra los nombres de todas las interconexiones ya registradas.

Descripción
Especifique una descripción que no supere los 50 caracteres para distinguir la interconexión de las otras interconexiones. Por ejemplo, utilice la descripción para indicar para qué se utiliza el sistema o el tipo de fuentes de datos que procesa el sistema.

Nombre de sistema principal
Especifique el nombre del nodo de interconexión que ejecuta esta interconexión.

Supervisada
Seleccione si el supervisor de aplicaciones notifica el estado de esta interconexión.

- **Sí** indica que desea supervisar el estado y las estadísticas de esta interconexión. Si esta interconexión se ha registrado correctamente en la Consola de configuración y el agente SNMP se está ejecutando en el nodo de la interconexión, el estado y las características de la interconexión se muestran en el panel **Estado**.
- **No** indica que desea registrar esta interconexión para direccionamiento pero no para supervisión. No se mostrará el estado ni las estadísticas de esta interconexión en el panel **Estado**, pero puede configurar normas de direccionamiento para la interconexión registrada.

Configuración de normas de direccionamiento

Las normas de direccionamiento permiten direccionar los resultados del proceso de interconexiones o del programa de adquisición a una base de datos, una interconexión o un sistema externo. Las normas de direccionamiento se configurar en la Consola de configuración, en el panel **Normas de direccionamiento**, pero sólo se pueden direccionar desde interconexiones o programas de adquisición que se han registrado en el supervisor de aplicaciones. Puede configurar una nueva norma de direccionamiento desde el principio o basarse en una norma de direccionamiento existente.

Antes de empezar

- La interconexión o el programa de adquisición desde los que desea realizar el direccionamiento deben estar registrados en el supervisor de aplicaciones.
- Debe conocer el nombre exclusivo exacto que se ha utilizado para registrar la interconexión o el programa de adquisición.
- Debe conocer el método de transporte que se debe utilizar y la sintaxis del URI de transporte específico que se debe utilizar para direccionar al destino.

Procedimiento

1. Pulse la pestaña **Configuración**.
2. Pulse la pestaña **General**.
3. Pulse la pestaña **Normas de direccionamiento**.
4. Realice una de las acciones siguientes:
   - Para configurar una nueva norma de direccionamiento, pulse el botón **Nuevo**.
   - Para configurar una nueva norma de direccionamiento basándose en una norma de direccionamiento existente, seleccione el recuadro de selección situado junto a la norma de direccionamiento en la que desea basar la nueva norma y pulse el botón **Clonar**.
5. Necesario: En el campo **Desde interconexión**, especifique el nombre registrado para la interconexión o el programa de aplicación desde el que desea realizar el direccionamiento. El nombre que escriba debe coincidir exactamente con el nombre registrado en el panel **Interconexiones**.
6. Necesario: En el campo **Orden**, especifique un número del 0 al 999 que represente el orden en el que el sistema debe utilizar esta norma de direccionamiento. El valor por omisión del sistema para este campo es 0, que es la primera norma de direccionamiento procesada para cualquier interconexión o programa de adquisición. El número de este campo debe ser exclusivo para la interconexión o programa de adquisición, especialmente si ya hay múltiples normas de direccionamiento configuradas para la interconexión o programa de adquisición.

   Nota: Examine en el parte izquierda de este panel, la lista de interconexiones o programas de adquisición que tienen configuradas normas de direccionamiento existentes. Si ve esta interconexión o nodo en la lista, busque el número más alto que sigue a los dos puntos después del nombre de interconexión o programa de adquisición y especifique el número más alto siguiente. Por ejemplo, si configura una nueva norma de direccionamiento para PIPE08, y ve PIPE08:0 en la lista del panel de la izquierda, debe especificar el número 1 o superior en el campo Orden.

7. Necesario: En el campo **Destino**, especifique el URI de transporte para el destino de la información direccionada. Esto informa al sistema la forma en que se debe direccionar a la interconexión, base de datos o destino de sistema externo previstos.

   Nota: Para que el direccionamiento sea satisfactorio, el proceso de destino debe ser accesible utilizando el mismo URI de transporte que se ha especificado. Por ejemplo, si el destino es una interconexión, ésta se debe haber iniciado utilizando el mismo URI de transporte.
8. Necesario: En la lista desplegable **Documento**, seleccione el tipo de documento UMF para indicar el tipo de mensaje que se debe direccionar al destino.
9. Opcional: En el campo **Filtro de direccionamiento**, especifique un filtro para aplicar a la información que se debe direccionar, de modo que el sistema sólo direccione determinada información al destino. Los filtros son una característica de las normas de direccionamiento avanzadas. Se escribe una expresión de filtro `MODDIST(`*`nombre_código_UMF`*`,` donde `(`*`nombre_código_UMF`* indica el nombre del código UMF que el sistema utiliza para distribuir los registros.
10. Necesario: En la lista desplegable **Habilitado**, seleccione **Sí** para habilitar esta norma de direccionamiento.
11. Necesario: Pulse el botón **Guardar**.

Ejemplo

Qué hacer a continuación

El nombre de la interconexión o del programa de adquisición se visualiza en el panel **Normas de direccionamiento** con los detalles de la norma de direccionamiento que acaba de configurar. El sistema empieza a direccionar la información desde la interconexión o programa de adquisición hacia el destino, utilizando la norma de direccionamiento configurada.

Normas de direccionamiento

Las normas de direccionamiento indican al supervisor de aplicaciones que envíe mensajes de un programa de adquisición a una interconexión o de una interconexión a una base de datos o sistema externo. Las normas de direccionamiento sólo se pueden configurar para interconexiones que se han registrado con el supervisor de aplicaciones, pero los resultados se pueden direccionar a cualquier destino mediante la sintaxis de transporte adecuada de URI (Universal Resource Indicator).

Las normas de direccionamiento tienen muchos usos, incluidos los siguientes usos comunes:

- Equilibrio de la carga de datos procedente de un programa de adquisición (como el programa de utilidad de bases de datos UMF) a varias interconexiones para el proceso de datos.
- Direccionamiento de los resultados del proceso de la interconexión (como por ejemplo alertas) a un sistema externo o a una base de datos de informes para su futura investigación y para la generación de informes.

Documentos UMF y tablas de direccionamiento

Las normas de direccionamiento se configuran para que direccionen mensajes utilizando uno o varios tipos de documentos UMF. Su elección depende de la información resultante de la interconexión o del nodo del sistema desde el que desea realizar el direccionamiento. Por ejemplo, una UMF_ALERT es un tipo de documento UMF que representa alertas generadas a partir del proceso de registros de identidades y de entidades a través de una interconexión. Podría direccionar cualquier alerta generada a partir de una interconexión específica a un sistema externo, como por ejemplo a una interfaz de usuario utilizada por los analistas que investigan las alertas generadas por el sistema.

Puede configurar una norma de direccionamiento para direccionar todos los tipos de documentos UMF o un tipo específico de documentos UMF, incluidos todos los tipos de documentos UMF personalizados configurados para el sistema.

Filtros

Puede filtrar la información que se direcciona al destino especificando una expresión de filtro cuando configure una norma de direccionamiento. Los filtros especifican que sólo se direccione determinada información al destino.

Puede construir un filtro de direccionamiento utilizando la expresión `MODDIST(`*`nombre_código_UMF`*`)`, donde

`MODDIST`
: es la expresión que indica una distribución de módulo.

`(`*`nombre_código_UMF`***`)`**
: identifica el código UMF que indica al sistema cómo distribuir los registros. Utilizando el código UMF identificado, el sistema suma los valores ASCII de todos los caracteres de dicho código para determinar el número de rutas necesarias para equilibrar la carga del proceso de datos.

Si desea direccionar todos los registros del código de la fuente de datos "datasource5" a otra base de datos de informes, podría configurar una norma de direccionamiento utilizando la expresión de filtro `MODDIST(datasource5)`, donde `datasource5` es el código de la fuente de datos.

Proceso de direccionamiento

Cuando una interconexión o programa de adquisición tiene una norma de direccionamiento configurada, el supervisor de aplicaciones completa el proceso de direccionamiento del siguiente modo:

1. Cuando se inicia la interconexión o el programa de interconexión, envía una solicitud al supervisor de aplicaciones utilizando un mensaje UMF.
2. El supervisor de aplicaciones recibe la solicitud y busca todas las normas de direccionamiento activas pertenecientes a la interconexión o programa de adquisición solicitante.
3. Si el supervisor de aplicaciones localiza una norma de direccionamiento activa para la interconexión o programa de adquisición solicitante, crea un documento UMF que contiene las instrucciones de direccionamiento y envía dicho documento UMF de nuevo a la interconexión o programa de adquisición solicitante.
4. La interconexión o programa de adquisición solicitante interpreta el mensaje del documento UMF y crea una archivo de direccionamiento con una extensión de

archivo *.RTE (donde * es el nombre de la interconexión o del programa de adquisición solicitante). Si la interconexión o el programa de adquisición no se puede comunicar con el supervisor de aplicaciones tras el arranque, busca instrucciones en el archivo de direccionamiento.

5. La interconexión o el programa de adquisición solicitante abre los transportes necesarios para comunicar con el destino configurado en la norma de direccionamiento.
   - Si la interconexión o el programa de adquisición puede abrir correctamente el transporte y localizar el destino, direcciona los mensajes de documentos UMF adecuados al destino siempre y cuando esté iniciado y procesando datos de forma activa.
   - Si la interconexión o el programa de adquisición no puede abrir el transporte o si no se puede localizar el destino, la interconexión o el programa de adquisición se detiene con un error.

Temas de ayuda

Panel Normas de direccionamiento

Utilice este panel para ver o suprimir normas de direccionamiento existentes y para configurar nuevas normas de direccionamiento para interconexiones registradas en el panel **Interconexiones**. Una vez configurada una norma de direccionamiento, no se puede editar; sólo se puede suprimir.

Desde interconexión
Muestra el nombre de la interconexión configurada con una norma de direccionamiento.

Orden Muestra el orden en que se procesa esta norma de direccionamiento para la interconexión en la columna **Desde interconexión**. El orden resulta útil cuando hay varias normas de direccionamiento; generalmente el orden se establece en 0.

Destino
Muestra el URI de transporte de la interconexión, base de datos o sistema externo receptores.

Tipo de documento
Muestra el tipo de documento UMF que envía esta norma de direccionamiento. Es el tipo de documento correspondiente a los resultados procesados por la interconexión en la columna **Desde interconexión**. Esta selección puede ser un tipo de documento UMF específico o un * (asterisco), lo que indica que esta norma de direccionamiento direcciona todos los tipos de documentos UMF.

Habilitado
Indica si esta norma de direccionamiento está o no activa:
- **Sí** indica que la norma de direccionamiento está habilitada. Siempre que la interconexión o nodo visualizados en la columna **Desde interconexión** procesan resultados para el tipo de documento especificado, el sistema direcciona los datos asociados al tipo de documento UMF al destino indicado en la columna **Destino**.
- **No** indica que la norma de direccionamiento no está habilitada.

Panel Detalles de normas de direccionamiento

Utilice este panel para configurar una nueva norma de direccionamiento o para ver los detalles de una norma de direccionamiento existente. Las normas de direccionamiento se suelen configurar para publicar tipos específicos de resultados

procesados desde una interconexión a otra base de datos o a un sistema externo. Sólo puede configurar normas de direccionamiento para interconexiones registradas en el panel **Interconexiones**.

Todos los campos excepto el campo **Filtro de direccionamiento** son obligatorios para configurar correctamente una nueva norma de direccionamiento. Una vez configurada una norma de direccionamiento, no se puede editar; si tiene que cambiar la norma de direccionamiento, debe suprimirla y volverla a añadir con la información correcta.

Desde interconexión
Especifique el nombre exclusivo de la interconexión desde la que desea direccionar resultados. El nombre de esta interconexión debe coincidir exactamente con el que está registrado en el panel **Interconexiones** y es sensible a mayúsculas y minúsculas; si el nombre no coincide, el sistema muestra un mensaje de error que indica que la interconexión especificada no existe.

Orden Especifique un número comprendido entre 0 y 999 que indique el orden en el que el sistema aplica esta norma de direccionamiento a la interconexión registrada en el campo **Desde interconexión**. El valor por omisión del campo es 0, lo que indica que el sistema procesa primero esta norma de direccionamiento. Si esta interconexión ya tiene una o varias normas de direccionamiento configuradas, especifique un número mayor que el orden superior

Compruebe el panel izquierdo para ver el orden establecido para las normas de direccionamiento existentes ya configuradas para esta interconexión, indicado por el número secuencial seguido de un signo de dos puntos tras el nombre de la interconexión. (Por ejemplo:PIPE08:0 indica que la interconexión PIPE08 ya tiene una norma de direccionamiento configurado, actualmente establecida para que se procese en primer lugar. Si ha configurado una nueva norma de direccionamiento para PIPE08, establezca el orden en 1.)

Destino
Especifique el UR de transporte a la interconexión, base de datos o sistema externo de destino al que direccionar los resultados procesados. Asegúrese de utilizar la sintaxis adecuada para el tipo de transporte que utilice.

Lista desplegable Tipo de documento
En la lista desplegable, seleccione el tipo de documento UMF desde el que direccionar la interconexión registrada al destino. Si desea direccionar todos los resultados procesados al destino, seleccione el carácter de asterisco *.

Filtro de direccionamiento
Si desea especificar que sólo se direccione determinada información al destino, escriba la expresión que debe utilizar el sistema para filtrar los valores UMF direccionados por esta norma de direccionamiento. (Por ejemplo, si desea direccionar únicamente los registros de identidad o de entidad procedentes de un determinado origen de datos, puede escribir el filtro DSRC_CODE=x, donde *x* es el código exclusivo de fuente de datos correspondiente al origen de datos para la que desea filtrar.)

Los filtros son una característica avanzada de normas de direccionamiento.

Lista desplegable Habilitado
Seleccione una opción en la lista desplegable:

- **Sí** significa que el supervisor de aplicaciones direcciona la información procedente de la interconexión al destino según esta norma de direccionamiento.
- **Sí** significa que el supervisor de aplicaciones no direcciona la información procedente de la interconexión según esta norma de direccionamiento.

Supresión de normas de direccionamiento

Una vez configurada una norma de direccionamiento, no se puede editar; si necesita corregir o actualizar información debe suprimir la norma de direccionamiento anterior y configurar una nueva. También puede que deba suprimir una norma de direccionamiento que ya no se necesite o utilice. Puede suprimir una o varias normas de direccionamiento configuradas en el panel **Normas de direccionamiento** de la Consola de configuración.

Procedimiento

1. Pulse la pestaña **Configuración**.
2. Pulse la pestaña **General**.
3. Pulse la pestaña **Normas de direccionamiento**.
4. Marque el recuadro de selección situado junto a cada norma de direccionamiento configurada que desee suprimir.
5. Pulse el botón **Suprimir**.

Qué hacer a continuación

El sistema suprimirá las normas de direccionamiento seleccionadas y ya no direccionará información utilizando las normas de direccionamiento suprimidas.

Estado y estadísticas de interconexión

La supervisión del estado, las estadísticas y el rendimiento es importante para mantener las interconexiones en ejecución, para equilibrar las cargas de datos de interconexión y para detectar problemas potenciales de interconexión antes de que se produzcan.

Para poder ver el estado y las estadísticas de una interconexión, se debe haber realizado lo siguiente:

1. Se debe haber instalado y configurado la interconexión en su nodo de interconexión.

Nota: (Sólo plataformas Windows) Si inicia la interconexión como un servicio, puede ver información de estado adicional en el Visor de sucesos de Windows que no puede ver en otros lugares.

Información de estado y estadísticas

Una vez que una interconexión comienza a procesar datos, puede ver información de excepción UMF en la Consola de configuración:

- Excepciones de UMF en el panel **Excepciones de UMF**

Agentes SNMP

Protocolo Simple de Gestión de Red (SNMP) es un protocolo estándar que se utiliza para supervisar sistemas y dispositivos de red. Los agentes SNMP solicitan información periódica sobre estado y estadísticas de cada interconexión registrada en el sistema. La información del agente SNMP que se obtiene sobre cada interconexión registrada se muestra en el panel **Estado de interconexión**.

Para que los agentes SNMP puedan supervisar interconexiones:

- Debe haber un agente SNMP instalado y configurado en el nodo de interconexión que ejecuta las interconexiones que desea supervisar.
- Cada interconexión que desea supervisar debe estar registrada en la Consola de configuración y configurada para supervisión.
- El agente SNMP se debe haber iniciado y debe estar en ejecución en el nodo de interconexión, utilizando el mismo número de puerto que el configurado durante la instalación de la interconexión. Este número de puerto de agente SNMP rige para todo el sistema, no para cada nodo de interconexión. El número de puerto SNMP predeterminado es 13516, pero puede localizar el número de puerto de agente SNMP configurado en el archivo server.xml situado en cada nodo de interconexión.

Los agentes SNMP son servicios y se pueden detener e iniciar según sea necesario.

Ejemplo de utilización de un agente SNMP

La empresa ABC supervisa todas sus interconexiones utilizando el supervisor de aplicaciones. Han añadido otro nodo de interconexión (EAS-2) que aloja tres nuevas interconexiones: Interconexión300, Interconexión310 e Interconexión 320. Para supervisar estas interconexiones, los operadores de la empresa ABC deben completar las siguientes tareas:

- Instalar y configurar un agente SNMP en el nodo de interconexión EAS-2.
- En la Consola de configuración, registrar cada nueva interconexión (Interconexión300, Interconexión 310 e Interconexión 320) en el panel **Interconexiones**.
- Iniciar el agente SNMP en el nodo de interconexión EAS-2. Asegúrese de que el agente SNMP utilice el número de puerto del sistema que se ha configurado al instalar las interconexiones en este nodo de interconexión.
- Iniciar cada interconexión registrada para el proceso. Asegúrese de escribir el nombre exacto que se ha registrado en la interconexión, puesto que los nombres de interconexión registrados son sensibles a mayúsculas y minúsculas.

Cuando las nuevas interconexiones se estén ejecutando, los operadores de la empresa ABC pueden supervisar su estado y sus estadísticas a través de la Consola de configuración.

Inicio de agentes SNMP

Para supervisar el estado y las estadísticas de una o varias interconexiones en la Consola de configuración, debe iniciar un agente SNMP en el nodo de interconexión donde se ejecutan las interconexiones.

Antes de empezar

- Un agente SNMP debe estar instalado y configurado en el nodo de interconexión donde se ejecutan las interconexiones.

- Las interconexiones deben estar registradas en el panel **Interconexiones** de la Consola de configuración y estar configuradas para la supervisión.

Procedimiento

1. En la línea de mandatos del nodo de interconexión, utilice el mandato **Change directory** para ir al directorio inicial.
2. Especifique el siguiente mandato: **java -jar SNMPAgent**-p *número de puerto* donde *número de puerto* es el número de puerto de todo el sistema, configurado durante la instalación de las interconexiones para agentes SNMP. El valor de número de puerto por omisión es 13516.

   Nota: Puede encontrar el número de puerto de agente SNMP configurado en el archivo server.xml, en el nodo de interconexión.

Resultados

Se inicia el agente SNMP.

Qué hacer a continuación

En la Consola de configuración, seleccione el panel **Estado de interconexión** para verificar que el agente SNMP está en ejecución. Si es así, el agente SNMP informará del estado y las estadísticas de todas las interconexiones que se ejecutan en este nodo de interconexión. No es necesario que reinicie el agente SNMP si añade más interconexiones, siempre que los archivos .SHM estén en el mismo directorio, que normalmente es el directorio donde se inicia el agente SNMP.

Detención de agentes SNMP

Detenga un agente SNMP de un nodo de interconexión siempre que deba realizar cambios en el nodo de interconexión como, por ejemplo, actualizaciones de la configuración.

Antes de empezar

Debe haber un agente SNMP en ejecución actualmente en el nodo de interconexión. También es aconsejable detener cualquier interconexión que se ejecute en este nodo de interconexión que el supervisor de aplicaciones esté supervisando.

Procedimiento

En la ventana que ejecuta el agente SNMP, pulse las teclas **Ctrl** + **C**.

Qué hacer a continuación

- El agente SNMP se detiene.
- En la Consola de configuración, el panel **Estado de interconexión** muestra el estado `STOPPED` para todas las interconexiones de este nodo de interconexión.

Comprobación del estado de las interconexiones en la Consola de configuración

El seguimiento del estado actual de las interconexiones es importante porque si una interconexión está desactivada, parte del sistema está desactivado. Puede ver rápidamente el último estado de las interconexiones y las estadísticas de rendimiento en el panel **Estado de interconexión** de la Consola de configuración.

El supervisor de aplicaciones recibe la información de los agentes SNMP activos, para ello sondea los agentes SNMP y después renueva el panel **Estado de interconexión** cada 60 segundos.

Antes de empezar

- Un agente SNMP debe estar instalado y configurado en el nodo de interconexión que ejecuta las interconexiones que se deben supervisar.
- El agente SNMP se debe haber iniciado utilizando el número de puerto de todo el sistema durante la instalación de la interconexión. (Puede ver este número de puerto configurado en el archivo server.xml.)
- La interconexión debe estar registrada en el panel **Interconexiones** de la Consola de configuración y estar configurada para la supervisión.
- La interconexión se debe haber iniciado utilizando exactamente el mismo nombre, y las mayúsculas y minúsculas, que el nombre de interconexión que se ha registrado en el panel **Interconexiones**.

Acerca de esta tarea

Si no puede ver el estado mediante la Consola de configuración, puede utilizar la línea de mandatos para comprobar el estado de la interconexión.

Procedimiento

1. Pulse el botón **Estado**.
2. Pulse el botón **Estado de interconexión**.
3. Consulte la columna **Nombre de interconexión** para localizar el nombre de la interconexión que desea comprobar. (Las interconexiones se listan por nombre en orden alfanumérico.) Después, consulte la información de las columnas de estadísticas de transacción y estado de la misma fila que el nombre de interconexión.

Qué hacer a continuación

También puede ver otra información acerca de esta interconexión pulsando en uno de los demás botones. Por ejemplo, si desea ver la última vez que se ha iniciado esta interconexión, pulse la pestaña **Sucesos**.

Comprobación del estado de interconexiones utilizando la línea de mandatos

El seguimiento del estado actual de las interconexiones es importante porque si una interconexión está desactivada, parte del sistema está desactivado. Muchas organizaciones comprueban las interconexiones mediante el panel **Estado de interconexión** de la Consola de configuración, porque visualiza el estado de las interconexiones y las estadísticas más recientes basándose en un sondeo automático del sistema realizado cada 60 segundos. Pero puede utilizar una línea de mandatos para comprobar el estado de una interconexión en particular o de todas las interconexiones de un nodo de interconexión determinado. (La comprobación de la línea de mandatos sólo proporciona el estado de las interconexiones, no la estadísticas de rendimiento de las interconexiones.)

Antes de empezar

- Un agente SNMP debe estar instalado y configurado en el nodo de interconexión que ejecuta la interconexión.

- El agente SNMP se debe haber iniciado y debe estar en ejecución en el nodo de interconexión, utilizando el mismo número de puerto que el configurado durante la instalación de la interconexión. Este número de puerto de agente SNMP rige para todo el sistema, no para cada nodo de interconexión. El número de puerto SNMP predeterminado es 13516, pero puede localizar el número de puerto de agente SNMP configurado en el archivo server.xml situado en cada nodo de interconexión.

Procedimiento

1. En una línea de mandatos del nodo de interconexión, complete uno de los pasos siguientes:
   - Para comprobar el estado de todas las interconexiones de este nodo de interconexión, escriba el siguiente mandato **pipeline -l**
   - Para comprobar el estado de una interconexión en particular de este nodo de interconexión, escriba el siguiente mandato **pipeline -n nombre_interconexión -l**

   donde *nombre_interconexión* es el nombre exclusivo de la interconexión que desea comprobar.

   Nota: El nombre que escriba debe coincidir con el nombre utilizado para iniciar la interconexión.
2. Pulse **Intro**.

Resultados

El sistema devuelve uno de los estados siguientes para cada interconexión:

- Running para cada interconexión activa actualmente.
- Stopped para cada interconexión inactiva actualmente.

Ejemplo

Por ejemplo, para comprobar el estado de pipeline08, escriba el siguiente mandato:
pipeline -n pipeline08 -l

Qué hacer a continuación

Si el estado de una interconexión aparece inesperadamente como Stopped, puede utilizar los temas de resolución de problemas para averiguar la razón.-

Visualización de sucesos del supervisor de aplicaciones

Los sucesos del supervisor de aplicaciones se producen cuando se intercambia un mensaje entre el supervisor de aplicaciones y las interconexiones registradas en el panel **Interconexiones** de la Consola de configuración. Estos mensajes incluyen información que va desde cuando se inicia o se detiene una interconexión hasta cuando el sistema registra errores o avisos, excepto las excepciones UMF (Universal Message Format). Esta información puede ayudarle a solucionar problemas de errores que se producen en una interconexión específica.

Antes de empezar

- La interconexión debe estar registrada en el panel **Interconexiones** de la Consola de configuración.

- La interconexión se debe haber iniciado en el nodo de interconexión registrado en el panel **Interconexiones** utilizando el mismo nombre de interconexión registrado que se visualiza en el panel **Interconexiones**.

Acerca de esta tarea

Si la interconexión está registrada en el panel **Interconexiones** de la Consola de configuración, puede ver los sucesos actuales o históricos en el panel **Sucesos** de la Consola de configuración.

Procedimiento

1. Pulse el botón **Estado**.
2. Pulse el botón **Sucesos**.
3. Opcional: En el campo **Desde fecha**, escriba la fecha de inicio con el formato mm/dd/aaaa desde la que desea ver los sucesos del supervisor de aplicaciones. Si deja este campo en blanco, el sistema visualizará todos los sucesos del supervisor de aplicaciones desde la primera fecha operativa del sistema que satisfagan los demás criterios especificados. Si escribe una fecha en este campo, no tendrá que escribir una fecha en el campo **Hasta fecha**.
4. Opcional: En el campo **Hasta fecha**, escriba la fecha final con el formato mm/dd/aaaa hasta la que desea ver los sucesos del supervisor de aplicaciones. Si deja este campo en blanco, el sistema visualizará todos los sucesos del supervisor de aplicaciones hasta la fecha de hoy que satisfagan los demás criterios especificados. Si escribe una fecha en este campo, no tendrá que escribir una fecha en el campo **Desde fecha**.
5. Opcional: En el campo **Desde interconexión**, escriba el nombre registrado de la interconexión específica para la que desea ver los sucesos del supervisor de aplicaciones. Si deja este campo en blanco, el sistema visualizará todos los sucesos del supervisor de aplicaciones para todas las interconexiones por nombre registrado que satisfagan los demás criterios especificados.
6. Opcional: En la lista desplegable **Recuento máx**, seleccione el número máximo de sucesos del supervisor de aplicaciones que se deben visualizar. El sistema sólo visualizará hasta ese número inclusive de sucesos del supervisor de aplicaciones que satisfagan todos los demás criterios especificados. Si hay más excepciones que el número especificado, el sistema no los visualizará. Si hay menos excepciones que el número especificado, se visualizarán todos los sucesos del supervisor de aplicaciones que satisfagan todos los demás criterios especificados.
7. Necesario: Pulse el botón **Buscar**.

Ejemplo

Por ejemplo, si desea ver los últimos 500 sucesos del supervisor de aplicaciones que se han producido hoy para pipeline08, debe especificar los criterios siguientes:

- En el campo **Desde fecha**, escriba la fecha de hoy.
- En el campo **Hasta fecha**, escriba la fecha de hoy.
- En el campo **Desde interconexión**, escriba `pipeline08`.
- Seleccione **500** en la lista desplegable **Recuento máx**.

Qué hacer a continuación

Puede consultar los detalles de un suceso del supervisor de aplicaciones pulsando en él. La información visualizada es la que se ha informado cuando se ha producido el suceso.

Visualización de excepciones UMF

Las excepciones UMF indican problemas con los datos de entrada que una interconexión está procesando. Se producen cuando la estructura de los datos de entrada no se puede analizar. Normalmente, las excepciones UMF no contribuyen al recuento del límite de errores de interconexión, por lo que el sistema registra la excepción UMF y generalmente la interconexión continúa el proceso. Esta información puede ayudar a solucionar problemas de datos de entrada para una interconexión en particular.

Antes de empezar

- La interconexión debe estar registrada en el panel **Interconexiones** de la Consola de configuración.
- La interconexión se debe haber iniciado en el nodo de interconexión registrado en el panel **Interconexiones** utilizando el nombre de interconexión registrado, tal como se visualiza en el panel **Interconexiones**.

Acerca de esta tarea

Si la interconexión está registrada en el panel **Interconexiones** de la Consola de configuración, puede ver las excepciones UMF actuales o históricas en el panel **Excepciones UMF** de la Consola de configuración.

Procedimiento

1. Pulse el botón **Estado**.
2. Pulse el botón **Excepciones UMF**.
3. Opcional: En el campo **Desde fecha**, escriba la fecha de inicio con el formato mm/dd/aaaa desde la que desea ver las excepciones UMF. Si deja este campo en blanco, el sistema visualizará todas las excepciones UMF desde la primera fecha operativa del sistema que satisfagan todos los demás criterios especificados. Si escribe una fecha en este campo, no tendrá que escribir una fecha en el campo **Hasta fecha**.
4. Opcional: En el campo **Hasta fecha**, escriba la fecha final con el formato mm/dd/aaaa hasta la que desea ver las excepciones UMF. Si deja este campo en blanco, el sistema visualizará todas las excepciones UMF hasta la fecha de hoy que satisfagan los demás criterios especificados. Si escribe una fecha en este campo, no tendrá que escribir una fecha en el campo **Desde fecha**.
5. Opcional: En el campo **Desde interconexión**, escriba el nombre registrado de la interconexión específica para la que desea ver las excepciones UMF. Si deja este campo en blanco, el sistema visualizará todas las excepciones UMF para todas las interconexiones por nombre registrado que satisfagan los demás criterios especificados.
6. Opcional: En la lista desplegable **Recuento máx**, seleccione el número máximo de excepciones UMF que se deben visualizar. El sistema sólo visualizará hasta ese número inclusive de excepciones UMF que satisfagan todos los demás criterios especificados. Si hay más excepciones que el número especificado, el sistema no las visualizará. Si hay menos excepciones que el número

especificado, se visualizarán todos los sucesos del supervisor de aplicaciones que satisfagan todos los demás criterios especificados.

7. Necesario: Pulse el botón **Buscar**.

Ejemplo

Por ejemplo, si desea ver las últimas 50 excepciones UMF que se han producido hoy para pipeline08, debe especificar los criterios siguientes:

- En el campo **Desde fecha**, escriba la fecha de hoy.
- En el campo **Hasta fecha**, escriba la fecha de hoy.
- En el campo **Desde nodo**, escriba `pipeline08`.
- En el campo **Recuento máx**, seleccione `50`.

Qué hacer a continuación

Puede consultar los detalles de una excepción UMF pulsando en ella. La información visualizada es la que se ha registrado acerca de la excepción cuando se ha producido.

Visualización de nuevas identidades

El panel **Nuevas identidades** de la Consola de configuración muestra las nuevas identidades procesadas por la interconexión del sistema durante los últimos siete días. Puede utilizar este panel para comprobar el volumen de datos de entrada y asegurarse de que los números son adecuados para la cantidad de datos de entrada o el número de interconexiones activas. También puede verificar las fuentes de datos que se están cargando en la interconexión, para ver qué fuentes suministran datos al sistema.

Procedimiento

1. Pulse el botón **Estado**.
2. Pulse el botón **Nuevas identidades**.

Resultados

El sistema visualiza la lista de todas las nuevas identidades procesadas durante los últimos siete días.

Temas de ayuda

Panel Estado de interconexión

Utilice este panel para revisar información actual sobre estado, estadísticas y rendimiento correspondiente a interconexiones registradas que están configuradas para la supervisión a través del supervisor de aplicaciones y el agente SNMP. El sistema recopila información de estado y estadísticas del agente SNMP cada minuto y renueva el panel **Estado de interconexión**.

Nota: Cada agente SNMP que se ejecuta en cada nodo de interconexión debe utilizar el mismo número de puerto a nivel de sistema. Este número de puerto se configura al instalar interconexiones en un nodo de interconexión. El número de puerto de agente SNMP por omisión es 13516, pero puede localizar el número de puerto SNMP configurado en el archivo server.xml.

Número total de interconexiones
Muestra el número total de interconexiones registradas para la supervisión

de aplicaciones en la Consola de configuración. (Número total de interconexiones es igual a Interconexiones activas más Interconexiones obsoletas más Interconexiones caídas.)

Interconexiones activas
Muestra el número total de interconexiones registradas que están configuradas para la supervisión en la Consola de configuración que se están ejecutando actualmente.

Interconexiones obsoletas
Muestra el número total de interconexiones cuya configuración se ha modificado desde que se inició la interconexión. Estas interconexiones se tienen que detener y volver a iniciar para que los cambios en la configuración entren en vigor.

Interconexiones caídas
Muestra el número total de interconexiones registradas que están configuradas para la supervisión en la Consola de configuración que actualmente no se están ejecutando ni notificando estadísticas. Cada interconexión actualmente caída se incluye en este total, de modo que si un nodo de interconexión no se está ejecutando, todas las interconexiones configuradas para supervisión en dicho servidor se contarán como caídas.

TPM Muestra el promedio del número total de transacciones que se procesan por minuto para todas las interconexiones activas configuradas para supervisión en la Consola de configuración. Este número indica rendimiento general del sistema; cuanto mayor es el número, mejor es el rendimiento de cada interconexión activa. Este número se renueva y se vuelve a calcular cada minuto, según la información recibida de cada agente SNMP que se ejecuta en cada nodo de interconexión en el que se ejecutan interconexiones activas. (TPM total es igual a TPM para interconexiones activas dividido por Número total de interconexiones activas.)

TPS Muestra el promedio del número total de transacciones que se procesan cada segundo para todos los nodos activos configurados para supervisión en la Consola de configuración. Este número indica rendimiento general del sistema; cuanto mayor es el número, mejor es el rendimiento de cada nodo activo. Este número se renueva y se vuelve a calcular cada minuto, según la información recibida de cada agente SNMP que se ejecuta en cada máquina de sistema principal en la que se ejecutan nodos activos. (TPS total es igual a TPS para nodos activos dividido por Número total de nodos activos.)

Nombre de interconexión
Lista los nombres de cada interconexión registrada para la supervisión de aplicaciones en la Consola de configuración, en orden alfanumérico.

Nombre de sistema principal
Muestra el nombre del nodo de interconexión registrado en esta interconexión. Si el estado de esta interconexión se muestra inesperadamente como `Inactiva`, puede utilizar el nombre del nodo de interconexión para ayudar a resolver el problema. (Por ejemplo, si todas las interconexiones de un determinado nodo de interconexión aparecen inesperadamente como `Inactivas`, significa que el nodo de interconexión es un buen punto de partida para resolver el problema.)

Estado
Muestra el último estado conocido de la interconexión: `Activa` (en ejecución) o `Inactiva` (no en ejecución). El sistema actualiza la información

de estado cada minuto, en función de la información recibida del agente SNMP que se ejecuta en el nodo de la interconexión.

TPM Muestra el número medio de transacciones que se procesan por minuto para esta interconexión. Si la interconexión está en el estado `Inactiva`, el sistema muestra `No disponible`. Este número indica rendimiento de la interconexión; cuanto mayor es el número, mejor es el rendimiento de la interconexión.

TPS Muestra el número total de transacciones que se procesan por segundo para esta interconexión. Si la interconexión está en el estado `Inactiva`, el sistema muestra `No disponible`. Este número indica rendimiento de la interconexión; cuanto mayor es el número, mejor es el rendimiento de la interconexión.

Panel Excepciones UMF

Utilice este panel para ver las excepciones UMF registradas a partir de los datos cargados por las interconexiones registradas para la supervisión de aplicaciones. En primer lugar, debe generar un informe en pantalla de las excepciones UMF que desea ver. Luego puede seleccionar una excepción UMF específica y mirar detenidamente sus detalles; esta información puede ser meramente informativa o puede resultar de utilidad para resolver las excepciones UMF de los archivos de datos. Cuando resuelva uno de estos errores, podrá volver a procesar de forma segura los registros de dicho archivo.

Las excepciones UMF son errores guiados por datos. Se producen cuando hay problemas con la estructura de datos UMF de un archivo fuente de datos de entrada que está procesando una interconexión. Por omisión, las excepciones UMF no contribuyen al recuento del límite de errores para la interconexión (establecido en el archivo de configuración de la interconexión); de modo que, por sí mismas, las excepciones UMF generalmente no cierran la interconexión. Encontrará un listado completo de excepciones UMF en la tabla UMF_EXCEPT o en el registro *nombre_interconexión*.msg, aunque las excepciones UMF correspondientes a las interconexiones no se registran para la supervisión de aplicaciones.

Criterios de informes en pantalla

Utilice estos campos para especificar los criterios correspondientes al informe de excepciones UMF en pantalla. Cuando especifique los criterios, pulse el botón **Buscar** para generar el informe.

Desde fecha

Fecha inicial desde la que notificar excepciones UMF dentro de los otros criterios especificados. (Este campo es opcional y se puede dejar en blanco. Si se deja el campo en blanco significa que se mostrarán las excepciones UMF a partir del primer día en que el sistema ha estado operativo dentro de los otros criterios especificados.)

El valor por omisión del campo es la fecha de hoy. Escriba la fecha en el formato `mm/dd/aaaa`.

Hasta fecha

Fecha final hasta la que notificar excepciones UMF dentro de los otros criterios especificados. (Este campo es opcional y se puede dejar en blanco. Si se deja el campo en blanco significa que se deben visualizar las excepciones UMF hasta hoy dentro de los otros criterios especificados.)

El valor por omisión del campo es la fecha de hoy. Escriba la fecha en el formato `mm/dd/aaaa`.

Desde nodo
Nombre de la interconexión registrada para la que se desea ver excepciones UMF. (Este campo es opcional y se puede dejar en blanco. Si se deja el campo en blanco significa que se mostrarán las excepciones UMF correspondientes a todas las interconexiones registradas dentro de los otros criterios especificados.)

Recuerde que sólo puede ver excepciones UMF en este panel para las interconexiones que están registradas para la supervisión de aplicaciones. Si desea ver todas las excepciones UMF, consulte la tabla UMF_EXCEPT o el registro *nombre_interconexión*.msg.

Código de fuente de datos
Código de fuente de datos (exacto) para el que se desea ver excepciones UMF. (Este campo es opcional y se puede dejar en blanco. Si se deja el campo en blanco significa que se mostrarán las excepciones UMF correspondientes a todas las fuentes de datos dentro de los otros criterios especificados.)

Recuento máx
Lista desplegable que contiene opciones correspondientes al número máximo de excepciones UMF que se mostrarán dentro de los otros criterios especificados. Sólo se muestran en pantalla el número de excepciones UMF hasta el número máximo, éste incluido. Si hay más excepciones UMF que cumplen con los criterios, el sistema no los muestra.

Botón Buscar
Al pulsar este botón, el sistema ejecuta la búsqueda; encuentra y muestra todos los registros que coinciden con los criterios especificados.

Visualización de resultados del informe en pantalla
Esta sección de la ventana muestra el informe de excepciones UMF en pantalla, basado en los criterios especificados. La lista está clasificada por número de `ID de UMF`.

ID de UMF
Muestra el número secuencial asignado por el sistema asociado a esta excepción UMF. El ID de UMF se correlaciona directamente con la tabla UMF_EXCEPT, donde se registras las excepciones UMF.

Desde interconexión
Muestra el nombre de la interconexión que estaba procesando el registro cuando se produjo la excepción UMF.

Creada el
Muestra la fecha en que se produjo la excepción UMF.

Documento de salida
Muestra el tipo de documento de salida UMF asociado a esta excepción UMF.

Código de fuente de datos
Muestra el código de fuente de datos asociado al archivo de datos de entrada en el que se ha producido la excepción UMF.

Referencia externa
Muestra la referencia externa correspondiente al registro de datos específico en el que se ha producido la excepción UMF. Esta

información puede ayudar a identificar el registro dentro del archivo de datos que se tiene que corregir.

Acción

Muestra la acción asociada al registro de datos de entrada en el que se ha producido la excepción UMF. (Esta acción está codificada en el UMF correspondiente al registro de datos.)

- A: Añadir
- C: Cambiar
- D: Suprimir

Panel Sucesos

Utilice este panel para ver mensajes intercambiados entre el supervisor de aplicaciones y las interconexiones registradas para supervisión o direccionamiento. Generalmente, estos mensajes quedan registrados en los archivos de registro del sistema, en función de cómo esté configurado el sistema para el registro. En primer lugar, debe generar un informe en pantalla de los sucesos del supervisor de aplicaciones para verlo. Luego puede seleccionar un suceso específico y mirar detenidamente sus detalles; esta información puede ser meramente informativa o puede resultar de utilidad para resolver errores o avisos de la interconexión.

Los sucesos del supervisor de aplicaciones suelen incluir mensajes o errores intercambiados durante el proceso de la interconexión, como inicio de la interconexión, detención de la interconexión o avisos o errores generados durante el proceso de la misma. El único tipo de errores y avisos no incluidos en este panel son las excepciones UMF, que son excepciones guiadas por datos en lugar de información o excepciones del proceso.

Criterios de informes en pantalla

Utilice estos campos para especificar los criterios correspondientes al informe de sucesos del supervisor de aplicaciones en pantalla. Cuando especifique los criterios, pulse el botón **Buscar** para generar el informe. Por omisión, este panel muestra sucesos del supervisor de aplicaciones que se han producido hoy para las interconexiones registradas para la supervisión de aplicaciones.

Desde fecha

Fecha inicial desde la que notificar sucesos del supervisor de aplicaciones dentro de los otros criterios especificados. (Este campo es opcional y se puede dejar en blanco. Si se deja el campo en blanco significa que se mostrarán los sucesos del supervisor de aplicaciones a partir del primer día en que el sistema ha estado operativo dentro de los otros criterios especificados.)

Hasta fecha

Fecha final hasta la que notificar sucesos del supervisor de aplicaciones dentro de los otros criterios especificados. (Este campo es opcional y se puede dejar en blanco. Si se deja el campo en blanco significa que se mostrarán los sucesos del supervisor de aplicaciones hasta hoy dentro de los otros criterios especificados.)

Desde interconexión

Nombre de la interconexión registrada sobre la que se desean ver sucesos del supervisor de aplicaciones. (Este campo es opcional y se puede dejar en blanco. Si se deja el campo en blanco significa que se mostrarán los sucesos del supervisor de aplicaciones correspondientes a todas las interconexiones registradas dentro de los otros criterios especificados.)

Recuerde que sólo puede ver sucesos del supervisor de aplicaciones en este panel para las interconexiones que están registradas para la supervisión de aplicaciones.

Recuento máx
Lista desplegable que contiene opciones correspondientes al número máximo de sucesos del supervisor de aplicaciones que se mostrarán dentro de los otros criterios especificados. Sólo se muestran en pantalla el número de sucesos de aplicaciones hasta el número máximo, éste incluido. Si hay más sucesos de aplicaciones que cumplen con los criterios, el sistema no los muestra.

Botón Buscar
Al pulsar este botón, el sistema ejecuta la búsqueda encontrando y mostrando todos los registros del supervisor de sucesos de la aplicación que coinciden con los criterios especificados.

Visualización de resultados del informe en pantalla
Esta sección de la ventana muestra el informe de sucesos del supervisor de aplicaciones en pantalla, basado en los criterios especificados. La lista está clasificado por número de ID.

ID Muestra el número secuencial asignado por el sistema asociado a este suceso del supervisor de aplicaciones.

Desde interconexión
Muestra la interconexión registrada que se ve afectada por el suceso del supervisor de aplicaciones o que interviene en este. Es la interconexión que puede necesitar para la resolución de problemas.

Fecha/Hora
Muestra la indicación de fecha y hora en que se ha producido el suceso del supervisor de aplicaciones.

Suceso
Muestra el tipo de suceso del supervisor de aplicaciones que se ha producido. Las columnas **Descripción del suceso** y **Nivel de error** contienen más información sobre este suceso e indican la gravedad del tipo de suceso. Actualmente hay dos tipos posibles de sucesos del supervisor de aplicaciones:

- `NODE-INFO` es una nota y otro tipo de suceso informativo que se ha producido en la interconexión afectada. Este tipo de suceso suele mostrarse cuando la interconexión afectada se inicia o se detiene.
- `NODE-ERROR` es un error que se ha producido en la interconexión afectada. Compruebe la columna **Nivel de error** para ver si necesita una acción inmediata. Generalmente, debe mirar detenidamente sobre este suceso del supervisor de aplicaciones; puede ayudarle a resolver un problema con esta interconexión.

Descripción del suceso
Ofrece un máximo de 30 caracteres de información adicional sobre el suceso del supervisor de aplicaciones.

Nivel de error
Muestra el tipo de nivel de error del suceso del supervisor de aplicaciones. Actualmente hay dos tipos posibles de sucesos:

- NOTE es el nivel de error asociado al suceso NODE-INFO. Este tipo de nivel de error suele ser informativo, de modo que no suele requerir ninguna acción del usuario.
- ERR es el nivel de error asociado al suceso NODE-ERROR. Este tipo de nivel de error suele indicar que debe mirar detenidamente los detalles de este suceso del supervisor de aplicaciones para resolver el error. Puede ver todos los detalles del suceso pulsando en el mismo.

Panel Detalles de sucesos

Cuando selecciona un determinado suceso del supervisor de aplicaciones en el panel **Sucesos**, se muestra una nueva ventana con detalles del suceso seleccionado. Estos detalles se toman directamente de los archivos de registro del sistema, excepto del archivo de registro de excepciones UMF. (Este archivo de registro tiene su propio panel **Excepciones de UMF** para que las pueda ver.) Los detalles aquí contenidos le pueden ayudar en la resolución de problemas de un error de interconexión.

ID El número secuencial asignado por el sistema a este suceso del supervisor de aplicaciones.

Interconexión
Lista el nombre de la interconexión en la que ha tenido lugar este suceso del supervisor de aplicaciones.

Fecha/Hora
Muestra la fecha y la hora del suceso CME en el formato Mes, DD, AAAA HH:MM:SS A/PM Huso horario. Esta fecha y hora corresponden a la fecha y la hora que ha registrado el suceso en el archivo de registro.

Suceso
Muestra el tipo de suceso del supervisor de aplicaciones:

- NODE-INFO es una nota y otro tipo de suceso informativo que se ha producido en la interconexión afectada. Este tipo de suceso suele mostrarse cuando la interconexión afectada se inicia o se detiene.
- NODE-ERROR es un error que se ha producido en la interconexión afectada. Compruebe la columna **Nivel de error** para ver si necesita una acción inmediata. Generalmente, debe mirar detenidamente la información correspondiente a este suceso; puede ayudarle a resolver un problema con esta interconexión.

Descripción del suceso
Muestra los primeros caracteres del suceso del supervisor de aplicaciones, tal como está registrado en el archivo de registro. Esta descripción tiene como objetivo proporcionar información más específica sobre lo que ha activado el tipo de suceso.

Nivel de error
Muestra el tipo de nivel de error del suceso del supervisor de aplicaciones:

- NOTE es el nivel de error asociado al suceso NODE-INFO. Este tipo de nivel de error suele ser informativo, de modo que no suele requerir ninguna acción del usuario.
- ERR es el nivel de error asociado al suceso NODE-ERROR. Este tipo de nivel de error suele indicar que debe mirar detenidamente los detalles de este suceso para resolver el error. Puede ver todos los detalles del suceso pulsando en el mismo.

Panel Nuevas cuentas

Utilice este panel para revisar cargas de datos de los siete últimos días. A primera vista, puede verificar qué fuentes de datos han contribuido con archivos para el proceso y el número de nuevos identidades resultantes de dicho proceso. Estas estadísticas le pueden dar una idea del volumen de proceso para ver rápidamente si los volúmenes de datos de entrada son adecuados para la cantidad de datos de entrada esperados.

Cuando pulsa esta pestaña, se muestran los últimos siete días. Si hay más registros de los que caben en la página visible, utilice la barra de desplazamiento para ver los otros registros. El panel **Nuevas cuentas** está clasificada por orden alfanumérico según el código de fuente de datos.

Código de fuente de datos
Muestra el código de fuente de datos asociado a este nuevo registro de identidad. Esta información se basa en el código de fuente de datos UMF (Universal Message Format) en el archivo de entrada que se ha procesado.

Nota: Puede ver una lista completa de todos los códigos de fuente de datos en la Consola de configuración pulsando en la pestaña **Configuración** y luego en la pestaña **Fuentes**.

Descripción
Muestra la descripción del origen de datos, tal como está configurada para este origen de datos en la Consola de configuración. La descripción debería proporcionar más información para ayudarle a identificar la fuente de datos de la que proceden estos registros de identidad.

Fecha de carga
Muestra la fecha en que se ha procesado este archivo de fuente de datos y en que ha contribuido al número de nuevas identidades de la columna **Recuento de registros**. La fecha se representa en el formato `Mes DD, AAAA`.

Recuento de registros
Muestra el número total de identidades nuevas procesadas a partir de este código de fuente de datos en la fecha indicada en la columna **Fecha de carga**. Es el número que puede indicar el volumen de proceso.

Capítulo 7. Cargar datos

Para utilizar IBM InfoSphere Identity Insight debe convertir los datos al formato Universal Message Format (UMF) y debe cargarlos en el sistema.

Adición de una nueva fuente de datos

Debe añadir una nueva fuente de datos cuando tenga una nueva fuente de datos para la base de datos de entidades.

Acerca de esta tarea

Todos los resultados son un producto de datos de calidad. Por lo tanto, la obtención de datos de alta calidad para la base de datos de entidades es una de las tareas más importantes, pero hacerlo requiere un análisis significativo de los datos y la configuración.

Procedimiento

1. Identifique la fuente de los datos. Es importante conocer dónde ir para la resolución de los problemas de datos.
2. Analice los metadatos. Cada fuente de datos configurada en la base de datos de entidades debe tener un identificador exclusivo en sus registros, por lo que la base de datos de entidades puede atribuir completamente todos los datos a su fuente original. Localice el campo que proporcionará la unicidad de los registros y asegúrese de que ese campo sea realmente exclusivo.
3. Utilice un programa de adquisición para transformar los datos desde su formato nativo a UMF.
4. Configure los datos.
   a. Defina un rol para la fuente de datos.
   b. Configure la fuente de datos.
   c. Cree cualquier tipo de número necesario.
   d. Cree cualquier tipo de característica necesaria.
   e. Revise la configuración de resolución y la personalización, si es necesario.
   f. Configure nuevas normas DQM.
   g. Valide las nuevas normas DQM.
   h. Configure las normas de alertas de rol.
5. Verifique los datos.
   a. Compruebe que la interconexión se ha iniciado.
   b. Verifique que la interconexión haya podido utilizar los transportes configurados y que ha recibido UMF del programa de adquisición.
   c. Verifique que el nodo de adquisición ha producido mensajes XML correctamente formados examinando el archivo `.bad`.
   d. Verifique que no se haya producido ninguna excepción UMF como resultado de una correlación o configuración no válida.
   e. Compruebe si hay resultados esperados visualizando los informes de fuente de datos y de resumen de carga.
   f. Busque una o varias entidades resueltas utilizando el Visualizador.
   g. Si es aplicable, examine las alertas de rol.

Conversión de datos a UMF

Para que el sistema procese los datos de entrada, deben convertirse a UMF (Universal Message Format). El proceso de convertir los datos de entrada a UMF se puede realizar utilizando diversas herramientas, incluyendo los programas de utilidad básicos que se proporcionan con el producto o con los productos de transformación XML estándar.

Procedimiento

1. Con el modelo de entidad que ha creado para el sistema, analice los datos de entrada para ver cómo encajan con el estándar UMF. Tener una idea clara de los segmentos y códigos UMF existentes antes de continuar con el siguiente paso.
2. Configure el programa de utilidad de conversión para producir registros UMF que coincidan con el modelo de entidad.
3. Ejecute el programa de utilidad de conversión.

Qué hacer a continuación

Tras convertir los datos a UMF, puede enviar los registros UMF a la interconexión para proceso.

Programas de adquisición

Un programa de adquisición contiene las herramientas y programas que adquieren datos, los transforman al formato UMF (Universal Message Format) y luego envían los datos transformados a la interconexión para su proceso.

Puede utilizar los programas de utilidad del programa de adquisición que se proporcionan con el producto para transformar datos en UMD o puede utilizar herramientas de extracción, transformación y carga (ETL), como WebSphere QualityStage, como programas de adquisición.

Transferencia de archivos UMF a una cola

Puede transferir archivos UMF a una cola utilizando el programa de utilidad de colas.

Procedimiento

1. Asegúrese de que los datos que desea enviar están en formato amplio (un registro por línea).
2. Especifique los valores de configuración en el archivo de configuración.
3. Ejecute el programa de utilidad de colas.

Programa de utilidad de cola

IBM ofrece un programa de utilidad de cola que gestiona la transferencia de datos UMF desde un proceso o archivo a una cola.

Aunque su principal trabajo consiste en mover datos a una o varias colas, también puede utilizar el programa de utilidad de cola para:

- Crear colas
- Eliminar colas de una cola
- Ver el estado de la cola

- Ver los registros de una cola

El programa de utilidad de colas espera datos en un determinado formato:
- Formato amplio UMF, que significa una línea por registro
- Una línea nueva al final de cada registro
- No hay ninguna otra línea nueva dentro de un registro

Debe utilizar uno de los siguientes gestores de colas para utilizar el programa de utilidad de cola.

Microsoft Windows Server x86
Microsoft Message Queuing, un componente de Microsoft Windows Server 2003 o 2008.

IBM Websphere MQ 6.0

Microsoft Windows Server x86_64
Microsoft Message Queuing, un componente de Microsoft Windows Server 2003 o 2008.

IBM Websphere MQ 7.0

Entorno operativo Solaris
IBM Websphere MQ 6.0

Linux IBM Websphere MQ 6.0

AIX IBM Websphere MQ 6.0

Cuando una interconexión se ejecuta en modalidad de cola, siempre se necesita el gestor de colas, que debe estar instalado y en ejecución. Cuando una interconexión se ejecuta en modalidad de archivo, el gestor de colas debe estar instalado, pero no es necesario que se esté ejecutando para las plataformas Windows y AIX. No es necesario que esté instalado ni en ejecución para Solaris ni para Linux.

Archivo de configuración del programa de utilidad de colas

Puede utilizar un archivo de configuración para enviar registros a múltiples colas, con el programa de utilidad de colas.

Cuando se suministra un conjunto de datos a varias colas, debe indicar al gestor de colas cómo configurar la distribución. La idea es crear un tipo de distribución en que la primera cola obtenga un registro, después la siguiente cola obtenga otro, etcétera.

El archivo de configuración del programa de utilidad de colas se denomina qutil.ini y debe estar en el mismo directorio que el archivo ejecutable del programa de utilidad de colas.

Parámetros

[sectionname]
Nombre de la sección. Puede especificar múltiples grupos de valores de configuración dentro de un solo archivo de configuración y, después, hacer referencia a estos valores en la línea de mandatos especificando el nombre de sección. Por ejemplo, puede nombrar las secciones CFG1 (configuración 1) o CFG2 (configuración 2) y hacer referencia a estas secciones cuando emita mandatos del programa de utilidad de colas.

MessageCountMax
Número máximo de registros permitidos en cada cola en cualquier momento especificado. Cuando una cola está llena, el programa de utilidad detiene el proceso de registros.

FullCountMax
Especifica el número total de registros que puede haber en todas las colas, en oposición a una sola cola. Cuando todas las colas están llenas, el programa de utilidad hace una pausa en el flujo de datos y espera a que los registros se muevan a interconexiones para proceso, liberando espacio en las colas. Trabaja con FullPause.

FullPause
El número de milisegundos que el programa de utilidad de colas detiene el flujo de datos, permitiendo que los datos de las colas se procesen cuando se alcanza FullCountMax.

Qout*n*=qname
Los nombres de las colas de salida de esta sección. El nombre de las colas de salida pueden ser cualquiera que tenga sentido, sin embargo, el parámetro debe ser Qout*n*, donde n es un entero que empieza por 0. El valor de *n* debe ser secuencia de 0 a *n* donde n es la última cola definida. Este formato es necesario. Cambie únicamente el número del identificador Qout*n* y los qnames.

Ejemplo

El ejemplo siguiente muestra que hay dos conjuntos de instrucciones (uno que utiliza 2 colas y otro que utiliza 4 colas). Un máximo de 2.500 registros en cada cola a la vez, el máximo de registros en todas las colas es 10.000, y el programa de utilidad de colas hace una pausa de 3 segundos antes de intentar cargar más registros en cualquier cola después de que haya alcanzado FullCountMax. A continuación, lista los nombres de las 4 colas que se deben utilizar.

```
[CFG1]
MessageCountMax=2500
FullCountMax=10000
FullPause=3000
Qout0=qnameA
Qout1=qnameB
[CFG2]
MessageCountMax=2500
FullCountMax=10000
FullPause=3000
Qout0=qnameA
Qout1=qnameB
Qout2=qnameC
Qout3=qnameD
```

Sintaxis de mandatos del programa de utilidad de colas

Los mandatos del programa de utilidad de colas se componen de operaciones y modificadores.

La sintaxis básica de un mandato de programa de utilidad de colas es:

qutil -operation *qname* **-modifier**

qname es el nombre de la cola.

Operaciones de mandato

Las operaciones definen las diferentes funciones del programa de utilidad de colas. Sólo se puede añadir una operación al mandato qutil.

-C Crea una nueva cola.

Necesita un nombre exclusivo para qname.

Debe ser una C en mayúsculas.

-f Copia la entrada estándar en la cola.

Requiere un qname.

-i Copia la entrada estándar en muchas colas.

Requiere que el nombre de sección esté definido en el archivo qutil.ini. Especifica una sección de qutil.ini para cargar y entregar mensajes a muchas colas.

-k Depura el recuento para cada registro.

Requiere un *qname*.

Se puede utilizar junto con el modificador -c para limitar el número de registros procesados.

-p Recuento máximo para cada registro.

No elimina registros de la cola.

Requiere un *qname*.

Graba en la salida estándar.

Se puede utilizar junto con el modificador -c para limitar el número de registros procesados.

-r Recuento de lecturas para cada registro.

Elimina registros de la cola.

Requiere un *qname*.

Graba en la salida estándar.

Se puede utilizar junto con el modificador -c para limitar el número de registros procesados.

-s Estado de la cola.

Requiere un *qname*.

-x Suprimir *qname*.

Requiere un *qname*.

Modificadores de mandato

Los modificadores configuran parámetros adicionales para una operación de programa de utilidad de colas. Puede utilizar más de un modificador en un mandato qutil.

-T Especifica si una cola es transaccional.

Por omisión, todas las colas nuevas son no transaccionales, a menos que se haya especificado durante la creación como transaccionales con un modificador -T.

Las colas transaccionales no se deben utilizar cuando una cola puede recibir información de direccionamiento desde un supervisor de aplicaciones.

Las colas transaccionales de Microsoft Message Queueing no permiten establecer un orden de prioridad ni procesar los mensajes en otro orden que no sea en el que se han recibido.

-c Especifica que se debe detener después de que se haya procesado el recuento de registros.

Necesita un entero.

Debe ser una c en minúsculas.

-l Especifica el nivel de prioridad para cada registro.

Necesita un entero.

Los valores enteros válidos son:

0-7
Microsoft Message Queueing
Los niveles de prioridad son de 0 a 7, donde 0 es la prioridad más baja y 7 la más alta.

3 es el valor predeterminado.

0-9
IBM Websphere MQ
Los niveles de prioridad son de 0 a 9, donde 0 es la prioridad más baja y 9 la más alta.

El valor por omisión depende una propiedad de cola. Puede cambiar esta propiedad en el gestor de IBM Websphere MQ.

-m Especifica el gestor de colas.

Solo AIX, HP-UX, Linux y Solaris

-o Especifica el número de segundos antes de que caduque un mensaje.

Necesita un entero.

-q Especifica el tipo de colas.

Solo Microsoft Windows

Los valores válidos son:

mq IBM WebSphere MQ

msmq Microsoft Message Queueing (MSMQ)

-t Especifica el número de milisegundos que se debe esperar entre cada registro.

Necesita un entero.

Relaciones entre operaciones y modificadores de mandatos

Sólo se recomienda el uso de determinados modificadores en determinadas operaciones. En la siguiente tabla se describe la relación de cada operación con los modificadores potenciales:

Tabla 31. Relaciones entre operaciones y modificadores de mandatos del programa de utilidad de cola

Operación	Modificadores válidos
`-C`	`-T, -q` *EJEMPLO:* qutil -C *qname* -T -q mq
`-f`	`-c, -t, -l, -o, -q` *EJEMPLO:* qutil -f *qname* -c 50 -t 20 -l 4 -o 10 -q msmq
`-i`	NONE *EJEMPLO:* qutil -i configsection
`-k`	`-c` *EJEMPLO:* qutil -k *qname* -c 50
`-p`	`-c` *EJEMPLO:* qutil -p *qname* -c 50
`-r`	`-c` *EJEMPLO:* qutil -r *qname* -c 50
`-s`	NONE *EJEMPLO:* qutil -s *qname*
`-x`	NONE *EJEMPLO:* qutil -x *qname*

Conversión de archivos UMF a formatos adecuados

Puede utilizar el programa de utilidad de formateo de UMF para conmutar los registros UMF entre los formatos ancho y alto.

Programa de utilidad de formateo de UMF

Puede utilizar el programa de utilidad de formateo de UMF para convertir registros UMF a formatos más anchos y altos y de estos a UMF. El programa de utilidad de formateo de UMF también puede extraer datos UMF definidos por un determinado código.

Los registros UMF se pueden mostrar en una sola línea (formato ancho) o como una serie de líneas en la que cada línea contiene un elemento XML y un valor (formato alto).

Ejemplo: formato ancho

```
<name><name_type>M</name_type><first_name>John</first_name>
<last_name>Smith</last_name></name>
```

Ejemplo: formato alto

```
<name>
  <name_type>M</name_type>
  <first_name>John</first_name>
  <last_name>Smith</last_name>
</name>
```

Sintaxis de mandatos del programa de utilidad de formateo de UMF

El programa de utilidad de formateo de UMF utiliza una variedad de mandatos para formatear y extraer datos.

La sintaxis básica de un mandato de programa de utilidad de formateo de UMF es:

```
xutil -o[switch] opción
```

Parámetros

-o **Out** Envía la salida a la salida estándar. Parámetro necesario. Los conmutadores del parámetro son los siguientes:

- **w** Define el formato de la salida. Todo el formato UMF para un registro está en una línea. Elimina todos los retornos y saltos de línea.
- **t** Define el formato de la salida. El formato UMF de un registro está en varias líneas. Coloca un código por línea y coloca códigos en el documento para que sea más legible.

-t **Tagname:** Filtra los registros basándose en un nombre de código. Sólo los registros dentro de estos códigos constituyen la salida que va a la salida estándar. Los errores se envían a la salida estándar

Utilice el parámetro tagname cuando desee filtrar registros. Por ejemplo, tal vez tenga un archivo con registros combinados: entidades y actividades. Es una buena idea procesar las entidades antes que las actividades para que las actividades tengan entidades existentes para la coincidencia.

Ejemplos

Este mandato filtra la salida para las entidades únicamente, utilizando mixedlist.xml como fuente de entrada y entity.xml como archivo de salida.

```
xutil -ow -t UMF_ENTITY < mixedlist.xml > entity.xml
```

Este mandato dirige la salida del proceso del programa de utilidad de formateado de UMF a una interconexión o al programa de utilidad de colas.

```
xutil -ow < file.xml |qutil -f qname
```

Ampliación del modelo de entidad

Un modelo de entidad es un conjunto de datos que define lo que se considera ser una entidad. Utilice estas instrucciones para ampliar el modelo de entidad por omisión. No se trata de una tarea común, pero puede ampliar el modelo de entidad para el entorno.

Universal Message Format (UMF)

Universal Message Format (UMF) es un dialecto de XML extensible utilizado para estructurar archivos de fuente de datos. UMF contiene códigos estándar que representan partes clave de identificadores, relaciones y actividades. Para que las interconexiones puedan procesar los datos, estos se deben convertir a UMF y deben seguir la especificación UMF.

UMF consta de estos componentes jerárquicos:

Documentos UMF
Colección de segmentos UMF que estructuran los datos e indican el tipo de registro de fuente de datos.

Segmentos UMF
Parte del documento UMF que estructura los datos correspondientes a la fuente de datos.

Elementos UMF
Códigos y valores XML que definen los datos dentro de un segmento UMF de un documento UMF.

La especificación UMF lista los tipos específicos de documentos UMF, los segmentos UMF que hay dentro de cada tipo de documento UMF y los elementos UMF válidos dentro de cada segmento UMF.

Análisis de datos fuente

La primera tarea para insertar los datos fuente en la base de datos de entidades es analizar los datos fuente para correlacionarlos con UMF.

Procedimiento

1. Identifique los datos que desea cargar en la base de datos de entidades.
2. Asegúrese de que los datos sean coherentes y estén completos.
3. Identifique el ancho de los valores de elementos de segmentos UMF entrantes con respecto al ancho de las columnas de la tabla de base de datos correspondiente.
4. Identifique los caracteres no válidos de los datos fuente.

Resultados

Los resultados del análisis pueden presentar varias opciones como, por ejemplo:

- Utilizar normas DQM para corregir datos con caracteres no válidos.
- Utilizar normas DQM para truncar datos con un ancho mayor que las columnas de la tabla de base de datos correspondiente.
- Solicitar a proveedores de fuentes de datos externas que suministren datos más completos.
- Cargar únicamente campos con datos válidos.

Revisión de la especificación UMF por omisión

Debe revisar la especificación UMF por omisión como ayuda en la creación de la especificación UMF personalizada y modelo de entidad. Estos elementos correlacionan datos de transferencia de fuentes de datos con códigos UMF que la base de datos de entidades tomará.

Correlación de segmentos UMF con la base de datos de entidades

Siempre que los datos necesiten nuevos segmentos UMF, deberá crear nuevas correlaciones de datos para los datos de esos segmentos UMF. Sin una correlación de datos válida, no puede cargar satisfactoriamente datos en la base de datos de entidades.

Riesgos de modificar la base de datos de entidades

El hecho de modificar la base de datos de entidades comporta riesgos y no debe realizarse sin la suficiente experiencia.

- No se deben añadir tablas a la base de datos de entidades sin la suficiente experiencia
- Añadir campos a tablas de la base de datos es un proceso que implica más que la tabla en cuestión. Se recomienda utilizar las tablas y los campos existentes para clasificar datos nuevos si es posible.
- Los índice de tabla de base de datos no se deben modificar. El modificar los índices en las tablas de base de datos puede producir resultados imprevisibles y no deseables, tales como el bloqueo del Visualizador.
- Se recomienda que los cambios de DQM sólo se realicen con la suficiente experiencia o con la ayuda de IBM.
- Utilice siempre una base de datos de prueba cuando verifique nuevas configuraciones antes de aplicar dichas nuevas configuraciones al entorno de producción.

Adición de tablas a la base de datos de entidades

Es posible que deba añadir una nueva tabla de base de datos al añadir una nueva fuente de datos.

Acerca de esta tarea

La adición de tablas a la base de datos de entidades no permite la resolución en los nuevos datos, sólo es un lugar para almacenarlos.

Se recomienda utilizar una base de datos de prueba al verificar nuevas configuraciones antes de aplicar esas nuevas configuraciones al entorno de producción.

Se recomienda utilizar tablas y campos existentes para clasificar los nuevos datos si es posible.

La adición de una nueva tabla acomodará los datos esperados que todavía no se han configurado en el sistema. Debe crear la nueva tabla de base de datos de modo que sea coherente con el modelo de datos actual.

Asegúrese de incluir los campos pertinentes necesarios:

- ENTITY_ID
- DSRC_ACCT_ID
- HIST_STAT - necesario si se utiliza el rastreo del historial secuencial.
- SYS_CREATE_DT
- SYS_DELETE_DT
- SYS_LSTUPD_DT
- SYS_LSTUPD_US

Procedimiento

1. Cree la nueva tabla en la base de datos de entidades.
2. Cree la correlación de datos para la nueva tabla.
3. Añada nuevas tablas de base de datos al diccionario.
4. Defina las correlaciones de datos para la nueva tabla.

5. Determine las normas DQM adecuadas que se deben aplicar al nuevo segmento y configure esas normas mediante la consola.
6. Verifique la nueva configuración ejecutando datos de prueba conocidos a través de una interconexión y comprobando los archivos de registro resultantes.
   a. Verifique que la prueba se ejecuta sin errores.
   b. Compruebe las excepciones UMF en la consola.
   c. Compruebe si hay errores en los archivos `nodename.Sql.Err.log` y `nodename.err`.
   d. Verifique que los resultados de la prueba coinciden con los resultados esperados.
   e. Compruebe la tabla UMF_LOG para asegurarse de que todos los registros se cargan correctamente.

Adición de campos a tablas de base de datos de entidades:

Es posible que deba añadir un nuevo campo a una tabla de base de datos de entidades existente para acomodar nuevos datos.

Acerca de esta tarea

Se puede añadir un nuevo campo a una tabla existente cuando un nuevo segmento UMF no necesita una tabla completamente nueva.

La adición de campos a una tabla de base de datos de entidades existente no permite la resolución en los nuevos datos, sólo es un lugar para almacenarlos.

Se recomienda utilizar una base de datos de prueba al verificar nuevas configuraciones antes de aplicar esas nuevas configuraciones al entorno de producción.

Se recomienda utilizar tablas y campos existentes para clasificar los nuevos datos si es posible.

Procedimiento

1. Añada el nuevo campo a la tabla de base de datos adecuada.
2. Cree la correlación de datos para el nuevo campo en la consola.
3. Determine las normas DQM adecuadas que se deben aplicar al nuevo campo y configure esas normas a través de la consola.
4. Verifique la nueva configuración ejecutando datos de prueba conocidos a través de una interconexión y comprobando los archivos de registro resultantes.
   a. Verifique que la prueba se ejecuta sin errores.
   b. Compruebe las excepciones UMF en la consola.
   c. Compruebe si hay errores en los archivos `nodename.Sql.Err.log` y `nodename.err`.
   d. Verifique que los resultados de la prueba coinciden con los resultados esperados.
   e. Compruebe la tabla UMF_LOG para asegurarse de que todos los registros se cargan correctamente.

Adición de nuevas tablas de base de datos al diccionario:

Cuando los datos (y el UMF) necesiten que cree una nueva tabla de base de datos, deberá añadir esta tabla al diccionario de tablas de bases de datos que el sistema utiliza. Si la tabla no existe en el diccionario, no podrá crear una correlación de datos para el UMF y la tabla.

Antes de empezar

Se debe otorgar al usuario el acceso adecuado para leer y almacenar datos en la tabla de base de datos.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Diccionario**.
4. Pulse el botón **Nuevo**
5. En el campo **Nombre de tabla**, escriba el nombre de la nueva tabla de base de datos.

Definición de correlaciones de datos

Debe crear una correlación de datos para los nuevos segmentos y códigos UMF. Cuando se añaden nuevos sistemas fuente al producto, a veces se crean nuevos segmentos y códigos UMF como resultado. Una correlación de datos correlaciona los datos de un UMF con las tablas y columnas de tablas correspondientes de la base de datos de entidades.

Correlaciones de datos:

Una correlación de datos correlaciona los datos de un archivo UMF con loas tablas y columnas de tablas correspondientes en la base de datos de entidades.

Sin una correlación de datos válida, no puede cargar correctamente datos en la base de datos de entidades. Siempre que los datos necesitan nuevos segmentos UMF, debe crear nuevas correlaciones de datos para los datos en dichos segmentos UMF.

Ejemplo

Finn's Auto Service ha empezado a recopilar datos sobre la compañía de seguros para sus clientes. Por ejemplo, los datos UMF correspondientes a una nueva compañía de seguros puede utilizar estos segmentos UMF:

```
<ATTRIBUTE>
<INSURANCECOMPANY>Mooninite Casualty Company</INSURANCECOMPANY>
</ATTRIBUTE>
```

Debe crear una nueva correlación de datos para la vía de acceso de datos UMF <ATTRIBUTE><INSURANCECOMPANY> con la columna de tabla adecuada en la base de datos de entidades. El valor de XPath para la vía de acceso de datos UMF es `./ATTRIBUTE/INSURANCECOMPANY/`

Visualización de correlaciones de datos:

Una correlación de datos correlaciona los datos de un archivo UMF con las tablas y columnas de tablas correspondientes de la base de datos de entidades.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Correlación de datos**.
4. En la lista desplegable **Segmento**, seleccione el segmento UMF que desea ver.
5. En la lista desplegable **Tabla**, seleccione la tabla de segmentos UMF cuya correlación desea ver.

Creación de correlaciones de datos:

Una correlación de datos correlaciona datos UMF con las tablas y columnas de tabla de la base de datos de entidades. Se necesitará una nueva correlación de datos cuando el sistema vaya a procesar datos de entrada con nuevos códigos UMF.

Antes de empezar

Si esta correlación de datos correlaciona datos con múltiples tablas, es necesario comprobar que las tablas se insertarán en la secuencia de carga correcta durante las operaciones de interconexiones. Si la tabla no existe en el diccionario, debe añadir la nueva tabla al diccionario para poder crear una correlación de datos para el UMF y la tabla.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Correlación de datos**.
4. En la lista desplegable **Segmento**, seleccione el segmento UMF en el que desea añadir una nueva correlación de datos con una tabla.
5. En la lista desplegable **Tabla**, seleccione la tabla de segmentos UMF donde desea añadir una nueva correlación de datos.
6. Complete uno de los pasos siguientes:
   - Para crear una nueva correlación de datos, pulse el botón **Nuevo**.
   - Para crear una correlación de datos basada en una correlación de datos existente, seleccione una correlación de datos en la lista y, después, pulse el botón **Clonar**.
7. Si se trata de un nuevo segmento, escriba el nombre del segmento UMF en el campo **Segmento**.
8. Seleccione la tabla de base de datos deseada en la lista desplegable **Tabla**
9. En el campo **Columna de tabla**, escriba el nombre de la columna de tabla de base de datos con la que desea correlacionar la vía de acceso de datos UMF.
10. En la lista desplegable **Tipo de campo**, seleccione el tipo de campo adecuado que representa el tipo de campo de la columna de tabla en la base de datos.
11. En la lista desplegable **Tipo de datos**, elija el tipo de datos adecuado que representa el valor de los datos.
12. En el campo **Vía de acceso de datos UMF**, especifique el código UMF.
13. En la lista de desplegable **Método de actualización**, elija el método de actualización adecuado para determinar qué valor, entre el valor de entrada y el valor almacenado previamente, se conservará.
14. En el campo **Estado** de la lista desplegable, elija el estado adecuado de la correlación de datos.

15. Pulse el botón **Guardar**.

Supresión de correlaciones de datos:

Una correlación de datos correlaciona datos UMF con las tablas y columnas de tabla de la base de datos de entidades. Puede suprimir una correlación de datos que el sistema ya no utilice.

Procedimiento

1. Pulse el botón **Configuración**.
2. Pulse el botón **UMF**.
3. Pulse la pestaña **Correlación de datos**.
4. En la lista desplegable **Segmento**, seleccione el segmento UMF donde desea seleccionar una tabla para suprimir una correlación de datos.
5. En la lista desplegable **Tabla**, seleccione la tabla de segmentos UMF donde desea suprimir una correlación de datos.
6. Seleccione una correlación de datos en la lista y, después, pulse el botón **Suprimir**.

Temas de ayuda:

Correlaciones de datos - Panel General:

Utilice el panel **General** para especificar los detalles de la correlación de datos.

Segmento
Escriba el nombre del segmento para el que desea crear una correlación de datos. El nombre del segmento se debe especificar en mayúsculas.

Tabla En la lista desplegable, seleccione la tabla correspondiente a la correlación de datos que desea crear.

Nombre de columna de tabla
Escriba el nombre de la columna de tabla que desea crear.

Tipo de columna de tabla
En la lista desplegable, seleccione el tipo de columna de tabla correspondiente al nombre de la columna de tabla.

ID exclusivo
La columna de tabla es una clave exclusiva que se incrementa automáticamente que genera el motor el motor de la base de datos. Sólo se puede configurar una columna de tabla con este valor.

Clave de entidad
Si esta opción está seleccionada, la columna de la tabla siempre se establece en ENTITY_ID.

Clave de negocio
La columna de la tabla junto con otras columnas de la tabla de claves de empresa designada forman una clave de búsqueda compuesta para determinar la existencia del mismo registro

Atributo
La columna de tabla se utiliza simplemente para almacenar datos y no tiene ningún efecto funcional sobre la inserción/actualización/supresión de la tabla.

Atributo de clave
El valor de columna de tabla se utiliza para determinar si hay un registro existente con el mismo valor. La base de datos realiza un seguimiento de los cambios en estos valores en el tiempo. Por ejemplo, si desea conservar una versión del registro si cambia el valor de ADDR1, identificará el valor de ADDR1 como un atributo de clave.

Este valor no tiene nada que ver con índices.

Secuencia de historial
La columna de tabla se utiliza para determinar qué registro proporcionado por una fuente determinada es el más reciente y cuáles son históricos.

La secuencia de historial siempre se asigna a la columna de tabla HIST_STAT.

Indicación horaria de supresión
La columna de tabla se utiliza para almacenar la última fecha/hora en que se suprimió el registro.

Indicación horaria de actualización
La columna de tabla se utiliza para almacenar la última fecha/hora en que se actualizó el registro.

Tipo de datos
En la lista desplegable, seleccione el tipo de datos correspondiente a la columna de tabla.

CHAR
Datos de tipo carácter (alfanuméricos).

INT Datos enteros.

DATE Datos de fechas. Por ejemplo: aaaa-mm-dd o mm-dd-aaaa.

DATE/TIME
Datos de fecha/hora. Por ejemplo: aaaa-mm-dd hh:mm:ss o mm-dd-aaaa hh:mm:ss.

Vía de acceso a datos UMF
Escriba la ubicación XPath del código UMF.

Método de actualización
En la lista desplegable, seleccione el método de actualización correspondiente a la correlación de datos que desea crear. El método de actualización determina el valor, entre el valor de entrada y el valor previamente almacenado, que se mantendrá.

Nunca Si existe un valor para el elemento UMF en la tabla de base de datos, ese valor no se puede actualizar.

Siempre
Si existe un valor para el elemento UMF en la tabla de base de datos, ese valor se puede actualizar.

Valor máximo
El valor superior, de entrada o almacenado, se conservará o se actualizará.

Esta opción está limitada a los tipos de datos de columna de tabla que sean INT, DATE o DATE/TIME.

Valor mínimo
El valor inferior, de entrada o almacenado, se conservará o se actualizará.

Esta opción está limitada a los tipos de datos de columna de tabla que sean INT, DATE o DATE/TIME.

Estado
En la lista desplegable, seleccione el estado de la correlación de datos que desea crear.

Activo La correlación de datos está activa.

Inactivo
La correlación de datos está inactiva.

Estandarización de direcciones con IBM InfoSphere QualityStage y AddressDoctor

La estandarización e higiene de direcciones es un proceso de interconexión que le permite corregir y estandarizar la información de direcciones para el proceso de resolución de entidad óptimo. Esta nueva característica de IBM® InfoSphere™ Identity Insight permite el uso de una solución de estandarización de datos de direcciones estándares del sector que incluye AddressDoctor®, IBM InfoSphere Information Server, IBM InfoSphere DataStage® e IBM WebSphere® QualityStage™.

El soporte para un módulo de estandarización de direcciones proporcionado por AddressDoctor elimina las dependencias y las limitaciones de otros módulos como WAVES (Worldwide Address Verification and Enhancement System). El módulo de estandarización de direcciones AddressDoctor puede utilizarse para la resolución de entidad de Identity Insight utilizando DataStage y la interfaz QualityStage Address Verification Interface (QS-AVI). QualityStage es un componente de IBM Information Server.

AddressDoctor® tiene las ventajas siguientes:

- Soporta más de 240 países y territorios.
- Tiene mejor cobertura a nivel de calle.
- Está habilitado para Unicode y soporta todos los conjuntos de caracteres principales.
- Proporciona transliteración.
- Proporciona un estado de validación del grado de entrega de la dirección.
- Proporciona formatos al estándar postal local.

La implementación de AddressDoctor con QS-AVI no es una tarea trivial. Se recomienda que se ponga en contacto con el representante de IBM para obtener ayuda.

Requisitos de limpieza de direcciones QS-AVI y visión general de tareas

Los pasos de proceso detallados para utilizar IBM QualityStage y la interfaz AddressDoctor (QS-AVI) para realizar una limpieza de direcciones de Identity Insight se describen en un documento técnico en ibm.com. Este tema proporciona una visión general del proceso, requisitos y un enlace a la información detallada.

Antes de empezar

Se necesitan los productos siguientes:

- IBM InfoSphere Information Server incluidos IBM InfoSphere DataStage e IBM InfoSphere QualityStage Versión 8.0.1
- Etapas de calidad de datos de QS-AVI
- Base de datos AddressDoctor(R) para el país necesario.

Acerca de esta tarea

El proceso sigue esta secuencia general:

Procedimiento

1. Definir un trabajo de etapas de QS-AVI en DataStage y QualityStage Designer.
2. Importar el archivo "AddressValidateWS.dsx" a la etapa. (Éste es un trabajo de limpieza de dirección predefinido y se ha diseñado para la integración de EAS y QS-AVI.) El archivo puede encontrarse en el disco de instalación de fixpack: `<RR_INSTALL>/srd-home/qsavi/AddressValidateWS.dsx`
3. Modificar la etapa de verificación de direcciones Habilitar el trabajo deDataStage para servicios de información.
4. Definir el trabajo DataStage como un servicio en la consola de Information Server.
5. Verificar el despliegue utilizando WebSphere Information Services Director (WISD) para generar y examinar un documento de lenguaje de definición de servicio web (WSDL) para este nuevo servicio.
6. Probar el servicio en un entorno como WebSphere Integration Developer.
7. Activar la característica QSAVI, cambiando AddrConnection bajo la sección OAC del archivo pipeline.ini al formato siguiente:

   [OAC]
   AddrConnection=qsavi://host:puerto/?timeout=ms

   host es el nombre de host o l a dirección IP de Infoserver.

   puerto es el número de puerto. El puerto predeterminado es 9080.

   timeout
   es un parámetro opcional. Puede establecer el parámetro de tiempo de espera de conexión externamente. El tiempo de espera de conexión predeterminado es de 10000 ms (10 segundos).

Qué hacer a continuación

Los pasos detallados para este proceso se describen en: QS-AVI address cleansing as a Web process for IBM InfoSphere Identity Insight.

Resolución de problemas de QS-AVI

QS-AVI devuelve 'valstatus_qsav' que describe la calidad de limpieza de dirección y permite la resolución de problemas relacionados.

Excepciones

Una excepción se genera basándose en el estado de valor de descriptor de contexto:

```
// estado de valor de descriptor de contexto
// V  - Validado
// C  - Corregido
// P3 - No corregido - Capacidad de entrega alta
// P2 - No corregido - Capacidad de entrega media
// P1 - No corregido - Capacidad de entrega baja
// N1 - No comprobado - País no reconocido
// N2 - No comprobado - Base de datos de país no encontrada
// N3 - No comprobado - País no desbloqueado
// N4 - No comprobado - Validación no llamada
// N5 - Información insuficiente
// Q1 - Sin sugerencias
// Q2 - Sugerencias incompletas
// Q3 – Sugerencias
```

QS-AVI también devuelve ‘resultstatus_qsav' que describe la probabilidad de limpieza de dirección:

```
// probabilidad de entrega de descriptor de contexto
// 0 - Vacío
// 1 - No comprobado
// 2 - No comprobado, pero estandarizado
// 3 - Comprobado y corregido
// 4 - Validado, pero cambiado
// 5 - Validado, pero estandarizado
// 6 - Validado y no cambiado
// 7 - No se proporciona ningún valor porque hay varias coincidencias
```

Mensajes de error

6301E - Respuesta no válida.

6302E - No se puede conectar con el servidor InforServer
Este mensaje se genera cuando EAS no puede conectarse a InfoServer. También se genera con respuesta ‘soapenv:Fault' de InforServer, que se trata como una respuesta no válida.

6303E - Error, no se puede conectar al servidor : {0}", __nombreServidor
Este mensaje se genera cuando EAS no puede conectarse al servidor InfoServer correcto.

Capítulo 8. Análisis de datos

El Kit de herramientas de analista proporciona un conjunto de prestaciones de desarrollo y personalización de aplicaciones a Identity Insight. Se trata de un conjunto de interfaces de usuario e informes que se pueden modificar según sea necesario o a los que otras aplicaciones pueden hacer referencia.

Análisis de datos utilizando el Visualizador

Puede utilizar el Visualizador para realizar diversas tareas de análisis: revisar y disponer alertas, encontrar entidades, ver datos de entidades, ver gráficos de entidades y sus relaciones con otras entidades, crear y gestionar generadores de alertas de atributo, añadir una sola entidad o un pequeño archivo de entidades, divulgar relaciones entre entidades, e imprimir informes.

Configuración del Visualizador

Para utilizar satisfactoriamente el Visualizador debe saber cómo acceder al Visualizador y cómo personalizar la manera en que el Visualizador visualiza información para que se ajuste a sus preferencias.

Visualizador

El Visualizador es una interfaz gráfica de usuario que los analistas e investigadores utilizan para analizar los resultados de alertas, relaciones y resoluciones de entidades.

El Visualizador está alojado en una versión incorporada de IBM WebSphere Application Server. Puede configurar el Visualizador a través de la Consola de configuración y a través de la selección **Preferencias** del Visualizador en el menú **Archivo**.

Los usuarios del Visualizador pueden realizar diversas tareas de análisis:

Análisis y visualización de alertas
Las alertas generadas por el proceso de resolución de entidades representan relaciones o resoluciones de entidades que interesan a una organización. Generalmente, los analistas revisan las alertas y deciden qué acción emprender, si deciden emprender alguna, basándose en la información de las alertas. Existen tres tipos de alertas: alertas de rol, alertas de atributo y alertas de suceso.

El Visualizador muestra las alertas, ofreciendo a los analistas vistas textuales y gráficas de las alertas y las entidades que participan en las alertas. Los analistas pueden profundizar en los detalles y luego establecer el estado de disposición de la alerta correctamente.

Crear y gestionar generadores de alertas de atributo
Con el Visualizador, los analistas pueden crear y gestionar búsquedas persistentes mediante la característica Generador de alertas de atributo, y gestionar cómo ven y reciben alertas de atributo. Los analistas pueden crear Generadores de alertas de atributo basándose en datos de atributos para localizar identidades que se han resuelto en entidades basadas en dichos datos de atributos. Los analistas también pueden crear un Generador de alertas de atributo para buscar de manera persistente en la base de datos de entidades en busca de una entidad determinada.

Encontrar entidades

Los usuarios del Visualizador también pueden buscar entidades para un análisis más profundo mediante varios métodos:

- Por atributos
- Por cuenta de origen de datos
- Por ID de entidad
- Por resolución (cuánto se acercan los criterios especificados a las identidades y entidades de la base de datos de entidades, basándose en umbrales de puntuación de resolución mínima)

Adición de entidades y relaciones divulgadas

Los analistas pueden utilizar el Visualizador para añadir registros para la resolución de entidades y la detección de relaciones. Pueden añadir un solo registro de identidad o cargar un archivo UMF que contenga unos pocos miles de registros de identidades. Al igual que cuando se añaden registros de identidades a través de programas de adquisición, una interconexión procesa los registros añadidos a través del Visualizador para la resolución de entidades y la detección de relaciones. Los resultados del proceso se graban en la base de datos de entidades y las alertas, si se generan, se publican en el Visualizador.

Los analistas también pueden divulgar relaciones entre entidades (por identidad), cuando saben de la existencia de un enlace entre las identidades. Ejemplos de relaciones divulgadas serían relacionar entidades basadas en contactos de emergencia o referencias listadas en una solicitud de empleo. La entidad ha divulgado estas relaciones en la solicitud.

Generación e impresión de informes

El Visualizador también contiene varios informes que los analistas pueden ver e imprimir como ayuda para gestionar y hacer el seguimiento de su trabajo en el Visualizador.

Configuración del Visualizador

Puede configurar valores del Visualizador para adaptar la manera en que se visualiza la información en sus sesiones del Visualizador.

Establecimiento de opciones de visualización del Visualizador:

Puede personalizar la visualización del Visualizador cambiando el color de fondo, el font, y otras opciones de visualización en el panel **Preferencias de ventana**.

Acerca de esta tarea

Las opciones de visualización del Visualizador se configuran para cada cliente del Visualizador. Al utilizar estas instrucciones, solamente cambia la visualización para el cliente del Visualizador al que está conectado actualmente.

Procedimiento

1. En el Visualizador, seleccione **Archivo** > **Preferencias** > **Preferencias de ventana**.
2. Elija las opciones de visualización de aspecto a utilizar. Solamente puede cambiar los valores en las listas desplegables **Tema**, **Font** y **Tamaño** si selecciona la opción *Metal* en **Aspecto**.
3. Pulse **Enviar**. Un mensaje de confirmación le informa de que debe reiniciar el Visualizador para que los cambios surtan efecto.
4. Pulse **Aceptar**.

5. Cierre el Visualizador. Inicie el Visualizador y vuelva a iniciar la sesión.

Resultados

Ahora el Visualizador utiliza las nuevas opciones de visualización de ventana que ha seleccionado.

Establecimiento de la vía de acceso predeterminada para archivos UMF:

Si carga registros de identidad de forma regular en archivos de datos UMF para procesarlos mediante el Visualizador, establecer la vía de acceso predeterminada puede ahorrarle un paso.

Acerca de esta tarea

Los valores de la vía de acceso predeterminada se configuran para cada cliente del Visualizador. Al especificar una vía de acceso predeterminada mediante esta tarea, solamente establece la vía de acceso en el Visualizador al que está conectado actualmente.

Procedimiento

1. En el Visualizador, seleccione **Archivo** > **Preferencias** > **Preferencias del sistema**.
2. En **Vía de acceso predeterminada para Carga de archivo**, realice una de las acciones siguientes:
   - Entre la vía de acceso completa del directorio a utilizar.
   - O bien examine para seleccionar el directorio.
3. Pulse **Enviar**. Un mensaje de confirmación le informa de que debe reiniciar el Visualizador para que los cambios surtan efecto.
4. En el mensaje de confirmación, pulse **Aceptar**.
5. Cierre el Visualizador, reinicie el Visualizador y vuelva a iniciar la sesión.

Resultados

Siempre que cargue un archivo UMF, la vía de acceso predeterminada es el directorio que ha especificado.

Establecimiento de la vía de acceso predeterminada para Centrifuge:

Si utiliza el Centrifuge Desktop opcional de Centrifuge Systems para visualizar y mostrar gráficos de entidad, debe especificar la vía de acceso al archivo de Centrifuge Desktop en las preferencias del Visualizador.

Acerca de esta tarea

Los valores de la vía de acceso predeterminada se configuran para cada cliente del Visualizador. Al especificar una vía de acceso predeterminada mediante esta tarea, solamente establece la vía de acceso en el Visualizador al que está conectado actualmente.

Procedimiento

1. En el Visualizador, pulse **Archivo** > **Preferencias** > **Preferencias del sistema**.
2. Bajo la sección **Vías de acceso a archivo** en **Vía de acceso de Centrifuge**:

- Especifique la vía de acceso a archivo o el URL (localizador universal de recursos) a la aplicación Centrifuge Desktop en el campo.
- O bien vaya a la aplicación Centrifuge Desktop y ábrala.

3. Pulse **Enviar**. Un mensaje de confirmación le informa de que debe reiniciar el Visualizador para que los cambios surtan efecto.
4. En el mensaje de confirmación, pulse **Aceptar**.
5. Cierre el Visualizador, vuelva a abrir el Visualizador y vuelva a iniciar la sesión.

Resultados

Una vez se ha configurado la vía de acceso, aparece el botón **Centrifuge** en las pantallas **Detalle de alerta de rol** y **Resumen de entidad** en la ventana **Investigación**. Pulse el botón para lanzar la aplicación Centrifuge Desktop directamente desde el Visualizador.

Establecimiento de valores de puntuación de umbral mínimos para consultas del Visualizador:

Cuando busque una entidad mediante la característica Buscar por resolución o un generador de alertas de atributo en el Visualizados, debe seleccionar una puntuación mínima de similitud como parte de los criterios. Su elección determina la fuerza de la resolución de entidades y relaciones que el sistema utiliza para buscar y devolver entidades. Puede cambiar los valores predeterminados para uno o varios de estos umbrales en el panel **Preferencias del sistema** del Visualizador.

Acerca de esta tarea

Estos valores se configuran para cada cliente del Visualizador. Al utilizar esta tarea, solamente cambia el umbral de puntuación mínima para el Visualizador al que está conectado actualmente.

Procedimiento

1. En el Visualizador, pulse **Archivo** > **Preferencias** > **Preferencias del sistema**.
2. En la sección **Valores de puntuación mínima**, especifique la puntuación de similitud más baja que desea utilizar para determinar qué resultados de la búsqueda se visualizan. Cuanto más alto sea el número, más datos de entidad deberán coincidir con los criterios de búsqueda, lo que puede reducir el número de resultados devueltos.
3. Pulse **Enviar**. Un mensaje de confirmación le informa de que debe reiniciar el Visualizador para que los cambios surtan efecto.
4. En el mensaje de confirmación, pulse **Aceptar**.
5. Cierre el Visualizador, vuelva a abrir el Visualizador y vuelva a iniciar la sesión.

Establecimiento de opciones de filtro predeterminadas de la ventana Resumen de alerta:

Utilice el panel **Valores de filtro de visualización de alertas** de la pantalla **Preferencias del sistema** para personalizar los valores predeterminados para las opciones de filtro en la ventana **Resumen de alerta**.

Acerca de esta tarea

Estos valores controlan los siguientes valores predeterminados en el Visualizador:

- El número máximo de alertas a visualizar en la **Lista de alertas**
- La puntuación mínima de relación para que se visualicen alertas de rol
- El número de días de resúmenes de alertas a visualizar (desde la fecha actual hacia atrás)

Los valores que establezca aquí determinarán los valores predeterminados de filtro que su instancia del Visualizador utiliza cada vez que abra una nueva ventana **Resumen de alerta**.

Procedimiento

1. En el Visualizador, seleccione **Archivo** > **Preferencias** > **Preferencias del sistema**.
2. Bajo la sección **Valores de filtro de visualización de alertas**, en **Máximo de alertas a visualizar en la lista de alertas**, entre un número que represente el número máximo de alertas a visualizar en la tabla **Lista de alertas**. El valor predeterminado es 100, lo que significa que cuando selecciona un resumen de alerta, las 100 primeras alertas asociadas se visualizan en la **Lista de alertas**. Puede interesarle cambiar el valor predeterminado para visualizar menos alertas.
3. En **Puntuación mínima de relación**, entre la puntuación más baja de relación que desea utilizar como umbral para visualizar alertas de rol. Cuanto mayor sea la puntuación de relación, menor será el número de alertas de rol y resúmenes de alertas de rol que se visualizarán.
4. En **Número de días de alertas para visualizar (incluido el día de hoy)**, entre un número de 1 a 99 que indique el número de días de alertas que se verán. El número empieza por la fecha actual y cuenta hacia atrás, por lo que sí entra un 1, solamente verá alertas generadas en el día actual. Si entra 10, solamente verá alertas de un total de 10 días: el día actual y los 9 días anteriores. El valor predeterminado es 99.
5. Opcional: Si el administrador del sistema ha habilitado la alteración temporal del umbral de alertas en la Consola de configuración, aparecerá el recuadro de selección **Incluir alertas de rol filtradas**.
   - Seleccione el recuadro de selección **Incluir alertas de rol filtradas** para visualizar todas las alertas de rol y los resúmenes de alertas de rol en la ventana **Resumen de alerta** con puntuaciones de relación fuera del umbral mínimo de alerta definido en la regla de alertas de rol.
   - Quite la marca del recuadro de selección **Incluir alertas de rol filtradas** para visualizar solamente aquellas alertas de rol y resúmenes de alertas de rol en la ventana **Resumen de alerta** que tengan puntuaciones de relación que cumplan el el umbral mínimo de alerta.
6. Pulse **Enviar**. Un mensaje de confirmación le informa de que debe reiniciar el Visualizador para que los cambios surtan efecto.
7. En el mensaje de confirmación, pulse **Aceptar**.
8. Cierre la sesión del Visualizador, reinicie el Visualizador y vuelva a iniciar la sesión.

Establecimiento de opciones de registro del Visualizador:

Puede activar o desactivar el registro de clientes del Visualizador configurando las opciones de registro del Visualizador. De forma predeterminada, el registro del

cliente de Visualizador está desactivado. Generalmente, solo activará el registro de clientes del Visualizador como ayuda para la resolución de problemas con la colaboración del administrador.

Acerca de esta tarea

Estos valores se configuran para cada cliente del Visualizador. Al utilizar esta tarea, solamente cambia las opciones de registro para el Visualizador al que está conectado actualmente.

Procedimiento

1. En el Visualizador, pulse **Archivo** > **Preferencias** > **Valores de registro y enlace**.
2. Lleve a cabo una de las siguientes acciones en el recuadro de selección **Activar registro**:
   - Marque el recuadro de selección para activar el registro de clientes del Visualizador.
   - Quite la marca del recuadro de selección para desactivar el registro de clientes del Visualizador.
3. Si ha activado el registro, especifique el tipo de registro seleccionando una opción en **Nivel de detalle del registro**. Si no está seguro de qué nivel debe seleccionar, consulte al administrador del sistema. Dado que generalmente solo activará el registro de clientes del Visualizador para la resolución de problemas, normalmente seleccionará el nivel de depuración. El nivel de depuración registra cada acción que lleva a cabo en el Visualizador y cada mensaje (error, aviso o informativo) que aparezca. Este nivel de registro llena rápidamente el archivo de registro del Visualizador, lo que significa que deberá suprimir el archivo de vez en cuando.
4. En **Vía de acceso al directorio de archivos de registro**:
   - Entre la vía de acceso para almacenar archivos de registro del Visualizador.
   - O bien vaya al directorio y selecciónelo.
5. Pulse **Enviar**. Un mensaje de confirmación le informa de que debe reiniciar el Visualizador para que los cambios surtan efecto.
6. En el mensaje de confirmación, pulse **Aceptar**.
7. Cierre el Visualizador, reinicie el Visualizador y vuelva a iniciar la sesión.

Establecimiento de opciones de hiperenlace del Visualizador para visualizar atributos personalizados:

Si su organización incluye enlaces a archivos o imágenes en otros sistemas como parte de atributos de registro de identidad, el Visualizador puede visualizar hiperenlaces a esos archivos. Pulse el hiperenlace para lanzar el navegador web o la aplicación para visualizar el archivo o imagen seleccionados. Utilice las preferencias del sistema del Visualizador para elegir qué navegador o programa abre los archivos al pulsar un hiperenlace.

Acerca de esta tarea

Estos valores se configuran para cada cliente del Visualizador. Al utilizar esta tarea, solamente cambia las opciones de hiperenlace para el Visualizador al que está conectado actualmente.

Procedimiento

1. En el Visualizador, seleccione **Archivo** > **Preferencias** > **Valores de registro y enlace**
2. Bajo **Valores de manejo de hiperenlaces**, seleccione una de las siguientes opciones:
   - **Valor de navegador predeterminado**
   - O **Utilizar programa** y especifique un navegador o programa a utilizar para abrir hiperenlaces.

   Nota: Es posible que solo sea necesario especificar un navegador web u otro programa para abrir enlaces que estén almacenados en sitios web seguros (https://).
3. Pulse **Enviar**. Un mensaje de confirmación le informa de que debe reiniciar el Visualizador para que los cambios surtan efecto.
4. En el mensaje de confirmación, pulse **Aceptar**.
5. Cierre el Visualizador, reinicie el Visualizador y vuelva a iniciar la sesión.

Establecimiento de opciones para gráficos del Visualizador:

Puede personalizar los valores de los gráficos que ve en el Visualizador cambiando el color o el grosor de las línea en el panel **Preferencias de gráficos**.

Acerca de esta tarea

Los valores de visualización de gráficos del Visualizador se configuran para cada cliente del Visualizador. Al utilizar estas instrucciones, solamente afecta a los valores para el cliente del Visualizador al que está conectado actualmente.

Procedimiento

1. En el Visualizador, pulse **Archivo** > **Preferencias** > **Preferencias de gráficos**.
2. Seleccione el grosor y el color de línea a utilizar.
3. Pulse **Enviar**. Un mensaje de confirmación le informa de que debe reiniciar el Visualizador para que los cambios surtan efecto.
4. En el mensaje de confirmación, pulse **Aceptar**.
5. Cierre el Visualizador, vuelva a abrir el Visualizador y vuelva a iniciar la sesión.

Resultados

Ahora el Visualizador visualiza gráficos utilizando las nuevas opciones de visualización que ha seleccionado.

Temas de ayuda:

Panel Preferencias de ventana:

Utilice este panel para configurar el modo en que el Visualizador muestra colores de fondo, fonts e iconos de navegación para las sesiones del Visualizador. Configurar las preferencias en este panel solo afecta a los valores para el cliente del Visualizador local. Si cambia alguno de estos valores, salga, vuelva a abrir e inicie la sesión en el Visualizador para ver los cambios.

Aspecto
Elija un grupo de valores de visualización formateados previamente. Los valores de visualización de grupo controlan las seleccione disponibles en **Tema**, **Font** y **Tamaño**.

Nota: La mayoría de valores de visualización no le permiten seleccionar ninguno de los demás campos. Actualmente, **Metal** es la única opción que le permite elegir otros valores de visualización.

El valor de visualización de grupo predeterminado es **Visualizador EAS**.

Tema Elija una combinación de colores de pantalla formateada previamente para el valor de visualización de grupo que ha seleccionado en **Aspecto**.

Font Elija un font de visualización.

Tamaño
Elija un tamaño de font.

Ejemplo
Muestra un ejemplo del aspecto que tendrá la pantalla del Visualizador según sus selecciones.

Color de fondo
Pulse este botón para elegir un color de fondo. Este campo solo está disponible si ha seleccionado **Metal** en el campo **Aspecto**.

Color de control
Pulse aquí para elegir un color de resaltado de control.

Color de texto
Pulse aquí para elegir un color de texto.

Panel Preferencias del sistema:

Utilice este panel para configurar preferencias del sistema para sus sesiones del Visualizador. Configurar aquí las preferencias solo afecta a los valores del sistema para el cliente del Visualizador local. Si cambia alguno de estos valores, salga, vuelva a abrir e inicie la sesión en el Visualizador para ver los cambios.

Sección Vías de acceso a archivo
Especifique las vías de acceso a archivo predeterminadas que el Visualizador utiliza para cargar archivos UMF y abra la herramienta gráfica Centrifuge Desktop. Si utiliza la aplicación Centrifuge Desktop para visualizar gráficos de entidades y datos de entidades, entre la vía de acceso completa a la aplicación. Si entra la vía de acceso completa aquí, puede acceder a Centrifuge directamente desde el Visualizador.

Sección Valores mínimos de puntuación
Defina los valores para los umbrales de puntuación mínima de similitud entre los que puede seleccionar al crear una consulta de Buscar por resolución o un generador de alertas de atributo.

De forma predeterminada, esta sección contiene los valores recomendados para cada uno de esos umbrales. Estos valores recomendados son valores conservadores, pensados para devolver menos positivos falsos. Puede volver a definir los valores para que se ajusten a sus objetivos.

Generalmente, cuanto más alto establezca el valor de un umbral de puntuación mínima, menos resultados se devolverán. Cuanto más bajo sea el valor establecido, más resultados se devolverán.

Es entidad

Entre la puntuación de resolución más baja que define cuándo la entidad de búsqueda definida en una consulta Buscar por resolución o un generador de alertas de atributo y una entidad de la base de datos de entidades son la misma entidad.

El valor predeterminado es 100. Este valor predeterminado significa que cuando se comparan la entidad de búsqueda y una identidad, si la puntuación de resolución es 100, la entidad devuelta es igual que la entidad de búsqueda.

Coincidencia de entidad ajustada

Entre la puntuación de resolución más baja que define cuándo existe una "coincidencia ajustada" entre la entidad de búsqueda definida por una consulta Buscar por resolución o un generador de alertas de atributo y una entidad de la base de datos de entidades.

El valor predeterminado es 85. Este valor predeterminado significa que cuando se comparan la entidad de búsqueda y una entidad de la base de datos de entidades, si la puntuación mínima de resolución es igual o superior a 85, pero menor que la puntuación de **Es entidad**, la entidad devuelta es una coincidencia de entidad ajustada respecto a la entidad de búsqueda.

Buena relación

Entre la puntuación más baja que define cuándo existe una relación cercana o fuerte entre la entidad de búsqueda definida por una consulta Buscar por resolución o un generador de alertas de atributo y una entidad de la base de datos de entidades. El valor representa la fuerza de la relación.

El valor predeterminado es 35, lo que significa que cuando se comparan la entidad de búsqueda y una entidad de la base de datos de entidades, si la puntuación mínima de resolución es igual o superior a 35, la relación entre las dos es buena.

Cualquier relación

Entre la puntuación más baja que define cuándo existe cualquier relación entre la entidad de búsqueda definida por una consulta Buscar por resolución o un generador de alertas de atributo y una entidad de la base de datos de entidades. (El valor representa la fuerza de la relación.)

El valor predeterminado es 1. Este valor predeterminado significa que cuando se comparan la entidad de búsqueda y una entidad de la base de datos de entidades, si la puntuación mínima de resolución es igual o superior a 1, las dos tienen una relación.

Sección Valores de Filtro de visualización de alertas

Utilice esta sección para configurar los valores de filtro de alertas predeterminados que afectan a qué resúmenes de alertas se visualizan en la ventana **Resumen de alerta**. Cada vez que abre una ventana **Resumen de alerta** nueva, el sistema utiliza estos valores predeterminados.

Máximo de alertas para visualizar en la lista de alertas

Entre un número que represente el número más alto de alertas a visualizar en la tabla **Lista de alertas** de la ventana **Resumen de alerta**.

El valor predeterminado del filtro es 100, lo que significa que, de forma predeterminada, solo se muestran las 100 primeras alertas de cualquier resumen de alerta seleccionado.

Puntuación mínima de relación
Entre la puntuación de relación más baja para filtrar resúmenes de alerta de rol no asignados menores que la puntuación de la pantalla en la ventana **Resumen de alerta**.

Por ejemplo, para ver solamente resúmenes de alertas de rol donde la puntuación de relación entre las dos entidades comparadas es igual o superior a 50, entre `50` en este campo.

El valor predeterminado es 0, lo que significa que todos los resúmenes de alertas para su grupo de analistas del Visualizador actualmente en estado "No asignado" se visualizan de forma predeterminada.

Número de días de alertas para visualizar (incluido el día de hoy)
Entre un número de 1 a 99 que indique el número de días de alertas desde la fecha actual que se visualizarán. Tenga en cuenta que este "día" es un día de calendario completo, que empieza a las 0:00:00 y finaliza a las 23:59:59.

El número empieza por la fecha actual y cuenta hacia atrás. Si desea ver alertas generadas en los últimos 90 días (el día actual y los 89 días anteriores), entre `90`.

El valor predeterminado es `99`, lo que significa que verá alertas generadas hoy y los 98 días de calendario anteriores.

Recuadro de selección Incluir alertas de rol filtradas
(Opcional) Marque este recuadro de selección para visualizar todas las alertas de rol no asignadas generadas, incluso aquellas alertas por debajo del umbral mínimo de alertas que se especifica en la configuración de normas de alertas de rol. Este recuadro de selección solo aparece si el administrador del sistema ha habilitado esta característica.

Se borra la selección predeterminada, lo que significa que solo se muestran en el Visualizador las alertas de rol no asignadas actualmente que cumplen o sobrepasan el umbral mínimo de alertas (definido en la regla de alertas de rol).

Sección Valores varios
Utilice esta sección para habilitar la ayuda contextual y la ventana de confirmación de salida.

Habilitar consejos
Si se habilitan los Consejos, siempre que el cursor pase por encima de un icono de barra de herramientas o sobre un área donde haya información adicional disponible, aparecerá la ayuda contextual. De forma predeterminada, los Consejos están habilitados.

Mostrar el diálogo de configuración de salida:
Esta opción determina si el sistema visualiza un diálogo de confirmación al salir del Visualizador.

- Marque este recuadro de selección para confirmar su elección de salir del Visualizador cada vez. El valor predeterminado es seleccionado.

- Quite la marca de este recuadro de selección para salir del Visualizador sin mostrar el diálogo **Confirmación de salida** cada vez que elija salir y finalizar la sesión en el Visualizador.

Panel Valores de registro y enlace:

Utilice este panel para configurar valores de registro de clientes e hiperenlaces del Visualizador. Configurar aquí las preferencias solo afecta a los valores para el cliente del Visualizador local. Si cambia alguno de estos valores, salga, vuelva a abrir e inicie la sesión en el Visualizador para ver los cambios.

Valores de registro
Marque el recuadro de selección para activar el registro de clientes del Visualizador o quite la marca del recuadro de selección para desactivar el registro de clientes. Normalmente, solo habilitará el registro de clientes del Visualizador si está trabajando con el administrador del sistema para resolver un mensaje de error o un problema que se ha producido durante la sesión del Visualizador. De forma predeterminada, el registro del cliente de Visualizador está desactivado.

Nivel de detalle del registro
Seleccione el nivel de detalle del registro, solo disponible si el registro de clientes del Visualizador está activado. El nivel de detalle controla cuánta información se recoge en las anotaciones del Visualizador mientras utiliza el Visualizador. Consulte con el administrador del sistema antes de realizar la selección. Normalmente, activará el registro para resolver problemas del Visualizador, por lo que seleccionará el nivel de depuración, que es el nivel superior de detalle de registro. El nivel de depuración registra cada acción y mensaje que se producen mientras se utiliza el Visualizador. Pero este nivel también llena el archivo de registro del cliente del Visualizador muy rápidamente, por lo que puede ser necesario borrar el archivo de registro de vez en cuando. Este es el motivo por el que normalmente desactivará el registro cuando se haya resuelto el problema.

Vía de acceso al directorio del archivo de registro
Especifique la ubicación del archivo y directorio de los archivos de registro del cliente del Visualizador. Normalmente solo necesitará revisar archivos de registro cuando esté investigando un mensaje o un problema. Los archivos de registro se llenan de información rápidamente, especialmente en el nivel de depuración. Si el registro de clientes del Visualizador está activado, podrá ser necesario depurar los archivos de registro de vez en cuando para impedir que los archivos crezcan demasiado.

Valores de Manejo de hiperenlaces
Seleccione una opción para determinar qué programa o navegador utiliza el Visualizador para abrir y visualizar hiperenlaces. Los registros de identidad entrantes pueden contener hiperenlaces, que pueden dirigirlo a otros archivos, sitios web o sistemas que contengan información de identidad o entidad relevante para el análisis. Los hiperenlaces forman parte del registro de identidad y se visualizan en el resumen de entidad y en el gráfico de resolución de entidad como atributos.

Si sufre problemas al pulsar un hiperenlace, seleccione la opción **Utilizar programa** y especifique qué navegador o programa debe utilizarse para abrir hiperenlaces. Por ejemplo, si su organización guarda archivos de huellas dactilares en un sitio web seguro (https://), utilice esta opción para

especificar su navegador web u otro programa para abrir enlaces que vayan al sitio seguro de los archivos de huellas dactilares.

Panel Preferencias de gráficos:

Utilice este panel para especificar las propiedades de visualización de las líneas que conectan entidades en gráficos del Visualizador. Configurar aquí las preferencias solo afecta a los valores para el cliente del Visualizador local. Si cambia alguno de estos valores, salga, vuelva a abrir e inicie la sesión en el Visualizador para ver los cambios.

Espesor de la línea
Seleccione un espesor de línea. El espesor de línea predeterminado es de 2 pixels.

Color de la línea
Seleccione un color de línea. El color de línea predeterminado es un azul medio.

Línea de ejemplo
Visualiza una línea de gráfico de ejemplo, según sus selecciones.

Inicio del Visualizador

Para utilizar el Visualizador para ver entidades y datos de entidades de la base de datos de entidades, primero debe iniciar el Visualizador e iniciar la sesión en él.

Para iniciar el Visualizador, la versión predeterminada del sistema Java procesa un archivo Java Web Start JNLP (Java Network Launch Protocol) que el servidor de aplicaciones del producto descarga en el cliente de la estación de trabajo. Se puede acceder al archivo JNLP de distintas maneras. No obstante, para abrir correctamente el Visualizador, la versión de cliente de Java Web Start debe abrir el archivo JNLP.

Si tiene varias versiones de Java instaladas en la máquina cliente, la versión predeterminada del sistema de Java Web Start se podría establecer en otra versión que no sea la versión de cliente necesaria. Todavía podrá abrir y ejecutar correctamente el Visualizador, pero primero debe configurar el navegador web para que utilice la versión de cliente de Java Web Start necesaria.

Nota: Es posible que la versión cliente de Java necesaria para abrir y ejecutar el Visualizador no sea la versión más actual de Java.

Inicio de sesión en el Visualizador

Antes de iniciar sesión en el visualizador, debe tener una cuenta de usuario del Visualizador (nombre de usuario y contraseña). El administrador del sistema puede proporcionarle información sobre la cuenta de usuario del Visualizador.

Procedimiento

1. Siga uno de los siguientes pasos:
   - Efectúe una doble pulsación en el icono del Visualizador en el escritorio.
   - O bien abra el navegador de Internet y especifique el localizador universal de recursos (URL) para el Visualizador en la línea de dirección.

   El URL para iniciar el Visualizador es:
   `http://servidor:puerto_instalación`

Por ejemplo, `http://localhost:13510`. Cuando se ha instalado el Visualizador, el *puerto_instalación* predeterminado es 13510, pero el número de puerto puede cambiarse. Consulte al administrador del sistema si no está seguro del nombre de servidor o número de puerto correctos.

2. Inicie la sesión entrando su nombre de usuario y contraseña.

   Nota: Los campos de nombre de usuario y contraseña son sensibles a las mayúsculas y minúsculas. La primera vez que inicie la sesión, utilice la contraseña que le ha asignado el administrador del sistema. Tras el primer inicio de sesión, normalmente se cambia la contraseña del Visualizador para proteger la seguridad de la cuenta del Visualizador.

3. Pulse **Iniciar sesión**.

Configuración del navegador web para que utilice la versión de cliente Java Web Start necesaria:

Si la estación de trabajo contiene varias versiones de Java y tiene dificultades para abrir el Visualizador, establezca las preferencias del navegador web para que seleccione la versión de cliente de Java Web Start necesaria. Si realiza esta acción, el navegador web automáticamente utilizará la versión de cliente de Java Web Stat necesaria para abrir el Visualizador.

Configuración de Microsoft Windows Internet Explorer para que utilice el Java Web Start necesario:

Microsoft Internet Explorer utiliza las asociaciones de archivo predeterminadas definidas en el sistema operativo Microsoft Windows para determinar cómo se manejan archivos JNLP (Java Network Launch Protocol). Si define o modifica la aplicación de archivos predeterminada asociada a los archivos JNLP de proceso, puede hacer que Internet Explorer utilice la versión correcta de Java Web Start. Si tiene varias versiones de Java instaladas, al modificar este valor puede evitar problemas relacionados con la apertura del Visualizador.

Acerca de esta tarea

Este procedimiento hace que Internet Explorer utilice la versión de Java Web Start para abrir todas las aplicaciones web. Si ejecuta otras aplicaciones de Web Start que necesitan versiones más actuales de Java, utilice el método de inicio directo.

Nota: Hay un par de problemas conocidos relacionados con la versión 1.6 de Java que debe tener en mente:

- La versión 1.6 de Java a veces sobrescribe la asociación de archivos Windows predeterminada para archivos JNLP. Si utiliza la versión 1.6 de Java como su JVM (Java Virtual Machine) del sistema y estos pasos no le permiten iniciar y abrir correctamente el Visualizador, intente utilizar otro navegador web para iniciar el Visualizador o utilice el método de inicio directo.
- Si la estación de trabajo utiliza la versión 1.6 de Java, es posible que necesite configurar JRE (Java Runtime Environment) para aceptar descargas automáticas. Si la estación de trabajo tiene este problema, al intentar iniciar el Visualizador verá un mensaje de error que le indicará que la aplicación ha solicitado un versión de JRE que no está instalada localmente.

Procedimiento

1. En el **Panel de control de Windows**, lleve a cabo uno de los siguientes pasos:

- En la Vista de categorías, efectúe doble pulsación en **Rendimiento y mantenimiento**. En el panel de navegación **Ver también** situado en la parte superior izquierda de la ventana, seleccione **Tipos de archivo**.
- En la Vista clásica, efectúe doble pulsación en **Opciones de carpeta**.

2. En el diálogo **Opciones de carpeta**, pulse el separador **Tipos de archivo**.
3. En la columna Extensiones, localice y seleccione la entrada **JNLP**. Las entradas están ordenadas alfabéticamente según la extensión.

   Nota: Si la entrada de JNLP no existe, pulse **Nueva** para crear la entrada.
4. Pulse **Cambiar**.
5. En el diálogo **Abrir con**, asegúrese de que esté seleccionado **Ejecutable de Java Web Start**. Pulse **Examinar** para navegar hacia el directorio del Java instalado.
6. Seleccione el archivo ejecutable denominado `javaws` y pulse **Aceptar**.
7. Pulse **Aceptar** para cerrar el diálogo **Opciones de carpeta**. (También puede cerrar la ventana **Panel de control**.)

Resultados

Ahora Internet Explorer utiliza el archivo de Java Web Start asociado para procesar y abrir correctamente el Visualizador.

Configuración de Mozilla Firefox para que utilice Java Web Start:

Si establece o modifica la manera en que Mozilla Firefox maneja archivos JNLP (Java Network Launch Protocol), puede hacer que Firefox utilice automáticamente la versión cliente de Java Web Start necesaria para iniciar el Visualizador. Si tiene varias versiones de Java instaladas, al modificar este valor puede evitar problemas relacionados con la apertura del Visualizador.

Acerca de esta tarea

Este procedimiento hace que Firefox utilice la versión de Java Web Start para abrir todas las aplicaciones web. Si ejecuta otras aplicaciones de Web Start que necesitan versiones más actuales de Java, utilice el método de inicio directo.

Procedimiento

1. Iniciar Mozilla Firefox.
2. Seleccione **Herramientas** > **Opciones**.
3. Seleccione **Aplicaciones**
4. En **Tipo de contenido**, ubique la entrada del **Archivo JNLP**.

   Nota: Si no ve la entrada del **Archivo JNLP**, cierre el diálogo **Opciones**. En la página Web Start del Visualizador, intente iniciar el Visualizador pulsando en enlace **Pulse aquí para iniciar el Visualizador de IBM Identity Insight**. A continuación, vuelva a empezar por el paso 1.
5. Seleccione la entrada **Archivo JNLP**.
6. En **Acción**, seleccione la opción **Utilizar otro**.
7. En el diálogo **Seleccionar aplicación de ayuda**, pulse **Examinar**, navegue hacia el directorio en el que está instalada la versión cliente de Java necesaria, y seleccione el archivo ejecutable `javaws`.
8. Pulse **Aceptar** para cerrar el diálogo **Seleccionar aplicación de ayuda**.
9. Pulse **Aceptar** para cerrar el diálogo **Opciones**.

Resultados

Mozilla Firefox ahora utiliza el archivo de Java Web Start seleccionado para manejar todos los tipos de archivos JNLP. El Visualizador se abrirá correctamente.

Inicio directo del Visualizador desde el ejecutable de Java Web Start:

Si desea iniciar el Visualizador sin cambiar Java u otros valores del sistema, puede utilizar el método de inicio directo. Este método inicia el Visualizador directamente desde el ejecutable de Java Web Start. Es posible que desee utilizar el método de inicio directo si tiene varias versiones de Java instaladas en el espacio de trabajo y utiliza otras aplicaciones Web Start además del Visualizador.

Antes de empezar

Ubique la vía de acceso que lleva al archivo ejecutable de Java Web Start (`javaws`) en el espacio de trabajo.

Acerca de esta tarea

También puede crear un atajo en el escritorio al archivo ejecutable de Java Web Start seleccionando el archivo `javaws` y especificando el URL en el campo **Destino** del Visualizador.

Procedimiento

1. En el escritorio, abra una ventana de mandatos DOS.
2. En la línea de mandatos, especifique el mandato de inicio directo: *vía_acceso_a_instalación_Java*`vía_acceso_a_archivo_ejecutable_javaws>javaws.exe` *URL del Visualizador* Por ejemplo: **`C:/IBM/Java60/jre/bin>javaws.exe http://localhost:13510/docs/rrmdi.jnlp`**

   Importante: Tenga en cuenta que hay un espacio entre la extensión del archivo ejecutable de Java Web Start y el URL.

Resultados

El Visualizador se abrirá correctamente.

Configuración de Java v1.6 para ejecutar el Visualizador en estaciones de trabajo Microsoft Windows:

Si intenta iniciar el Visualizador y ve un mensaje de error que indica que la aplicación ha solicitado una versión de JRE que no está instalada localmente, intente cambiar los valores de descarga automática de Java. Este mensaje de error es un problema conocido de las estaciones de trabajo Microsoft Windows que tiene la versión 1.6 de Java instalada.

Procedimiento

1. En el **Panel de control de Windows**, seleccione una de las siguientes opciones:
   - Para instalaciones IBM de Java, seleccione **Panel de control de IBM para Java**.
   - Para instalaciones de Sun de Java, seleccione **Java**.
2. En el separador **Avanzado**, expanda el valor **Descarga automática de JRE**. Si no puede ver esta opción y tiene varias versiones de Java instaladas en esta estación de trabajo, cierre el **Panel de control de Java** y seleccione otra entrada.

3. Asegúrese de que el valor **Descarga automática de JRE** está establecido en **Siempre descarga automática** (recomendado) o **Solicitar al usuario**. El valor **Nunca descarga automática** prohíbe abrir el Visualizador o la Consola de configuración.
4. Pulse **Aplicar** .
5. Pulse **Aceptar**.
6. Cierre la ventana **Panel de control**.

Cierre del Visualizador

Cuando haya terminado de utilizar el Visualizador, cierre la aplicación. Al cerrar el Visualizador, también cierra la sesión. Si se toma un descanso y desea asegurar la estación de trabajo durante unos minutos, puede bloquear el Visualizador.

Procedimiento

Para cerrar el Visualizador y cerrar la sesión:

- Seleccione **Archivo** > **Salir**.
- O bien pulse **Control** + **Q**.

Bloqueo del Visualizador

Si va a tomarse un descanso o va a alejarse de su estación de trabajo unos minutos, en lugar de cerrar y finalizar la sesión en el Visualizador, puede bloquearlo. Bloquear el Visualizador asegura su trabajo actuando como un protector de pantalla seguro. Al bloquear el Visualizador, aparece la ventana **Inicio de sesión**. Puede volver a la sesión del Visualizador entrando su contraseña de usuario.

Procedimiento

Para bloquear el Visualizador:

- Seleccione **Archivo** > **Bloquear aplicación**.
- O bien pulse **Control** + **L**.

Resultados

Ahora la sesión del Visualizador ha quedado bloqueada.

Qué hacer a continuación

Para seguir utilizando el Visualizador, entre su contraseña y pulse **Desbloquear**.

Cambio de la contraseña del Visualizador

Cambiar la contraseña del Visualizador regularmente es una buena manera de proteger la seguridad de su cuenta de usuario del Visualizador.

Antes de empezar

Debe haber iniciado la sesión en el Visualizador para cambiar la contraseña.

Acerca de esta tarea

No hay un número mínimo de caracteres requerido para las contraseñas del Visualizador. Puede utilizar cualquier combinación de letras (mayúsculas o minúsculas), caracteres especiales y números. La contraseña es sensible a las mayúsculas y minúsculas, por lo que cuando inicie la sesión, la contraseña que

entre deberá coincidir con la contraseña de su cuenta del Visualizador. Por ejemplo, si su contraseña es `PASSw0rd`, e intenta iniciar la sesión utilizando `passw0rd`, las contraseñas no coinciden y el sistema visualiza un mensaje de error.

Procedimiento

1. En el Visualizador, pulse **Archivo** > **Cambiar contraseña**.
2. En **Contraseña actual**, entre la contraseña que ha utilizado para iniciar esta sesión del Visualizador. Si su contraseña se le asignó o se restableció, esta contraseña será la contraseña del administrador del sistema.
3. En **Contraseña nueva**, entre la nueva contraseña que será su contraseña del Visualizador.
4. En **Repetir contraseña nueva**, entre la misma contraseña que ha entrado en **Contraseña nueva**.
5. Pulse **Cambiar contraseña**.

Resultados

- Si las entradas de **Contraseña nueva** y **Repetir contraseña nueva** son iguales, el sistema visualiza un mensaje indicando que se ha cambiado la contraseña. Pulse **Aceptar**. Utilice la nueva contraseña la próxima vez que inicie la sesión en el Visualizador
- Si las entradas no coinciden, el sistema visualiza un mensaje de error que indica que las contraseñas nuevas no coinciden. Pulse **Aceptar**. No se ha cambiado la contraseña. Para cambiar la contraseña, vuelva a empezar en el paso 2.

Análisis de alertas en el Visualizador

Una de las tareas más comunes que realizan los usuarios del Visualizador es evaluar alertas para decidir qué alertas deben revisarse y cuáles deben transferirse a otros grupos del Visualizador.

Las alertas se visualizan en la ventana **Resumen de alerta** del Visualizador. Esta ventana es el punto de partida para evaluar, asignar o transferir y revisar alertas.

Las alertas se agrupan en resúmenes de alertas. Los resúmenes de alertas contienen todas las alertas del mismo tipo de alerta con la misma descripción, gravedad de alerta, estado, regla de resolución, puntuación de relación, y puntuación de resolución (similitud). Un resumen de alertas contiene normalmente varias alertas individuales, cada una de las cuales necesita revisión y análisis. Parte de la revisión incluye asignar una disposición a la alerta, de manera que usted y otros usuarios del Visualizador puedan conocer el estado del análisis y puedan ver comentarios que indiquen sus descubrimientos.

Recuerde que la ventana de **Resumen de alerta** solamente muestra lo siguiente:

- Los resúmenes de alertas para el grupo de analistas del Visualizador que contienen alertas no asignadas
- Las alertas que ya ha asignado a sí mismo

No verá las alertas que otros analistas del grupo de analistas del Visualizador hayan asignado a sí mismos. Tampoco verá las alertas que estén asignadas a otros grupos de analistas del Visualizador.

Evaluación de resúmenes de alertas

¿Cómo se decide qué alertas deben asignarse a uno mismo para el análisis? Empiece por revisar los resúmenes de alertas en la ventana **Resumen de alerta**. A

medida que observa los resúmenes de alertas, compare la importancia de la información que conforma ese resumen de alerta con los objetivos de su análisis. Podría ser necesario evaluar varios fragmentos de información de alertas para poder decidir.

Sugerencias para establecer un orden de prioridades en los resúmenes de alertas:

- **Gravedad de alerta:** Empiece por ordenar los resúmenes de alerta por gravedad. Pulse la cabecera de columna **Gravedad de alerta**. Esta información podría ser suficiente para ayudarle a decidir qué alertas son las primeras a analizar dada su importancia. Por ejemplo, si su empresa utiliza "C" para las alertas con una gravedad crítica, podrá ver de inmediato qué alertas son críticas al observar su gravedad.
- **Descripción de alerta:** Es posible que la gravedad en sí no aporte suficiente información. La descripción de la alerta podría ayudarle a elegir qué alertas están más arriba en la lista de prioridades, si hay múltiples resúmenes de alertas con la misma gravedad de alerta. Por ejemplo, podría ser más importante analizar alertas que estén agrupadas por la descripción "Exclusión aérea conoce a Pasajero" que por la descripción "Pasajero conoce Empleado".
- **Puntuación de similitud y Puntuación de relación:** Cuanto mayores sean las puntuaciones, más probabilidades de que haya una relación de interés o de que la identidad sea la entidad. En el ejemplo "Exclusión aérea conoce a Pasajero", si tanto la puntuación de Similitud como la de Relación son de 100, la persona en la lista de Exclusión aérea es el Pasajero, y le interesará tomar medidas de inmediato. Si la puntuación de similitud es menor de 70 y la puntuación de relación es menor de 85, esta alerta aún es importante, pero no crítica. Aún puede interesarle analizar las entidades involucradas en la alerta, pero es posible que no sea necesario tomar medidas inmediatas.

Como usuario del Visualizador, está familiarizado con los objetivos de su organización, por lo que probablemente puede añadir sus propios factores personales a utilizar al ordenar las prioridades de las alertas. Estas sugerencias le ayudarán en su iniciación.

Asignación de alertas

Una vez ya sabe con qué alertas quiere trabajar, basándose en la prioridad, puede autoasignarse esas alertas. Asignar alertas permite al grupo de analistas del Visualizador abordar la lista de alertas entrantes bajo la máxima de "divide y vencerás". Cuando se le asigna una alerta, esa alerta solo se visualiza en su ventana Resumen de alerta, evitando que se realice un trabajo duplicado en la alerta por parte de otro usuario del Visualizador. Puede ver inmediatamente las alertas que está investigando personalmente.

Si ve una o más alertas en la ventana Resumen de alerta que cree que pueden pertenecer a otro grupo de analistas del Visualizador, puede transferir esas alertas. Por ejemplo, imaginemos que trabaja como encargado de reservas y evalúa las alertas generadas por reservas nuevas o modificadas. Ve una alerta listada que es responsabilidad de la seguridad. Puede asignar esa alerta al grupo Seguridad, ya que la alerta está bajo la jurisdicción de ese grupo.

Revisión y disposición de alertas

Cuando se asigna a sí mismo una o más alertas, puede proceder directamente a investigar y analizar esas alertas. El Visualizador simplifica la tarea en la ventana

Investigación, que muestra toda la información asociada relevante sobre la alerta en una ventana. Desde la ventana Investigación, puede realizar las siguientes tareas como parte de su análisis:

- Revisar los detalles de alertas
- Observar los resúmenes de entidades de las entidades relacionadas
- Ver la entidad asociada o gráficos de alertas para visualizar y explorar los aspectos comunes de las entidades o atributos que forman parte de la alerta
- Añadir comentarios que indiquen los descubrimientos de su análisis
- Cambiar el estado (disposición) de la alerta a medida que progresa el análisis

Alertas de atributos

Las alertas de atributos son alertas generadas por los generadores de alertas de atributo, que crean una consulta del sistema persistente en busca de atributos o identidades específicos en la base de datos de entidades. Siempre que los atributos para entidades coinciden con los criterios del generador de alertas de atributo, el sistema crea una alerta de atributo.

Los usuarios del Visualizador crean sus propios generadores de alertas de atributo personales. Si está buscando una identidad específica o cualquier identidad o entidad que coincida con un conjunto de atributos específico, puede crear su propio generador de alertas de atributo personal que busque coincidencias hasta la fecha de caducidad especificada.

A continuación se muestran algunos ejemplos de posibles atributos de entidades sobre los que puede ser notificado:

- Nombre y número exclusivo (como un número de tarjeta de crédito)
- Nombre y número de teléfono
- Dirección
- Nombre y número no exclusivo

Los generadores de alertas de atributo se configuran y se consultan en el Visualizador. Los generadores de alertas de atributo que puede crear solo estarán disponibles para usted.

Ejemplo de una alerta de atributos de dirección

Está viendo la dirección 675 Hickory Street Las Vegas, NV. Puede configurar un generador de alertas de atributo para crear una alerta de atributo siempre que la dirección se asocie a un registro de identidad de entrada añadido a la base de datos de entidades.

Alertas de sucesos

Una alerta de suceso se produce cuando uno de los sucesos más complejos cumple los criterios establecidos en un lapso de vida especificado. Las alertas de sucesos están basadas en reglas empresariales de sucesos complejas y otras configuraciones contenidas en un archivo de reglas de sucesos (`cep.xml`). Estas alertas pueden indicar situaciones de interés, tales como "Se han producido dos o más compras de más de 10.000$ de EE.UU. en la última hora en ubicaciones separadas 200 millas entre sí".

Alertas de rol

Una alerta de rol identifica cuándo una o dos entidades están enlazadas a través de una relación que cumple o excede una regla de alerta de rol configurada. Las alertas de roles se basan en los roles configurados y en las normas de alertas de

roles. Pueden indicar un aviso o un problema (como por ejemplo que un cliente conoce a un malo) o simplemente indicar relaciones interesantes (por ejemplo, un cliente conoce a un empleado).

Puede definir relaciones *interesantes* o como *conflictivas* configurando normas de alertas de rol, que identifican qué roles no deben existir en una sola entidad o no se pueden enlazar entre una o varias entidades. Utilice la Consola de configuración para configurar filtros para alertas de rol, que determinan si el sistema vuelve a alertar cuando hay información nueva (como una nueva identidad o un nuevo código de origen de datos).

Durante la resolución de entidades, la interconexión evalúa relaciones entre la identidad de entrada y entidades de la lista de candidatos. Después de determinar que existe una relación entre la identidad de entrada y una entidad candidata, el sistema evalúa si los roles asignados cumplen una regla de alerta de rol configurada. Si es así, el sistema genera una alerta de rol.

Una alerta de rol identifica datos de entidades en el momento en que se creó la alerta de rol. La pantalla de detalles de Alerta de rol muestra los datos de la entidad tal como existían en el momento en que se creó la alerta de rol. A medida que los datos de la entidad cambian con el tiempo, el resumen de la entidad contiene los últimos datos sobre la entidad. Si desea ver los datos actuales correspondientes a una entidad en particular, consulte el resumen de la entidad.

Puede ver y trabajar con alertas de rol en los componentes del kit de herramientas de analista (informes de Cognos, el plug-in de Identity Insight para i2 e Identity Insight Explorer).

Visualización de alertas

Puede ver las alertas en la ventana **Resumen de alerta** para evaluar qué alertas deben analizarse y asignarse a uno mismo o transferir a otros grupo de analistas del Visualizador. A continuación, puede empezar a investigar y disponer las alertas que se haya asignado a sí mismo.

Acerca de esta tarea

Las alertas que se visualizan en la ventana **Resumen de alerta** incluyen lo siguiente:

- Alertas que se ha asignado a sí mismo para análisis.
- Alertas no asignadas para su grupo de analistas del Visualizador
- Alertas de atributo generadas desde uno de sus generadores de alertas de atributo

Los resúmenes de alertas no asignadas se filtran según los valores predeterminados de filtros de visualización de alertas en la ventana **Resumen de alerta** que se configuran en el panel **Preferencias del sistema** de la ventana **Configurar preferencias de pantalla**. Puede cambiar uno o varios valores de filtro de visualización de alertas en el recuadro de grupo **Filtros de visualización**.

Procedimiento

1. Seleccione **Ver** > **Resumen de alerta**.
2. A continuación seleccione el tipo de alertas que desee visualizar o seleccione **Mostrar todos los tipos de alerta**.

Resultados

En la ventana **Resumen de alerta**, puede decidir con qué alertas desea trabajar. Puede asignarse alertas a sí mismo o transferir alertas a otro grupo de analistas del Visualizador. Puede seleccionar las alertas que se ha asignado a sí mismo para analizar y añadir comentarios sobre su análisis.

Filtrado de la visualización de alertas en la ventana Resumen de alerta

Mientras revisa las alertas en la ventana **Resumen de alerta**, puede filtrar qué resúmenes de alertas se visualizarán cambiando los valores del recuadro de grupo **Filtros de visualización**. Los filtros de visualización solo afectan a los resúmenes de alertas que estén actualmente en estado de "No asignado".

Acerca de esta tarea

Los valores predeterminados para estos filtros de alertas se configuran en el panel **Preferencias del sistema** de la ventana **Configurar preferencias de pantalla**. Al cambiar los filtros de visualización de alertas en la ventana **Resumen de alerta**, altera temporalmente esos valores predeterminados. La próxima vez que abra una nueva ventana **Resumen de alerta**, los filtros volverán a sus valores predeterminados.

Procedimiento

1. En la ventana **Resumen de alerta**, abra el giro del recuadro de grupo **Filtros de visualización**.
2. Realice los cambios en uno o varios de los filtros de visualización de alertas.
3. Pulse **Aplicar** para renovar la ventana **Resumen de alerta** y aplicar los filtros de alerta especificados.

Asignación de alertas a uno mismo

Al asignarse una alerta a uno mismo, uno se convierte en propietario para revisar, investigar y disponer esa alerta. Después de asignarse una alerta a uno mismo, esa alerta solo se visualiza en su ventana **Resumen de alerta**, lo que facilita la identificación de sus alertas.

Procedimiento

1. Desde el Visualizador, en la ventana **Resumen de alerta**, en la tabla **Resumen de alerta**, pulse un resumen de alerta no asignado. El resumen de alerta contiene una o más alertas agrupadas por tipo de alerta, y comparten la misma descripción, estado, regla de resolución, puntuación de similitud y puntuación de relación.
2. Desde la tabla **Lista de alertas**, pulse dos veces en la alerta que va a asignarse a sí mismo.
3. En la ventana **Investigación**, pulse **Establecer estado**.
4. En **Establecer estado**, realice las siguientes acciones:
   a. En **Seleccione la acción que desee llevar a cabo**, seleccione **Establecer estado**. Aparece un código de actividad correspondiente en **Seleccionar código de actividad**.
   b. Necesario: En **Seleccionar estado**, seleccione **Asignado**. Si selecciona otro estado, no se le asignará la alerta.
   c. Opcional: Para asignar un código de actividad distinto, selecciónelo en **Seleccionar código de actividad**. Si no ve el código de estado de actividad

que desea seleccionar, póngase en contacto con el administrador del sistema para configurar el código de actividad.

d. Especifique comentarios o notas en el recuadro de texto **Comentarios**. Por ejemplo, podría elegir especificar comentarios sobre por qué va a cambiar el estado, o incluir notas sobre su análisis de esta alerta.

e. Pulse **Aceptar** para guardar los cambios.

Resultados

Ahora la alerta refleja el estado de asignada y solo se visualiza en su ventana **Resumen de alerta**, después de renovar la pantalla de la ventana. Los demás analistas de su grupo de analistas del Visualizador ya no verán esta alerta después de renovar la pantalla de la ventana **Resumen de alerta**.

Asignación de alertas a otros grupos de analistas

Si determina que una alerta debe asignarse a otro grupo de analistas del Visualizador, puede transferir esa alerta. No puede transferir una alerta a un usuario específico del Visualizador, pero puede transferir esa alerta al grupo de analistas del Visualizador al que pertenece el usuario.

Procedimiento

1. Desde el Visualizador, en la ventana **Resumen de alerta**, en la tabla **Resumen de alerta**, pulse el resumen de alerta al que está asociada la alerta.
2. Desde la tabla **Lista de alertas**, pulse dos veces en la alerta a transferir.
3. En la ventana **Investigación**, pulse **Establecer estado**.
4. En **Establecer estado**, haga lo siguiente:
   a. Desde **Seleccione la acción que desee llevar a cabo**, seleccione **Transferir alerta**.
   b. En **Transferir alerta a**, seleccione el grupo de analistas del Visualizador al que se transferirá la alerta. Si no ve el grupo de analistas del Visualizador que desea seleccionar, póngase en contacto con el administrador del sistema para configurar el grupo de analistas. Aparece un código de actividad correspondiente en **Seleccionar código de actividad**.
   c. Opcional: Para asignar un código de actividad distinto, selecciónelo en **Seleccionar código de actividad**. Si no ve el código de estado de actividad que desea seleccionar, póngase en contacto con el administrador del sistema para configurar el código de actividad.
   d. Especifique comentarios o notas en el recuadro de texto **Comentarios**. Por ejemplo, podría elegir especificar comentarios sobre por qué va a transferir la alerta.
   e. Pulse **Aceptar** para completar la transferencia.

Resultados

Ahora la alerta se ha transferido al grupo de analistas del Visualizador seleccionado y se visualiza en las ventanas **Resumen de alerta** de los analistas de ese grupo de analistas del Visualizador. (Es posible que los analistas de ese grupo tengan que renovar primero la ventana **Resumen de alerta**). Esta alerta ya no aparece en la ventana **Resumen de alerta** de los analistas de su grupo de analistas del Visualizador, incluido usted, después de renovar la pantalla de la ventana **Resumen de alerta**.

Cambio del estado de una alerta

A medida que analiza las alertas que se le asignan a usted o al grupo de analistas del Visualizador, puede utilizar el Visualizador para hacer el seguimiento de su investigación, los comentarios y la manera en que dispone la alerta.

Acerca de esta tarea

Puede actualizar el estado de alertas para las alertas que se le asignan a usted o al grupo de analistas del Visualizador en cualquier momento. También puede añadir comentarios a estas alertas en cualquier momento. No obstante, no puede editar los comentarios existentes.

Procedimiento

1. Desde el Visualizador, en la ventana **Resumen de alerta**, en la tabla **Resumen de alerta**, pulse el resumen de alerta que contiene la alerta a actualizar.
2. Desde **Lista de alertas**, pulse dos veces en la alerta cuyo estado debe cambiarse.
3. En la ventana **Investigación**, pulse **Establecer estado**.
4. En **Establecer estado**, haga lo siguiente:
   a. Desde **Seleccione la acción que desee llevar a cabo**, seleccione **Establecer estado**. Aparece un código de actividad correspondiente en **Seleccionar código de actividad**.
   b. Opcional: Para asignar un código de actividad distinto, selecciónelo en **Seleccionar código de actividad**. Si no ve el código de estado de actividad que desea seleccionar, póngase en contacto con el administrador del sistema para configurar el código de actividad.
   c. Especifique comentarios o notas en **Comentarios**. Por ejemplo, podría especificar comentarios indicando por qué va a cambiar el estado, o incluir notas sobre su análisis de esta alerta.
   d. Pulse **Aceptar** para guardar los cambios.

Resultados

Ahora la alerta refleja el nuevo estado en la ventana **Resumen de alerta**.

La actualización más reciente de estado o comentarios para una alerta de atributo se visualiza en la parte superior de la sección **Resumen de estado**.

Si el cambio de estado ha implicado asignarse la alerta de atributo a sí mismo, ahora esta alerta de atributo solo se visualizará en su ventana **Resumen de alerta**, después de renovar la pantalla. Los demás analistas de su grupo de analistas del Visualizador ya no verán esta alerta en su ventana **Resumen de alerta**, después de renovar la pantalla.

Temas de ayuda

Ventana Resumen de alerta:

Utilice esta ventana para ver resúmenes de alertas no asignadas para su grupo de analistas del Visualizador o alertas que se haya asignado a sí mismo.

Utilice los giros para expandir o contraer las secciones de la pantalla para ayudarle a centrarse en un detalle específico.

Visualizar alertas por tipo
Seleccione un tipo de alerta a visualizar o mostrar todos los tipos de alerta.

Recuadro de grupo Visualizar filtros
Cambia los valores de filtro predeterminados que determinan qué resúmenes de alerta se muestran en la ventana **Resumen de alerta**. Estos filtros solo cambian la visualización de los resúmenes de alertas que están asignadas actualmente y solo son un cambio temporal. Si cierra la ventana **Resumen de alerta** y vuelve a abrirla en otro momento, estos valores revierten a los valores de filtro predeterminados.

Los valores predeterminados son los valores de filtro de alertas que están configurados para su estación de trabajo. (Puede cambiar los valores predeterminados en **Preferencias del sistema** en la ventana **Configurar preferencias de pantalla**.)

Tabla Resumen de alerta
Las alertas que comparten el mismo tipo de alerta, descripción, gravedad, estado, regla de resolución, Puntuación de similitud, y Puntuación de relación, se agrupan en resúmenes de alertas. La columna **Recuento** muestra cuántas alertas individuales se agrupan en el resumen.

Puede ordenar la tabla pulsando una cabecera de columna en la tabla. La primera pulsación ordena los valores de columna en orden ascendente. La segunda pulsación ordena los valores de columna en orden descendente.

De forma predeterminada, la tabla se ordena por tipo de alerta.

Tipo Tipo de alerta representado por el resumen de alerta.

Descripción
Descripción de las alertas en este resumen.

Para las alertas de atributos, esta descripción es el número de caso. Para las alertas de sucesos, esta descripción es la descripción de situación del suceso. Para las alertas de rol, esta descripción es la descripción de regla de alerta de rol.

Estado
Estado de actividad actual de las alertas en este resumen.

Regla de resolución
Nombre de la regla de resolución utilizada para relacionar las entidades dentro de las alertas en este resumen de alerta.

Puntuación de similitud
Puntuación (0-100) que indica la probabilidad de que las entidades relacionadas representen la misma entidad.

Puntuación de relación
Puntuación (0-100) que indica el grado en que las entidades dentro de la alerta están relacionadas entre sí.

Recuento
Número de alertas individuales agrupadas en este resumen de alerta que cumplen los criterios de recuadro de grupo **Visualizar filtros** seleccionados actualmente.

Tabla Lista de alertas
Después de seleccionar un resumen de alerta de la tabla **Resumen de alerta**, las alertas individuales que forman parte de ese resumen se muestran en esta sección. El número de alertas (líneas) que se muestren depende del número total de alertas en el resumen (encontrado en la

columna **Recuento** de la tabla Resumen de alerta), y el número en el campo **Máximo de líneas en Lista de alertas** en el recuadro de grupo **Visualizar filtros**. Un recuento de lista en la barra de título de la tabla **Lista de alertas** muestra cómo el número de alertas visualizado actualmente encaja en el número total de alertas para este resumen.

Ordene la tabla pulsando una cabecera de columna en la tabla. La primera pulsación ordena los valores de columna en orden ascendente. La segunda pulsación ordena los valores de columna en orden descendente.

Los campos que se visualizan están basados en el tipo de resumen de alerta seleccionado.

Pantalla Alerta de atributo:

Utilice esta pantalla para establecer o cambiar el estado de análisis de una alerta de atributo y revisar los detalles que forman la alerta.

Utilice los giros para expandir o contraer las secciones de la pantalla para ayudarle a centrarse en un detalle específico.

Resumen de estado
Resume el estado de análisis actual y la disposición de la alerta.

Resumen de alerta
Proporciona la descripción del resumen de alerta y la fecha y hora en que se ha generado la alerta.

Sección Coincidir con la entidad
Contiene detalles sobre qué atributos coincidían entre los criterios de búsqueda del generador de alertas de atributo y las entidades existentes en la base de datos de entidad. Pulse en un atributo específico para resaltar la información coincidente de las identidades en la entidad coincidente.

Detalles del Generador de alertas de atributos
Resume los criterios para el generador de alertas de atributo que ha generado esta alerta de atributo. Pulse el origen de datos para resaltar todos los criterios.

Sección Entidad
Visualiza información acerca de la entidad que cumple con los criterios del generador de alertas de atributo. Pulse el origen de datos para resaltar los datos que venían en un registro de identidad de este origen de datos.

Botón Resumen de entidad
Pulse para visualizar el resumen de la entidad para la entidad coincidente. Puede interesarle ver otras identidades asociadas con la entidad para un análisis más profundo de esta alerta.

Pantalla Alerta de suceso:

Utilice la pantalla **Alerta de suceso** para establecer o cambiar el estado de análisis y revisar los detalles de una alerta de suceso. Las alertas de sucesos solamente aparecen si Event Manager está habilitado para el sistema, si hay códigos de actividad configurados para alertas de sucesos, y si existe una o más alertas de sucesos.

Utilice los giros para expandir o contraer las secciones de la pantalla para ayudarle a centrarse en un detalle específico.

Resumen de estado
Resume el estado de análisis actual y la disposición de la alerta de suceso.

Resumen de alerta
Proporciona la descripción de la alerta de suceso y la fecha y hora en que se ha generado la alerta.

Sección Alerta de suceso
Proporciona los detalles del suceso que forman esta alerta de suceso.

Sección Entidad
Proporciona un resumen breve para cada entidad involucrada en esta alerta de suceso.

Botón Informe
Pulse este botón para crear un informe **Detalle de Alerta de suceso**.

Pantalla Alerta de rol:

Utilice esta ventana para ver los detalles de una alerta de rol y para establecer o cambiar el estado de análisis de la alerta de rol.

Pulse los giros para expandir o contraer las secciones de la pantalla para ayudarle a centrarse en un detalle específico.

Degrees of Separation
Indica el número de grados de separación entre las entidades en esta alerta de rol.

Resumen de estado
Resume el estado de análisis actual y la disposición de la alerta.

Resumen de alerta
Proporciona una descripción del resumen de alerta, el código de gravedad de alerta para esta alerta, la regla de resolución utilizada para comparar entidades dentro de la alerta, la puntuación de resolución que indica el grado de similitud entre dos entidades, y la puntuación de relación que indica la probabilidad de que estas dos entidades se conozcan.

Paneles Detalles de coincidencias
Contiene detalles sobre qué atributos coincidían entre las dos entidades. Pulse en un atributo específico para resaltar la información coincidente de las identidades en la entidad coincidente.

Contiene detalles sobre qué atributos coincidían entre los criterios de búsqueda del generador de alertas de atributo y las entidades existentes en la base de datos de entidad.

Botón Informe
Pulse este botón para crear un informe **Detalle de alerta de rol** para esta alerta de rol.

Botón Resumen de entidad
Pulse para visualizar el resumen de entidad para la entidad seleccionada. Puede interesarle ver otras identidades asociadas con la entidad para un análisis más profundo de esta alerta.

Pantalla Sucesos de entidad:

Utilice la pantalla **Sucesos de entidad** para revisar los sucesos para una entidad que se hayan producido dentro de un rango de fechas específico. Inicialmente accederá a esta pantalla pulsando **Mostrar sucesos** desde la pantalla **Resumen de entidad**.

Sección Resumen de sucesos

Visualiza un resumen de todos los sucesos para esta entidad con el rango de fechas indicado. De forma predeterminada, la pantalla visualiza todos los sucesos asociados con la entidad desde la fecha del primer suceso hasta la fecha actual. Cambie el rango de fechas utilizando el filtro de fechas de sucesos para ver sucesos dentro de un rango de fechas distinto.

Filtro de fechas de sucesos en pantalla

Filtra los sucesos visualizados por el rango de fechas especificado cuando pulsa **Actualizar vista**.

Desde fecha

Especifique una fecha o pulse en el control del calendario para seleccionar la fecha inicial en el rango de fechas.

Si decide teclear una fecha, utilice uno de los siguientes formatos de fecha:

- `MM/dd/aaaa`, `MM-dd-aaaa`, `MM.dd.aaaa`, o `MMddaaaa`
- `aaaa/MM/dd`, `aaaa-MM-dd`, o `aaaa.MM.dd`
- `Enero 3, 2008` o `Enero 03, 2008`
- `Enero 3, 08` o `Enero 03, 08`
- `Ene 03, 2008` o `Ene 3, 2008`
- `Ene 3, 08` o `Ene 03, 08`

El campo toma de forma predeterminada la instancia de fecha del primer suceso.

Hasta fecha

Especifique una fecha o pulse en el control del calendario para utilizarla como fecha final en el rango de fechas.

Si decide teclear una fecha, utilice uno de los siguientes formatos de fecha:

- `MM/dd/aaaa`, `MM-dd-aaaa`, `MM.dd.aaaa`, o `MMddaaaa`
- `aaaa/MM/dd`, `aaaa-MM-dd`, o `aaaa.MM.dd`
- `Enero 3, 2008` o `Enero 03, 2008`
- `Enero 3, 08` o `Enero 03, 08`
- `Ene 03, 2008` o `Ene 3, 2008`
- `Ene 3, 08` o `Ene 03, 08`

El campo toma de forma predeterminada la fecha actual.

Botón Actualizar vista

Pulse el botón para ver sucesos para esta entidad dentro del rango de fechas especificado. Este botón está inhabilitado hasta que cambia las fechas predeterminadas en los campos de fecha.

Botón Informe

Pulse el botón para generar un informe de **Todos los sucesos** para esta entidad.

En pantalla

Esta sección de la pantalla resumen los sucesos para esta entidad por tipo de suceso dentro del rango de fechas especificado.

Tipo de suceso

Describe el tipo de suceso.

Recuento

Indica el número total de los sucesos para esta entidad por tipo de suceso, dentro del rango de fechas especificado. (Por ejemplo, si el recuento es 4, se han producido cuatro sucesos del mismo tipo de suceso para esta entidad dentro del rango de fechas especificado.)

Valor Indica el valor total de los sucesos para esta entidad por tipo de suceso, dentro del rango de fechas especificado. (Por ejemplo, si hay cuatro sucesos, este número es el total de la suma del valor de esos cuatro sucesos.)

Cantidad

Indica el número total de unidades para los sucesos para esta entidad por tipo de suceso, dentro del rango de fechas especificado.

Unidad de medida

Describe la unidad de medida para el valor de suceso. La unidad de medida se configura por tipo de suceso en la Consola de configuración.

Recuento total

Indica el número que representa el número total de todos los sucesos para esta entidad dentro del rango de fechas especificado.

Valor total

Indica el número que representa el valor total de todos los sucesos para esta entidad dentro del rango de fechas especificado.

Sección Detalles de suceso

Seleccione una fila de sucesos en la sección Resumen de sucesos para ver más detalles sobre los sucesos individuales incluidos en el resumen de tipo de suceso. Si pulsa dos veces en cualquier fila de sucesos de esta sección, aparece la pantalla **Detalles de suceso** para mostrar información más detallada sobre el suceso seleccionado.

Fecha Indica la fecha y hora del suceso.

Origen de datos - Descripción

Describe el origen de datos asociado con el suceso.

ID externo

Visualiza la clave exclusiva que identifica el registro de entrada en el origen de datos original para este suceso.

Referencia de suceso

Proporciona información adicional sobre el suceso en el origen de datos original, si esa información forma parte del registro de entrada.

Valor Indica la cantidad de valor del suceso.

Cantidad
Indica el número de unidades en el suceso.

Memorándum o *Etiqueta personalizada*
Proporciona información adicional sobre el suceso, tal como notas o comentarios, que puede proporcionar un mayor contexto para la transacción del suceso.

Los usuarios pueden definir una etiqueta personalizada para esta columna, como una de las opciones al configurar un tipo de suceso en la Consola de configuración. Así, en lugar de **Memorándum**, podría ver una etiqueta personalizada más descriptiva, (por ejemplo **Notas de transferencia electrónica**).

Encontrar entidades

Puede utilizar varios métodos de Buscar por en el Visualizador para buscar una entidad en la base de datos de entidades. Si desea que se le notifique cada vez que el sistema procese un registro que contenga un nombre, dirección, número o dirección de correo electrónico concretos, puede crear un generador de alertas de atributo para que "busque" entidades automáticamente.

Búsqueda de entidades por atributo

Si está utilizando el Visualizador y desea buscar una entidad en la base de datos de entidades, puede buscar esa entidad especificando criterios sobre los atributos asociados con la entidad. Puede especificar los criterios de atributo, y el Visualizado crea una consulta basada en esos criterios. Este tipo de consulta de entidad no pasa por el proceso de resolución de entidad para devolver resultados de búsqueda.

Procedimiento

1. En el visualizador, realice una de las acciones siguientes:
   a. Pulse **Ver** > **Buscar por** > **Atributo**.
   b. En la barra de herramientas, pulse el icono (Buscar).
   c. En la barra de herramientas, pulse la flecha y seleccione **Atributo**.
   d. En la ventana **Buscar por**, seleccione **Atributo** de la lista desplegable **Buscar por**.
2. Especifique los criterios para cada tipo de atributo que desee utilizar para buscar entidades.
   a. Pulse **+** para añadir una fila para especificar criterios para otro tipo de atributo.
   b. Pulse **-** para eliminar la entrada de criterios de consulta seleccionada.
3. Opcional: Pulse **Mostrar resumen** para ver un resumen de la consulta Buscar por atributo. El resumen es una manera útil de asegurarse de que la consulta contiene los valores que desea. Si no, cierre el resumen y corrija los criterios de consulta.

   Dos criterios de consulta del mismo tipo de atributo constituyen una cláusula "OR". Todos los demás criterios de consulta se combinan para formar cláusulas "AND".

   El orden de los criterios de tipo de atributo no afecta a los resultados.
4. Pulse **Buscar**.

Resultados

Las entidades que coinciden con los criterios de consulta se muestran en el panel **Resultados**.

De forma predeterminada, los resultados visualizados para las consultas Buscar por atributo están limitados a las 1.000 primeras entidades coincidentes. Si existen más de 1.000 coincidencias, el panel **Resultados** indica que existen más resultados. (El número de resultados mostrados puede ser configurado por el administrador del sistema en la Consola de configuración estableciendo el parámetro MAX_ENTITIES_RETURNED bajo parámetros del sistema.)

Nota: Si el sistema utiliza una aplicación adicional de higiene de direcciones, las direcciones que incluyan caracteres especiales pueden experimentar una transliteración. Por ejemplo, la búsqueda de direcciones alemanas con una o más diéresis en la dirección puede devolver un resultado que no contiene las diéresis correspondientes.

Qué hacer a continuación

Pulse una entidad para visualizar el resumen de entidad para la entidad seleccionada.

Búsqueda de entidades por cuenta de origen de datos

Cuando conoce el número de cuenta (o ID externo) de una identidad, y desea buscar la entidad que contiene esa identidad, utilice Buscar por cuenta de origen de datos en el Visualizador. También puede buscar una entidad que haya añadido mediante la pantalla **Añadir entidad**.

Antes de empezar

Debe conocer la descripción de origen de datos y el ID externo de la identidad (o cuenta). Si está intentando buscar una entidad por nombre, utilice el método Buscar por atributo.

Procedimiento

1. En el visualizador, realice una de las acciones siguientes:
   a. Pulse **Ver** > **Buscar por** > **Cuenta de origen de datos**.
   b. En la barra de herramientas, pulse la flecha y seleccione **Cuenta de origen de datos**.
   c. En la ventana **Buscar por**, seleccione **Cuenta de origen de datos** en la lista desplegable **Buscar por**.
2. En **Especificar ID externo**, entre el número de cuenta para la identidad. La cuenta es la manera en que se conoce a la identidad en el origen de datos original.
3. En **Origen de datos**, seleccione el código del origen de datos y la descripción.
4. Pulse **Buscar**.

Resultados

Si el sistema encuentra una entidad que contiene una identidad con los criterios de ID externo y origen de datos especificados, el Visualizador muestra el **Resumen de entidad** para esa entidad.

Búsqueda de entidades por ID de entidad

Cuando conozca el número de ID de entidad de una entidad, utilice el método Buscar por ID de entidad en el Visualizador para localizar rápidamente la entidad y visualizar el resumen de esa entidad.

Antes de empezar

Debe conocer el número de ID de entidad de la entidad que desea buscar. Si está intentando buscar una entidad por nombre, es mejor utilizar el método Buscar por atributo.

Procedimiento

1. En el visualizador, realice una de las acciones siguientes:
   a. Pulse **Ver** > **Buscar por** > **ID de entidad**.
   b. En la barra de herramientas, pulse la flecha y seleccione **ID de entidad**.
   c. En la ventana **Buscar por**, seleccione **ID de entidad** de la lista desplegable **Buscar por**.
2. En **Especificar ID de entidad**, entre el número de ID de entidad de la entidad que desea encontrar.
3. Pulse **Buscar**.

Resultados

Si el ID de entidad coincide con una entidad en la base de datos de entidades, el Visualizador muestra el resumen de entidad para esa entidad.

Búsqueda de entidades por resolución

Utilice Buscar por resolución para crear una entidad de búsqueda que pase por el proceso de resolución de entidad para ver si alguna identidad de la base de datos de entidades cumple los criterios de la consulta.

Antes de empezar

La característica Buscar por resolución requiere que haya una interconexión en ejecución disponible para comunicarse con el servidor del Visualizador. La interconexión es el componente donde se produce la resolución de entidades y relaciones.

Acerca de esta tarea

Para sacar el mejor provecho de la característica Buscar por resolución, es importante comprender el funcionamiento de la resolución de entidades y cómo está configurada para el sistema, pues la resolución de entidades se utiliza para buscar los resultados. Por ejemplo, si la resolución de entidades no está configurada para encontrar coincidencias basadas únicamente en un nombre, Buscar por resolución no devolverá resultados si se realiza una búsqueda únicamente sobre un valor de nombre. De la misma manera, debido a que la resolución de entidades no resuelve entidades basándose solamente en un código postal, especificar solo un código postal no devuelve ningún resultado.

Buscar por resolución utiliza los valores de puntuación mínima definidos en el panel **Preferencias del sistema** del menú **Archivo**.

Procedimiento

1. En el visualizador, realice una de las acciones siguientes:
   a. Pulse **Ver** > **Buscar por** > **Resolución**.
   b. En la barra de herramientas, pulse la flecha y seleccione **Resolución**.
   c. En la ventana **Buscar por**, seleccione **Resolución** en la lista desplegable **Buscar por**.
2. Especifique tantos atributos como conozca sobre la identidad.
   - Si especifica algo en la sección **Nombre**, entonces **Apellido** será necesario.
   - Si especifica información en la sección **Lista de direcciones**, **Dirección** será necesario.
   - Si selecciona un **Tipo** en la sección **Lista de números**, debe entrar un valor de número en el campo **Valor**. (**Ubicación** es opcional.)
   - Si selecciona un **Tipo** en la sección **Lista de características**, debe entrar un valor de característica en el campo **Valor**.
   - Si selecciona un **Tipo** en la sección **Lista de correo electrónico**, debe especificar un valor de dirección de correo electrónico en el campo **Dirección**.
3. Pulse **Buscar**.

Búsqueda de entidades mediante generadores de alertas de atributo

Cuando tiene una entidad que está observando, puede crear generadores de alertas de atributo con los criterios para esa entidad. Siempre que los registros de identidades o las entidades contienen atributos que coinciden con los criterios, el sistema genera una alerta de atributo. Cada usuario del Visualizador crea y gestiona generadores de alertas de atributo personales para un rango de fechas específico.

Debido a que los generadores de alertas de atributo se envían a través de la interconexión, el proceso de resolución de entidades se realiza en esas peticiones de búsqueda de la misma forma que se realiza sobre datos de entidad de entrada:

- Los nombres y direcciones se estandarizan
- Se realizan búsquedas y comparaciones parciales o aproximadas para que las entidades aplicables queden identificadas en las alertas de atributo posteriores

Para sacar el mejor provecho de los generadores de alertas de atributo, es importante comprender el funcionamiento de la resolución de entidades y cómo está configurada para el sistema, pues la resolución de entidades se utiliza para buscar los resultados de las alertas de atributo. Por ejemplo, si la resolución de entidades no está configurada para encontrar coincidencias basadas únicamente en un nombre, un generador de alertas de atributo configurado para buscar solo un valor de nombre no devolverá resultados. De la misma manera, debido a que la resolución de entidades no resuelve entidades basándose solamente en un código postal, un generador de alertas de atributo que sólo especifique un código postal no devuelve ningún resultado.

Cuando cree un generador de alertas de atributo, siga las siguientes directrices:

- Utilice **Puntuación mínima** para filtrar resultados de alertas de atributo. El valor por omisión de este campo es "Cualquier relación". Esta opción ofrece la mayor cantidad de resultados. Elija un nivel superior para que se generen menos resultados. Estos valores se configuran en las preferencias del sistema del Visualizador, disponibles en el menú **Archivo**.

- Para nombres: Proporcione una combinación formada por un primer apellido y un nombre de pila o por un primer apellido y un segundo apellido. Los generadores de alertas de atributo que sólo especifican un primer apellido, un nombre de pila o un segundo apellido no devuelven ningún resultado.
- Para direcciones: Son obligatorios una dirección y un código postal. Los generadores de alertas de atributo que sólo especifican ciudad, estado, código postal, dirección o país no devuelven ningún resultado.

Creación de generadores de alertas de atributo:

Para recibir una alerta cada vez que el sistema procese un valor de atributo específico o una combinación de valores de atributos, cree un generador de alertas de atributo. Los generadores de alertas de atributo siguen produciendo alertas hasta que se alcanza la fecha de caducidad especificada.

Procedimiento

1. En el visualizador, realice una de las acciones siguientes:
   a. Seleccione **Ver** > **Gestor de Generador de alertas de atributo**.
   b. En la barra de herramientas, pulse el icono (Gestor de Generador de alertas de atributo).
2. En la ventana **Gestor de Generador de alertas de atributo**, pulse **Crear**.
3. Utilice las listas desplegables y campos para especificar los criterios específicos para la nueva alerta de atributo, incluida una fecha de caducidad. La fecha de caducidad predeterminada está establecida en seis meses a partir de hoy.
4. Pulse **Crear**.

Resultados

Siempre que los datos que se resuelven con los criterios que ha especificado se procesen mediante resolución de entidad, se visualizará una nueva alerta de atributo en su ventana **Resumen de alerta**. Si la información que busca se encuentra actualmente en la base de datos de entidades, verá una nueva alerta de atributo en la ventana **Resumen de alerta**.

Edición de generadores de alertas de atributo:

Edite un generador de alertas de atributo activo cuando desee cambiar el número de caso, comentario o fecha de caducidad.

Acerca de esta tarea

No puede cambiar los atributos o la puntuación mínima de resolución para esos atributos. Si eso es lo que desea hacer, cree un generador de alertas de atributo. Además, si el nuevo generador de alertas de atributo sustituye a uno existente, utilice estos pasos para hacer que caduque el generador de alertas de atributo que ya no necesita.

Procedimiento

1. En el visualizador, realice una de las acciones siguientes:
   a. Pulse **Ver** > **Gestor de Generador de alertas de atributo**.
   b. En la barra de herramientas, pulse (Gestor de Generador de alertas de atributo).
2. Seleccione el generador de alertas de atributo a editar y pulse **Crear**.

3. En la ventana **Información del Generador de alertas de atributo**, realice los cambios.
   - Puede cambiar la fecha de caducidad, incluido establecer la fecha en una fecha anterior para hacer que caduque el generador de alertas de atributo.
   - También puede actualizar el número de caso y los comentarios.
   - No puede cambiar el código de razón, los atributos que seleccionó para el generador de alertas de atributo cuando se creó, ni la puntuación mínima de resolución.
4. Pulse **Actualizar**.

Resultados

El sistema registra los cambios que ha realizado en el generador de alertas de atributo. Vea o imprima un informe **Historial del Generador de alertas de atributo** para ver todos los cambios en los generadores de alertas de atributo.

Temas de ayuda:

Pantalla Buscar por atributo:

Utilice esta ventana para crear una consulta para buscar entidades en la base de datos de entidades por atributos: nombre, direcciones, números, características, y demás. Este tipo de consulta no utiliza el proceso de resolución de entidad para devolver los resultados de la consulta.

Tipo de atributo

El tipo de atributo de entidad que desea utilizar como criterios para la consulta: nombre, dirección, números, características, dirección de correo electrónico, origen de datos, o fecha de carga del archivo. Al seleccionar un tipo de atributo, la ventana muestra campos de criterios de consulta adecuados para ese tipo.

La sentencia de consulta que cree dependerá de qué tipos de atributo haya seleccionado para la consulta:

- En una sola consulta, los criterios para más de uno del mismo tipo de atributo crea una sentencia de consulta "OR". Por ejemplo, "Bob Hayes" OR "Rob Hays".
- En una sola consulta, los criterios para varios tipos de atributo crea una sentencia de consulta "AND". Por ejemplo, "Bob Hayes" AND número de tarjeta de crédito "5252-1010-5252-1010".

Utilizando este ejemplo, si ha entrado los dos nombres siguientes y una tarjeta de crédito, la sentencia de consulta tiene el aspecto de esta sentencia: Bob Hayes" OR "Rob Hays AND número de tarjeta de crédito "5252-1010-5252-1010".

Utilice el botón **Mostrar resumen** para ver la sentencia de consulta completa.

Campos de valor

Entre los valores específicos del tipo de atributo a utilizar para buscar entidades. Cada tipo de atributo tiene sus propios campos de valor. Si deja en blanco campos de valores, la consulta buscará todos los valores potenciales. No obstante, si entra datos en todos los campos de valores, la consulta se ejecuta con mayor rapidez y devuelve mejores resultados.

- Los criterios de nombre son necesarios.

- Si especifica información en un campo de criterios de dirección o correo electrónico, serán necesarios todos los campos de dirección.
- Si selecciona un tipo Número o Característica, el campo **Valor** es necesario.

Botón +
Añade una nueva fila de atributos a los criterios.

Botón -
Elimina la fila de atributos y la entrada de criterios seleccionadas.

Panel Buscar por atributo - Resultados
Contiene los resultados de la consulta Buscar por atributo, de acuerdo con las entradas de criterios. De forma predeterminada, el área de visualización solamente muestra los primeros 1.000 registros que coinciden con los criterios de consulta. (Pero el administrador del sistema puede configurar esta opción).

Los resultados se muestran para cada entidad y representan la información más reciente sobre cada entidad. Si hace una doble pulsación sobre una entidad en el panel de resultados, el Visualizador abre el resumen completo de la entidad.

ID de entidad
Visualiza el ID de la entidad que cumple los criterios de consulta.

Nombre (*recuento*)
Visualiza el mejor nombre de la entidad que cumple los criterios de consulta, junto con un número que representa el número de nombres asociados a la entidad. Por ejemplo, Bob M. Smith (4) indica que existen cuatro nombres asociados a la entidad Bob Smith.

Dirección (*recuento*)
Visualiza la mejor dirección de la entidad que cumple los criterios de consulta, junto con un número que representa el número de direcciones asociados a la entidad. Por ejemplo, 1024 Daisy Lane, Akron, OH 43596 (24) indica que existen 24 direcciones asociadas a esta entidad.

Tipo de número: *valor*
Visualiza los mejores tipos de número y valores de número de la entidad que cumple los criterios de consulta.

Tipo de característica: *valor*
Visualiza los mejores tipos y valores de característica de la entidad que cumple los criterios de consulta.

Relaciones
Visualiza el número de relaciones mantenidas por la entidad que cumple los criterios de consulta.

Alertas
Visualiza el número de alertas asociadas a la entidad que cumple los criterios de consulta.

Pantalla Buscar por cuenta de origen de datos:

Utilice esta ventana para buscar una entidad por información de cuenta desde el origen de datos original.

Entrar el ID externo
Entre la información de cuenta del origen de datos que está asociado con la entidad en el origen de datos especificada en **Origen de datos**.

Origen de datos
Seleccione el origen de datos que corresponda a la cuenta especificada en **Entrar el ID externo**.

Pantalla Buscar por ID de entidad:

Utilice este método Buscar por para buscar rápidamente una entidad por el ID de entidad en la base de datos de entidades. Si la consulta localiza la entidad en la base de datos de entidades, el Visualizador muestra el Resumen de entidad para esa entidad.

Ventana Buscar por resolución:

Utilice la ventana **Buscar por resolución** para crear una entidad de búsqueda para comparar con identidades en la base de datos de entidades.

Código de origen de datos - Descripción
Seleccione un código de origen de datos y descripción a asociar con las identidades encontradas por el proceso Buscar por resolución.

Puntuación mínima de resolución
Seleccione la puntuación mínima de resolución a utilizar al comparar identidades con los criterios especificados para la consulta Buscar por resolución.

La puntuación que seleccione determina el número y tipo de resultados que la consulta devuelve.

Sección de criterios de Buscar por resolución
Especifique los atributos para crear la entidad de búsqueda que se compara con identidades de la base de datos de entidades. El sistema devuelve identidades de acuerdo con la puntuación mínima de resolución que haya especificado.

Lista de nombres
Entre los criterios de nombres en los campos de lista de nombres, si está buscando un nombre específico. Si entra cualquiera de los campos de nombres, **Apellido** será necesario.

Lista de direcciones
Entre los criterios de direcciones en los campos de lista de direcciones, si está buscando una dirección específica. Si entra cualquiera de los campos de direcciones, **Calle** será necesario.

Lista de números
Entre los criterios de números específicos, por ejemplo un número de pasaporte o un número de tarjeta de crédito, en los campos de lista de números. Tanto **Tipo** como **Valor** son necesarios.

Lista de características
Entre los criterios de características específicos, por ejemplo sexo o fecha de nacimiento, en los campos de características. Tanto **Tipo** como **Valor** son necesarios.

Lista de correo electrónico
Entre los criterios de direcciones de correo electrónico específicos

en los campos de lista de direcciones de correo electrónico. Tanto **Tipo** como **Dirección** son necesarios.

Ventana Gestor de Generador de alertas de atributos:

Utilice esta ventana para ver y gestionar sus generadores de alertas de atributo activos actualmente. La ventana **Gestor de Generador de alertas de atributos** no visualiza generadores de alertas de atributo caducados.

Fecha de caducidad
Visualiza la fecha en que caduca el generador de alertas de atributo.

Fecha de creación
Visualiza la fecha en que se creó el generador de alertas de atributo.

ID de entidad
El ID de entidad de la entidad de búsqueda creada por los criterios del generador de alertas de atributos.

Razón El código de razón asignado durante el proceso de creación del generador de alertas de atributo.

Puntuación mínima de resolución
Visualiza la puntuación mínima de resolución que las entidades deben alcanzar al comparar los criterios de alerta de atributo con las entidades existentes en la base de datos de entidades antes de que se genere una alerta de atributo para esa entidad.

Número de caso
Visualiza el número de caso asignado durante el proceso de creación del generador de alertas de atributo.

Botón Crear
Visualiza la ventana **Crear Generador de alertas de atributos**, para que pueda crear un generador de alertas de atributo.

Botón Editar
Visualiza la ventana **Información del Generador de alertas de atributos**, para que pueda editar el generador de alertas de atributo seleccionado. (Seleccione el generador de alertas de atributo y luego pulse este botón.)

Ventana Crear Generador de alertas de atributo:

Utilice esta ventana para crear un generador de alertas de atributo, que utiliza criterios de atributo especificados para la búsqueda persistente en la base de datos de entidades de las entidades que tengan datos de atributo coincidentes.

Código de origen de datos - Descripción
Seleccione un código de origen de datos y descripción de la lista desplegable para asociarlos con alertas de atributo creadas desde este generador de alertas de atributo. La selección predeterminada suele ser "Buscar".

Puntuación mínima de resolución
Seleccione la puntuación mínima de resolución de la lista desplegable para utilizarla al comparar identidades con los criterios especificados para el generador de alertas de atributo.

Código de razón
Seleccione un código de razón de la lista desplegable para asociarlo con este generador de alertas de atributo.

Número de caso
Especifique un número de caso opcional para las alertas de atributo creadas desde este generador de alertas de atributo.

Comentario
Especifique un comentario opcional para las alertas de atributo creadas desde este generador de alertas de atributo.

Fecha de caducidad
Seleccione la fecha en que caduca este generador de alertas de atributo o pulse el icono de calendario y seleccione una fecha utilizando el control del calendario. La fecha de caducidad toma como valor predeterminado seis meses a partir de hoy. Debido a que los generadores de alertas de atributo siempre se ejecutan en segundo plano, es recomendable establecer una fecha de caducidad.

Sección Criterios de atributo
Especifique los atributos que desee que generen una alerta de atributo siempre que el sistema procese un registro de identidad que contenga los atributos especificados.

Lista de nombres
Si está buscando un nombre específico, entre los criterios de nombres en los campos de lista de nombres.

Lista de direcciones
Si está buscando una dirección específica, entre los criterios de direcciones en los campos de lista de direcciones.

Lista de números
Si está buscando un número específico, por ejemplo un número de pasaporte o un número de tarjeta de crédito, entre los criterios de números en los campos de lista de números.

Lista de características
Si está buscando una característica específica, por ejemplo sexo o fecha de nacimiento, entre los criterios de características en los campos de lista de características.

Lista de correo electrónico
Si está buscando una dirección de correo electrónico específica, entre los criterios de direcciones de correo electrónico en los campos de lista de direcciones de correo electrónico.

Ventana de información de Generador de alertas de atributo:

Utilice esta ventana para editar un generador de alertas de atributo existente. Solo puede cambiar el número de caso, la fecha de caducidad y los comentarios.

Código de razón
(Solo visualización) Visualiza el código de razón seleccionado para este generador de alertas de atributo.

Número de caso
Visualiza el número de caso alfanumérico opcional, especificado por el usuario que ha creado el generador de alertas de atributo.

Comentario
Visualiza los comentarios especificados por el usuario que ha creado el generador de alertas de atributo.

Fecha de caducidad
Visualiza la fecha de caducidad actual para el generador de alertas de atributo.

Nombres utilizados
(Solo visualización) Si se ha especificado información de nombres como criterios para este generador de alertas de atributo, esta sección lista toda la información de nombres especificada por el usuario que ha creado el generador de alertas de atributo.

Dirección
(Solo visualización) Si se ha especificado información de direcciones como criterios para este generador de alertas de atributo, esta sección lista toda la información de direcciones especificada por el usuario que ha creado el generador de alertas de atributo.

Números
(Solo visualización) Si se ha especificado información de números como criterios para este generador de alertas de atributo, esta sección lista toda la información de números especificada por el usuario que ha creado el generador de alertas de atributo.

Otros atributos
(Solo visualización) Si se ha especificado información de características como criterios para este generador de alertas de atributo, esta sección lista toda la información de características especificada por el usuario que ha creado el generador de alertas de atributo.

Botón Actualizar
Pulse el botón para aplicar los cambios.

Análisis de entidades

Puede utilizar el Visualizador para revisar, analizar y crear gráficos de entidades de la base de datos de entidades que utilicen el Visualizador.

Entidades

Una entidad es una colección de una o varias entidades que representan la misma persona, organización, lugar o elemento. Las entidades se guardan en la base de datos de entidades.

Aunque las entidades suelen identificarse con personas, también pueden ser cosas, como empresas o vehículos. De hecho, puede utilizar la configuración extensible del sistema para correlacionar los datos de la organización y crear cualquier tipo de entidad que desee resolver o relacionar.

Las entidades suelen estar compuestas de identidades que provienen de distintos sistemas origen. La resolución de entidades determina qué identidades son realmente la misma entidad y crea una entidad compuesta que contiene todas las identidades asociadas a dicha entidad compuesta. El sistema mantiene una atribución completa de registros, que identifican el origen asociado a cada identidad de la entidad compuesta.

Puede configurar el sistema de modo que resuelva y relacione entidades de forma que se ajuste a los objetivos de la organización.

Resúmenes de entidades

Un resumen de entidades es una recopilación unificada de toda la información de la base de datos de entidades sobre una entidad específica.

Las entidades se organizan dentro de la base de datos de entidades mediante los ID de entidad. Cada ID de entidad tiene su propio resumen de entidad.

Utilice el Visualizador para ver resúmenes de entidades. Los resúmenes de entidades pueden contener los siguientes tipos de información:

- Referencias a documentos origen
- Roles
- Nombres utilizados
- Direcciones
- Números
- Características
- Divulgaciones
- Entidades relacionadas
- Historial de alertas de rol
- Historial de alertas de sucesos
- Direcciones de correo electrónico

Visualización de resúmenes de entidades

Para ver toda la información acerca de una entidad específica de la base de datos de entidades, vea el resumen de entidad.

Acerca de esta tarea

Puede acceder a un resumen de entidad desde cualquiera de las siguientes ubicaciones del Visualizador:

- Cualquier ventana de detalles de alerta
- Cualquier ventana de gráfico
- Cualquier ventana **Buscar por:**

Procedimiento

- Desde una ventana **Detalle de alerta de rol** una ventana **Detalle de alerta de atributo** o una ventana **Detalle de alerta de suceso**, pulse **Resumen de entidad**.
- Desde un gráfico de entidad, pulse con el botón derecho del ratón en el icono **Entidad** que contiene el ID de entidad cuya información desea ver y seleccione **Resumen de entidad**.
- Desde la sección **Resultados** de una ventana **Buscar por:**, pulse dos veces en la fila que contiene la entidad cuyo resumen desea ver.

Impresión de resúmenes de entidades

Si desea una copia impresa de un resumen de entidad, si desea una versión en PDF de un resumen de entidad, o si desea copiar la información de resumen de entidad en otra aplicación como un procesador de la palabra o una hoja de cálculo, hay varias maneras de imprimir un resumen de entidad.

Procedimiento

- Para imprimir una instantánea de la ventana **Resumen de entidad**, haga lo siguiente:
  1. En la ventana **Resumen de entidad**, pulse **Imprimir**.
  2. Desde el diálogo de impresión, especifique los valores de impresión.
  3. Pulse **Aceptar**.

- Para imprimir el resumen de entidad en un archivo PDF, en la ventana **Resumen de entidad**, pulse **Informe**.
- Para copiar (imprimir) la información de resumen de entidad para pegarla en otra aplicación, haga lo siguiente:
  1. En la ventana **Resumen de entidad**, en el menú **Editar**, seleccione **Copiar pantalla en el área común**.

     Nota: La combinación de teclas **Control** + **C** sólo copia valores de un solo campo.
  2. Pegue el contenido del área común en la aplicación a utilizar.
  3. Utilice la característica de impresión de la aplicación para imprimir la información de resumen de la entidad.

Impresión de la ventana actual

Puede imprimir cualquier ventana del Visualizador, incluyendo gráficos y resúmenes de entidades, directamente desde esa ventana utilizando el mandato de impresión.

Procedimiento

1. En el Visualizador, desde la ventana que desea imprimir, seleccione **Imprimir** en el menú **Archivo**.
2. En el diálogo **Imprimir**, especifique los valores de impresión.
3. Pulse **Aceptar**.

Visualización de gráficos de entidades

Una de las ventajas principales del Visualizador es que puede crear gráficos de la información de alerta de rol y relación de entidades. Los gráficos proporcionan una representación visual de la información acerca de la entidad seleccionada.

Acerca de esta tarea

Puede acceder a un gráfico de entidad desde cualquiera de las siguientes ubicaciones del Visualizador:

- Ventana **Resumen de entidad**
- Ventana **Gráfico**
- Ventana **Detalle de alerta de suceso**

Procedimiento

- Desde una ventana **Resumen de entidad**, pulse **Gráfico**.
- Desde una ventana **Gráfico**, pulse con el botón derecho del ratón en el icono **Entidad** que contiene el ID de entidad cuya información desea ver, y seleccione **Mostrar gráfico de entidad**. Para ver el resumen de una entidad en un gráfico, pulse con el botón derecho del ratón en la entidad y seleccione **Resumen de entidad**.
- Desde una ventana **Detalle de alerta de suceso**, pulse **Gráfico**.
- Opcional: Para cambiar la manera en que se visualiza la información en un gráfico, pulse con el botón derecho del ratón en cualquier espacio en blanco dentro del gráfico y después:
  1. Seleccione un valor de **Diseño del gráfico** diferente para cambiar la organización visual de la información en el gráfico.
  2. Seleccione un valor de **Aumentar/Disminuir** para cambiar el nivel de aumento/disminución actual.

Cada vez que cambia los valores del gráfico, se utilizan los nuevos valores como valores predeterminados para cada gráfico adicional que visualice durante la sesión del Visualizador actual.

Visualización de gráficos de alertas de rol

Si desea ver una representación gráfica de cómo se relacionan las entidades que se han identificado en una alerta de rol, puede ver un gráfico de alerta de rol.

Procedimiento

1. En el Visualizador, en la ventana **Resumen de alerta**, pulse dos veces en la alerta de rol.
2. En la pantalla **Detalle de alerta de rol**, pulse **Gráfico**.
3. Opcional: Para cambiar la manera en que se visualiza la información en un gráfico, pulse con el botón derecho del ratón en cualquier espacio en blanco dentro del gráfico y después:
   a. Seleccione un valor de **Diseño del gráfico** diferente para cambiar la organización visual de la información en el gráfico.
   b. Seleccione un valor de **Aumentar/Disminuir** para cambiar el nivel de aumento/disminución actual.

   Cada vez que cambia los valores del gráfico, se utilizan los nuevos valores como valores por omisión para cada gráfico adicional que visualice durante la sesión del Visualizador actual.
4. Opcional: Para ver el resumen de una entidad en un gráfico, pulse con el botón derecho del ratón en la entidad y seleccione **Resumen de entidad**.

Personalizar iconos de gráficos

Todos los gráficos del Visualizador utilizan iconos predefinidos para representar entidades y los tipos de atributos, tales como direcciones y números. Puede personalizar los iconos que se visualizan en gráficos del Visualizador o especificar un icono a utilizar para un tipo de atributo nuevo.

Antes de empezar

Tenga en cuenta las siguientes restricciones antes de personalizar iconos de gráficos del Visualizador:

- Los iconos personalizados residen en el servidor de aplicaciones. Solo los usuarios con privilegios de administración para el servidor de aplicaciones pueden añadir o cambiar iconos de gráficos personalizados. Todos los clientes del Visualizador con base en ese servidor de aplicaciones utilizan el mismo juego de iconos, por lo que el cambio que realice afecta a qué iconos se visualizan en gráficos del Visualizador para cada uno de esos clientes.
- Guarde los iconos personalizados en una carpeta de iconos aparte en el servidor de aplicaciones. La instalación de un nuevo archivo *.EAR para el Visualizador elimina todos los iconos de gráficos personalizados. Después de instalar un archivo *.EAR nuevo del Visualizador, puede copiar los iconos de gráficos personalizados desde la carpeta de iconos a la carpeta de iconos del servidor de aplicaciones designada.
- Los iconos deben tener formato .GIF. El tamaño recomendado para la imagen es de 24 x 24 píxeles.
- Los nombres de los iconos deben coincidir con su tipo de atributo correspondiente, solo en minúsculas. Por ejemplo, si añade un nuevo tipo de atributo denominado "Foto de prueba", el archivo debe denominarse "foto de prueba.gif" para que el Visualizador reconozca la foto de prueba personalizada.

Observe que en este ejemplo, tanto el nombre de tipo de atributo como el nombre del archivo de icono contienen espacios.

Acerca de esta tarea

Los archivos de imagen de iconos predeterminados del Visualizador se almacenan en el servidor de aplicaciones, normalmente en una carpeta denominada `imágenes`.

Procedimiento

1. Detenga el servidor de aplicaciones.
2. En el servidor de aplicaciones, busque la carpeta de iconos de gráficos predeterminados del Visualizador. Normalmente, esta carpeta está ubicada en *la vía de acceso de instalación del servidor de aplicaciones IBM Infosphere Identity Insight*/ `was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images`.
3. Necesario: Cree una carpeta denominada `graph` bajo la carpeta de iconos de gráficos predeterminados del Visualizador (la carpeta `/images`) para sus archivos de imagen de iconos de gráficos personalizados.

   Nota: El nombre de la carpeta debe ser `graph`.
4. Guarde, copie o mueva cada archivo de imagen de iconos a la nueva carpeta.

Ejemplo

Si ha creado un tipo de atributo denominado `ARCHIVO_HUELLAS` y desea un icono de gráfico personalizado para representar a ese tipo de atributo en los gráficos del Visualizador, siga estos pasos:

1. Cree u obtenga un archivo de imagen .GIF adecuado que sea de 24 x 24 píxeles para representar el tipo de atributo `ARCHIVO_HUELLAS`. Asegúrese de que el nombre del archivo de imagen coincide con el nombre del tipo de atributo y que utiliza solo minúsculas, como este nombre de archivo: `archivo_huellas.gif`
2. En el servidor de aplicaciones de IBM InfoSphere Identity Insight, localice la carpeta `images`. Para este ejemplo, la carpeta de imágenes está ubicada aquí: `IBM-II_install/ was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images`.
3. Bajo la carpeta de imágenes, cree una carpeta denominada `graph`. De este modo, la vía de acceso al archivo tiene este aspecto: `IBM-II_install/ was_apps/ibm-is-ii-visualizer.ear/eas-visualizer-client.war/images/graph`
4. Copie el icono de imagen `archivo_huellas.gif` a la carpeta `graph`.

Qué hacer a continuación

Reinicie el servidor de aplicaciones.

Temas de ayuda

Pantalla Resumen de entidad:

Utilice esta pantalla para revisar en detalle toda la información conocida sobre una entidad, incluidos los atributos de las identidades asociadas con la entidad, todas las entidades relacionadas, y el historial de todas las alertas asociadas con la entidad.

Utilice los giros para expandir o contraer las secciones de la pantalla para ayudarle a centrarse en un detalle específico.

Información de origen de datos
Muestra las orígenes de datos que han proporcionado registros de identidad que se han resuelto en esta entidad. Pulse un origen de datos para resaltar los atributos que forman el registro de identidad que se procesó desde este origen de datos. La información de origen de datos le ayuda a rastrear el registro de identidad hasta su origen original.

Cuando las entidades tienen varias identidades, el resaltado puede ayudarle a distinguir una identidad de otra y el origen de datos original donde reside esa identidad.

Roles Visualiza los roles asignados a las identidades que se han resuelto en esta entidad.

Nombres
Visualiza los nombres utilizados por las identidades que se han resuelto en esta entidad.

Direcciones
Visualiza las direcciones conocidas utilizadas por las identidades que se han resuelto en esta entidad, incluido el rango de fechas en que cada dirección era válida para la identidad (si esa información está disponible).

Números
Visualiza los números conocidos utilizados por las identidades que se han resuelto en esta entidad, incluido el rango de fechas en que cada número era válido para la identidad (si esa información está disponible).

Características
Visualiza las características conocidas utilizadas por las identidades que se han resuelto en esta entidad, incluido el rango de fechas en que cada característica era válida para la identidad (si esa información está disponible).

Direcciones de correo electrónico
Visualiza las direcciones de correo electrónico conocidas utilizadas por las identidades que se han resuelto en esta entidad, incluido el rango de fechas en que cada dirección de correo electrónico era válida para la identidad (si esa información está disponible).

Divulgaciones
Visualiza relaciones divulgadas que un analista o un usuario autorizado del Visualizador añadió de manera explícita para enlazar dos identidades. Las divulgaciones crean una relación con una fuerza del 100% entre dos identidades.

Entidades relacionadas
Lista información básica sobre otras entidades que están relacionadas con esta entidad. Seleccione una entidad relacionada para resaltar la información que creó la relación.

Historial de alertas de rol
Lista información básica sobre las alertas de rol que están asociadas con esta entidad.

Historial de alertas de sucesos
Visualiza información sobre las alertas de sucesos que están asociadas con esta entidad.

Botón Imprimir
Abre el diálogo de impresión para que pueda imprimir el resumen de entidad.

Botón Informe
Genera un informe **Resumen de entidad**, que contiene toda la información del resumen de entidad.

Pantalla Gráfico de relaciones de entidad:

Utilice esta pantalla para ver una representación visual de detalles de relaciones para la entidad seleccionada, incluidos atributos de entidad, entidades relacionadas y sucesos de entidad.

Área de gráfico (Lienzo)

El cuerpo del gráfico es conocido como el lienzo. Contiene la representación gráfica de las relaciones y le muestra qué atributos enlazan las entidades.

Pulse en los objetos (nodos) en el gráfico para volver a posicionarlos en el gráfico. Si existe un atributo de hiperenlace, utilice **Control** + **pulsación** para seguir el enlace.

Opciones de menú del botón derecho

Diseño del gráfico
Cambia el diseño actual y la posición de los nodos del gráfico. Se hace referencia a cada objeto del gráfico como un nodo

Experimente con los valores de diseño del gráfico hasta que encuentre el valor que le satisfaga. Estos valores son puramente subjetivos respecto a sus gustos y necesidades al revisar las relaciones de entidades en este gráfico.

Templar
Seleccione este valor para distribuir los nodos de manera uniforme. El valor de templar hace que las longitudes de los bordes del gráfico sean uniformes, minimiza los cruces de líneas, y evita que los nodos se acerquen demasiado al borde del gráfico.

Jerárquico
Seleccione este valor para visualizar los nodos según la jerarquía. El valor jerárquico funciona mejor en gráficos dirigidos que tienen un flujo global, o gráficos que tienen algunos puntos de inicio, algunos puntos finales, y flujo global entre esos puntos.

Orgánico
Seleccione este valor para distribuir los vértices del gráfico de forma uniforme. El valor orgánico hace que las longitudes de los bordes sean uniformes y refleja la simetría del gráfico, pero no le permite mostrar entidades relacionadas.

Auto-organizativo
Seleccione este valor para crear clústeres espaciados de forma uniforme a partir de los nodos del gráfico enlazados.

Al azar
Seleccione este valor para esparcir nodos de gráfico de forma aleatoria.

Inclinar
Seleccione este valor para desplazar o inclinar la colocación del nodo de gráfico del diseño de gráfico seleccionado anteriormente.

Trazar círculo
Seleccione este valor para organizar los nodos del gráfico en un círculo con un espaciando uniforme entre los nodos del gráfico que están alrededor.

Aumentar/Disminuir
Seleccione un valor para cambiar el tamaño de visualización del lienzo dentro del tamaño de pantalla actual.

75% Muestra el gráfico al 75% de su tamaño original.

50% Muestra el gráfico al 50% de su tamaño original.

Mostrar todos los atributos
Muestra todos los atributos asignados a esa entidad.

Ocultar atributo
Oculta el atributo seleccionado.

Mostrar las entidades relacionadas
Muestra todas las entidades relacionadas con dicha entidad, así como una representación gráfica del modo en que estas entidades se relacionan. Esta opción no está disponible si el valor de Diseño de gráfico actual es **Orgánico**.

Resumen de entidad
Abre la ventana Resumen de entidad y muestra un resumen detallado de toda la información conocida sobre dicha entidad.

Sucesos de entidad
Abre la pantalla Sucesos de entidad y visualiza información sobre los sucesos que está asociados con la entidad. Esta acción sólo está disponible si la entidad seleccionada tiene sucesos asociados.

Mostrar el gráfico de entidad
Abre la ventana Gráfico de entidad y muestra una representación visual de información sólo sobre dicha entidad

Opciones de Ajustar gráfico

Graduador de aumentar/disminuir
Mueva el indicador de aumentar/disminuir para redimensionar el lienzo.

Restricción de diseño
Seleccione una restricción de límites de diseño para el tamaño del lienzo.

Tabla de propiedades

Seleccione un nodo del gráfico, y esta tabla proporcionará las propiedades del nodo seleccionado: Atributos o entidades.

Pantalla Gráfico de alertas de rol:

Utilice esta pantalla para ver una representación visual de detalles de alerta de rol para la entidad seleccionada, incluidos atributos de entidad, entidades relacionadas y sucesos de entidad.

Área de gráfico (Lienzo)

El cuerpo del gráfico es conocido como el lienzo. Contiene la representación gráfica de los detalles de la alerta de rol.

Pulse en los objetos (nodos) en el gráfico para volver a posicionarlos en el gráfico. Si existe un atributo de hiperenlace, utilice **Control** + **pulsación** para seguir el enlace.

Opciones de menú del botón derecho

El menú del botón derecho del ratón le ofrece control sobre la visualización del gráfico y proporciona opciones para navegar a ventanas de entidades relacionadas.

Diseño del gráfico
Cambia el diseño actual y la posición de los nodos del gráfico. Se hace referencia a cada objeto del gráfico como un nodo

Experimente con los valores de diseño del gráfico hasta que encuentre el valor que le satisfaga. Estos valores son puramente subjetivos respecto a sus gustos y necesidades al revisar las alertas de rol en este gráfico.

Templar
Seleccione este valor para distribuir los nodos de manera uniforme. El valor de templar hace que las longitudes de los bordes del gráfico sean uniformes, minimiza los cruces de líneas, y evita que los nodos se acerquen demasiado al borde del gráfico.

Jerárquico
Seleccione este valor para visualizar los nodos según la jerarquía. El valor jerárquico funciona mejor en gráficos dirigidos que tienen un flujo global, o gráficos que tienen algunos puntos de inicio, algunos puntos finales, y flujo global entre esos puntos.

Orgánico
Seleccione este valor para distribuir los vértices del gráfico de forma uniforme. El valor orgánico hace que las longitudes de los bordes sean uniformes y refleja la simetría del gráfico, pero no le permite mostrar entidades relacionadas.

Auto-organizativo
Seleccione este valor para crear clústeres espaciados de forma uniforme a partir de los nodos del gráfico enlazados.

Al azar
Seleccione este valor para esparcir nodos de gráfico de forma aleatoria.

Inclinar
Seleccione este valor para desplazar o inclinar la colocación del nodo de gráfico del diseño de gráfico seleccionado anteriormente.

Trazar círculo
Seleccione este valor para organizar los nodos del gráfico en un círculo con un espaciando uniforme entre los nodos del gráfico que están alrededor.

Aumentar/Disminuir
Seleccione un valor para cambiar el tamaño de visualización del lienzo dentro del tamaño de pantalla actual.

75% Muestra el gráfico al 75% de su tamaño original.

50% Muestra el gráfico al 50% de su tamaño original.

Mostrar todos los atributos
Muestra todos los atributos asignados a esa entidad.

Ocultar atributo
Oculta el atributo seleccionado.

Mostrar las entidades relacionadas
Muestra todas las entidades relacionadas con dicha entidad, así como una representación gráfica del modo en que estas entidades se relacionan. Esta opción no está disponible si el valor de Diseño de gráfico actual es **Orgánico**.

Resumen de entidad
Abre la ventana Resumen de entidad y muestra un resumen detallado de toda la información conocida sobre dicha entidad.

Sucesos de entidad
Abre la pantalla Sucesos de entidad y visualiza información sobre los sucesos que está asociados con la entidad. Esta acción sólo está disponible si la entidad seleccionada tiene sucesos asociados.

Mostrar el gráfico de entidad
Abre la ventana Gráfico de entidad y muestra una representación visual de información sólo sobre dicha entidad

Opciones de Ajustar gráfico

Graduador de aumentar/disminuir
Mueva el indicador de aumentar/disminuir para redimensionar el lienzo.

Restricción de diseño
Seleccione una restricción de límites de diseño para el tamaño del lienzo.

Tabla de propiedades

Seleccione un nodo del gráfico, y esta tabla proporcionará las propiedades del nodo seleccionado: Atributos o entidades.

Adición de datos utilizando el visualizador

Normalmente, el archivo de datos UMF carga los datos de entidad en modalidad de proceso por lotes o mediante procesos en tiempo real en las interconexiones. Esta acción la realizan los operadores del sistema. No obstante, los usuarios del visualizador pueden utilizarlo para añadir manualmente una entidad única, revelar una relación entre dos entidades (por identidad), cargar y procesar un archivo de datos UMF o validar un archivo de datos UMF antes de cargarlo.

Antes de empezar

Para la adición de datos siempre es necesaria una interconexión en ejecución disponible para procesar los datos. Pero los usuarios del visualizador no tienen que iniciar ni ejecutar su propia interconexión. Cuando el visualizador añade los datos, este envía automáticamente los datos a través de una interconexión del visualizador designada.

Adición de una sola entidad

Puede añadir una sola entidad a la base de datos de entidades, sin crear manualmente un registro UMF. Puede crear una entidad sólo con información sobre el nombre, pero debe introducir toda la información que tenga sobre ella

(direcciones conocidas, números, características o direcciones de correo electrónico), para obtener una resolución de entidad y de relación óptimas.

Procedimiento

1. En el visualizador, realice una de las acciones siguientes:
   a. Pulse **Ver** > **Añadir** > **Entidad**.
   b. En la barra de herramientas, pulse el icono (añadir) y seleccione **Entidad**.
   c. En la barra de herramientas, pulse la flecha y seleccione **Entidad**.
   d. En la ventana **Añadir**, en el menú desplegable **Añadir**, seleccione **Entidad**.
2. Utilice las listas desplegables y campos para especificar la información de la entidad. A medida que introduzca los datos, la pantalla le guiará destacando los campos necesarios en amarillo. Un campo destacado en amarillo indica que, basándose en las otras selecciones de la pantalla, debe entrar los datos.
   - Campo de **referencia**: debe entrar información en este campo. La información de referencia es un identificador para la entidad. Por ejemplo, entre el número de cuenta del origen de datos, como por ejemplo la cuenta bancaria.
   - Campos de nombre: si introduce una parte del nombre (nombre de pila, segundo nombre o generación), será necesario el apellido.
   - Campos de dirección: puede añadir información en el campo **Dirección** sin introducir la localidad, la provincia, el código postal o el país. Sin embargo, debe introducir información en el campo **Dirección** si introduce cualquier otra parte de la dirección.
   - Campos de número, característica o correo electrónico: si desea introducir información sobre cualquiera de estos atributos, debe seleccionar un tipo e introducir un valor para el atributo.

   Atención: Toda la información introducida en esta pantalla formará parte de la entidad que añada. No indique relaciones con otras entidades o características y números compartidos. Sólo debe introducir información sobre la entidad que se esté editando, como por ejemplo los alias u otros nombres asociados con la entidad; así como direcciones, números, características y direcciones de correo electrónico asociados con la entidad.
3. Pulse **Enviar**.

Resultados

El visualizador crea un registro de identidades UMF que incluye toda la información introducida para dicha entidad y envía el registro a una interconexión, donde se procesa para la resolución de entidad y relación y se añade a la base de datos de entidades.

Carga de datos de un archivo

Utilice la característica **Carga de archivo** en el Visualizador para cargar datos para múltiples identidades que están definidas en un archivo UMF. **Carga de archivo** solo cargará los registros `<UMF_ENTITY>`. Al seleccionar un archivo UMF, el sistema abre el archivo, carga los datos en la interconexión y, a continuación, la interconexión procesa las identidades del archivo, lo que las añade a la base de datos de entidades y resuelve cualquier entidad y relaciones identificadas. Se generan alertas basándose en las normas que se han configurado.

Acerca de esta tarea

La resolución de entidades y relaciones se produce en el componente de interconexión. Para cargar y procesar archivos UMF mediante el Visualizador, debe haber una interconexión en ejecución y disponible para comunicarse con el servidor del Visualizador.

Antes de cargar un archivo, puede interesarle validar el UMF en el archivo, para asegurarse de que no hay errores en el archivo.

Procedimiento

1. En el Visualizador, realice una de las acciones siguientes:
   a. Pulse **Ver** > **UMF** > **Carga de archivo**.
   b. En la barra de herramientas, pulse el icono (UMF).
   c. Desde la ventana **UMF**, en el campo desplegable **UMF**, seleccione **Carga de archivo**.
2. Pulse **Cargar archivo...** para seleccionar el archivo UMF a cargar, y luego pulse **Abrir**. El sistema carga el archivo seleccionado en la interconexión, y ésta empieza a procesar los datos del archivo. La **Barra de progreso del archivo** le muestra el tiempo transcurrido durante el proceso, el número de registros procesados, y el estado de la carga de archivo.
   a. Para detener la carga del archivo y el proceso, pulse el botón de icono (Detener).
   b. Para pausar la carga del archivo y el proceso, pulse el botón de icono (Pausar).
   c. Para reanudar la carga y proceso del archivo después de pausar, pulse el botón de icono (Continuar).

   A medida que se cargan los datos del archivo, una interconexión procesa los datos mediante la resolución de entidades y relaciones. Si ve un error, póngase en contacto con el administrador del sistema. El error es probablemente un problema de la interconexión.

   Se añaden nuevas identidades a la base de datos, junto con entidades y relaciones resueltas. El sistema genera alertas relacionadas con los datos, basándose en las normas del sistema configuradas.
3. Opcional: Una vez el archivo se ha cargado y procesado, pulse **Ver resultados** para visualizar el diálogo **Resultados de la carga de archivo**, que incluye la siguiente información:
   - El número de registros enviados a la interconexión.
   - El número de entidades nuevas creadas en la base de datos de entidades, de acuerdo con los datos del archivo que ha cargado.
   - El número de excepciones de UMF que la interconexión ha encontrado al procesar los datos de este archivo. (Este número puede indicar errores en el archivo UMF o problemas en la sintaxis que impiden que la interconexión procese los datos en su totalidad.)

Qué hacer a continuación

Si el diálogo **Resultados de la carga de archivo** indica que ha habido alguna excepción UMF en el archivo que ha cargado, valide el archivo, utilizando la característica Validación de archivos UMF como ayuda para buscar los errores en el archivo y poder corregirlos. Una vez corregidos los errores, vuelva a cargar los

datos que contenían los errores, de forma que la interconexión puede procesar los datos en su totalidad.

Validación de un archivo UMF antes de cargar los datos

Si tiene intención de utilizar el Visualizador para cargar y procesar registros de archivos UMF pequeños, puede interesarle validar los datos del archivo primero.

Acerca de esta tarea

El proceso de validación comprueba si los datos cumplen los requisitos mínimos para el proceso de la resolución de entidades y relaciones. El proceso de validación también proporciona información de utilidad sobre áreas del archivo a revisar o corregir antes de cargar y procesar los datos. Cuanto mejor sea la calidad de los datos que entren en el sistema, mejores serán los resultados.

Procedimiento

1. En el Visualizador, realice una de las acciones siguientes:
   - Pulse **Ver** > **UMF** > **Archivo de validación UMF**.
   - En la barra de herramientas, pulse la flecha a la derecha del icono y pulse **Archivo de validación UMF**.
   - Desde la ventana **UMF**, en la lista **UMF**, seleccione **Archivo de validación UMF**.
2. Pulse **Validar archivo...**.
3. Elija el archivo UMF a validar.

   Nota: Si ya ha validado uno o más archivos UMF y ha mantenido abierta la ventana **UMF**, los campos **Archivo a validar** y **Archivo de error/aviso** contendrán los valores de la última validación de archivo UMF.
4. Opcional: Para cambiar la vía de acceso al directorio o el nombre de archivo del archivo de registro del proceso de validación en la ventana **Configuración de validación UMF**, elija una de las siguientes acciones:
   - Seleccione el directorio y nombre de archivo a utilizar, pulse **Examinar...**, y luego pulse **Abrir**.
   - Escriba la vía de acceso completa y el nombre de archivo del archivo de registro de errores y avisos de validación. Puede escribir el nombre de un archivo de registro existente o el nombre de un archivo de registro nuevo.

   Nota: Si valida más de un archivo UMF y mantiene la ventana **UMF** abierta, observe que el valor de archivo de registro en la ventana **Configuración de validación UMF** toma la misma vía de acceso y el mismo nombre de archivo que el último archivo de registro de errores y avisos de validación. Al cerrar la ventana **UMF** se borran los campos de vía de acceso y archivo de registro.
5. Pulse **Validar archivo UMF** para iniciar el proceso de validación. Mientras se ejecuta el proceso de validación, se visualizan estadísticas de validación, incluida información dinámica sobre el porcentaje completado, el tiempo transcurrido, el número de registros procesados, y el estado del proceso. Puede pausar o detener el proceso de validación en cualquier momento.
6. Opcional: Al pulsar **Validar archivo UMF**, si existe otro archivo de registro de validación con la misma ubicación y nombre que el que ha tecleado en el paso 4, el sistema muestra un mensaje informativo. El mensaje incluye el nombre y la ubicación del archivo. Lleve a cabo una de las siguientes acciones:
   - Pulse **Sí** para utilizar el mismo archivo de registro de errores y avisos de validación. Esta opción sobrescribe el archivo de registro anterior.

- Pulse **No** para crear o utilizar un archivo de registro de errores/avisos de validación distinto. El sistema le devuelve a la ventana **Configuración de validación UMF** para que pueda cambiar manualmente la vía de acceso y el nombre de archivo del archivo de registro de errores y avisos de validación.

7. Cuando se haya completado el proceso de validación, pulse **Ver resultados** si desea ver un resumen de los resultados.

Qué hacer a continuación

Utilice la información de la ventana **Vista de resultados de la validación UMF** para ver los resultados y la información del archivo de registro de errores y avisos.

Divulgación de relaciones entre identidades

Si determina que tiene datos que enlazan dos identidades (o cuentas), puede especificar ese enlace para divulgar la relación utilizando el Visualizador.

Procedimiento

1. En el visualizador, realice una de las acciones siguientes:
   a. Pulse **Ver** > **Añadir** > **Divulgación**.
   b. En la barra de herramientas, pulse la flecha a la derecha del icono (añadir) y seleccione **Divulgación**.
   c. En la ventana **Añadir**, en el desplegable **Añadir**, seleccione **Divulgación**.
2. Necesario: En los campos **ID de entidad**, entre los números de ID de entidad de las entidades que contienen las identidades a relacionar.
3. Necesario: Pulse **Búsqueda** para cada ID de entidad para recuperar sus identidades asociadas. Revise la lista de identidades recuperadas para asegurarse de que ha entrado el ID de entidad deseado.
4. Seleccione, para cada entidad, el botón de opción de la identidad (o cuenta de origen de datos) para la que va a divulgar una relación.
5. En **Descripción de la relación divulgada**, especifique una descripción de cómo están relacionadas las identidades.
6. Pulse **Crear**. Se visualizará un recuadro de confirmación verificando que la relación divulgada se ha creado satisfactoriamente.

Temas de ayuda

Ventana Añadir entidad:

Utilice esta ventana para añadir una sola identidad nueva a la base de datos de entidades mediante el Visualizador. Toda la información que entre en esta pantalla pasa a ser atributos de la identidad recién creada. (Las identidades se crean de una en una.) Después de someter los datos que ha entrado para la identidad, el sistema procesa los datos a través de la interconexión para la resolución de entidad y relación, durante lo cual la identidad puede asociarse con una o varias entidades existentes.

Código de origen de datos - Descripción

Seleccione el origen de datos a asociar con la identidad que está añadiendo. El origen de datos debe existir en el sistema. (No puede añadir un origen de datos nuevo aquí. Si no ve el código de origen de datos y la descripción que desea utilizar, póngase en contacto con el administrador del sistema para que cree el origen de datos.)

Para añadir una identidad, el código de origen de datos y la descripción son necesarios.

Referencia

Especifique un identificador para esta cuenta de origen de datos, que se utiliza para asociar la cuenta con la identidad que está especificando. (Algunos ejemplos de números de referencia son los números de caso, los números de cuenta bancaria o los números de recompensa al cliente.)

Para añadir una identidad, la referencia es necesaria

Lista de nombres

Especifique los nombres a asociar con la identidad que está añadiendo. Para añadir una identidad, la información de nombres (al menos nombre y apellido) es necesaria. Puede indicar que la identidad que está añadiendo tiene más de un nombre entrando cada nombre para la identidad en una línea aparte. Por ejemplo, si conoce el nombre apropiado para la identidad, así como uno o varios alias ("conocido también como"), puede entrarlos todos en esta pantalla.

Nota: Asegúrese de que solo entra un nombre por línea.

Todos los nombres que entre en esta lista se asocian automáticamente con la identidad recién creada, como atributos de esa identidad. Por ejemplo, si entra "Robert Hays" y "Bob J. Hayes, Jr.", ambos nombres se asocian con la identidad recién creada.

Lista de direcciones

Especifique una o más direcciones que estén asociadas con la identidad que está añadiendo. Por ejemplo, si conoce la dirección actual y la anterior de la identidad, entre cada dirección completa, una dirección por línea. Todas las direcciones que entre en esta lista se asocian automáticamente con la identidad que está añadiendo.

Las direcciones no son necesarias para añadir una identidad. Si no hay direcciones conocidas para esta identidad, puede dejar en blanco esta sección de lista.

Dirección

Típicamente, esta información es la información especificada en las líneas Dirección 1 y Dirección 2. Por ejemplo: 555 Main Street Building 17 Suite 102-B

Si entra datos en cualquiera de los campos de dirección, debe entrar datos en el campo **Dirección**.

Desde fecha

Especifique la fecha en que esta información de dirección pasó a ser válida para esta identidad, si se conoce. Por ejemplo, si se sabía que esta identidad estaba en esta dirección a partir del 15 de marzo de 1999, entre esa fecha.

Puede entrar Desde fecha sin Hasta fecha.

Hasta fecha

Especifique la fecha en que esta información de dirección pasó a no ser válida para esta identidad, si se conoce. Por ejemplo, si se sabía que esta identidad dejó esta dirección el 1 de junio de 2001, entre esa fecha.

Puede entrar Hasta fecha sin Desde fecha.

Lista de números

Indique uno o varios números que estén asociados con la identidad que está añadiendo. Por ejemplo, si conoce una tarjeta de crédito utilizada por

la identidad, un número de permiso de conducir, un número de identificación, un número de pasaporte, y un número de teléfono, entre cada número en una línea aparte. Todos los números que entre en esta lista se asocian automáticamente con la identidad que está añadiendo.

Los números no son necesarios para añadir una identidad, por lo que puede dejar en blanco esta sección de lista. No obstante, si entra datos numéricos, los campos **Tipo de número** y **Valor** son necesarios.

Tipo de número
Seleccione el tipo de número en la lista desplegable de los tipos de números disponibles. Estos tipos de número deben existir en el sistema. (No puede añadir un tipo de número nuevo aquí. Si no ve el tipo de número que desea utilizar, póngase en contacto con el administrador del sistema para que lo cree.)

Si desea asociar un número con la identidad que está añadiendo, debe seleccionar un tipo de número.

Valor Entre el valor de número para el tipo de número seleccionado. Por ejemplo, si está asociando un pasaporte con esta identidad, entre aquí el número de pasaporte.

Si desea asociar un número con la identidad que está añadiendo, debe entrar un valor de número que se corresponda con el tipo de número.

Ubicación
Entre la ubicación asociada con el número, si se conoce o si existe. Por ejemplo, si está asociando un pasaporte con esta identidad, entre aquí el nombre del país que emitió el pasaporte. O bien entre el nombre del estado/provincia que emitió un permiso de conducir.

Desde fecha
Especifique la fecha en que este número pasó a ser válido para esta identidad, si se conoce. Puede entrar Desde fecha sin Hasta fecha.

Hasta fecha
Especifique la fecha en que este número pasó a no ser válido para esta identidad, si se conoce. Por ejemplo, la fecha de caducidad de un permiso de conducir, pasaporte o tarjeta de crédito.

Puede entrar Hasta fecha sin Desde fecha.

Lista de características
Indique una o varias características que pertenezcan o que estén asociadas con la identidad que está añadiendo. Por ejemplo, si el sistema recoge características tales como la fecha de nacimiento, el estado civil, el color de ojos o la altura, puede entrar cada característica conocida en esta lista, una por línea. Todas las características que entre en esta sección de lista se asocian automáticamente con la identidad que está añadiendo.

Las características no son necesarias para añadir una identidad, por lo que puede dejar en blanco esta sección de lista. No obstante, si entra datos de características, son necesarios todos los campos de características.

Tipo Seleccione un tipo de característica en la lista desplegable de tipos disponibles. El tipo de característica debe existir en el sistema. (No puede añadir un tipo nuevo aquí. Si no ve el tipo de característica que desea utilizar, póngase en contacto con el administrador del sistema para que cree la característica.)

Si desea asociar una característica con la identidad que está añadiendo, debe seleccionar un tipo de característica.

Valor Entre el valor de la característica. Si desea asociar una característica con la identidad que está añadiendo, debe entrar el valor de característica que se corresponda con el tipo de característica.

Desde fecha
Especifique la fecha en que esta característica pasó a ser válida para esta identidad, si se conoce. Puede entrar Desde fecha sin Hasta fecha.

Hasta fecha
Especifique la fecha en que esta característica pasó a no ser válida para esta identidad, si se conoce. Puede entrar Hasta fecha sin Desde fecha.

Lista de correos electrónicos
Indique una o varias direcciones de correo electrónico que pertenezcan o que estén asociadas con la identidad que está añadiendo. Entre cada dirección de correo electrónico conocida en esta lista, una dirección de correo electrónico por línea. Todas las direcciones de correo electrónico que entre en esta sección de lista se asocian automáticamente con la identidad que está añadiendo.

Las direcciones de correo electrónico no son necesarias para añadir una identidad, por lo que puede dejar en blanco esta sección de lista. No obstante, si entra datos de correo electrónico, los campos **Tipo** y **Dirección** son necesarios.

Tipo Seleccione un tipo de dirección de correo electrónico en la lista desplegable de tipos disponibles. El tipo de dirección de correo electrónico debe existir en el sistema. (No puede añadir un tipo nuevo aquí. Si no ve el tipo de dirección de correo electrónico que desea utilizar, póngase en contacto con el administrador del sistema para que cree el tipo de dirección de correo electrónico.)

Si desea asociar una dirección de correo electrónico con la identidad que está añadiendo, debe seleccionar un tipo.

Valor Entre la dirección de correo electrónico completa. Si desea asociar una dirección de correo electrónico con la identidad que está añadiendo, debe entrar el valor de dirección de correo electrónico que se corresponda con el tipo de dirección de correo electrónico.

Desde fecha
Especifique la fecha en que esta información de dirección de correo electrónico pasó a ser válida para esta identidad, si se conoce. Por ejemplo, si conoce la fecha en que se abrió esta cuenta de correo electrónico, puede entrarla aquí.

Puede entrar Desde fecha sin Hasta fecha.

Hasta fecha
Especifique la fecha en que esta información de dirección de correo electrónico pasó a no ser válida para esta identidad, si se conoce. Por ejemplo, si conoce la fecha en que se cerró esta cuenta de correo electrónico, puede entrarla aquí.

Puede entrar Hasta fecha sin Desde fecha.

Botón Someter
Para procesar la identidad a través de la resolución de entidad y relación y añadir la identidad a la base de datos de entidades, después de especificar toda la información conocida y pertinente acerca de la identidad que desea añadir, pulse **Someter**.

Botón Restaurar
Para borrar de la ventana toda la información entrada sin someterla, pulse el botón **Restaurar**. La identidad no se procesa a través de la resolución de entidad y relación, ni se añade a la base de datos de entidades.

Ventana Añadir divulgación:

Utilice esta ventana para divulgar una relación entre dos identidades existentes. Al revelar la relación, crea un enlace entre las identidades, así como entre las entidades que contienen esas identidades. Revelar una relación indica que el enlace entre estas dos identidades aún no ha sido detectado por la resolución de entidad y relación, y que tiene un motivo específico para enlazar las dos identidades manualmente.

ID de entidad
Especifique el número de ID de entidad de cada identidad que desee relacionar, uno en cada campo de **ID de entidad**.

Búsqueda
Pulse para visualizar la información de identidad correspondiente al ID de entidad que ha especificado. Realice esta operación para ambos números de ID de entidad. Revisando la información que se muestra, puede verificar que los ID de entidad corresponden a las identidades que tiene intención de relacionar. O bien, puede corregir el ID de entidad para una o ambas identidades antes de enlazarlas.

Botones de opciones (junto a cada identidad asociada con cada ID de entidad)
Seleccione una identidad para ambos ID de entidad. Estos ID son las dos identidades que desea relacionar.

Nota: Es posible que solo vea una identidad para cada entidad, lo que significa que actualmente la entidad tiene una sola identidad en el sistema.

Descripción de relación divulgada
Escriba una descripción de cómo están enlazadas las dos identidades seleccionadas. Esta descripción proporciona información de ayuda para otros usuarios del Visualizador cuando vean esta relación. Ayuda a esos usuarios a comprender cómo y por qué se enlazan estas dos identidades.

Crear Pulse **Crear** para divulgar la relación entre las dos identidades seleccionadas. El sistema envía la información acerca de ambas identidades por la interconexión para su proceso y luego actualiza los datos de ambas identidades, así como de todas las entidades asociadas con esas identidades.

Ventana Carga de archivos UMF:

Utilice esta ventana para cargar datos desde un archivo UMF a la base de datos de entidades mediante el Visualizador.

Barra de estado de carga de archivos
Después de seleccionar un archivo UMF a abrir y cargar, y después de pulsar el botón **Cargar archivo...**, esta barra de estado muestra el progreso del proceso de los datos en el archivo. El sistema muestra estadísticas que

incluyen el porcentaje completado, el tiempo transcurrido desde que el archivo empezó a procesarse, y el estado del sistema que procesa.

Botón (Continuar)
Si ha pausado la carga y proceso del archivo utilizando el botón (Pausar), pulse este botón para reanudar la carga y proceso de los registros restantes no procesados del archivo. El sistema continúa con el siguiente registro del archivo seleccionado.

Botón (Pausar)
Pulse este botón si desea pausar temporalmente la carga y proceso del archivo. El archivo permanece en la memoria, y el sistema averigua qué registros ya se han procesado. Los registros del archivo que aún no se han procesado no estarán en la base de datos de entidades hasta que continúe la carga del archivo.

Este botón solo está activo mientras el sistema está cargando el archivo.

Botón (Detener)
Pulse este botón si desea detener la carga y proceso del archivo. El archivo se borra de la memoria. Los registros del archivo que aún no se han procesado no estarán en la base de datos de entidades. Si desea continuar cargando registros de este archivo, debe volver a cargarlo. Durante la nueva carga del archivo, los archivos que ya se hayan procesado volverán a procesarse.

Este botón solo está activo mientras el sistema está cargando el archivo.

Botón Ver resultados
Pulse este botón para visualizar el diálogo **Resultados de la carga de archivos**, que incluye la siguiente información:

- El número de registros enviados a la interconexión.
- El número de entidades nuevas creadas en la base de datos de entidades, de acuerdo con los datos del archivo que ha cargado.
- El número de excepciones de UMF que la interconexión ha encontrado al procesar los datos de este archivo. (Este número puede indicar errores en el archivo UMF o problemas en la sintaxis que impiden que la interconexión procese los datos en su totalidad. Póngase en contacto con el administrador del sistema para obtener ayuda para arreglar las excepciones de UMF. El administrador del sistema puede revisar el registro cronológico de las excepciones de UMF para obtener más detalles.)
- El número de alertas de rol creadas, según los datos del archivo que ha cargado.

Botón Cargar archivo...
Pulse este botón para cargar el archivo en la interconexión y empiece a procesar cada registro del archivo para la resolución de entidad y relación.

Ventana Archivo de validación UMF:

Utilice esta ventana para validar datos de un archivo UMF que desee cargar y procesar a través de la resolución de entidad y relación. Validando los datos primero puede corregir errores o avisos potenciales antes de cargar y procesar el archivo.

Botón Validar...
Muestra la ventana **Configuración de validación UMF**, donde seleccionará

el archivo UMF a validar, establecerá la vía de acceso y el nombre de archivo del archivo de registro de errores y avisos, e iniciará el proceso de validación de UMF.

Si mantiene la ventana **Configuración de validación UMF** abierta y valida otro archivo UMF, cuando pulse **Validar...**, los campos de vía de acceso y archivo de registro se rellenarán con las ubicaciones del último archivo UMF validado y la ubicación del último archivo de registro de errores y avisos. Puede volver a validar el mismo archivo, o puede seleccionar un nuevo archivo UMF a validar.

Al cerrar la ventana **Configuración de validación UMF** se borran los campos de vía de acceso y archivo de registro.

Ejecución de informes desde el Visualizador

Desde el Visualizador, puede ver e imprimir informes que le muestren resúmenes de estadísticas por orígenes de datos e informes que le ayuden a ver y a gestionar alertas y relaciones divulgadas.

Visualización e impresión de informes en el Visualizador

Utilice los informes del Visualizador para ver las estadísticas y los resúmenes de calidad de los archivos de origen de datos, como ayuda para gestionar las alertas asignadas y para revisar relaciones divulgadas, alertas de sucesos o información de sucesos. Puede ver los informes en línea o imprimir una copia.

Acerca de esta tarea

Puede acceder a la mayoría de informes del Visualizador desde el menú **Ver** o desde la barra de herramientas. No obstante, algunos informes solo puede verlos e imprimirlos desde una pantalla específica, tal como el informe Resumen de entidad o el informe Detalle de alerta de suceso.

Los informes se visualizan en su navegador web seleccionado utilizando Adobe Acrobat Reader. Debe tener instalado Adobe Acrobat Reader versión 7.0 o superior en la estación de trabajo para ver e imprimir informes del Visualizador.

Nota: Las indicaciones de fecha y hora generadas por el sistema impresas en los informes de un cliente del Visualizador se ajustan para el huso horario del servidor de aplicaciones del Visualizador. Las fechas aparecen ajustadas correctamente para el huso horario del cliente del Visualizador cuando se ven en la pantalla. Por ejemplo, en Estados Unidos, un cliente del Visualizador EST (Eastern Standard Time) conectado a un servidor de aplicaciones del Visualizador PST (Pacific Standard Time) visualiza una indicación de fecha y hora generada por el sistema como 8:00 PM en la pantalla, pero se imprime desde un cliente del Visualizador EST en un informe como 5:00 PM.

Procedimiento

- Para ver un informe Historial del Generador de atributos, un informe Generador de atributos, un informe Alerta de atributo, un informe Resumen de origen de datos, un informe Divulgación, un informe Resumen de carga, o un informe Estado de alerta de rol, haga lo siguiente:
  1. Pulse **Ver** > **Informes**, y luego seleccione el informe que desee ver o imprimir.
  2. Complete los criterios del informe.
  3. Pulse **Ejecutar informe** para generar el informe seleccionado.

- Para ver un informe Resumen de entidad, en la pantalla **Resumen de entidad**, pulse **Informe**.
- Para ver un informe Detalle de alerta de rol, en la pantalla **ID de alerta de rol**, pulse **Informe**.
- Para ver un informe Detalle de alerta de suceso, en la pantalla **ID de alerta de suceso**, pulse **Informe**.
- Para ver un informe de Todos los sucesos, en la pantalla **Sucesos de entidad**, pulse **Informe**.

Resultados

El sistema genera el informe seleccionado basándose en todos los criterios especificados y visualiza el informe en una ventana diferente. Si desea imprimir el informe, pulse el botón del icono **Impresora** o utilice la función **Imprimir** del navegador web.

Informe Historial del generador de alertas de atributo:

El informe Historial del Generador de alertas de atributo lista los cambios realizados en los generadores de alertas de atributo, por ejemplo cambios en las fechas de caducidad, los números de caso, los comentarios o el estado. El informe se clasifica por ID de entidad de búsqueda.

Entidad de búsqueda
Muestra el ID de entidad (y nombre, si se suministra) desde los criterios de búsqueda del generador de alertas de atributo.

Fecha y hora de creación
Muestra la fecha y hora en que se creó este generador de alertas de atributo.

Sección de historial de estado
Esta sección del informe muestra cada actualización realizada en el generador de alertas de atributo, empezando por la actualización más reciente (última).

Comentario
Muestra comentarios especificados por el usuario que realiza la actualización.

Fecha y hora de actualización
Muestra la última fecha y hora en que se modificó este generador de alertas de atributo. Si no se ha modificado este generador de alertas de atributo, la fecha y la hora es la misma que la **Fecha y hora de creación**.

Fecha y hora de caducidad
Muestra la fecha y hora en que este generador de alertas de atributo debe caducar, o la última fecha en que este generador de alertas de atributo generará alertas de atributo.

Estado
Indica si el generador de alertas de atributo está activo o ha caducado.

Usuario
Muestra el nombre del usuario que ha realizado esta actualización.

Grupo analizador
Muestra el Grupo analizador del Visualizador al que pertenece el último usuario que ha modificado este generador de alertas de atributo.

Mín. puntuación de resolución
Indica la puntuación mínima de resolución y descripción de la Puntuación mínima seleccionada como parte de los criterios del generador de alertas de atributo. Este umbral de puntuación indica cuánto deben coincidir los atributos para generar una alerta para este generador de alertas de atributo. Así, "Es entidad" es la coincidencia más aproximada y "Cualquier relación" es la coincidencia menos aproximada. Puede establecer el umbral para cada una de estas puntuaciones en la pantalla **Preferencias del sistema** en la ventana **Configurar preferencias de pantalla**.

Código de razón
Muestra el código seleccionado por el usuario que indica la razón para el generador de alertas de atributo.

Número de caso
Visualiza el número de caso alfanumérico opcional, especificado por el usuario que ha creado el generador de alertas de atributo.

Informe Generador de alertas de atributo:

Utilice el informe Generador de alertas de atributo para gestionar generadores de alertas de atributo. Mediante la visualización de este informe, puede ver un resumen rápido de todos los generadores de alertas de atributo del sistema, incluyendo la fecha y la hora en que se creó cada generador de alertas de atributo, la fecha y hora de caducidad, el estado y la última fecha y hora en que se actualizó el generador de alertas de atributo. El informe se clasifica por ID de entidad de búsqueda.

Entidad de búsqueda
Indica el ID de la Entidad de búsqueda creada por el generador de alertas de atributos.

Fecha y hora de creación
Indica la fecha y hora en que se creó este generador de alertas de atributo.

Comentario
Muestra el texto de comentario añadido por el usuario como parte del generador de alertas de atributo.

Fecha y hora de actualización
Indica la última fecha y hora en que se modificó este generador de alertas de atributo. Si no se ha modificado este generador de alertas de atributo, la fecha y la hora es la misma que la **Fecha y hora de creación**.

Fecha y hora de caducidad
Indica la fecha y hora en que este generador de alertas de atributo tiene establecida la caducidad.

Estado
Estado actual de este generador de alertas de atributo, desde la última fecha y hora en que se actualizó este generador de alertas de atributo.

Usuario
Indica el último usuario en modificar este generador de alertas de atributo.

Si el generador de alertas de atributo no se ha modificado nunca, este usuario es el que ha creado el generador de alertas de atributo original.

Grupo analizador
Indica el nombre del Grupo analizador al que pertenece el último usuario que ha modificado este generador de alertas de atributo.

Mín. puntuación de resolución
Muestra la selección en la lista desplegable **Puntuación mínima** cuando se creó el generador de alertas de atributo. Este umbral de puntuación determina cuánto deben coincidir los atributos para generar una alerta para este generador de alertas de atributo.

El umbral para cada una de estas puntuaciones se establece en el panel **Preferencias del sistema**, que forma parte del diálogo **Configurar preferencias de pantalla** accedido desde el menú **Archivo**.

Código de razón
Código seleccionado por el usuario que indica la razón para el generador de alertas de atributo.

Número de caso
Número de caso alfanumérico opcional, especificado por el usuario que ha creado el generador de alertas de atributo.

Informe Alerta de atributo:

Utilice el informe Alerta de atributo para gestionar alertas de atributo individuales. Al visualizar este informe, se ve un lista de todas las entidades que han coincidido con los criterios del generador de alertas de atributo, así como el estado y la actividad más reciente en la alerta.

El informe se clasifica por ID de Entidad de búsqueda en orden ascendente. Si existe más de una entidad coincidente por entidad de búsqueda, las entidades coincidentes se clasifican por orden ascendente del ID de entidad.

Entidad de búsqueda
Muestra el ID de entidad creado por la búsqueda de alertas de atributo.

Entidad coincidente
Muestra el ID y nombre de la entidad que ha coincidido con la Entidad de búsqueda, según los criterios del generador de alertas de atributo. Si una alerta de atributo tiene más de una Entidad coincidente, se visualizan en orden alfanumérico por ID de entidad. Por ejemplo, el `ID de entidad 37` se visualiza antes que el `ID de entidad 1003`.

Información de alerta de atributo
Esta sección del informe visualiza información general acerca de los resultados de la alerta.

Estado de alerta de atributo
Muestra el estado actual de esta alerta de atributo.

Fecha y hora de resultado de la búsqueda
Muestra la fecha y hora en que se creó la alerta de atributo.

Estado de búsqueda de atributos
Muestra el estado actual del generador de alertas de atributo que ha generado esta alerta de atributo.

Puntuación mínima de resolución
Muestra la puntuación mínima de resolución y descripción de la

Puntuación mínima seleccionada como parte de los criterios del generador de alertas de atributo. Este umbral de puntuación indica cuánto deben coincidir los atributos para generar una alerta de atributo.

Información de estado de alerta de atributo

En esta sección del informe, se ve el historial de cada estado de esta alerta. La información de estado se visualiza por orden de actualización, de modo que la última actualización de estado se visualiza en primer lugar.

Fecha y hora de estado

Muestra la fecha y hora en que se produjo la actualización de la alerta de atributo.

Usuario

Muestra el nombre del usuario que ha actualizado la alerta.

Código de actividad

Muestra el código definido por el usuario que indica la acción realizada por un usuario en esta alerta de atributo. Cuando los usuarios actualizan alertas, seleccionan un código de actividad. Algunos ejemplos de códigos de actividad son Abierto, Asignado, Retenido y Cerrado. Los códigos de actividad se configuran en la Consola de configuración.

Estado

Muestra el estado de disposición para la actualización de esta alerta, modificada en la fecha y hora de estado. Los estados de disposición se visualizan por orden de actualización, de modo que la última actualización de estado se lista en último lugar.

Comentario

Muestra comentarios especificados por el usuario que realiza la actualización en esta alerta.

Información coincidente

Esta sección muestra qué atributos por tipo de datos y valor han coincidido entre la Entidad de búsqueda y la Entidad coincidente.

Tipo de datos

Muestra el nombre del atributo que ha coincidido entre la Entidad de búsqueda y la Entidad coincidente. Los dos valores de este atributo coincidente se visualizan en las columnas Valor de coincidencia y Criterios de búsqueda.

Criterios de búsqueda

Muestra el valor de datos que pertenece a la Entidad de búsqueda que coincide con el valor correspondiente mostrado en la columna Entidad coincidente.

Valor de coincidencia

Muestra el valor de datos que pertenece a la Entidad coincidente, que coincide con el mismo tipo de datos y el valor de datos que para la Entidad de búsqueda.

Descripción de precisión

Muestra el texto que describe el nivel de precisión en el que coinciden los Criterios de búsqueda y el Valor de coincidencia. Los niveles de precisión se configuran durante la configuración de resolución de entidades, por atributo.

Precisión/Precisión máxima
El primer número es la puntuación de precisión generada por el sistema, que indica el grado de coincidencia del valor de Criterios de búsqueda y el Valor de coincidencia. El segundo número es la puntuación máxima de precisión que se puede lograr.

Mediante la coincidencia de los dos números, puede determinar mejor el grado de coincidencia entre la Entidad de búsqueda y la Entidad coincidente. También puede utilizar estas puntuaciones para determinar si los criterios de búsqueda de alertas de atributo necesitan un ajuste.

Ajuste de puntuación
Muestra el número asociado con este atributo que se utiliza para ajustar la puntuación de resolución hacia arriba o hacia abajo durante la resolución de entidad. Este número se configura como parte de la configuración global de la resolución de entidades.

Informe Resumen de origen de datos:

El informe Resumen de origen de datos proporciona un resumen rápido de estadísticas por origen de datos de los registros cargados en el sistema para proceso. Desde este informe puede ver el número total de procesados por ID de carga. De estos registros totales cargados, el informe muestra el número de registros que representan nuevas identidades o nuevas entidades y calcula el porcentaje de registros que son nuevas identidades, así como el porcentaje de registros que son entidades recién creadas.

Estadísticas por carga dentro de orígenes de datos

Fecha de la carga
Muestra la fecha en que se ha cargado este archivo de origen de datos

ID de carga
Muestra el número de ID de carga asignado por el sistema.

Origen de datos
Muestra el código de origen de datos y descripción (separados mediante un guión) para el archivo de origen de datos que se ha cargado.

Registros UMF cargados
Indica el número total de registros de identidad en este archivo de origen de datos que se han cargado.

Nuevas identidades
Indica el número total de nuevas identidades descubiertas en el archivo de datos que se ha cargado. (Este número indica una identidad que el sistema no ha procesado antes.)

% de nueva identidad
Indica el porcentaje del total de registros cargados (Nuevas identidades dividido por Registros UMF cargados) que representan nuevas identidades.

Nuevas entidades
Indica el número total de nuevas entidades creadas desde esta carga de datos.

% Entidades nuevas
Indica el porcentaje del total de registros cargados (Nuevas entidades dividido por Cargados) que representan nuevas entidades.

Gráficas de estadísticas por origen de datos

Registros cargados por origen de datos
Muestra un diagrama de barras que muestra gráficamente cuántos registros de cada origen de datos se han cargado en el sistema, basándose en los demás criterios del informe especificados. Puede ver los orígenes de datos que han proporcionado más registros o menos registros y compararlo con los números de carga estimados.

- El eje vertical muestra los orígenes de datos por código de origen de datos.
- El eje horizontal muestra el número de registros cargados.

Si hay menos registros cargados para un origen de datos determinado que los esperados, puede inspeccionar los archivos de datos para este origen de datos. (También puede tomar en consideración la ejecución del Informe de resumen de carga para ver la calidad de los datos de los archivos cargados para este origen de datos; la calidad de los datos influye directamente en el número de registros cargados.)

Nuevas entidades por origen de datos
Muestra un diagrama de barras que muestra gráficamente los orígenes de datos que han dado lugar al mayor número de nuevas entidades, basándose en los demás criterios del informe especificados.

- El eje vertical muestra los orígenes de datos por código de origen de datos.
- El eje horizontal muestra el número de nuevas entidades creadas.

Informe Divulgaciones:

Utilice este informe para ver y gestionar las relaciones divulgadas que se han creado entre identidades. Las relaciones divulgadas son relaciones que los usuarios del Visualizador han creado manualmente en la pantalla **Añadir divulgaciones**, o bien incluyendo el par de códigos de relación divulgada (<DR> y </DR>) en los registros de identidad entrantes.

El informe se clasifica por ID de relación.

ID de relación
Muestra el número generado por el sistema que se asigna a cada relación divulgada cuando se crea la relación.

Fecha y hora de creación
Muestra la fecha y hora en que se creó la relación divulgada.

Descripción de relación
Muestra texto que describe la razón para crear la relación divulgada. Este texto lo escribe el usuario que ha creado la relación divulgada.

Fecha y hora de actualización
Muestra la fecha y hora de la última actualización de esta relación divulgada.

Estado
Muestra el estado de la relación divulgada.

Fecha de supresión
Muestra la fecha y hora en que se ha suprimido manualmente la relación divulgada. Este campo sólo se llena con una fecha y hora si un usuario ha determinado que la relación no era válida y ha suprimido la relación divulgada.

Origen de datos
Lista un código de origen de datos y la descripción de las dos entidades (uno para cada una, en filas separadas) que ahora están enlazadas por esta relación divulgada. El código de origen de datos apunta al archivo origen original.

ID externo
Lista un ID externo para ambas entidades (uno para cada una, en filas separadas) que ahora están enlazadas por esta relación divulgada. El ID externo apunta con frecuencia a un número de cuenta dentro del archivo origen original que pertenece exclusivamente a la entidad.

Informe Detalle de alerta de suceso:

Utilice el informe Detalle de alerta de suceso para ver detalles completos acerca de una alerta de suceso específica y las entidades implicadas en la alerta. Este informe es de utilidad cuando se desea un informe en papel del panel **Alerta de suceso** en la ventana **Investigación**.

ID de alerta
Muestra la descripción e ID de alerta para una alerta de suceso específica. El ID de alerta aparece antes de la descripción en la cabecera de informe.

Información de alertas de suceso
Esta sección visualiza información general para las alertas de suceso globales, tal como una descripción de la regla de alertas de suceso que ha desencadenado esta alerta y el estado actual de la alerta de suceso.

Fecha y hora de alerta
Indica la fecha y hora en que se generó esta alerta de suceso.

ID de regla
Muestra un número interno generado por el sistema al configurarse inicialmente la regla de alertas de suceso. Este ID está asociado con la regla de alertas de suceso que ha desencadenado esta alerta de suceso.

Descripción de regla
Muestra texto que describe la regla de alertas de suceso, definido por el usuario que ha configurado la regla de alertas de suceso.

Estado
Indica el estado actual de esta alerta de suceso.

Detalles del suceso
Esta sección proporciona más información sobre los datos de la alerta de suceso.

Fecha y hora
Indica la fecha y hora en que se generó la alerta de suceso.

Origen de datos
Muestra, para cada suceso, el código y descripción del origen de datos que ha suministrado los datos del suceso. Esta información identifica el archivo origen original.

ID externo
Muestra, para cada suceso, el ID externo asociado al código de origen de datos que ha suministrado los datos del suceso. Esta información identifica con frecuencia un número de cuenta para la entidad en el archivo origen original.

Referencia de suceso
Muestra, para cada suceso, el código exclusivo creado por el procesador de sucesos complejos durante el procesador de sucesos.

Cantidad
Indica, para cada suceso, el número que representa la cantidad implicada en este suceso. Por ejemplo, 1 podría significar una transferencia electrónica del valor en la columna **Valor**.

Valor Indica, para cada suceso, el valor total de este suceso.

Información de entidad
Para la entidad implicada en el suceso, esta sección proporciona la lista de tipos de atributo y sus valores asociados implicados en el suceso.

Disposiciones de las alertas
Esta sección proporciona un resumen de los estados para la alerta de suceso.

Código de actividad
Muestra el código de actividad del suceso seleccionado por el usuario que cambió el estado de esta alerta de suceso.

Estado
Muestra el estado (Activo o Inactivo) asociado con el código de actividad del suceso.

Comentarios de estados
Muestra comentarios de analista especificados acerca de esta actualización de estado.

Usuario
Indica el ID de usuario del usuario que cambió el estado de esta alerta de suceso.

Fecha y hora
Indica la fecha y la hora en que se cambió el estado.

Sección Historial de alertas de suceso de rol
Esta sección lista todas las alertas de rol en que ha estado implicada la entidad responsable de esta alerta de suceso.

Sección Historial de alertas de suceso
Esta sección del informe lista el historial completo de la entidad implicada en la alerta de suceso principal. Utilice esta sección para ver el número de alertas de suceso en que está implicada esta entidad.

Fecha y hora de alerta
Indica la fecha y hora en que se generó la alerta de suceso.

ID de alerta
Muestra el ID para esta alerta de suceso.

Descripción
Muestra texto para describir la regla de sucesos complejos que ha desencadenado esta alerta de suceso.

Código de actividad
Muestra un código definido por el usuario que indica una acción realizada por un usuario en esta alerta. Los códigos de actividad se configuran en la Consola de configuración y se seleccionan en una

lista desplegable en el Visualizador cuando se actualiza una alerta. Algunos ejemplos de códigos de actividad son Asignado, Cerrado y Pendiente.

Estado
Muestra el estado para la actualización de esta alerta, modificada en la fecha y hora de estado. Los estados se visualizan por orden de actualización, de modo que la última actualización de estado se lista en último lugar.

Informe Todos los sucesos:

Utilice el informe Todos los sucesos para ver todos los sucesos asociados con una sola entidad, independientemente de si los sucesos han generado una alerta de suceso o no. El informe es de utilidad cuando se desea un informe en papel de la pantalla **Sucesos de entidad** en la ventana **Investigación**. Los sucesos que se muestran en el informe dependen del tipo de suceso y el rango de fechas que haya seleccionado en esa pantalla.

Si no ha seleccionado un tipo de suceso, el informe visualiza sucesos de todos los tipos para la entidad dada dentro del rango de fechas definido. Si ha seleccionado un tipo de suceso, solo se mostrarán los sucesos de ese tipo dentro del rango de fechas definido.

Información básica del informe
Esta sección proporciona la información básica de cabecera de informe, tal como el rango de fechas para informes y más sobre la entidad asociada con estos sucesos.

Fechas de informe: Desde y Hasta
Indica las fechas de inicio y final para el informe. Solamente se visualizarán en el informe los sucesos producidos dentro del rango de fechas para esta entidad.

Entidad asociada
Indica el ID de entidad perteneciente a la entidad asociada con estos sucesos.

Nombre actual
Indica el nombre actual para la entidad en la base de datos de entidades.

Dirección actual
Indica la dirección actual para la entidad en la base de datos de entidades.

Información del suceso
Esta sección proporciona los detalles de los sucesos asociados con esta entidad por tipo de suceso.

Tipo de suceso
Describe el tipo de suceso. Esta descripción se configura con el tipo de suceso en la Consola de configuración.

ID de suceso
Muestra el número generado por el sistema que identifica a este suceso específico.

Fecha y hora de creación
Muestra la fecha y hora en que se produjo el suceso.

Origen de datos
Muestra el código de origen de datos y la descripción de origen de datos asociados con el suceso.

ID externo
Muestra la clave exclusiva que identifica el registro de identidad de entrada en el origen de datos original para este suceso.

Referencia de suceso
Muestra información adicional sobre el suceso, normalmente el nombre de la ubicación donde se produjo el suceso.

Ubicación
Muestra la información de dirección para la ubicación donde se produjo el suceso.

Valor Muestra la cantidad de valor asociada con el suceso.

Cantidad
Muestra el número de unidades asociado con el suceso.

Unidad de medida
Indica la unidad de medida asociada con el valor del suceso. La unidad de medida se configura por tipo de suceso en la Consola de configuración. La unidad de medida le ayuda a comprender el valor. Por ejemplo, si la unidad de medida es dólares estadounidenses y el valor del suceso es 5000, sabrá que en este suceso estaban involucrados $5.000,00.

Memorándum o *Etiqueta personalizada*
Muestra información adicional sobre el suceso, tal como notas o comentarios, que puede proporcionar un mayor contexto para la transacción del suceso.

Los usuarios pueden definir una etiqueta personalizada para esta columna como una de las opciones al configurar un tipo de suceso en la Consola de configuración. En lugar de **Memorándum**, podría ver una etiqueta personalizada más descriptiva. Por ejemplo, **Notas de transferencia electrónica**.

Memorándum adicional o *Etiqueta personalizada*
Muestra más información sobre el suceso, si está disponible.

Los usuarios pueden definir una etiqueta personalizada para esta columna como una de las opciones al configurar un tipo de suceso en la Consola de configuración. En lugar de **Memorándum adicional**, podría ver una etiqueta personalizada más descriptiva, por ejemplo **Comentarios del asistente**.

Informe Resumen de carga:

El informe Resumen de carga resume las estadísticas y las características de calidad por origen de datos. Contiene información acerca de los archivos de origen de datos. Utilice este informe para determinar las estadísticas de carga de rendimiento, el número de entidades y alertas creadas por la carga, información general acerca de la calidad de los datos cargados, un resumen de las acciones sobre los registros UMF por carga, y cualquier excepción de UMF generada por carga. El informe se agrupa por ID de carga.

Para cada carga, el informe divide las estadísticas en secciones:

- Resumen de carga

- Resumen de alertas de rol
- Resumen de relaciones
- Resumen de calidad
- Resumen de documentos UMF
- Resumen de excepción

Resumen de carga

Utilice esta sección como ayuda para determinar cuánto se ha tardado en procesar un archivo en particular, así como para tener una idea general de la utilidad de este archivo de origen de datos en la resolución global de entidades y la detección de relaciones.

Fecha y hora de inicio
Indica la fecha y la hora en que se inició la carga de datos.

Fecha y hora de finalización
Indica la fecha y la hora en que finalizó la carga de archivos de origen de datos.

Recuento de registros UMF
Indica el número total de registros cargados desde este archivo de origen de datos dentro del rango de **Fecha y hora de inicio** y **Fecha y hora de finalización**.

El número de **Fecha y hora de finalización** menos el número de **Fecha y hora de inicio** es el número de minutos que ha tardado la carga de este archivo de origen de datos en particular, lo que puede dar una idea del rendimiento del sistema. También puede indicar que un archivo de origen de datos mayor se debe dividir entre archivos más pequeños para un proceso más rápido.

Nuevas identidades
Indica el número total de nuevas identidades cargadas dentro del rango de **Fecha y hora de inicio** y **Fecha y hora de finalización**.

% de nueva identidad
Indica el porcentaje del total de identidades de esta carga de datos que son nuevas identidades (identidades que son nuevas para la base de datos de entidades).

Nuevas entidades
Indica el número total de identidades recién creadas dentro del rango de **Fecha y hora de inicio** y **Fecha y hora de finalización**.

% Entidades nuevas
Indica el porcentaje del total de entidades que son entidades recién creadas como resultado de esta carga de origen de datos.

El número de nuevas identidades y nuevas entidades puede proporcionar una idea general del valor de este origen de datos en la resolución global de entidades y la detección de relaciones. Si estos números son bajos y siguen bajos durante un tiempo, puede que este origen de datos no sea útil para conseguir los objetivos de resolución de entidades de su empresa.

Resumen de alertas de rol

Utilice esta sección para ver las normas de resolución y las puntuaciones de resolución comunes para las relaciones detectadas que han dado lugar a alertas de rol. Cada fila representa el número de alertas de rol que se han generado, basándose en los criterios listados.

Regla de resolución
Muestra el nombre de la regla de resolución utilizada para evaluar la identidad y entidad durante la resolución de entidades y la detección de relaciones.

Descripción de alerta
Muestra el nombre de la regla de alerta de rol que ha desencadenado la alerta de rol.

Gravedad
Muestra un indicador definido por el usuario para medir la prioridad o importancia de esta alerta de rol.

Puntuación de resolución
Muestra una puntuación de relación (0-100) para la regla de resolución dada a la identidad y entidad implicadas en la alerta de rol. Esta puntuación indica el grado de similitud entre la identidad y la entidad. Una puntuación de 100 significa que el registro de identidad se ha resuelto para la entidad.

Recuento de alertas
Indica el número total de alertas de rol generadas basándose en la descripción de regla de alerta de rol, la regla de resolución y la puntuación de resolución.

Resumen de relaciones

Utilice esta sección para ver los atributos comunes para las relaciones detectadas que no han generado una alerta de rol. Cada fila representa el número de relaciones que se han detectado, basándose en los criterios listados.

Regla de resolución
Muestra el nombre de la regla de resolución utilizada para evaluar los registros de identidad entrantes y las entidades existentes durante la resolución de entidades y la detección de relaciones.

Puntuación de resolución
Muestra una puntuación de relación (0-100) para la regla de resolución dada a la identidad y entidad durante la resolución de entidades. Esta puntuación indica el grado de similitud entre la identidad y la entidad. Una puntuación de 100 significa que el registro de identidad se ha resuelto para la entidad.

Puntuación de relación
Muestra una puntuación de relación (0-100) para la norma de resolución dada a la identidad y entidad durante la resolución de relaciones. Esta puntuación indica el grado de relación entre la identidad y la entidad.

Cuanto mayor sea la puntuación de relación, más próxima será la relación entre la identidad y la entidad, basándose en los atributos de coincidencia.

Recuento de relaciones
Indica el número total de relaciones que se detectan basándose en la regla de resolución, la puntuación de resolución y la puntuación de relación.

Resumen de calidad

Utilice la información de esta sección para evaluar la calidad de los datos de cada archivo de origen de datos. La sección indica la calidad por tipo de atributo de un segmento UMF y tipo de documento UMF. Mediante la revisión del resumen de calidad con el resumen de excepciones UMF, puede ver los archivos de origen de datos que tienen problemas de calidad o con un UMF mal formado que se deben arreglar. Normalmente, puede resolver estos temas a través de ETL o la configuración de DQM/origen de datos antes de procesar el archivo de origen de datos.

En algunos casos, esta sección puede indicar que un origen de datos tiene una calidad tan pobre que no le interesa utilizar este origen de datos para la resolución de entidades.

Tipo de documento
Muestra el nombre del tipo de documento UMF que contiene el tipo de datos listado en Tipo de datos. Normalmente, este valor es UMF_ENTITY.

Nombre de tabla
Muestra el nombre de la tabla de base de datos que almacena datos de segmentos UMF con nombres similares. Por ejemplo, los datos del segmento NUMBER se almacenan en la tabla NUMS.

Tipo de datos
Indica el tipo de datos, tal como se lista en los códigos UMF de tipo de atributo de los registros de entrada. Este tipo corresponde a un segmento UMF listado en Nombre de tabla. Por ejemplo, si el Nombre de tabla es *ADDRESS* y el Tipo de datos listado es *H*, la información de calidad evalúa el tipo de dirección de tipo *Domicilio*.

Si no reconoce un tipo de datos, puede indicar que el archivo de origen de datos no está correlacionado correctamente con la combinación adecuada de documentos, segmentos y códigos UMF. Compruebe la sección Resumen de excepción para ver si un segmento UMF y un código UMF coincidentes han causado una o varias excepciones de segmento. Si el problema es un UMF no válido, con frecuencia coinciden los números del Recuento de baja calidad de la sección Resumen de calidad con el Recuento de excepción de segmentos de la sección Excepción UMF.

Recuento de registros
Indica el número total de registros de identidad entrantes para el Tipo de documento, Nombre de tabla y Tipo de datos dados.

Recuento genérico
Indica el número total de registros de identidad entrantes con el Tipo de documento, Nombre de tabla y Tipo de datos dados que contienen valores considerados genéricos.

Recuento de baja calidad
Indica el número total de registros de identidad entrantes con el Tipo de documento, Nombre de tabla y Tipo de datos dados que están considerados como de baja calidad. Este número puede indicar un problema de entrada de datos o de transformación ETL en el archivo de origen de datos.

Porcentaje utilizable
Indica el porcentaje de registros de identidad entrantes con el Tipo de documento, Nombre de tabla (de este segmento UMF) y Tipo de datos dados que se pueden utilizar para la resolución de entidades y la detección

de relaciones. (Recuento de registros menos Recuento genérico menos Recuento de baja calidad) dividido por el Recuento de registros es igual al Porcentaje utilizable.

Porcentaje de identidad
Indica el porcentaje de registros de identidad entrantes que contenían el Tipo de documento, Nombre de tabla y Tipo de datos dados.

Resumen de atributos

Utilice esta sección para ver los atributos del archivo de origen de datos que han ayudado a detectar relaciones y generar alertas de rol. Cada atributo se correlaciona con un segmento UMF específico, y esta sección muestra el número de relaciones detectadas y alertas de rol generadas, basadas en los datos del segmento UMF de entrada.

Nombre de segmento
Muestra el nombre del segmento UMF, que se correlaciona directamente con un atributo.

Tipo de datos
Lista el tipo de atributo (o tipo de datos) del segmento UMF correspondiente a la Descripción de precisión. El informe puede listar un tipo de atributo específico o listar *ALL*, que indica todos los tipos de atributo del segmento UMF.

Descripción de precisión
Describe el umbral de coincidencia entre un atributo de una identidad de entrada y un atributo de una entidad existente.

Alertas de rol
Indica el número total de alertas de rol generadas basándose en este segmento UMF, el tipo de datos y la descripción de precisión.

Relaciones
Indica el número total de relaciones detectadas basándose en este segmento UMF, el tipo de datos y la descripción de precisión.

Resumen de documentos UMF

Puede utilizar esta sección para validar el número total de registros de entrada en un archivo de origen de datos, basándose en la acción que se debe realizar en el registro. Puede conciliar estos números en el Recuento de registros de la sección Resumen de carga.

Tipo de documento
Muestra el nombre del tipo de documento UMF. Normalmente, este valor es UMF_ENTITY.

Acción
Indica el tipo de acción para el registro de identidad de entrada. He aquí una lista de las acciones utilizadas más comúnmente:

- *A* para añadir
- *C* para cambiar
- *D* para suprimir

Como parte del proceso ETL, normalmente los registros de identidad se codifican a través de UMF para indicar cómo se debe actuar en cada registro de entrada durante el proceso del sistema.

Recuento de registros UMF
Indica el número total de registros procesados para cada tipo de acción dentro del tipo de documento.

Porcentaje
Indica el porcentaje del total de registros cargados que el Recuento de registros representa. (La suma no debe exceder del 100%.)

Resumen de excepción

Utilice esta información como ayuda para señalar los registros de identidad incorrectos, como los que tienen un UMF incorrectamente formado. La excepción describe el problema, mientras que el nombre de tabla y elemento muestran el segmento y registros que son incorrectos. El recuento muestra cuántos registros del archivo contenían este UMF incorrecto.

Tipo de documento
Muestra el nombre del tipo de documento UMF. Normalmente, este valor es UMF_ENTITY.

Acción
Indica el tipo de acción para el registro de identidad de entrada:

- *A* para añadir
- *C* para cambiar
- *D* para suprimir

Como parte del proceso ETL, normalmente los registros de identidad se codifican a través de UMF para indicar cómo se debe actuar en cada registro de entrada durante el proceso del sistema.

Segmento
Muestra el nombre del segmento UMF donde se ha producido la excepción.

Código UMF
Muestra el valor del código UMF que ha causado la excepción UMF.

Excepción
Muestra el ID de mensaje u otro código de excepción para indicar el tipo de excepción UMF que se ha producido y dar información acerca de cómo resolver la excepción. Esta información también está disponible en la tabla UMF_EXCEPT.

Recuento de excepción de segmentos
Indica el número total de este tipo de excepción UMF.

Compruebe el Recuento de baja calidad en la sección Resumen de calidad para ver si se ha informado que un tipo de datos coincidente tiene baja calidad o no se puede utilizar. Si el problema es un UMF incorrecto, los números del Recuento de baja calidad de la sección Resumen de calidad y el Recuento de excepción de segmentos en la sección Excepción UMF coinciden con frecuencia para el mismo segmento UMF y códigos UMF.

Informe Detalle de alerta de rol:

Utilice el informe Detalle de alerta de rol para ver detalles completos acerca de una alerta de rol específica y las entidades implicadas en la alerta en cada grado de separación. Este informe es útil cuando se desea realizar más análisis de las entidades implicadas en cada alerta de rol.

Para cada grado de separación, el informe visualiza información acerca de las dos entidades implicadas en la alerta para que la compare y contraste. Después, el informe muestra otras alertas asociadas a cada entidad, de manera que se obtiene una imagen completa de cada entidad y sus alertas de rol asociadas. Normalmente, los detalles de cada alerta de rol abarcan varias páginas.

ID de alerta
Descripción e ID de alerta para una alerta de rol específica. El ID de alerta aparece antes de la descripción en la cabecera de informe.

Información de alertas de rol
Esta sección visualiza información general para las alertas de rol globales, como una descripción de la regla de alertas de rol que ha desencadenado esta alerta y el estado de la alerta de rol.

Fecha y hora de alerta
Fecha y hora en que se ha generado esta alerta de rol.

ID de regla
Número interno generado por el sistema al configurar inicialmente la regla de alertas de rol, este ID se asocia a la regla de alertas de rol que ha desencadenado esta alerta de rol.

Descripción de regla
Texto que describe la regla de alertas de rol, definido por el usuario que ha configurado la regla de alertas de rol.

Gravedad
Código definido por el usuario utilizado para indicar la prioridad o importancia de esta alerta.

Estado
Disposición actual de esta alerta de rol.

Confianza de relación
Puntuación que representa la proximidad de la relación de dos entidades que se listan bajo la sección Detalles de la coincidencia: Grado *n*. Cuanto más alta es la puntuación, más próxima es la relación. Una puntuación de 100 indica que la entidad de entrada y la entidad coincidente son la misma entidad.

El sistema genera la puntuación de confianza de relación como parte del proceso de resolución de entidades.

Puntuación de resolución
Puntuación que representa el grado de coincidencia de las dos entidades. Cuanto más alta es la puntuación, más coinciden. Una puntuación de 100 indica que la entidad de entrada y la entidad coincidente son la misma entidad.

El sistema genera la puntuación de resolución como parte del proceso de resolución de entidades.

Confianza de resolución
Puntuación de resolución base configurada como parte de la resolución de entidades que representa la puntuación mínima para resolver la entidad de entrada y la entidad coincidente en una entidad. Con frecuencia, la puntuación de resolución y la puntuación de confianza de resolución son iguales.

Sección Detalles de coincidencias: Grado *n*
Esta sección proporciona detalles de coincidencias para entidades

implicadas en la información de alertas e identidades para las entidades respectivas. Las dos entidades se representan como Entidad *x* (Identidad de entrada) y Entidad *y* (Identidad coincidente).

Para cada entidad y cada tipo de datos de atributo, el informe indica los valores de datos coincidentes, así como el origen de datos y el ID externo asociado a los valores de datos de cada entidad. Después el informe visualiza las descripciones y puntuaciones de precisión para los atributos de coincidencia. Si uno de los atributos coincidentes es el nombre, el informe también podría indicar detalles acerca de cómo la resolución de entidades ha puntuado los nombres, según las opciones de puntuación de nombres que estén configuradas para la resolución de entidades.

Tipo de datos
Nombre del atributo coincidente.

Valor Valor de los datos que han coincidido.

Origen de datos
Para cada entidad, el código y descripción del origen de datos que ha suministrado el atributo coincidente y el valor de los datos. Esta información identifica el archivo origen original.

ID externo
Para cada entidad, ID externo asociado al código de origen de datos que ha suministrado el atributo coincidente y el valor de los datos. Esta información identifica con frecuencia un número de cuenta para la entidad en el archivo origen original.

Descripción de precisión
Texto que describe el nivel de precisión en el que las entidades han coincidido.

Los niveles de precisión se configuran durante la configuración de resolución de entidades, por atributo.

Precisión/Precisión máxima
El primer número es la puntuación de precisión generada por el sistema, que indica el grado de precisión con que Entidad *x* (Identidad de entrada) coincide con Entidad *y* (Identidad coincidente). El segundo número es la puntuación máxima de precisión que se puede lograr.

Mediante la comparación de los dos números, puede determinar mejor el grado de coincidencia entre las entidades, por ejemplo el valor de exploración adicional de la coincidencia. También puede utilizar estas puntuaciones para determinar si los criterios de búsqueda de alertas necesitan un ajuste.

Ajuste de puntuación
La puntuación de resolución se ha ajustado por este número. Este número se configura durante la configuración de resolución de entidades.

Detalles de puntuación de nombres
Si uno de los atributos coincidentes es el tipo de datos de nombre, el informe también podría proporcionar detalles sobre cómo el proceso de resolución de entidades ha puntuado las coincidencias de nombres. Para que se visualice esta sección del informe, se debe configurar una de las siguientes opciones de nombre como parte de la resolución de entidades:

- Name Manager
- Comparador de nombres 2

Nombre completo
Puntuación (0-100) que representa el grado de coincidencia del nombre completo de ambas entidades coincidentes. Esta puntuación se configura como parte de la resolución de entidades.

Apellido
Puntuación (0-100) que representa el grado de coincidencia del apellido de ambas entidades coincidentes. Esta puntuación se configura como parte de la resolución de entidades.

Nombre de pila
Puntuación (0-100) que representa el grado de coincidencia del nombre de pila completo de ambas entidades coincidentes. Esta puntuación se configura como parte de la resolución de entidades.

Sección Información de Identidad de Entidad *x* **e** *y*
Esta sección del informe lista información específica sobre cada identidad.

Tipo de datos
Nombre de característica. (Por ejemplo, Nombre.)

Valor Valor de característica. (Por ejemplo, SMITH, BRUCE.)

Sección Otras alertas para las entidades *x* **e** *y*
Esta sección del informe lista el historial de alertas de rol de todas las demás alertas de rol y las relaciones asociadas a esta entidad de entrada (Entidad *x*) y la entidad coincidente (Entidad *y*). También lista el historial de alertas de suceso de todas las alertas de suceso asociadas con la entidad de entrada (Entidad *x*) y la entidad coincidente (Entidad *y*). Esta información puede proporcionar una imagen más completa de cada entidad, sus alertas y relaciones asociadas a otras entidades, que pueden ayudarle en el análisis.

Historial de alertas de rol
Contiene la información del historial de alertas de rol de Resumen de entidad.

Fecha y hora de alerta
Fecha y hora en que se ha generado la alerta de rol.

ID de alerta
Descripción e ID de alerta para esta alerta de rol.

Descripción
Texto para describir la regla de alertas de rol que ha desencadenado esta alerta.

ID de entidad
Número de ID para la entidad de esta fila que ha coincidido con la entidad listada por el número de Otras alertas para la entidad *n*.

Nombre
Nombre de la otra entidad que ha coincidido con la entidad listada por el número de Otras alertas para la entidad *n*.

Relaciones
Número de relaciones asociadas a la entidad relacionada.

Puntuación de relación
Puntuación que representa la proximidad de la relación de dos entidades. Cuanto más alta es la puntuación, más próxima es la relación. Una puntuación de 100 indica que la entidad de entrada y la entidad coincidente son la misma entidad.

El sistema genera esta puntuación como parte del proceso de resolución de entidades.

Código de actividad
Código definido por el usuario que indica una acción realizada por un usuario en esta alerta. Los códigos de actividad se configuran en la Consola de configuración y se seleccionan en una ventana desplegable en el Visualizador cuando se actualiza una alerta. Algunos ejemplos de códigos de actividad son Abierto, Asignado, Retenido y Cerrado.

Estado
Estado de disposición para la actualización de esta alerta, modificada en la fecha y hora de estado. Los estados se visualizan por orden de actualización, de modo que la última actualización de estado se lista en último lugar.

Historial de alertas de sucesos
Contiene la información del historial de alertas de suceso de Resumen de entidad.

Fecha y hora de alerta
Fecha y hora en que se ha generado la alerta de suceso

ID de alerta
Identificador exclusivo generado por el sistema para la alerta de suceso.

Descripción
Descripción de la alerta de suceso, a partir de la configuración de suceso en la Consola de configuración.

Informe Estado de alertas de rol:

El informe Estado de alertas de rol resume el estado de todas las alertas de rol para un tiempo especificado. Utilice este informe para ver y gestionar alertas de rol.

El informe se clasifica por ID de alerta de rol y fecha y hora de alerta.

ID de alerta - Descripción
Muestra el ID de alerta de rol generado por el sistema, y la descripción de la alerta de rol obtenido de la regla de alerta de rol asociada.

Fecha y hora de alerta
Indica la fecha y hora en que se creó la alerta de rol.

Información de entidad coincidente
Esta sección muestra el historial de disposición de la alerta, empezando por la actualización de estado más reciente.

Entidad 1 y Entidad 2
Muestra los ID de entidades y normalmente los nombres completos de las dos entidades que han coincidido, basándose en los criterios para esta alerta de rol (por descripción de ID de alerta).

Código de actividad
Muestra un código definido por el usuario que indica una acción realizada por un usuario en esta alerta. Los códigos de actividad se configuran en la Consola de configuración y se seleccionan en una ventana desplegable en el Visualizador cuando se actualiza una alerta. Algunos ejemplos de códigos de actividad son Abierto, Asignado, Retenido y Cerrado.

Estado
Muestra el estado de disposición para la actualización de esta alerta, modificada en la fecha y hora de estado. Los estados se visualizan por orden de actualización, de modo que la última actualización de estado se lista en último lugar.

Fecha y hora de estado
Indica la fecha y hora en que se produjo el estado de alerta.

Usuario
Muestra el nombre del usuario que ha actualizado la alerta con este estado de alerta.

Temas de ayuda

Ventana Criterios de informes de Historial del generador de alertas de atributos:

Utilice esta ventana del Visualizador para especificar los criterios para ver el informe Historial del generador de alertas de atributo. Este informe puede ayudarle a ver y auditar cambios realizados en los generadores de alertas de atributo, por ejemplo cambios en las fechas de caducidad, los números de caso, los comentarios o el estado. Si desea ver los resultados de un generador de alertas de atributo, vea el informe Generador de alertas de atributo.

Desde fecha
Escriba la primera fecha del rango de fechas para ver datos en el informe seleccionado. Utilice el formato `MM/DD/AA`. Por ejemplo, `01/01/01` representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Desde fecha** predeterminada es la de hoy.

Hasta fecha
Escriba la última fecha del rango de fechas para ver datos en el informe seleccionado. Utilice el formato `MM/DD/AA`. Por ejemplo, `01/01/01` representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Hasta fecha** predeterminada es la de hoy.

Para ver datos de un solo día, utilice la misma fecha en los campos **Desde fecha** y **Hasta fecha**.

Lista desplegable Estado
Seleccione un estado específico o seleccione **Todos** para realizar un informe de todos los estados para todos los generadores de alertas de atributo. Por ejemplo, si solo desea ver los cambios realizados en los generadores de

alertas de atributo abiertos actualmente dentro del rango de fechas especificado, seleccionará **Abrir** en la lista desplegable.

El estado predeterminado en la lista desplegable **Estado** es **Todos**, lo que muestra los generadores de alertas de atributo activos y caducados.

Lista desplegable Usuario
Seleccione una opción para ver sus generadores de alertas de atributo o los generadores de alertas de atributo creados por cualquier miembro de su grupo de usuarios del Visualizador.

La opción predeterminada es `Mis búsquedas`.

Botón Ejecutar informe
Pulse este botón para generar el informe.

Ventana Criterios de informes de Generador de alertas de atributo:

Utilice esta ventana para especificar los criterios para ver el informe Generador de alertas de atributo desde el Visualizador. El informe de Generador de alertas de atributo se puede utilizar para gestionar sus generadores de alertas de atributo o esos analistas de su grupo de usuarios del Visualizador. Si desea ver el historial de cambios de los generadores de alertas de atributo, utilice el informe Historial de Generador de alertas de atributo.

Desde fecha
Teclee la primera fecha del rango de datos. Utilice el formato `MM/DD/AA`. Por ejemplo, `01/01/01` representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Desde fecha** predeterminada es la de hoy.

Hasta fecha
Teclee la última fecha del rango de datos. Utilice el formato `MM/DD/AA`. Por ejemplo, `01/01/01` representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Hasta fecha** predeterminada es la de hoy.

Para ver datos de un solo día, utilice la misma fecha en los campos **Desde fecha** y **Hasta fecha**.

Lista desplegable Estado
Seleccione un estado específico o seleccione **Todos** para realizar un informe de todos los estados para todos los generadores de alertas de atributo. Por ejemplo, si solo desea ver los generadores de alertas de atributo dentro del rango de fechas especificado activos actualmente, seleccione **Abrir**.

El estado predeterminado es **Todos**, lo que significa que el informe muestra generadores de alertas de atributo tanto caducados como activos.

Lista desplegable Usuario
Realice una selección:

- Para ver solamente sus generadores de alertas de atributo, seleccione **Mis búsquedas** (la selección predeterminada).
- Para ver todos los generadores de alertas de atributo creados por usuarios de su grupo de usuarios del Visualizador, seleccione **Mi grupo**.

Botón Ejecutar informe
Pulse este botón para generar el informe.

Ventana Criterios de informes de Alerta de atributo:

Utilice esta ventana del Visualizador para especificar los criterios para ver el informe Alerta de atributo, que puede utilizarse como ayuda para ver y gestionar las alertas de atributos.

Desde fecha
Escriba la primera fecha del rango de fechas para ver datos en el informe seleccionado. Utilice el formato `MM/DD/AA`. Por ejemplo, `01/01/01` representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Desde fecha** predeterminada es la de hoy.

Hasta fecha
Escriba la última fecha del rango de fechas para ver datos en el informe seleccionado. Utilice el formato `MM/DD/AA`. Por ejemplo, `01/01/01` representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Hasta fecha** predeterminada es la de hoy.

Para ver datos de un solo día, utilice la misma fecha en los campos **Desde fecha** y **Hasta fecha**.

Lista desplegable Estado
Seleccione un estado específico o seleccione **Todos** para realizar un informe de todos los estados para todas las alertas de atributos. Por ejemplo, si solo desea ver los cambios realizados en las alertas de atributos abiertas actualmente dentro del rango de fechas especificado, seleccione **Abrir** en la lista desplegable.

El estado predeterminado en la lista desplegable **Estado** es **Todos**, lo que muestra los generadores de alertas de atributo activos y caducados.

Lista desplegable Usuario
Seleccione un usuario del Visualizador por nombre de usuario o seleccione **Todos** para realizar informes de las alertas de atributos para todos los usuarios del Visualizador.

El usuario predeterminado en la lista desplegable es su nombre de usuario.

Botón Ejecutar informe
Pulse este botón para generar el informe.

Ventana Criterios de informes de Resumen de origen de datos:

Utilice esta ventana para especificar los criterios para ver el informe Resumen de origen de datos desde el Visualizador. El informe Resumen de origen de datos visualiza datos cargados en el sistema por el origen de datos. Los orígenes de datos le ayudan a saber dónde se originaron los datos de identidad.

Lista desplegable Origen de datos
Seleccione un origen de datos específica o seleccione **[todas]** para ver datos de todas los orígenes de datos.

Desde fecha
Escriba la primera fecha del rango de fechas para ver datos en el informe seleccionado. Utilice el formato `MM/DD/AA`. Por ejemplo, `01/01/01` representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Desde fecha** predeterminada es la de hoy.

Hasta fecha
Escriba la última fecha del rango de fechas para ver datos en el informe seleccionado. Utilice el formato MM/DD/AA. Por ejemplo, 01/01/01 representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Hasta fecha** predeterminada es la de hoy.

Para ver datos de un solo día, utilice la misma fecha en los campos **Desde fecha** y **Hasta fecha**.

Botón Ejecutar informe
Pulse este botón para generar el informe.

Ventana Criterios de informes de Divulgación:

Utilice esta ventana del Visualizador para especificar los criterios para ver el informe Divulgación, que puede ayudarle a ver y gestionar relaciones divulgadas. Las relaciones divulgadas no se descubren mediante la resolución de entidad y relación, si no que son enlaces manuales entre dos identidades. Estos enlaces manuales suelen crearse en el Visualizador, pero también pueden crearse colocando el par de códigos UMF de relación divulgada (<DR> y </DR>) en registros de identidad cargados y procesados por las interconexiones.

Desde fecha
Escriba la primera fecha del rango de fechas para ver datos en el informe seleccionado. Utilice el formato MM/DD/AA. Por ejemplo, 01/01/01 representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Desde fecha** predeterminada es la de hoy.

Hasta fecha
Escriba la última fecha del rango de fechas para ver datos en el informe seleccionado. Utilice el formato MM/DD/AA. Por ejemplo, 01/01/01 representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Hasta fecha** predeterminada es la de hoy.

Para ver datos de un solo día, utilice la misma fecha en los campos **Desde fecha** y **Hasta fecha**.

Botón Ejecutar informe
Pulse este botón para generar el informe.

Ventana Criterios de informes de Resumen de carga:

Utilice esta ventana para especificar los criterios para ver el informe Resumen de carga desde el Visualizador. Puede utilizar el informe Resumen de carga para determinar información general sobre la calidad de los datos de los archivos UMF que ha cargado en el Visualizador, junto con información de utilidad, tal como estadísticas de rendimiento y el número de resoluciones de entidades y alertas generadas por la carga del archivo.

Lista desplegable Código de origen de datos - Descripción
Seleccione un origen de datos específica o seleccione **[todas]** para ver datos cargados desde todas los orígenes de datos. Por ejemplo, si ha cargado registros de identidad desde varios archivos UMF en una sola fecha, puede restringir los datos del reporte a un solo origen de datos seleccionando el código de origen de datos correspondiente.

Desde fecha
Escriba la primera fecha del rango de fechas para ver datos en el informe seleccionado. Utilice el formato MM/DD/AA. Por ejemplo, 01/01/01 representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Desde fecha** predeterminada es la de hoy.

Hasta fecha
Escriba la última fecha del rango de fechas para ver datos en el informe seleccionado. Utilice el formato MM/DD/AA. Por ejemplo, 01/01/01 representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

La fecha **Hasta fecha** predeterminada es la de hoy.

Para ver datos de un solo día, utilice la misma fecha en los campos **Desde fecha** y **Hasta fecha**.

Botón Ejecutar informe
Pulse este botón para generar el informe.

Ventana Criterios de informes de Estado de alertas de rol:

Utilice esta ventana del Visualizador para especificar los criterios para generar el informe Estado de alertas de rol, que resume el estado de las alertas de rol dentro de un período de tiempo especificado y que puede utilizarse para gestionar las alertas de rol.

Desde fecha y Hora
Teclee la primera fecha del rango de fechas para generar datos en el informe. Utilice el formato MM/DD/AA. Por ejemplo, 01/01/01 representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

Utilizando el formato de 24 horas, entre la primera hora en el rango de horas para generar datos en el informe. Utilice el formato HH:MM. Por ejemplo, 09:00 representa 9:00 AM, y 20:30 representa 8:30 PM.

El valor predeterminado de **Desde fecha** y **Hora** es la fecha de hoy a las 00:00.

Hasta fecha y Hora
Teclee la última fecha del rango de fechas para ver imprimir datos en el informe. Utilice el formato MM/DD/AA. Por ejemplo, 01/01/01 representa el 1 de enero de 2001. O bien pulse el control del calendario y seleccione la fecha.

El valor predeterminado de **Hasta fecha** y **Hora** es la fecha de hoy a las 23:59.

Para ver datos de un solo día, seleccione una de las opciones siguientes:

- Entre la misma fecha en los campos **Desde fecha** y **Hasta fecha**.
- Entre 00:00 en el campo **Desde hora**, y 23:59 en el campo **Hasta hora**.

Rango de informes de puntuación de relación
Si desea restringir los resultados por puntuación de relación, teclee un rango de puntuaciones de relación en los campos **Desde** y **Hasta**.

El rango predeterminado es de 0 a 100, que son todas las puntuaciones de relación.

Lista desplegable regla de alerta de rol
Seleccione una regla específica de alerta de rol sobre la que realizar el informe.

Lista desplegable Nivel de alerta de rol
Seleccione un nivel de alerta de rol específico o seleccione **Todos** para realizar un informe de todas las alertas de rol.

Botón Ejecutar informe
Pulse este botón para generar el informe.

Análisis de datos con el kit de herramientas Analyst

Puede utilizar las herramientas y plantillas del kit de herramientas de Identity Insight Analyst para crear y personalizar informes de análisis y la información en un entorno de aplicación basado en navegador.

Informes sobre datos con los informes de IBM Cognos

El Kit de herramientas de analista proporciona un conjunto de informes de Cognos que se pueden utilizar para crear informes de Identity Insight personalizados.

La integración de IBM Cognos en Identity Insight crea una base para la posibilidad de personalizar los informes de Identity Insight para ajustar la información que necesita.

El kit de herramientas de analista incluye los siguientes elementos que se deben utilizar con IBM Cognos:

- Herramientas de Cognos Business Intelligence para consulta y desarrollo de aplicaciones
- Creación y despliegue de un modelo de datos de Identity Insight (desarrollado con Cognos Framework Manager)
- Informes de plantilla para el resumen de entidad y detalle de alerta de rol. Estos están pensados como punto de partida para la personalización y el desarrollo de aplicaciones.

Con los informes de Cognos y el modelo de infraestructura, tiene las herramientas necesarias para crear interfaces de usuario de Cognos personalizadas e informes basándose en el repositorio de Identity Insight. Puede utilizar las herramientas de Cognos incluidas para crear interfaces personalizadas y modificar plantillas proporcionadas por EAS.

En esta información del producto se utilizan los siguientes términos y conceptos:

Kit de herramientas de analista
Empaquetado de Identity Insight para los componentes de Cognos instalados y plantillas de ejemplo.

EntitySearcher
Aplicación de navegador de cliente ligero que combina lo mejor de las posibilidades de búsqueda por atributo y búsqueda por resolución en un cliente basado en navegador.

IBM Cognos Business Intelligence
El nombre de producto general del componente de Cognos que se incluye con Identity Insight.

Informe de Cognos
Especificación de salida basada en XML que se puede representar como:

una interfaz de usuario interactiva en el visor de Cognos, un archivo PDF, un archivo XML (para la representación personalizada) o varios formatos Excel (incluido CSV).

Informe activo
Cognos 10 presentaba informes activos, que son informes autocontenidos que tienen un aspecto más parecido al de las aplicaciones web que al de los informes de Cognos estándares.

Cognos Framework Manager
Herramienta de Cognos utilizada para modelar un origen de datos (normalmente una base de datos). El modelo de datos de Identity Insight se ha creado utilizando Framework Manager.

Modelo de datos Cognos
Representación lógica de uno o más orígenes de datos. Los autores de informe de Cognos utilizan el modelo de datos para crear informes interactivos.

Almacén de contenido de Cognos
Base de datos independiente utilizada por Cognos para almacenar objetos de Cognos como definiciones de informe, modelos de datos y consultas. El almacén de contenido no se utiliza para almacenar los datos de Identity Insight.

Análisis de datos utilizando el cliente ligero EntitySearcher

El cliente ligero EntitySearcher combina lo mejor de las prestaciones de búsqueda por atributo y de búsqueda por resolución en un cliente basado en navegador.

Identity Insight ofrece dos funciones de búsqueda principales para buscar entidades. La búsqueda por resolución, a veces se denomina PSearch o búsqueda de interconexión, utiliza la resolución de entidad para buscar resultados. La búsqueda por atributo, conocido como EQ o consulta mejorada, utiliza una búsqueda SQL más tradicional.

EntitySearcher combina estos dos criterios de búsqueda para ayudar a producir resultados óptimos y evitar la confusión sobre qué enfoque utilizar. La interfaz de cliente proporciona la familiar interfaz de búsqueda por atributo para especificar criterios de búsqueda. Se llama a uno o a ambos tipos de búsqueda dependiendo de los criterios de entrada y los resultados de cada búsqueda. Los resultados de ambas búsquedas se compilan, deduplican, se clasifican y se presentan en una cuadrícula de resultados de búsqueda.

Una mejora adicional de búsqueda permite buscar entidades que tienen una fecha de nacimiento que está dentro de un rango de fechas especificado. Esta búsqueda se produce cuando se utilizan la lista desplegable y el recuadro de selección **Expandir búsqueda por**. Por ejemplo, si se proporciona una fecha 1/6/1960 y un rango de 30 días, el rango de fechas efectivas utilizado en la búsqueda será del 2/5/1960 al 1/7/1960 [1/6/1960 menos 30 días y 1/6/1960 más 30 días]. El rango incluye los puntos finales.

Puede elegir la opción “Búsqueda estricta” y sólo se utilizará la búsqueda por atributo (EQ). Una búsqueda estricta se realiza de forma predeterminada si se cumple alguna de las condiciones siguientes.

- Se entra un único atributo para los criterios de búsqueda.
- Hay elementos incompletos en los criterios de búsqueda de atributos.

- Se utilizan caracteres comodín en los criterios de búsqueda de atributos. Por ejemplo *.
- Los criterios de búsqueda de atributos DOB (Fecha de nacimiento) incluyen un rango de fechas.

El URL para iniciar EntitySearcher es:

`http://servidor:puerto_instalación/EntitySearcher/`

En los resultados de búsqueda, puede pulsar en una versión de informe de Cognos del resumen de entidad de Identity Insight, el componente de gráfico o cualquier otro destino enlazable por http solicitando al administrador del sistema que configure los valores URL_ENTITY_DETAIL y URL_ENTITY_GRAPH de la tabla de base de datos COMPONENT_CONFIG

Búsqueda de entidades utilizando EntitySearcher:

Puede buscar entidades basándose en datos de atributos y en qué clase de búsqueda desea realizar.

Acerca de esta tarea

El cliente ligero EntitySearcher combina lo mejor de las prestaciones de búsqueda por atributo y de búsqueda por resolución en un cliente basado en navegador. Una vez que se realiza una búsqueda está disponible una interfaz de usuario para ver los resultados de búsqueda.

Procedimiento

1. Abra EntitySearcher en el navegador.

   El URL para iniciar EntitySearcher es:

   `http://servidor:puerto_instalación/EntitySearcher/`

   Por ejemplo, `http://localhost:13510/EntitySearcher/`. El *puerto_instalación* predeterminado es 13510, pero el número de puerto puede cambiarse. Consulte al administrador del sistema si no está seguro del nombre de servidor o número de puerto correctos.
2. En el panel **Buscar entidades**, especifique los criterios de búsqueda. De forma predeterminada se visualiza un único atributo para la búsqueda de entidad.
   a. En la **Lista de atributos**, seleccione el tipo de atributo para los criterios de búsqueda de atributo.
   b. Especifique los criterios de búsqueda.

Opción	Descripción
Tiene criterios de búsqueda de atributos adicionales.	A la derecha del atributo existente, pulse **+**.
No tiene criterios de búsqueda de atributos adicionales.	Vaya al paso siguiente. **Nota:** Se realiza una búsqueda estricta cuando se especifica sólo un único atributo para los criterios de búsqueda.

3. Decida si desea realizar una búsqueda combinada o sólo una búsqueda estricta.

Opción	Descripción
Realizar una búsqueda combinada	La búsqueda combinada se realiza de forma predeterminada.

Opción	Descripción
Realizar sólo una búsqueda estricta.	Seleccione el recuadro de selección **Búsqueda estricta**. **Nota:** De forma predeterminada se realizará una búsqueda estricta si se cumple alguna de las siguientes condiciones. • Se entra un único atributo para los criterios de búsqueda. • Hay elementos incompletos en los criterios de búsqueda de atributos. • Se utilizan caracteres comodín en los criterios de búsqueda de atributos. Por ejemplo *. • Los criterios de búsqueda de atributos DOB (Fecha de nacimiento) incluyen un rango de fechas.

4. Pulse **Buscar**.

Resultados

El panel **Resultados de búsqueda** lista todos los resultados de búsqueda de entidad. Los resultados se clasifican de acuerdo con la puntuación de similitud y, si está disponible, la puntuación de nombre. Los resultados de búsqueda por resolución de puntuación alta (>86) se clasifican en primer lugar, seguidos de los resultados de búsqueda por atributo de puntuación alta. Siguen los resultados de búsqueda de resolución de puntuación más baja.

Qué hacer a continuación

Ver un resumen de entidad para un resultado de búsqueda.
En la columna **ID de entidad** de fila de resultado de búsqueda deseada en el panel **Resultados de búsqueda**, pulse el valor de número de **ID de entidad** subrayado.

Nota: Es posible que el administrador del sistema tenga que configurar el valor URL_ENTITY_DETAIL de la tabla de base de datos COMPONENT_CONFIG para habilitar esta funcionalidad.

Ver un gráfico de entidad para un resultado de búsqueda.
En la columna **ID de entidad** de fila de resultado de búsqueda deseada en el panel **Resultados de búsqueda**, pulse el icono de gráfico.

Nota: Es posible que el administrador del sistema tenga que configurar el valor URL_ENTITY_GRAPH de la tabla de base de datos COMPONENT_CONFIG para habilitar esta funcionalidad.

Informe de alerta de rol de Cognos de ejemplo

El informe de alerta de rol de Cognos de ejemplo muestra información sobre las entidades y las relaciones de entidad implicadas en la alerta y se puede personalizar utilizando herramientas de Cognos.

El informe de alerta de rol hace uso de la tecnología de Informe activo presentado en Cognos 10 y proporciona una experiencia de usuario más rica.

Para presentar la información de alerta cada vía de acceso de una alerta aparece en una pestaña independiente creada de forma dinámica. La información de resumen de alerta de rol se presenta en la parte superior del informe y están disponibles instantáneas de entidad (el estado de la entidad en el momento en que se ha generado la alerta) si el usuario desea ver esa información. Una sección de detalles coincidentes expandida muestra información de puntuación de Identity Insight.

Acceso a datos

El informe de detalle de alerta de rol hace un amplio uso de nuevas vistas de base de datos de Identity Insight. Este enfoque permite más control sobre el acceso a datos. Por ejemplo, las estructuras de unión y consulta las define el SQL de vista y no se dejan al motor de Cognos. También proporciona una capa de abstracción de las tablas de datos subyacentes, lo que permite que el esquema subyacente se modifique sin que ello afecte directamente a los informes de Cognos.

Aunque hay nuevas vistas de base de datos de Identity Insight para soportar la pantalla de detalle de alerta de rol de Cognos, el servidor Cognos proporciona y controla el acceso a datos mediante el modelo.

Notas técnicas

El informe de detalle de alerta de rol de Cognos hace uso de la tecnología de Informe activo. Esto significa que el único tipo de salida soportado es HTML. A diferencia de un informe de Cognos estándar, se consultan todos los datos utilizados por el informe antes de que se visualice el informe. Esto permite que los Informes activos mantengan su interactividad cuando se desconectan del servidor Cognos. Los Informes activos se pueden distribuir como archivos .MHT (HTML MIME) y se crean desde la página de inicio de Cognos o accediendo a un URL para el informe desde cualquier navegador web que soporte archivos MHT. Otro efecto secundario de la carga de todos los datos de informe por adelantado es que no es necesario volver a cargar la página cuando el usuario interactúa con la interfaz de usuario.

El informe de alerta de rol de Cognos necesita un ID de alerta de rol como parámetro. Si se accede directamente al informe, se le solicitará al usuario un ID de alerta de rol. Si se accede al informe como un componente, el ID de alerta de rol se puede pasar como un parámetro de URL. El formato de parámetro para pasar parámetros de Cognos a través de URL consiste en añadir una “p_” al principio del nombre de solicitud. En el caso del informe de alerta de rol, el parámetro que se espera es **pAlertID**, por lo tanto la sintaxis será: **p_pAlertID**. Por ejemplo: **&p_pAlertID=55&**.

Las vistas de base de datos de Identity Insight creadas para soportar los componentes de Cognos se denominan utilizando el prefijo COG para que sean identificables más fácilmente.

Firefox 3.x necesita que se instalen plug-ins adicionales para permitirles visualizar archivos MHT correctamente.

Informe de resumen de entidad de Cognos de ejemplo

El informe de resumen de entidad de Cognos de ejemplo proporciona toda la información conocida sobre una entidad y se puede personalizar utilizando herramientas de Cognos.

En el informe de resumen de Cognos, los datos de entidad se resumen y el usuario puede decidir qué detalles de entidad se deben explorar.

Notas técnicas

El resumen de entidad de Cognos hace un amplio uso de objetos de consulta definidos por informe, a diferencia de las vistas de base de datos reales. Estas consultas virtuales se basan en el modelo de datos de Cognos y se crean arrastrando objetos de modelo hasta el creador de consultas de informe y estableciendo propiedades. El resumen utiliza un objeto de "bloque condicional" para visualizar la sección de detalles. Debido al uso de un bloque condicional para hacer que la pantalla se parezca más a una interfaz de usuario (y no un informe), las versiones de salida en PDF, texto y Excel de este informe no tienen el aspecto ni se comportan como la salida HTML predeterminada.

El servidor de informes de Cognos consulta sólo la información que necesita para visualizar las secciones visibles del informe. Por ejemplo, la información de alerta de rol sólo se consulta cuando el usuario elige ver esa información. Aunque esto produce tiempos de carga inicial más rápidos y acceso a datos más inteligente, tiene un coste. La página debe volverse a cargar cuando cambia la sección de detalle. Esta recarga de página es automática y no se necesita ninguna interacción del usuario, pero éste debe esperar a que se renueve la página antes de que pueda tener lugar cualquier interacción de usuario adicional.

El informe de resumen de Cognos necesita un ID de entidad de Identity Insight como único parámetro. Si el informe se ejecuta desde la página de inicio de Cognos, se le solicitará al usuario que especifique un ID de entidad. Aunque es posible que algunos usuarios lo inicien desde la página de inicio de Cognos y especifiquen un ID de entidad, es más probable que el resumen de Cognos sea un componente integrado y se le llame desde otra aplicación como una herramienta de gestión de casos o de flujo de trabajo. En este último caso de uso, el ID de entidad de Identity Insight se puede pasar como un parámetro de URL al resumen de Cognos y la página de solicitud de ID de entidad no se visualizará.

El formato de parámetro para pasar parámetros de Cognos a través de URL consiste en añadir una "p_" al principio del nombre de solicitud. En el caso del informe de resumen, el parámetro que se espera es **pEntityID**, por lo tanto la sintaxis será: **p_pEntityID**. Por ejemplo: **&p_pEntityID=5&**.

Identificación e instalación de componentes de Cognos

Los componentes de IBM Cognos se instalan para utilizar y modificar las característica de creación de informes de IBM Identity Insight Cognos.

Antes de empezar

Debe instalar IBM Business Intelligence Reporting antes de desplegar los informes de IBM Identity Insight Cognos.

Nota: Si tiene instalada una instancia existente de IBM Cognos Business Intelligence Reporting v10.1.0 o posterior, puede desplegar los informes de IBM Cognos Insight Cognos en ella.

Para modificar los metadatos de los informes de Identity Insight Cognos, debe instalar IBM Cognos Framework Manager.

Procedimiento

1. Instale IBM Business Intelligence Reporting v10.1.0 o posterior.
   a. Instale el componente Cognos Reporting utilizando las instrucciones de Cognos detalladas.
2. Instale IBM Cognos Framework Manager v10.1.0 o posterior.
   a. Instale el componente Cognos Reporting utilizando las instrucciones de Cognos detalladas.

Qué hacer a continuación

Desplegar los informes de Identity Insight en Cognos.

Despliegue de informes de Identity Insight en Cognos:

Para habilitar los informes de resumen de entidad y alerta de rol de IBM Identity Insight Cognos, primero debe desplegarlos en IBM Cognos Business Intelligence Reporting.

Antes de empezar

Instale IBM Cognos Business Intelligence Reporting.

Procedimiento

1. Copie el paquete de despliegue de informes de Identity Insight Cognos en la instalación de IBM Cognos Business Intelligence Reporting. Identity Insight proporciona dos versiones de los informes, dependiendo si desea aprovechar la modalidad de consulta dinámica o compatible de Cognos

Tabla 32. Ubicaciones de paquete de despliegue de informes de Identity Insight Cognos

Copiar de archivo de	Copiar de archivo en
*<directorio de instalación de producto>*ibm-home/cognos/deployment/IdentityInsight_v9.0_CompatibleQueryMode.zip o *<directorio de instalación de producto>*/ibm-home/cognos/deployment/IdentityInsight_v9.0_DynamicQueryMode.zip	*<directorio de instalación de Cognos>*/deployment/

2. Vaya a la página Cognos Connection del navegador. La página está ubicada en http://*<nombre_servidor_cognos_o_dirección_IP>*:*<núm_puerto_cognos>*:cognos/index.html .
3. Pulse **Iniciar** > **IBM Cognos Administration**.

   Nota: Para acceder a IBM Cognos Administration, debe tener los permisos necesarios para la característica protegida de tareas de administración.
4. Pulse la pestaña **Configuración** y pulse **Administración de contenido**. En la barra de herramientas, pulse el icono **Nueva importación**
5. En la lista de paquetes de despliegue disponibles, seleccione IdentityInsight_v9.0_Cognos. Cuando se le solicite una contraseña, escriba ISII4YOU. Pulse **Aceptar**.
6. En el panel nombre y descripción, pulse **Siguiente**. El panel nombre y descripción no necesita modificación.

7. En el panel de contenido de carpeta pública, en la lista de **contenido de carpetas públicas** disponible, seleccione el recuadro de selección de carpeta **ISII**. Pulse **Siguiente**.
8. En el panel contenido de directorio, pulse **Siguiente**. El panel contenido de directorio no necesita modificarse.
9. En el panel opciones generales, pulse **Siguiente**. El panel opciones generales no necesita modificarse.
10. Revise el resumen y pulse **Siguiente**.
11. Seleccione **Guardar y ejecutar una vez**. Pulse **Finalizar** para importar el informe. Pulse **Ejecutar**. Las opciones de ejecución no necesitan modificarse.
12. Antes de cerrar el recuadro de diálogo, elija ver los detalles de la importación. Pulse **Aceptar**. Si el estado se visualiza como `"En ejecución"`, pulse **Renovar**. Tras el despliegue satisfactorio, el estado se visualiza como `"Con éxito"`. Pulse **Cerrar**.

Qué hacer a continuación

1. Verifique que los informes se han desplegado.
2. Modifique la configuración de base de datos de despliegue de informes de Cognos de Identity Insight.

Verificación del despliegue de informes de Identity Insight:

Después de desplegar los informes, debe verificar el despliegue antes de ejecutar los informes.

Antes de empezar

Desplegar los informes de Identity Insight en Cognos.

Procedimiento

1. Vaya a la página Cognos Connection en el navegador. La página se encuentra en http://<*nombre_servidor_cognos_o_dirección_IP*>:<*núm_puerto_cognos*>:cognos/index.html.
2. En la pestaña de carpetas públicas, verifique que la carpeta pública **ISII** existe.
3. Seleccione la carpeta **ISII**.
4. Verifique que existe un único objeto de paquete de **Identity_Insight**. Un objeto de paquete se visualiza como una carpeta azul.
5. Verifique que los informes de **ISII_EntityResume** y de **ISII_RoleAlertDetailActive** existen.

Qué hacer a continuación

Modifique la configuración de base de datos de despliegue de informes de Cognos de Identity Insight.

Modificación de la configuración de base de datos de despliegue de informe de Identity Insight Cognos:

Después de desplegar y verificar los informes, debe modificar la configuración de base de datos de despliegue de informe de Identity Insight Cognos. Nota: si está utilizando los informes de modalidad de consulta dinámica, consulte la documentación de Cognos para crear una conexión JDBC dentro dentro de Cognos (en lugar de seguir el procedimiento listado a continuación).

Antes de empezar

Desplegar los informes de Identity Insight en Cognos.

Procedimiento

1. Vaya a la página de Administrador de Cognos en el navegador.
2. En el lado izquierdo, pulse **Conexión de origen de datos**.
3. Seleccione el objeto de origen de datos **ISII**.
4. Seleccione el objeto de conexión de origen de datos **ISII**.
5. Seleccione el objeto de inicio de sesión **ISII**.
   a. Pulse **Establecer propiedades**.
   b. En la pestaña **Inicio de sesión**, pulse **Editar el inicio de sesión ...**.
   c. Modifique el enlace para incluir el nombre de usuario y la contraseña de base de datos de Identity Insight. Pulse **Aceptar**.
   d. Pulse **Aceptar**.
6. Pulse **Establecer propiedades** para el objeto de conexión de origen de datos.
7. En la pestaña **Conexiones**, siga las instrucciones para el tipo de base de datos de Identity Insight.

Tipo de base de datos de Identity Insight	Instrucciones
DB2	1. Seleccione **IBM DB2** para el tipo. 2. Seleccione el icono **Editar la cadena de conexión**. 3. Modifique el valor de nombre de base de datos DB2. Si se necesita un esquema, añada `currentSCHEMA=<esquema>` al parámetro de serie de conexión DB2. 4. Pulse **Probar la conexión...**. 5. Pulse **Probar**. 6. Verifique que el estado es `Con éxito`.
Oracle	1. Seleccione **Oracle** para el tipo. 2. Pulse **Aceptar** cuando aparezca el aviso `la serie de conexión actual se perderá`. 3. Seleccione el icono **Editar la cadena de conexión**. 4. Modifique la serie de conexión SQL*Net. 5. Pulse **Probar la conexión...**. 6. Pulse **Probar**. 7. Verifique que el estado es `Con éxito`.

8. Pulse **Cerrar** para cerrar el panel de resultados de prueba.
9. Pulse **Cerrar** para cerrar el panel de conexiones de prueba.
10. Pulse **Aceptar** para cerrar el panel de conexiones de prueba.
11. Pulse **Aceptar** para cerrar el panel de propiedades establecidas.

Análisis de datos utilizando la herramienta gráfica

La herramienta gráfica InfoSphere Identity Insight proporciona a los usuarios la posibilidad de analizar gráficos basados en web que visualizan alertas, relaciones de entidad y otra información de entidad de Identity Insight.

Para representar gráficos, la herramienta gráfica necesita que una interconexión de producto esté activa y en ejecución en segundo plano.

Los gráficos representados por la herramienta gráfica son similares a los gráficos representados en el componente i2 Analyst Notebook. Sin embargo, las ventajas de utilizar la herramienta gráfica incluyen la posibilidad de incorporar e iniciar los gráficos dentro de una herramienta de gestión de casos existente u otra aplicación. O los usuarios pueden utilizar un URL o página de inicio web para ver e iniciar los gráficos dentro de un navegador web. No es necesario instalar e iniciar i2 Analyst Notebook para ver los gráficos representados por la herramienta gráfica.

Gráfico de alerta

El gráfico de alerta producido por la herramienta gráfica muestra una alerta de rol específica, basándose en el ID de alerta. El gráfico de alerta le ayuda a visualizar las entidades involucradas en la alerta de rol y los atributos que enlazan las entidades.

Una alerta de rol se produce cuando una o más entidades está enlazada mediante una relación que cumple o excede una regla de alerta de rol configurada. Las alertas de rol se basan en roles y normas de alerta de rol configurados y pueden indicar:

- un aviso o un problema, por ejemplo un cliente está enlazado a un sospechoso en una lista de observación
- relaciones de interés, por ejemplo un cliente también es proveedor o un empleado está enlazados a varios clientes a través de un número de teléfono particular

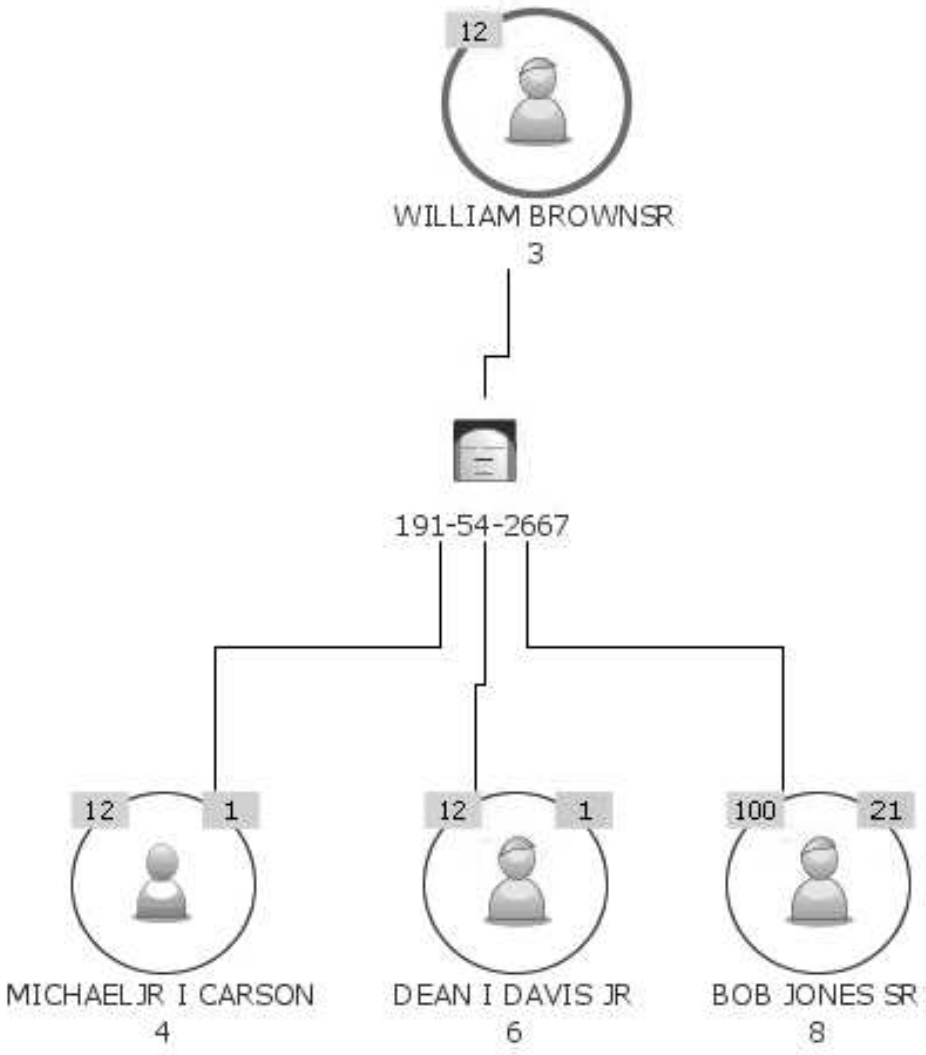
Sugerencias para utilizar el gráfico de alerta

- Si ve un indicador de entidades relacionadas para una entidad implicada en la alerta, utilice la opción de menú que aparece al pulsar el botón derecho del ratón **Mostrar entidades relacionadas restantes** para mostrar las entidades relacionadas restantes. El gráfico vuelve a dibujarse para visualizar todas las entidades relacionadas con la entidad seleccionada. El gráfico también enlaza automáticamente esas entidades restantes con las entidades existentes en el gráfico con el que esas entidades restantes también están relacionadas.
- El gráfico de alerta muestra sólo los atributos para cada entidad que ha contribuido a la alerta. Para ver todos los atributos asociados con una entidad determinada, pulse el botón derecho del ratón en la entidad y seleccione **Mostrar atributos restantes**.
- Para ver el resumen de entidad para una entidad determinada en el gráfico, pulse el botón derecho del ratón en la entidad y seleccione **Mostrar resumen**. El resumen de entidad proporciona detalles adicionales sobre la entidad, incluidas las identidades de esa entidad y otras alertas en las que la entidad está implicada. Esta opción del menú que aparece al pulsar el botón derecho del ratón sólo está disponible si el enlace está configurado correctamente y se tiene acceso al producto que genera resúmenes de entidades, como el kit de herramientas de analista.

Gráfico de entidad

El gráfico de entidad producido por la herramienta gráfica le ayuda a visualizar las relaciones entre la entidad especificada y todas las entidades relacionadas con dicha entidad, basándose en los atributos compartidos.

El gráfico Entidad muestra las relaciones entre entidades utilizando capas alternativas de entidades y atributos.



Primera capa - Entidad principal

Cuando inicialmente examine el gráfico, la primera capa contiene la entidad principal. La *entidad principal* es siempre la entidad que ha especificado o seleccionado para representar el gráfico de entidad. Visualmente, la línea alrededor del nodo de entidad principal siempre es más gruesa, para que pueda detectar la entidad principal independientemente de dónde se puede mostrar en el gráfico.

La *entidad superior* es la entidad visualizada en la primera capa del gráfico, en la parte superior. Inicialmente, la entidad principal es también la entidad superior. Pero cualquier entidad puede convertirse en la entidad superior, simplemente utilizando la opción que aparece al pulsar el botón derecho del ratón **Mover a la parte superior**.

Segunda capa (y capas pares adicionales) - Atributos compartidos

La segunda capa consta de los atributos compartidos que enlazan la entidad superior a las entidades en la tercera capa del gráfico. Los atributos que se muestran en el gráfico muestran el tipo y el valor del atributo.

Si hay capas adicionales del gráfico, las capas pares siempre contienen los atributos compartidos que enlazan las entidades visualizadas por encima y por debajo de la capa de atributo.

Tercera capa (y capas impares adicionales) - Entidades relacionadas
La tercera capa del gráfico muestra las entidades que están relacionadas con la entidad superior a 1 grado de separación.

Si hay capas adicionales del gráfico, las capas impares siempre contienen entidades relacionadas con la capa de entidad anterior, basándose en la capa de atributos compartidos entre las dos capas de entidad. Las entidades visualizadas en estas capas de entidad subsiguientes están relacionadas con la entidad superior en los correspondientes grados de separación: las entidades en la tercera capa están relacionadas con la entidad superior a 2 grados de separación. Las entidades en la quinta capa están relacionadas con la entidad superior a 3 grados de separación y así sucesivamente.

Consejos para utilizar el gráfico de entidad

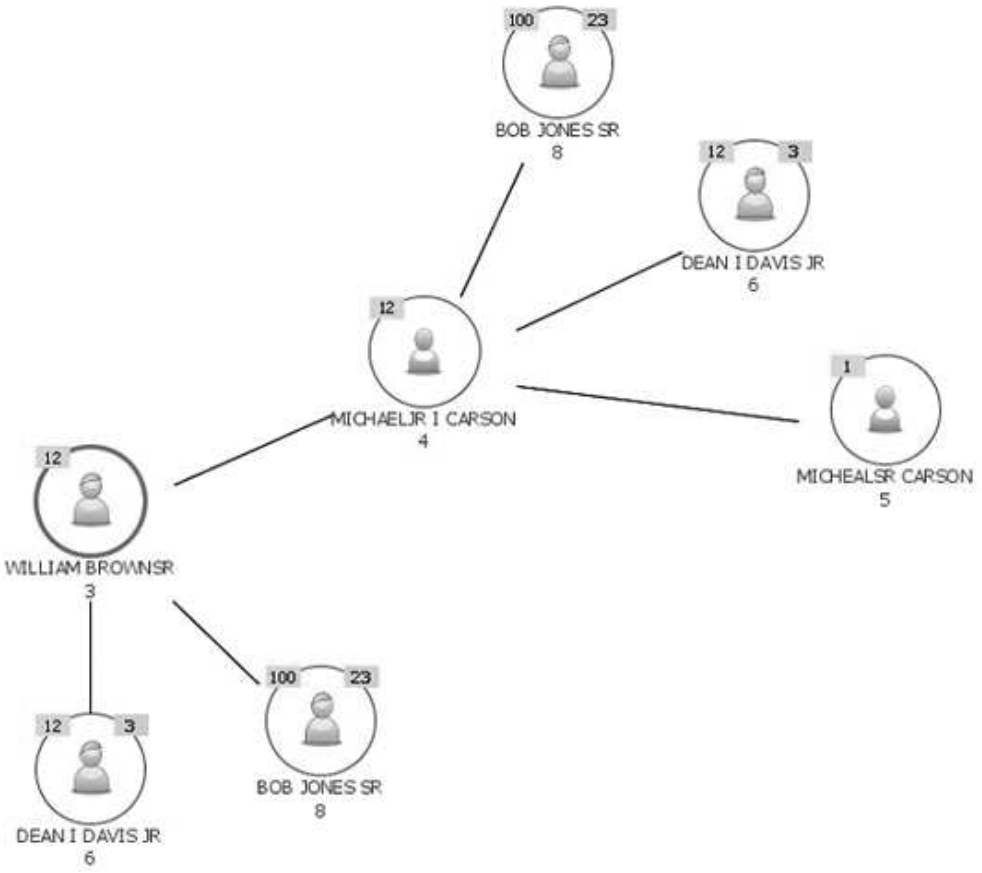
Los gráficos de entidad pueden contener muchas capas. A continuación se proporcionan algunos consejos para ayudarle a clasificar toda la información de atributos y entidades visualizada en un gráfico de entidad.

- Para ver más detalles sobre una entidad:
  - Utilice la opción del menú que aparece al pulsar el botón derecho del ratón **Mostrar entidades relacionadas restantes** para explorar las relaciones para una entidad específica que no se visualizan actualmente en el gráfico.
  - Utilice el filtro rápido **Mostrar la vía de acceso en la parte superior** para mostrar cómo una entidad o atributo está relacionado con la entidad superior. Este filtro oculta temporalmente las entidades y los atributos no relacionados del gráfico.
  - Conmute al gráfico de red social para crear un gráfico que le ayude a ver y centrarse en las relaciones entre entidades. El gráfico de red social no visualiza atributos compartidos en el gráfico, pero los atributos compartidos se listan en el Explorador de atributos. Pulse el botón derecho del ratón en la entidad desde la que desea crear el gráfico de red social y seleccione **Crear nuevo gráfico - Red social**.
  - Utilice el filtro rápido **Mostrar sólo entidades relacionadas** para crear un "mini" gráfico de red social. Este filtro rápido oculta todos los atributos del gráfico y muestra sólo entidades relacionadas con la entidad elegida a 1 grado de separación. (La *entidad elegida* es la entidad en la que ha pulsado el botón derecho del ratón para aplicar el filtro rápido.)
  - Utilice el filtro rápido **Mostrar sólo atributos y entidades relacionados** para resaltar la entidad y mostrar sólo los atributos y entidades que están relacionados con la entidad seleccionada.
  - Utilice la opción del menú que aparece al pulsar el botón derecho del ratón **Mostrar resumen de entidad** para ver el resumen de entidad de cualquier entidad del gráfico. El resumen de entidad proporciona detalles adicionales y contexto sobre dicha entidad, como las identidades asociadas con la entidad, otras alertas en las que la entidad está implicada, etcétera. (Si el enlace al resumen de entidad no se ha configurado, como por ejemplo al resumen de entidad en el kit de herramientas de analista, esta opción no aparece en el menú que aparece el pulsar el botón derecho del ratón.)
- Para ver la vía de acceso entre dos entidades en el gráfico:

  - Utilice el filtro rápido **Mostrar la vía de acceso en la parte superior** para visualizar cómo una entidad determinada en el gráfico está relacionada con la entidad superior. Este filtro rápido es especialmente útil cuando el gráfico contiene varias capas.
  - Utilice la opción del menú que aparece al pulsar el botón derecho del ratón **Mover a la parte superior** para mover una entidad a la parte superior del gráfico y volver a visualizar los atributos y entidades existentes basándose en cómo se relacionan con la nueva entidad superior. No se añade información nueva al gráfico
- Para ver más detalles sobre un atributo:
  - Utilice el filtro rápido **Mostrar sólo atributos** para centrar la información del gráfico en una entidad. El filtro le ayuda a ver sólo los atributos para la entidad seleccionada.
  - Utilice la opción del menú que aparece al pulsar el botón derecho del ratón **Mostrar atributos restantes** para visualizar todos los atributos para una entidad determinada, incluso aquellos atributos no compartidos por ninguna otra entidad en el gráfico actual.
  - Utilice el **Explorador de atributos** para resaltar las entidades en el gráfico que comparten un atributo determinado. El valor de la columna **Entidades** puede guiarle. Cuanto mayor es el número en la columna, más entidades visualizadas en el gráfico comparten ese atributo.
- Para reorganizar las entidades y atributos en otros patrones y formas, utilice el menú que aparece al pulsar el botón derecho del ratón para cambiar el diseño de gráfico de **En capas** a **Radial**.

Gráfico de red social

El gráfico de red social le ayuda a visualizar las relaciones entre la entidad seleccionada y todas las entidades a las que está enlazada la entidad seleccionada. Al utilizar este gráfico exclusivo, obtiene otra forma de ver "quién conoce a quién".



El gráfico de red social muestra:

- Enlaces de entidad a entidad: Puede ver todas las entidades relacionadas con la entidad principal (concentrador). Sin embargo, los atributos que enlazan las entidades no se muestran en el gráfico pero son accesibles utilizando el Explorador de atributos en combinación con el gráfico.
- Clústeres de relaciones: El gráfico de red social es exclusivo en el sentido que muestra las entidades relacionadas en grupos o clústeres. Este gráfico puede ayudarle a ver todos los clústeres de relaciones a los que pertenece una entidad particular y a buscar patrones entre los clústeres y las relaciones.

Puede expandir el gráfico para mostrar todas las entidades relacionadas para cualquier entidad. Cada vez que muestra todas las entidades relacionadas con una entidad determinada, ese nodo de entidad se convierte en la entidad concentradora de un nuevo clúster de relaciones.

Para mantener la integridad de cada clúster de relaciones, una entidad puede mostrarse en el gráfico varias veces en varios clústeres de relaciones. Pero cada entidad sólo se muestra una vez en cada clúster de relaciones. Para ver cada clúster de relaciones del que forma parte la entidad, seleccione la entidad pulsando en ese nodo. El interior del nodo de entidad seleccionado cambia a azul en cada clúster de relaciones del que forma parte la entidad.

Cuando una entidad es la entidad concentradora, el indicador de entidades relacionadas no se visualiza, porque todas las entidades relacionadas con la entidad concentradora ya se muestran en el clúster de relaciones. Cuando la

entidad es una de las entidades relacionadas del clúster de relaciones y tiene otras relaciones que no se visualizan en ese clúster, se muestra un indicador de entidades relacionadas.

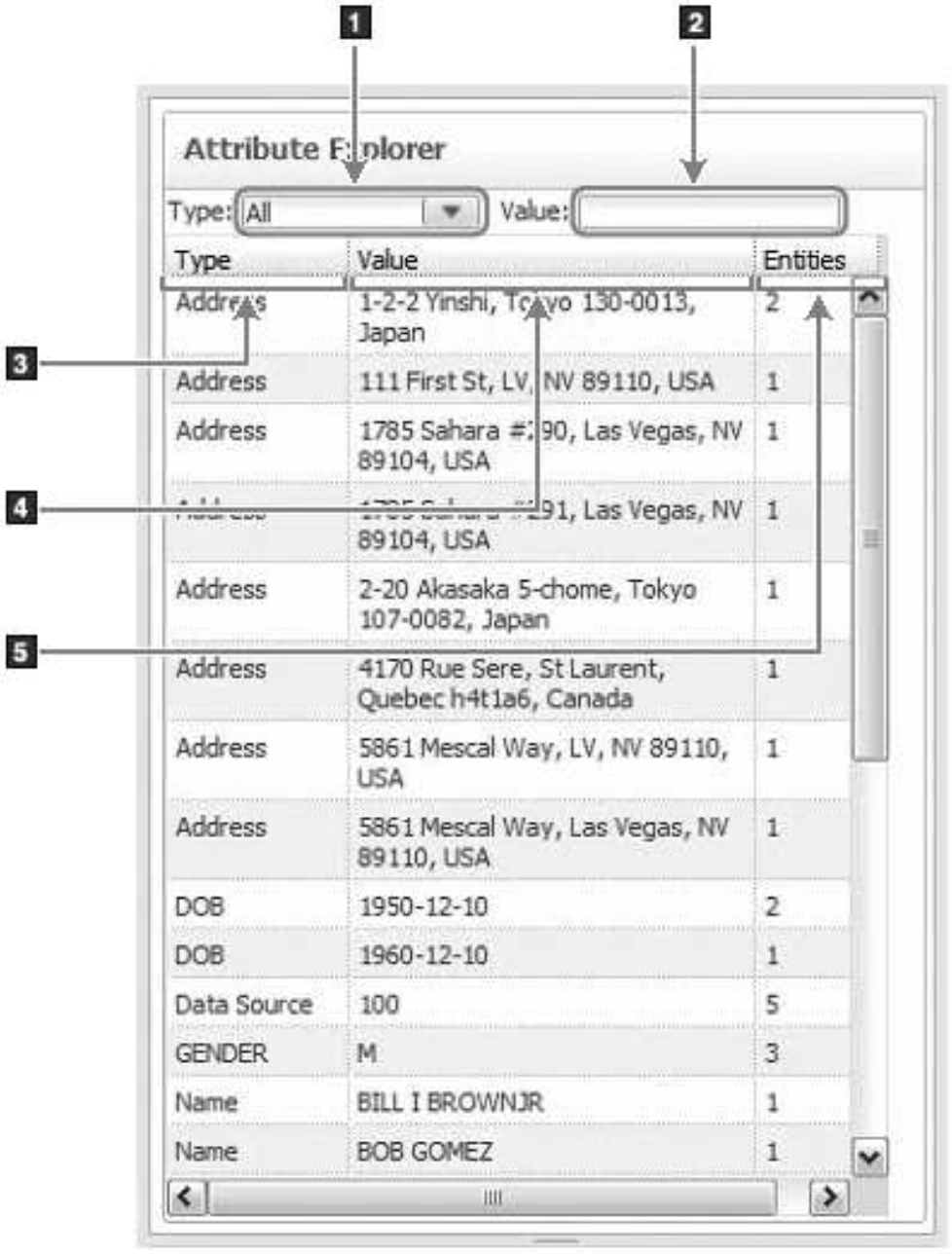
Sugerencias para utilizar el gráfico de la red social

- Utilice la opción que aparece al pulsar el botón derecho del ratón **Mostrar entidades relacionadas restantes** para expandir las entidades relacionadas para una o más entidades en el gráfico. Cada expansión crea otro clúster de relaciones. Busque patrones entre los clústeres.
- Si aparecen en el gráfico varios clústeres de relaciones, intente alejarse para buscar patrones mayores y contexto en los clústeres. Por ejemplo, si una entidad determinada aparece en cada clúster o varios clústeres, es posible que esa entidad tenga una gran influencia dentro de una esfera particular. O esa entidad puede ser clave para conectar varios clústeres de relaciones.
- Utilice el **Explorador de atributos** para ver qué atributos enlazan las entidades relacionadas. Seleccione una fila de atributos determinada para resaltar cada entidad en el gráfico que comparte ese atributo. El valor de la columna **Entidades** puede mostrarle qué atributos están compartidos por la mayoría de las entidades.

Explorador de atributos

Componente de la herramienta gráfica, el explorador de atributos es una tabla que lista todos los atributos por tipo y valor que están asociados con todas las entidades en el gráfico visualizado actualmente. El Explorador de atributos se acopla automáticamente a la derecha del lienzo de gráfico.

Partes del explorador de atributos



Número de llamada de imagen	Elemento	Descripción
1	Lista desplegable de tipo	Seleccione un tipo de atributo para filtrar los datos de atributo que se visualizan en el Explorador de atributos. Cuando se utiliza la lista desplegable Tipo, no se filtra el gráfico, sólo se filtran los datos del Explorador de atributos. Por ejemplo, puede seleccionar **SSN** para filtrar los datos en el Explorador de atributos para mostrar sólo los números de seguridad social. Esta lista desplegable no contiene necesariamente cada tipo de atributo configurado para el producto. La lista contiene sólo los tipos de atributos asociados con las entidades que se visualizan actualmente en el gráfico.
2	Recuadro de texto de valor	Escriba datos en este campo para limitar la información de atributo visualizada en la tabla, basándose en valores de atributo. El Explorador de atributos busca cada carácter especificado y devuelve la lista de valores de atributo que coinciden exactamente con la entrada, si la coincidencia es una coincidencia de datos exacta o parcial. Por ejemplo, si especifica 123, el Explorador de atributos filtra la lista de atributos sólo a los tipos de atributos que contienen 123 en algún lugar del valor de atributo. **Nota:** El Explorador de atributos no reconoce los caracteres comodín. Cualesquiera que sean los caracteres que especifique en el recuadro de texto, el Explorador de atributos busca una coincidencia literal exacta con ese carácter. Por lo tanto, si especifica un carácter comodín típico, como por ejemplo un * (asterisco), el Explorador de atributos busca una coincidencia de valor de datos literal con el carácter *.

Número de llamada de imagen	Elemento	Descripción
3	Columna de tipo	Muestra los tipos de atributo que se visualizan actualmente en el gráfico. Los elementos de columna coinciden con las descripciones configuradas para los tipos de atributo en la Consola de configuración. Por ejemplo, un tipo de atributo de tarjeta de crédito puede mostrarse como **CC** o **tarjeta de crédito**, en función de cómo se haya configurado en la Consola de configuración. La columna no contiene necesariamente cada tipo de atributo configurado para el producto. La columna sólo contiene los tipos de atributo que se visualizan actualmente en el gráfico.
4	Columna de valor	Muestra los valores para los tipos de atributo que se visualizan actualmente en el gráfico. Por ejemplo, puede ver un valor de **04-01-1962** que corresponde a un tipo de atributo de fecha de nacimiento.
5	Columna de entidades	Indica cuántas entidades visualizadas en el gráfico comparten este tipo y valor de atributo. Esta información puede ayudarle a identificar los atributos compartidos con más frecuencia para la exploración adicional.

Sugerencias para utilizar el Explorador de atributos

El Explorador de atributos puede ayudar al análisis de los gráficos, especialmente cuando el gráfico contiene mucha información.

- Utilice la columna **Entidades** para buscar atributos que sólo están asociados con una entidad en el gráfico. Busque un 1 en la columna. Aunque el gráfico muestra sólo los atributos que enlazan entidades, el Explorador de atributos muestra todos los atributos asociados con todas las entidades en el gráfico. Estos atributos no enlazan la entidad con ningún otro nodo de entidad en el gráfico, pero pueden hacer que merezca la pena explorar adicionalmente una entidad determinada.
- Restrinja la información que aparece en el Explorador de atributos a un tipo de atributo seleccionando un tipo en la lista desplegable **Tipo**. Por ejemplo, si ve y selecciona **Números de teléfono**, el Explorador de atributos muestra sólo los atributos de número de teléfono y sus valores.
- Resalte todas las entidades en el gráfico que comparten el mismo atributo seleccionando un atributo (fila de tabla) en el Explorador de atributos.
- Busque en los datos del gráfico existente coincidencias o valores de atributo comunes entrando datos en **Valor**. Por ejemplo, si ha entrado 123, el Explorador de atributos puede devolver cualquiera o todos los atributos coincidentes siguientes:

Tipo	Valor
Dirección	**123** Main Street, Anywhere, California, 1**123**4, USA
Dirección	97-**123** Rue Sere, St. Laurent, Quebec, H4T1A6, Canada
Número de teléfono	555-222-5**123**
Identificador de impuesto	554-**123**-3**123**

- También puede especificar más de un valor completo o parcial a la vez en **Valor**. Entonces el Explorador de atributos trata los valores múltiples como una consulta "AND". Por ejemplo, si entra `dog cat`, el Explorador de atributos busca en cada fila una que incluya `dog` AND `cat`. No importa el orden de los diversos valores en la consulta. Por ejemplo, si uno de los valores de atributo del Explorador de atributos es `her cats and his dogs`, este valor forma parte de los resultados de la consulta de valor `dog cat` .
- Ordene la información del Explorador de atributos por columna. Pulse la cabecera de columna y verá una flecha que indica la dirección de clasificación.

Propiedades seleccionadas

Componente de la herramienta gráfica, la tabla Propiedades seleccionadas muestra las propiedades del nodo de entidad o atributo que se ha seleccionado en el gráfico. La tabla sólo muestra las propiedades para un nodo seleccionado (atributo o entidad) a la vez.

- Si selecciona una entidad, esta sección muestra todos los atributos (tipos y valores) asociados con la entidad seleccionada.
- Si selecciona un atributo, esta sección muestra todas las entidades que comparten el atributo seleccionado, incluyendo el ID de cada entidad. La tercera columna de esta sección también muestra el ID de la identidad del origen de datos, del que proceden los datos de atributo.

Navegación y exploración de los gráficos de la herramienta gráfica

Puede navegar y explorar los gráficos representados en la herramienta gráfica utilizando la barra de herramientas de navegación o las opciones del menú que aparece al pulsar el botón derecho del ratón en cada gráfico.

Barra de herramientas de navegación

La barra de herramientas de navegación justo debajo del título de gráfico contiene los iconos para la navegación gráfica estándar.

- Opciones de modalidad de selección: Seleccione elementos gráficos individuales o seleccione varios elementos gráficos (o seleccione un área específica del gráfico)
- Reposicione el gráfico en el lienzo
- Restablezca el gráfico en la vista predeterminada
- Opciones de zoom: Acercarse o alejarse

Selección y resaltado

En los gráficos de alerta y entidad, al seleccionar (pulsación del botón izquierdo del ratón) un nodo, quedan resaltados los atributos y entidades directamente

relacionados. El aspecto del nodo seleccionado cambia para mostrar un rectángulo de selección azul en la parte superior del nodo. El interior de los nodos resaltados cambia a azul.

Tabla 33. Descripciones de opciones del menú que aparece al pulsar el botón derecho del ratón de la herramienta gráfica

Cuando se selecciona este tipo de nodo...	**En este tipo de gráfico...**	**Estos datos quedan resaltados...**
Atributo	Gráfico de alerta Gráfico de entidad	Todas las entidades que comparten ese atributo Todos los atributos relacionados
Entidad	Gráfico de alerta Gráfico de entidad	Todas las entidades relacionadas con la entidad seleccionada en grado 1 Los atributos que producen la relación de grado 1
Entidad	Gráfico de red social	Cada vez que la entidad se visualiza en el gráfico, en cada concentrador con el que está relacionada la entidad seleccionada. (Una entidad puede mostrarse varias veces en varios concentradores en este tipo de gráfico.)

Puede seleccionar varios nodos utilizando **Ctrl**. También puede mover los nodos seleccionados actualmente arrastrándolos y soltándolos en el gráfico.

Opciones del menú que aparece al pulsar el botón derecho del ratón

Elija una entidad o un atributo apuntando el cursor en el mismo y pulsando el botón derecho del ratón.

Tabla 34. Descripciones de opciones del menú que aparece al pulsar el botón derecho del ratón de la herramienta gráfica

Esta opción del menú que aparece al pulsar el botón derecho del ratón...	**Realiza esta acción...**	**Gráfico de alerta**	**Gráfico de entidad**	**Gráfico de red social**
Aumentar/Disminuir	Aumenta, disminuye o ajusta el lienzo de gráfico al tamaño de la pantalla.	X	X	X

Tabla 34. Descripciones de opciones del menú que aparece al pulsar el botón derecho del ratón de la herramienta gráfica (continuación)

Esta opción del menú que aparece al pulsar el botón derecho del ratón...	Realiza esta acción...	Gráfico de alerta	Gráfico de entidad	Gráfico de red social
Filtros rápidos (general)	Ayuda a centrarse en los datos gráficos interesantes ocultando temporalmente los datos menos interesantes. Los filtros rápidos no añaden o eliminan datos del gráfico. Cuando se activa un filtro rápido, se visualiza la barra de título de gráfico [Filtro rápido activado]. Sólo puede estar activo a la vez un solo filtro rápido, pero se puede seleccionar un filtro rápido diferente cuando el filtrado rápido está activo. **Nota:** Cuando un filtro rápido está activo, el filtro muestra sólo los datos gráficos que se aplican a la entidad o atributo seleccionado actualmente. Por ejemplo, si selecciona la entidad ABC y selecciona el filtro rápido **Mostrar sólo entidades relacionadas**, verá las entidades visualizadas actualmente en el gráfico que están relacionadas en grado 1 con ABC.	X	X	
Filtro rápido – Mostrar sólo atributos	Oculta las entidades, de modo que puede ver los atributos asociados con la entidad en la que ha pulsado el botón derecho del ratón.	X	X	

Tabla 34. Descripciones de opciones del menú que aparece al pulsar el botón derecho del ratón de la herramienta gráfica (continuación)

Esta opción del menú que aparece al pulsar el botón derecho del ratón...	Realiza esta acción...	Gráfico de alerta	Gráfico de entidad	Gráfico de red social
Filtro rápido - Mostrar sólo entidades relacionadas	Oculta todos los atributos, incluidos los atributos que enlazan las entidades entre sí, para poder ver las entidades que están relacionadas en grado 1 con la entidad en la que ha pulsado el botón derecho del ratón. Este filtro rápido le da el aspecto de un gráfico de red social desde un gráfico de entidad o alertas.	X	X	
Filtro rápido – Mostrar atributos y entidades relacionados	Oculta todos los datos gráficos excepto para las entidades enlazadas en grado 1 con la entidad en la que ha pulsado el botón derecho del ratón y los atributos que producen la relación en grado 1. Este filtro rápido es particularmente útil cuando hay una gran cantidad de datos en el gráfico y desea eliminar el exceso de desorden.	X	X	
Filtro rápido – Mostrar la vía de acceso a la parte superior	Filtra los datos de gráfico para mostrar la vía de acceso que conecta la entidad o el atributo a la entidad superior. Si ha pulsado el botón derecho del ratón en un atributo, el filtro incluye todas las entidades y atributos a lo largo de la vía de acceso de relación con la entidad superior. Si ha pulsado el botón derecho del ratón en una entidad, el filtro incluye todos los atributos y entidades a lo largo de la vía de acceso a la entidad superior.	X	X	
Filtro rápido - Desactivar el filtrado rápido	Desactiva el filtro rápido actual y vuelve a visualizar los datos filtrados desde el gráfico.	X	X	

Tabla 34. Descripciones de opciones del menú que aparece al pulsar el botón derecho del ratón de la herramienta gráfica (continuación)

Esta opción del menú que aparece al pulsar el botón derecho del ratón...	Realiza esta acción...	Gráfico de alerta	Gráfico de entidad	Gráfico de red social
Mover a la parte superior	Mueve la entidad seleccionada a la parte superior del gráfico, convirtiendo la entidad en la entidad superior. Esta opción no añade datos nuevos al gráfico o al Explorador de atributos. Pero el gráfico se vuelve a dibujar para mostrar los datos desde la perspectiva de la nueva entidad superior.	X	X	
Mostrar atributos restantes	Visualiza todos los atributos asociados con la entidad en la que ha pulsado el botón derecho del ratón, incluso si esos atributos no enlazan la entidad a ninguna otra entidad en el gráfico. El Explorador de atributos siempre lista todos los atributos asociados con una entidad, por lo tanto esta opción no cambia datos en el Explorador de atributos. La visualización de otros atributos para una entidad puede proporcionar otra pieza de un rompecabezas o llevarle a realizar una exploración adicional de una entidad o atributo.	X	X	
Ocultar atributos restantes	Elimina del gráfico los atributos que no enlazan ninguna entidad visualizada en el gráfico. Si todos los atributos visualizados en el gráfico enlazan entidades que actualmente se visualizan en el gráfico, esta opción no está disponible.	X	X	

Tabla 34. Descripciones de opciones del menú que aparece al pulsar el botón derecho del ratón de la herramienta gráfica (continuación)

Esta opción del menú que aparece al pulsar el botón derecho del ratón...	Realiza esta acción...	Gráfico de alerta	Gráfico de entidad	Gráfico de red social
Mostrar entidades relacionadas restantes	Visualiza todas las relaciones que aún no se han visualizado para la entidad en la que ha pulsado el botón derecho del ratón. También se visualizan los atributos que producen las relaciones.	X	X	X
Crear nuevo gráfico	Crea un nuevo gráfico del tipo que ha seleccionado, que presenta la entidad en la que ha pulsado el botón derecho del ratón como la entidad principal.	X	X	X
Diseño del gráfico	Controla la visualización del diseño de gráfico: • En capas: Visualiza los datos de gráfico en capas, mostrando filas alternas de atributos y las entidades enlazadas a esos atributos. Este diseño es el diseño predeterminado para los gráficos de alerta y entidad. • Radial: Muestra los datos de gráfico como nodos y líneas de conexión, dispersos de forma aleatoria en el lienzo de gráfico. Este diseño puede ser útil si desea organizar personalmente las entidades y los atributos.	X	X	

Tabla 34. Descripciones de opciones del menú que aparece al pulsar el botón derecho del ratón de la herramienta gráfica (continuación)

Esta opción del menú que aparece al pulsar el botón derecho del ratón...	Realiza esta acción...	Gráfico de alerta	Gráfico de entidad	Gráfico de red social
Mostrar resumen	Muestra el resumen de entidad en una nueva ventana, si el enlace está configurado en el archivo `graph.properties`. El resumen de entidad proporciona información detallada sobre la entidad seleccionada, incluyendo todas las alertas en las que la entidad está implicada y todas las identidades asociadas con la entidad. El resumen es una herramienta de análisis útil, especialmente cuando se utiliza con los gráficos de la herramienta gráfica. Esta opción que aparece al pulsar el botón derecho del ratón sólo está disponible si el URL de resumen de entidad está configurado en el archivo `graph.properties`. Por ejemplo, si la organización ha instalado el kit de herramientas de analista, el administrador de sistema de Identity Insight puede configurar el enlace para que el resumen de entidad basado en Cognos se visualice en una ventana de navegador web. Si no ve este enlace, póngase en contacto con el administrador de sistema de Identity Insight.	X	X	X

Elementos comunes en los gráficos de la herramienta gráfica

Los gráficos tienen muchos elementos comunes: iconos, indicadores y espesor de línea. Estos elementos comunes proporcionan un significado adicional que puede ayudarle a obtener una historia más completa de cada gráfico y a identificar más fácilmente las áreas de interés.

Iconos de entidad

Cada nodo de entidad se visualiza como un icono rodeado por un círculo sólido.

Las entidades pueden definirse como personas, lugares o cosas (como organizaciones, barcos o aviones). Normalmente, las entidades son personas. El nodo de entidad más común es uno representado como un icono de persona: masculino, femenino o desconocido. El sexo visualizados por el icono se basa en uno de estos dos posibles asignaciones de sexo:

- El sexo asignado durante el análisis de nombre de la resolución de entidad
- El valor del atributo GENDER que forma parte de los datos en el registro de identidad de entrada

Si el sexo es indeterminado, se visualiza un icono de entidad de persona genérica.

La tabla siguiente muestra los iconos de entidad de persona predeterminados utilizados en los gráficos de la herramienta gráfica.

Tabla 35. Ejemplo de los iconos de entidad predeterminados utilizados en los gráficos de herramienta gráfica

Este icono...	**Representa este tipo de entidad...**
 Indicador de entidad de persona femenina de la herramienta gráfica	Entidad femenina (persona)
 Indicador de entidad de persona masculina de la herramienta gráfica	Entidad (persona) masculina
 Indicador de entidad de persona desconocida de la herramienta gráfica	Entidad de sexo desconocido

La entidad principal en un gráfico de entidad o red social tiene siempre un círculo más grueso. Independientemente del lugar donde se visualice la entidad principal en el gráfico, siempre puede identificarla por el círculo más grueso.

En un gráfico de alerta, todas las entidades en la vía de acceso de alerta tienen un círculo más grueso. Independientemente del número de entidades que se muestran en el gráfico, como por ejemplo si elige mostrar entidades relacionadas restantes, siempre puede identificar las entidades implicadas en la alerta.

Iconos de atributo

Los nodos de atributo se representan en los gráficos de la herramienta gráfica como iconos. Cada icono representa un tipo de atributo específico. La tabla siguiente proporciona un ejemplo de los iconos de atributo predeterminados visualizados en los gráficos de la herramienta gráfica.

Tabla 36. Ejemplo de los iconos predeterminados visualizados en la herramienta gráfica

Este icono...	Representa este tipo de atributo...
 Icono de atributo de dirección de herramienta gráfica	Dirección
 Icono de atributo de nombre de herramienta gráfica	Nombre
 Icono de atributo de número de Seguridad social de herramienta gráfica	Número de la Seguridad social
 Icono de atributo de fecha de nacimiento e herramienta gráfica	Fecha de nacimiento
 Icono de otro tipo de atributo de herramienta gráfica	Otro atributo (no asignado a un icono de atributo existente)

Puede personalizar los iconos que representan atributos en los gráficos, sustituyendo el icono de atributo predeterminado o añadiendo iconos para representar los atributos que son específicos de la organización. Consulte “Adición de iconos personalizados a los gráficos de herramienta gráfica” en la página 361 para obtener más información.

Indicadores de alerta

Cada entidad muestra un indicador para mostrar el número de alertas para la entidad. El indicador de alerta se visualiza en la esquina superior izquierda del círculo sólido que rodea el icono de entidad.

El indicador de alerta tiene un fondo de oro y el número de alertas aparece en texto negro. Por ejemplo, este indicador de alerta  en un icono de entidad muestra que esta entidad tiene 25 alertas.

Indicador de alerta de herramienta gráfica

Indicadores de entidades relacionadas

Los nodos de entidad también tienen un indicador que muestra el número de relaciones que pertenecen a esta entidad, basándose en los atributos compartidos. Estas relaciones aún no se muestran como pertenecientes a esta entidad.

El indicador de entidades relacionadas tiene un fondo azul claro, y el número de relaciones se visualiza en texto negro en negrita. Por ejemplo, este indicador de

entidades relacionadas 

Indicador de entidades relacionadas de herramienta gráfica

muestra que hay seis entidades adicionales que aún no se muestran como con una relación con la entidad.

El indicador de entidades relacionadas se comporta de forma diferente dependiendo del tipo de gráfico:

- En el gráfico de alerta: dos entidades implicadas en la alerta visualizan un indicador de entidades relacionadas, si la entidad está relacionada con más entidades que no actualmente no se visualizan en el gráfico. Puede expandir el gráfico para mostrar todas las entidades relacionadas con cada entidad visualizada en el gráfico. En este caso, ya no ve un indicador de entidades relacionadas en ninguna entidad.
- En el gráfico de entidad:
  - La entidad principal no tiene un indicador de entidades relacionadas. El gráfico muestra automáticamente todas las entidades relacionadas con esa entidad principal.
  - Las otras entidades del gráfico de entidad visualizan un indicador de entidades relacionadas, si están relacionadas con otras entidades que ya no se visualizan en el gráfico. Puede utilizar el menú que aparece al pulsar el botón derecho del ratón para mostrar las entidades restantes para dicha entidad, para que el indicador de entidades relacionadas ya no se muestre.
  - Al igual que en el gráfico de alertas, puede expandir el gráfico para mostrar todas las entidades relacionadas con cada entidad visualizada en el gráfico. En este caso, ninguna entidad muestra un indicador de entidades relacionadas.
- En el gráfico de red social:
  - La entidad concentradora (en el medio del clúster) no tiene indicador de entidades relacionadas, porque el gráfico muestra automáticamente todas las entidades relacionadas dentro de la formación de clúster.
  - Las entidades que no son la entidad concentradora de un clúster de relaciones puede contener un indicador de entidades relacionadas, si están relacionados con otras entidades que aún no están enlazadas al nodo especificado.
  - Si expande el gráfico para incluir varios clústeres de relaciones, es posible que una entidad se visualice en el gráfico más de una vez. Cuando la entidad es el concentrador de un clúster, no se visualiza ningún indicador de entidades relacionadas. Pero cuando esa misma entidad forma parte del clúster de relaciones y no la entidad concentradora, si hay entidades relacionadas adicionales para dicha entidad que todavía no están presentes en el gráfico, se visualiza el indicador de entidades relacionadas. Por este motivo, siempre se ven algunos indicadores de entidad relacionada en el gráfico.

Indicadores de línea

Las líneas que rodean los nodos de entidad y conectan entidades y atributos pueden proporcionar información adicional:

- Las líneas discontinuas que conectan los atributos indican una rigurosa coincidencia de atributo.
- Una línea gruesa que rodea el nodo de entidad indica la entidad principal: la entidad que se ha seleccionado o solicitado al crear este gráfico en concreto.

Sintaxis y parámetros de URL de la herramienta gráfica

Para acceder a un gráfico de la herramienta gráfica, debe enlazar con el URL apropiado. El URL puede estar incorporado en una aplicación personalizada existente (como una página de inicio web, un panel de control o una herramienta de gestión de casos) o entrarse manualmente en un navegador web.

La sintaxis y los parámetros de URL correctos para los gráficos de componente gráfico tienen el aspecto siguiente:

`http://`*`servidor`*`:`*`puerto`*`/graphs/run/`*`tipo_gráfico`*`.jsp?height=`*`nnnn`*`&width=`*`yyyy`*`&`*`identificador=xxxx`*

servidor_host*:*puerto
: Indica el nombre del servidor de aplicaciones de producto y el número de puerto donde se encuentra IBM InfoSphere Identity Insight. Normalmente, el servidor de aplicaciones de producto es el servidor WebSphere.

  El número de puerto toma de forma predeterminada 13510.

/graphs/run
: Apunta a los directorios de producto donde están ubicados los archivos de la herramienta gráfica. Los directorios `/graphs/run` son la ubicación donde el programa de instalación del producto instala la herramienta gráfica de forma predeterminada.

***tipo_gráfico*.jsp**
: Indica qué gráfico se debe crear:
  - Para el gráfico de alerta, escriba `role-alert.jsp`
  - Para el gráfico de entidad, escriba `entity.jsp`
  - Para el gráfico de red social, escriba `social-network.jsp`

? Indica un elemento URL.

height=*nnnn*
: Indica la altura del lienzo de gráfico: la altura a la que se debe representar el lienzo de gráfico en la ventana de navegador web. Escriba el número en píxeles.

  La altura del gráfico se determina del modo siguiente:
  - Si se especifica una altura en el URL, ésa será la altura de gráfico predeterminada.
  - Si un valor se establece en la propiedad **`defaultGraphHeight`** en el archivo `graph.properties`, ésa es la altura de gráfico predeterminada.
  - En ausencia de una altura de gráfico especificada en el URL o la propiedad **`defaultGraphHeight`**, la altura de gráfico predeterminada se establece en 800 píxeles.

  .

  Para aproximar un lienzo de gráfico que encaje en una ventana de navegador web estándar de 1024 x 768, establezca la altura en 450 píxeles.

? Indica una señal separadora de URL entre parámetros.

width=*yyyy*
Indica la anchura del lienzo de gráfico: la anchura con la que se debe representar el lienzo de gráfico dentro de la ventana de navegador web. El Explorador de atributos no está incluido en este número, ya que es un componente independiente que se acopla a la derecha del lienzo de gráfico en la ventana de navegador web.

La anchura de gráfico se determina de la siguiente manera:

- Si se especifica una anchura en el URL, ésa es la anchura de gráfico predeterminada.
- Si un valor se establece en la propiedad **defaultGraphWidth** en el archivo `graph.properties`, ésa es la anchura de gráfico predeterminada.
- En ausencia de cualquier anchura de gráfico especificada en el URL o en la propiedad **defaultGraphHeight**, la anchura de gráfico predeterminada se establece en 800 píxeles.

.

Para aproximar un lienzo de gráfico que se ajuste en una ventana de navegador web estándar de 1024 x 768,, establezca la anchura en 640 píxeles.

identificador=xxxx
Indica el tipo de ID (de entidad o alerta) y el número específico para esa entidad o alerta. Cuando se utiliza el ID de entidad, el valor del ID es la entidad principal en el gráfico de entidad o la entidad de concentrador en el gráfico de red social Cuando se utiliza el ID de alerta, el valor es la alerta a visualizar en el gráfico de alerta.

- Para el gráfico de alerta, escriba `alertID=`*`número_ID_alerta_específico`*
- Para los gráficos de entidad o red social, escriba `entityID=`*`número_ID_entidad_específica`*

Tareas administrativas comunes para la herramienta gráfica

Algunas de las tareas para la herramienta gráfica sólo las puede completar un usuario administrador.

Adición de iconos personalizados a los gráficos de herramienta gráfica:

La herramienta gráfica incluye iconos estándares que representan los diferentes tipos de atributos visualizados en los gráficos. Puede cambiar el icono predeterminado para uno o varios atributos o añadir iconos para los atributos personalizados configurados en el producto. Todos los gráficos de herramienta gráfica utilizan el mismo conjunto de iconos de imagen en el servidor de aplicaciones de producto, por lo que cuando personalice el conjunto de iconos de atributos, cada usuario ve los mismos iconos de atributo.

Antes de empezar

Los iconos de gráficos se inician como archivos SVG (Scalable Vector Graphic). Los archivos SVG se pueden crear utilizando varias herramientas de dibujo basadas en vector o pueden descargarse de diversos orígenes de Internet. Se recomienda encarecidamente que los archivos SVG utilizados para iconos se mantengan en un tamaño relativamente pequeño (para mejorar la legibilidad cuando se escala la imagen).

El gráfico necesita una definición de forma almacenada en formato JSON (Javascript Object Notation). Para convertir de SVG a JSON es necesario utilizar dos programas de utilidad de mandatos independientes: **xlstproc** y **sed**.

Si está en un sistema basado en Unix, es posible que ya tenga estas herramientas. Si está en un sistema basado en Windows, tendrá que adquirir estas herramientas basadas en Unix mediante el uso de un emulador Unix (como la aplicación gratuita Cygwin). *Nota: si utiliza Cygwin, asegúrese de incluir las bibliotecas libxml2 y libxslt en la instalación para obtener los programas de utilidad necesarios.*

Finalmente, necesitará el archivo svg2gfx.xsl de la biblioteca DOJO gratuita (disponible en https://dojotoolkit.org/download). Una vez que DOJO se ha descargado, el archivo svg2gfx.xsl puede ubicarse en el directorio <raíz instalación>/dojox/gfx/resources.

Procedimiento

1. Copie el archivo svg2gfx.xsl de la ubicación DOJO al mismo directorio que contiene el archivo o los archivos SVG que desea convertir
2. Abra una ventana de línea de mandatos/terminal Unix y navegue al directorio que contiene el archivo o los archivos SVG
3. Ejecute el mandato siguiente: `xsltproc ./svg2gfx.xsl <su archivo .SVG> > <nombre_archivo_temp>.json`
4. Ejecute el mandato siguiente: `sed -e 's/,}/}/g' -e 's/,]/]/g' <nombre_archivo_temp.json> > <nombre final>.json`
5. Localice la carpeta de instalación de Identity Insight
6. Bajo la carpeta de instalación, vaya a /ibm-home/graphs
7. Cree una carpeta denominada (sensible a las mayúsculas y minúsculas): customImages
8. Mueva el icono personalizado (archivo .json) a la carpeta customImages

Ejemplo

Si ha creado un tipo de atributo denominado `FLIGHT` y desea que un icono de gráfico personalizado represente a ese tipo de atributo en los gráficos de la herramienta gráfica, realice los pasos siguientes:

1. Cree u obtenga un archivo de imagen adecuado para representar el tipo de atributo `FLIGHT`. Asegúrese de que el nombre de archivo de imagen coincide con el nombre de tipo de atributo configurado en la Consola de configuración y utiliza letras minúsculas, como este nombre de archivo: `flight.svg`
2. Asegúrese de svg2gfx.xsl se encuentra en el mismo directorio que `flight.svg`
3. Abra una ventana de terminal/línea de mandatos de Unix y vaya al mismo directorio que `flight.svg`
4. Ejecute el siguiente mandato: `xsltproc ./svg2gfx.xsl flight.svg > flight_tmp.json`
5. Ejecute el siguiente mandato: `sed -e 's/,}/}/g' -e 's/,]/]/g' flight_tmp.json > flight.json`
6. Copie el archivo de icono `flight.json` en la carpeta `/customImages`.

Requisitos para iconos de gráficos personalizados:

Puede personalizar los iconos de atributo que se muestran en los gráficos. Pero los nuevos iconos deben satisfacer los requisitos para iconos de gráficos personalizados, de modo que los gráficos reconozcan y los iconos y los visualicen.

Requisitos para los iconos personalizados

Para que los gráficos de producto reconozcan y muestren iconos personalizados, los iconos de atributo deben cumplir los siguientes requisitos:

- Formato de archivo: Scalable Vector Graphics (SVG)
- Nombre:
  - El nombre de icono personalizado debe coincidir con el nombre del tipo de atributo correspondiente que se ha configurado en la Consola de configuración.
  - El nombre de icono personalizado debe contener sólo letras minúsculas.
- El archivo SVG debe convertirse en una definición de forma JSON (consulte "Adición de iconos personalizados a los gráficos de herramienta gráfica" en la página 361)

Por ejemplo, si desea asociar un icono de atributo con el tipo de atributo FINGERPRINTS que se ha configurado en la Consola de configuración, el nombre del archivo de icono debe ser `fingerprints.svg`.

Ejemplos de nombre

Para alterar temporalmente un icono de tipo base existente, el icono personalizados debe denominarse de una de las siguientes maneras (todo en minúsculas):

- address.json
- female.json
- male.json
- name.json
- undetermined_gender.json

Para los números de entidad, el archivo de icono .json debe denominarse igual que el código de tipo de número (NUM_TYPE.NUM_TYPE en la base de datos). Por ejemplo:

- cc.json
- dl.json
- ff.json
- ssn.json
- pp.json
- ph.json

Para las características de entidad, el archivo de icono .json debe tener el mismo nombre que el código de tipo de atributo (ATTR_TYPE.ATTR_TYPE en la base de datos). Por ejemplo:

- dob.json
- died.json
- marital.json
- circa_dob.json
- pop.json
- nat.json
- cit.json

Enlace con el resumen de entidad desde la herramienta gráfica:

El resumen de entidad proporciona información detallada acerca de las entidades individuales y es útil cuando se están analizando alertas y relaciones de entidad. Si establece las propiedades de URL en la aplicación web que genera el resumen de entidad, los usuarios de la herramienta gráfica pueden abrir el resumen de entidad desde dentro de uno de los gráficos de la herramienta gráfica.

Acerca de esta tarea

El establecimiento del enlace es una tarea global. Después de que se haya establecido el enlace, todos los usuarios que ven gráficos de la herramienta gráfica tienen acceso al enlace desde el menú que aparece al pulsar el botón derecho del ratón. Si las propiedades de enlace no se han establecido, no se visualiza la opción que aparece al pulsar el botón derecho del ratón **Mostrar resumen**.

Procedimiento

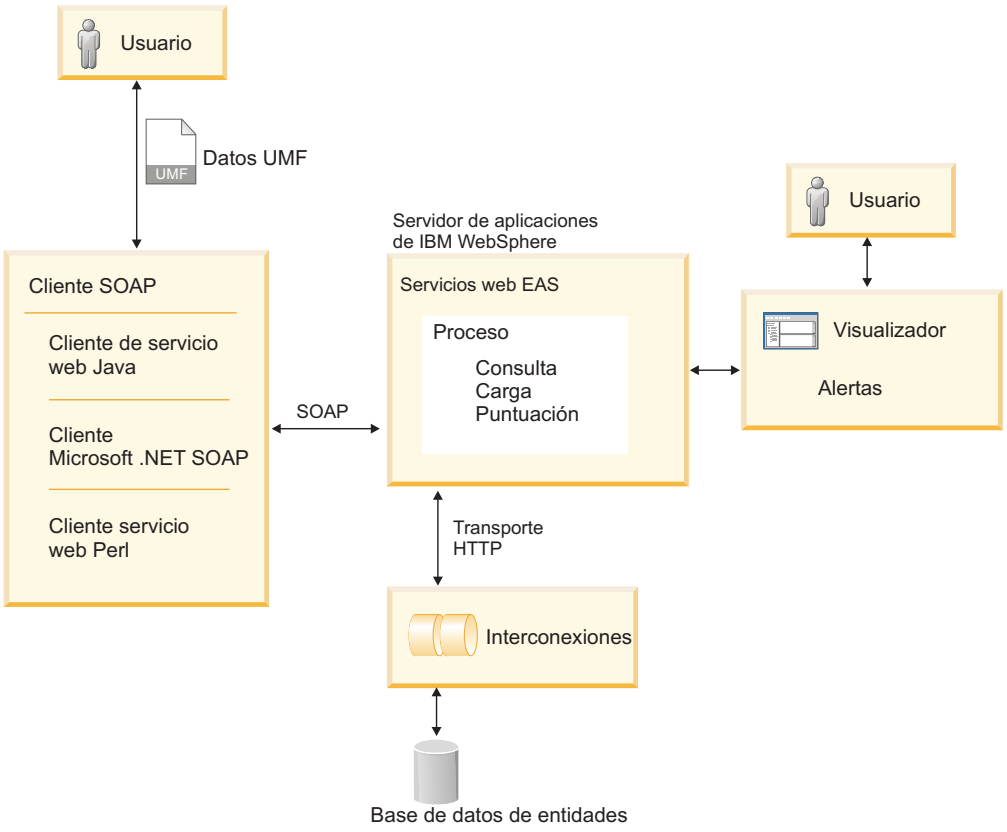
1. Solicite al administrador del sistema que actualice la propiedad RESUMESERVER de la tabla COMPONENT_CONFIG con un enlace al informe kit de herramientas de Cognos.
   a. Sustituya el valor de esta propiedad por el URL real. Especifique el servidor de host, el nombre de puerto y la vía de acceso a la aplicación web. Consulte el valor de ejemplo para tener una idea del aspecto que puede tener la vía de acceso. Por ejemplo, si la organización ha instalado y está utilizando el kit de herramientas de Analista basado en Cognos, especifique la vía de acceso al resumen de entidad generado por el kit de herramientas de analista.
   b. Asegúrese de que la señal **%ISIIEntityID%** está dentro del valor de parámetro. Este parámetro envía el ID de entidad apropiado a la aplicación web para generar el resumen de entidad correcto.
2. Opcional: Pruebe el enlace.

Capítulo 9. Desarrollo

Si necesita utilizar servicios Web en su entorno de trabajo, IBM InfoSphere Identity Insight proporciona un servicio Web simple basado en XML.

Servicios web

IBM InfoSphere Identity Insight proporciona un conjunto de servicios Web que puede utilizar para crear aplicaciones externas que pueden cargar datos de UMF (Universal Message Format) para el proceso de interconexiones o la búsqueda de entidades en la base de datos de entidades. Puede utilizar el método de transporte HTTP (protocolo de transferencia de hipertexto) bidireccional, que es una característica estándar de la interconexión.



Los servicios Web de IBM InfoSphere Identity Insight utilizan cuatro métodos SOAP (Simple Object Access Protocol): proceso, búsqueda, carga y puntuación. El producto soporta la versión SOAP 1.1.

El producto incluye varios componentes que le ayudan a comenzar a utilizar los servicios Web.

srd.wsdl

Este archivo contiene una definición de lenguaje de descripción de servicios Web (WSDL) de los servicios Web del producto. Puede utilizar este archivo con cualquier kit de herramientas SOAP o con alguna

tecnología para iniciar los servicios Web. Puede encontrarse iniciando WebSphere Liberty y cargando el archivo de http://nombrehost:puerto/easws/resources/wsdl/srd.wsdl

wsutil.jar
Este archivo es un cliente de prueba de servicios Web que se proporciona para la prueba de la instalación y configuración de servicios Web. Este programa de utilidad se puede encontrar en el directorio `ibm-home/easws`.

Requisitos de software de los servicios Web

Para utilizar los servicios Web de IBM InfoSphere Identity Insight es necesario que se haya instalado determinado software y que sea funcional.

Antes de utilizar los servicios Web, asegúrese de que el siguiente software está instalado y es funcional:

- Los servicios Web de IBM InfoSphere Identity Insight deben estar instalados y en ejecución.
- El servidor de IBM WebSphere Application Server debe estar en ejecución donde están desplegados los servicios web de IBM InfoSphere Identity Insight. En la mayoría de los casos, es el mismo servidor de aplicaciones en el que están instalados la Consola de configuración y el Visualizador.
- La interconexión de servicios Web debe haberse iniciado y estar a la escucha en el URL HTTP adecuado. El servidor de aplicaciones intenta enviar datos UMF a esta interconexión de servicios Web a través del URL de HTTP especificado, siempre que se recibe una petición SOAP.

  Nota: El URL de HTTP utilizado para la comunicación entre el servidor de aplicaciones y la interconexión *no* es el mismo que el URL utilizado por los clientes del servicio Web que envían peticiones SOAP. El envío de peticiones SOAP directamente al URL HTTP de la interconexión de servicios Web dará lugar a un error.

  Por ejemplo, si WebSphere Application Server está configurado con el rango de puerto predeterminado, los números y el uso de puerto serán:
  - *nnn*0 - puerto HTTP para Webserver
  - *nnn*1 - puerto HTTPS para Webserver
  - *nnn*2 - puerto de administración HTTP
  - *nnn*3 - puerto de administración HTTPS
  - *nnn*4 - puerto SOAP
  - *nnn*5 - Puerto del servidor de aplicaciones
- El archivo webservices.properties debe estar configurado con el URL de HTTP de la interconexión en ejecución, para que WebSphere Application Server incrustado sepa dónde encontrar la interconexión que manejará las peticiones de servicios Web. Habitualmente este archivo reside en el directorio siguiente: *directorio_inicial_producto*`/srd-home/easws`
- Debe existir un cliente de servicios Web compatible con SOAP y WSDL, utilizado para invocar IBM InfoSphere Identity Insight. Un cliente de ejemplo, wsutil.jar, se instala con los servicios web de IBM InfoSphere Identity Insight para probar servicios de releases anteriores, pero no se aplica a servicios mejorados para la versión 8.0, fixpack 2.

Inicio de interconexiones de servicios Web

Para enviar y procesar datos enviados mediante un servicio web, inicie las interconexiones utilizando el transporte HTTP bidireccional. Normalmente, las interconexiones utilizadas con los servicios Web se ejecutan constantemente en el fondo, escuchando los datos que se deben procesar en los puertos asignados. Utilice estos pasos para iniciar una interconexión de servicios Web.

Antes de empezar

- Asegúrese de que conoce el valor de URL de interconexión que está configurado en el archivo webservices.properties. Este valor apunta al componente de servicios Web que se ejecuta en el servidor incorporado IBM WebSphere Application Server de la interconexión, y debe coincidir con el URL utilizado para iniciar interconexiones de servicios Web.
- El nodo de interconexión donde reside esta interconexión debe tener instalado el ejecutable de interconexión.
- Se debe haber configurado como mínimo un archivo de configuración de interconexiones para utilizarlo con la interconexión que desea iniciar. Puede especificar el archivo de configuración de interconexiones que se debe utilizar como parte del mandato para iniciar la interconexión. Si no especifica el nombre de archivo de configuración como parte del mandato de interconexión, el archivo de configuración de interconexiones debe estar ubicado en el nodo de interconexión, y debe utilizar el nombre de archivo de configuración de interconexiones por omisión pipeline.ini.
- Si utiliza un script para iniciar las interconexiones, asegúrese de que el script está ubicado en el mismo directorio en el que inicia la interconexión.
- Si desea direccionar los resultados del proceso de esta interconexión o supervisar las estadísticas y el estado de esta interconexión, registre la interconexión en la pestaña **Interconexiones** de la Consola de configuración. Debe utilizar uno de los nombres de interconexión que ya están registrados para iniciar esta interconexión a fin de que la supervisión o direccionamiento se completen satisfactoriamente.
- Si utiliza el supervisor de aplicaciones para supervisar el estado y las estadísticas de las interconexiones, asegúrese de que el nodo de interconexión tiene instalado un agente SNMP y que está en ejecución antes de iniciar esta interconexión.
- Si esta interconexión direcciona los resultados a otro sistema u otra base de datos, asegúrese de que el archivo de direccionamiento para esta interconexión está ubicado en el mismo directorio en el que inicia la interconexión.
- Si el valor del parámetro del sistema *DEFAULT_CONCURRENCY* se ha establecido en mayor que 1 o si ha configurado el parámetro de *simultaneidad* en el archivo de configuración de interconexiones para el nodo de interconexión, puede iniciar múltiples hebras de proceso de interconexiones paralelas utilizando un solo mandato de inicio de interconexión.

Acerca de esta tarea

Existen tres pasos para iniciar una interconexión:

Procedimiento

1. Verifique que actualmente no haya otras interconexiones en ejecución en el nodo de interconexión que tengan el mismo nombre que la interconexión que

desea iniciar. Cada interconexión debe tener un nombre exclusivo para este nodo de interconexión. (El nombre de interconexión por omisión es `pipeline`.) Hay dos maneras de verificarlo:

a. Si utiliza el supervisor de aplicaciones para comprobar el estado de interconexiones o dirigir los resultados hacia otros sistemas, examine el panel **Estado** para ver si hay otra interconexión en ejecución que tenga el mismo nombre que desea utilizar.
b. O bien, en un indicador de mandatos, escriba el siguiente mandato:

   ```
   pipeline -n nombre_interconexión -l
   ```

   donde *nombre_interconexión* es el nombre que desea utilizar para iniciar la nueva interconexión. Asegúrese de que este nombre coincide con el nombre registrado en la Consola de configuración para esta interconexión.

2. En un indicador de mandatos, inicie una o varias interconexiones especificando el tipo de opciones y parámetros del mandato de interconexión adecuados utilizando este formato:

   ```
   pipeline -opción parámetro
   ```

   Nota: Si utiliza el supervisor de aplicaciones para esta interconexión y se ha registrado en la Consola de configuración para supervisión o direccionamiento, asegúrese de utilizar la opción `-n` como parte del mandato de inicio de interconexión y especifique el nombre de interconexión registrado. Si el nombre de interconexión especificado no coincide exactamente con el nombre de interconexión registrado (incluyendo las mayúsculas y minúsculas), el estado de la interconexión no se visualizará correctamente en el panel **Estado de interconexión** de la Consola de configuración y cualquier direccionamiento configurado para esta interconexión no será satisfactorio.

   Nota: Normalmente, se utilizan las opciones de interconexión `-s` o `-d` para iniciar la interconexión en modalidad de servicio/daemon o depuración, según sea adecuado.

3. Verifique que el mandato ha funcionado y que la interconexión se ha iniciado y está activa.
   a. Si utiliza el supervisor de aplicaciones y esta interconexión se ha registrado en la Consola de configuración, compruebe el panel **Estado de interconexión**. Si la interconexión está activa, el estado se visualiza como `Activo`.
   b. Si el sistema se ejecuta en una plataforma Microsoft Windows y utiliza la opción de interconexión de servicios, puede ver el estado de la interconexión en el panel de control de los servicios de Microsoft Windows.
   c. Si el sistema se ejecuta en una plataforma UNIX y utiliza la opción de interconexión de daemons, puede escribir el siguiente mandato para comprobar si hay procesos en ejecución:

      ```
      ps -fu id_usuario
      ```

      donde *id_usuario* es la identificación del usuario que inicia la interconexión.
   d. O bien, en un indicador de mandatos, escriba el siguiente mandato:

      ```
      pipeline -nnombre_interconexión -l
      ```

      donde *nombre_interconexión* es el nombre de la interconexión que acaba de iniciar. Si la interconexión está activa, el indicador de mandatos devuelve `Running`.

Qué hacer a continuación

Este mandato de interconexión inicia el número de hebras de proceso de interconexión igual al parámetro de simultaneidad del archivo de configuración de interconexiones. El número de registros procesados simultáneamente se determina mediante el parámetro de simultaneidad incluido en la opción de transporte HTTP.

Prueba de servicios Web

Con el cliente de prueba proporcionado, wsutil.jar, puede probar la instalación y configuración de los servicios Web de IBM InfoSphere Identity Insight.

Antes de empezar

- Los servicios Web deben estar instalados.
- Asegúrese de que el servidor WebSphere Application Server incrustado está en ejecución.
- El servidor de aplicaciones debe tener configurado al menos un archivo de configuración de interconexiones para interconexiones de servicios Web.
- Compruebe que el archivo webservices.properties esté configurado con el valor apropiado de URL de interconexión. Esta interconexión de servicios Web debe estar en ejecución.
- Cree como mínimo un documento de entrada UMF de prueba para utilizarlo durante la prueba.

Procedimiento

1. En el servidor WebSphere Application Server incrustado, vaya al directorio donde reside el archivo wsutil.jar. Este archivo normalmente se encuentra en *directorio_raiz_instalación*/ewas/webservice/wsutil.jar
2. En una línea de mandatos de este directorio, especifique la sintaxis del mandato wsutil.jar para la operación que desea realizar: `java -jar wsutil.jar –-<SOAP method>=<URI> --input=<URL> –-output=<URI>`

Ejemplo de prueba del método de carga de servicios Web

El siguiente mandato wsutil.jar carga registros de un archivo UMF denominado “raw_entities.umf” y guarda los resultados en un archivo UMF denominado “results.umf”:

```
java -jar wsutil.jar --load=http://localhost:13510/easws/services/SRDWebService
--input=raw_entities.umf --output=results.umf
```

Archivo srd.wsdl

Para establecer la comunicación con los servicios web de IBM InfoSphere Identity Insight, necesita un cliente de servicios web. Cuando instala los servicios Web de IBM InfoSphere Identity Insight, también se instala el archivo srd.wsdl; contiene los métodos SRDWebService que se utilizan para establecer comunicación con los servicios Web de InfoSphere Identity Insight. Puede utilizar el archivo srd.wsdl para crear un cliente de servicios Web para utilizarlo con los servicios Web de IBM InfoSphere Identity Insight.

Puede acceder la archivo srd.wsdl mediante el navegador web accediendo al servidor WebSphere Application Server incrustado donde residen los servicios web. Generalmente, este archivo se encuentra en el servidor de aplicaciones situado en este URL raíz:

`http://sistema_de_IBM_WebSphere_Application_Server:puerto_instalación/easws/resources/wsdl/srd.wsdl`

Por ejemplo:

```
http://localhost:13510/easws/resources/wsdl/srd.wsdl
```

Nota: Asegúrese de que el servidor de aplicaciones está en ejecución antes de intentar acceder al archivo srd.wsdl.

También puede crear un cliente wsdl de servicios Web utilizando cualquier plataforma de desarrollo que sea compatible con servicios Web mediante un kit de herramientas de SOAP, tal como:

- Java con IBM WebSphere Application Server
- Java con Apache Axis
- Microsoft .NET
- Perl

Consulte la documentación de la plataforma de desarrollo para ver instrucciones sobre cómo crear un cliente de servicios Web utilizando un archivo wsdl.

Si crea un wsdl de cliente de servicios Web que no sea el cliente de servicios Web srd,wsdl, asegúrese de que el URL de despliegue apunte correctamente al cliente wsdl.

Métodos SRDWebService

El archivo srd.wsdl contiene los métodos SRDWebService que se utilizan para comunicarse con los servicios Web IBM InfoSphere Identity Insight. SRDWebService incluye tres métodos: uno para cargar datos en la base de datos de entidades, otro para realizar una búsqueda a fin de consultar la base de datos de entidades y, por último, otro para procesar la funcionalidad de interconexión disponible a través de UMF.

Método loadRecord

```
LoadResult loadRecord(String umfEntity)
```

El objeto LoadResult devuelto por el método loadRecord() contiene dos miembros:

Miembro	Descripción	Tipo
entityID	ID de la entidad devuelta	Long
merged	Distintivo que indica si la entidad se ha resuelto en una entidad existente o se trataba de una nueva entidad	Boolean

El parámetro umfEntity es una serie XML en UMF que representa los datos para una sola entidad. Utilice la especificación UMF para obtener instrucciones sobre cómo construir correctamente un registro UMF_ENTITY, asegurándose de definir los valores adecuados para DSRC_ACCT y DSRC_REF.

Aunque el método load le permite procesar documentos UMF_ENTITY, no devuelve como resultado el documento UMF en bruto de salida. En lugar de ello, el método devuelve un objeto LoadResult que contiene el ID de identidad, y un distintivo que indica si la entidad es nueva o se resolvió mediante una entidad existente. Puede utilizar el método process lugar del

método load, pero deberá analizar el documento UMF de salida. El método load le ahorra tener que analizar el documento UMF de salida resultante de la operación load.

Método basicQuery()

```
String basicQuery(String umfSearch)
```

La serie de entrada para el método basicQuery() debe estar en formato de registro UMF_SEARCH. La serie XML devuelta por basicQuery() contiene el registro UMF_SEARCH_RESULT de la consulta.

Hay dos tipos de consultas incorporadas: Consultas de conjunto de resultados de resumen y consultas de detallar más los detalles.

Nota: Este método se proporciona solamente para mantener la compatibilidad con versiones anteriores del producto. En el presente release, este método se comporta igual que el método process. Utilice el método process en lugar del método basicQuery() para todas las nuevas aplicaciones cliente.

Método process()

```
String process(String umfRequestDocument)
```

Utilice el método process para procesar un documento UMF de entrada cualquiera y obtener como resultado un documento UMF de salida. El método process está pensado para manejar todas las peticiones y respuestas compatibles con la interconexión y debe ser el método preferido para todas las operaciones.

Este método toma un parámetro String y devuelve un resultado String.

wsutil.jar

Wsutil.jar es una aplicación Java, de línea de mandatos, que se instala cuando el usuario instala los servicios Web de IBM InfoSphere Identity Insight. Es un programa cliente de ejemplo que puede utilizar para ensayar cada método SOAP de los servicios web, a fin de probar la instalación y configuración de los servicios web.

El cliente de prueba wsutil.jar debe estar en la siguiente ubicación:

instalación_raíz/ewas/webservice

Sintaxis de uso de wsutil.jar

Wsutil.jar es una aplicación Java basada en la línea de mandatos que se proporciona como cliente de prueba para probar la instalación y configuración de los servicios Web de IBM InfoSphere Identity Insight. Para utilizar wsutil.jar, se especifica un operador wsutil.jar con los modificadores correspondientes de entrada y salida.

La sintaxis para el uso de wsutil.jar se basa en la operación de los servicios Web que desea probar:

```
wsutil (unix) or wsutil.bat (win) --operator=URI --input=URI --output=URI
```

help

Visualiza ayuda en línea e información de línea de mandatos para el cliente de prueba wsutil.jar.

```
wsutil (unix) or wsutil.bat (win) --help
```

load=*URI*
Especifica registros UMF de estilo de interconexión y el URI (identificador uniforme de recursos) para la interfaz de servicios Web de IBM InfoSphere Identity.

```
wsutil (unix) or wsutil.bat (win) --load=URI [--xslt=URI][--
input=URI][--output=URI]
```

Esta operación carga los registros UMF desde el URI especificado a las interconexiones de servicios Web para el proceso de resolución de entidades. Después del proceso, la operación devuelve el ID de entidad y un distintivo que indica si la entidad de entrada se fusionó con una entidad existente o hizo que se creara una nueva entidad.

process=*URI*
Especifica registros genéricos UMF y el URI (identificador uniforme de recursos) para la interfaz de servicios Web de IBM InfoSphere Identity Insight.

```
wsutil (unix) or wsutil.bat (win) --process=URI [--xslt=URI][--
input=URI][--output=URI]
```

Utilice esta operación para procesar un documento UMF de entrada cualquiera y obtener como resultado un documento UMF de salida. El método process está pensado para manejar todas las peticiones y respuestas compatibles con la interconexión. A menudo es el método preferible para todas las operaciones.

search=*URI*
Especifica las peticiones y respuestas UMF de estilo de búsqueda de interconexión con el URI (identificador uniforme de recursos) para la interfaz de servicios Web de IBM InfoSphere Identity.

```
wsutil (unix) or wsutil.bat (win) --score=URI [--xslt=URI][--
input=URI][--output=URI]
```

Esta operación puede realizar una búsqueda de una entidad específica en una base de datos de entidades y devolver la información solicitada acerca de esa entidad, o puede consultar las entidades que coinciden con un atributo determinado en la base de datos de entidades y devolver la lista de entidades que han coincidido con la consulta.

xslt=*URI*
Especifica la transformación XSLT y el archivo XML que la operación transformará en registros UMF.

```
wsutil (unix) or wsutil.bat (win) --xslt=URI][--input=URI][--output=URI]
```

Utilice esta operación para transformar los registros XML en UMF antes de utilizar una de las operaciones de servicios Web.

Modificadores de wsutil.jar

Utilice estos modificadores con operadores de wsutil.jar para especificar los métodos de entrada y salida para el mandato de servicios Web.

input=*URI*
Especifica el método de entrada para registros UMF. El método de entrada por omisión es entrada estándar.

output=*URI*
Especifica el método de salida para registros UMF. El método de salida por

omisión es la salida estándar. Puede utilizar este método para especificar una ubicación y nombre de archivo en el que se debe guardar la salida UMF en un archivo.

Ejemplo de uso wsutil.jar

El siguiente mandato wsutil.jar en un sistema UNIX carga registros de un archivo, transforma esos registros en UMF y visualiza los resultados en la consola de interfaz de línea de mandatos:

```
wsutil --load=http://localhost:13510/easws/services/SRDWebService
--input=raw_entities.xml --xslt=transform.xsl
```

El siguiente mandato wsutil.jar en un sistema Windows adquiere peticiones de la entrada estándar y visualiza los resultados en la consola de la interfaz de línea de mandatos:

```
wsutil.bat --process=http://localhost:13510/SRDWebService
```

Creación de consultas sobre la base de datos de entidades

IBM InfoSphere Identity Insight proporciona varias maneras de consultar la base de datos de entidades. Puede crear búsquedas de interconexiones de servicios Web para buscar la base de datos de entidades a fin de encontrar las entidades que coinciden con criterios específicos de búsqueda de atributos. También puede crear búsquedas de interconexiones de servicios Web para consultar la base de datos en busca de una entidad específica.

Búsquedas de interconexión de servicio Web

Las interconexiones tienen una interfaz dinámica incorporada de búsqueda y consulta que ofrece un punto de acceso único para servicios Web a fin de consultar la base de datos de entidades. Puede utilizar documentos de entrada UMF para estructurar la consulta y luego enviar el documento de entrada UMF a través de servicios Web a las interconexiones para su proceso. Una vez procesado, la interconexión devuelve un documento de salida UMF que contiene los resultados.

Las búsquedas de interconexión de servicios Web ofrecen respuestas a dos tipos de preguntas:

¿Qué entidades de la base de datos de entidades coinciden con un determinado atributo o conjunto de atributos? (UMF_SEARCH)

Este tipo de búsqueda de interconexión de servicios Web aprovecha la resolución de entidades para reconocer y estandarizar los criterios de búsqueda de entrada y luego para comparar los criterios de búsqueda con las entidades de la base de datos. Se denomina consulta de resumen o de conjunto de resultados y devuelve una lista de entidades con valores de datos que coinciden con el valor de atributo solicitado o con la lista de valores de atributos.

Para realizar una consulta de resumen o de conjunto de resultados, debe crear un documento de entrada UMF_SEARCH que contenga los criterios de búsqueda que utiliza la interconexión para realizar la resolución de entidades. La interconexión responde devolviendo un documento de salida UMF_SEARCH_RESULT con los resultados de la búsqueda, que son la lista de entidades que coinciden con los criterios de búsqueda.

¿Qué sabe la base de datos de entidades sobre una determinada entidad? (UMF_QUERY)

Este tipo de búsqueda de interconexión de servicios Web utiliza sentencias

SQL y parámetros para consultar la base de datos de entidades. Se denomina una consulta detallada o de profundización y devuelve una lista detallada de la información sobre una sola entidad.

Para realizar una consulta detallada o de profundización, debe crear un documento de entrada UMF_QUERY que indique la entidad de la base de datos de entidades sobre la que desea obtener información. La interconexión responde devolviendo un documento de salida UMF_QUERY_RESULT con detalles sobre la entidad solicitada.

Mientras realizan búsquedas de interconexión de servicios Web, las interconexiones realizan todas las funciones estándar de interconexión, incluido el registro.

Tanto la entrada (solicitud) como la salida (respuesta) de las búsquedas de interconexión de servicios Web utilizan documentos UMF y estructuran la información en UMF.

Formatos de búsqueda de interconexión de servicio Web

El producto se proporciona con varios formatos incorporados para cada una de las búsquedas de interconexión de servicios Web:

Formatos UMF_SEARCH

WS_SUMMARY_TOP10
Devuelve una lista de las 10 principales entidades de la base de datos que se parecen más a los datos de atributos especificados en los criterios de búsqueda.

WS_SUMMARY_TOP100
Devuelve una lista de las 100 principales entidades de la base de datos que se parecen más a los datos de atributos especificados en los criterios de búsqueda.

WS_SUMMARY
Devuelve una lista de todas las entidades de la base de datos que coinciden con los datos de atributos especificados en los criterios de búsqueda.

Formatos UMF_QUERY

WS_DETAIL
Devuelve todos los datos de la base de datos de entidades correspondientes al ID de entidad solicitado.

WS_RELATION
Devuelve una lista de todas las entidades de la base de datos de entidades que están relacionadas con la entidad de entrada con 1 grado

WS_ALERT
Devuelve una lista de todas las alertas de la base de datos de entidades que incluyen el ID de la entidad de entrada

El usuario indica qué formato incorporado desea utilizar en el código FORMAT_CODE del documento de entrada UMF adecuado.

Consideraciones sobre el rendimiento

Las solicitudes de búsqueda de interconexión de servicios Web que contienen más de un criterio de búsqueda suelen implicar que el sistema realiza una comparación con un menor número de entidades de la base de datos. Esto, a su vez, significa que el sistema devuelve resultados con mayor rapidez que las solicitudes con menos criterios de búsqueda.

Creación de consultas de servicios Web para encontrar una entidad específica

Utilice estas instrucciones para crear un documento de entrada UMF_QUERY a fin de buscar una entidad específica en la base de datos de entidades. El documento de entrada UMF_QUERY se envía mediante los servicios Web a una interconexión de servicios Web para proceso. Después de que la interconexión procese la consulta, los servicios Web devuelven un documento de salida UMF_QUERY_RESULT que contiene los detalles acerca de la entidad de entrada solicitada.

Antes de empezar

El servidor WebSphere Application Server incrustado debe estar en ejecución y se debe haber iniciado al menos una interconexión de servicios Web y estar en ejecución para recibir y procesar el documento de entrada UMF_QUERY.

Acerca de esta tarea

Puesto que la solicitud de búsqueda es un documento de entrada UMF, se deben formatear los criterios utilizando códigos UMF válidos. Puede utilizar cualquier editor de texto o programa de utilidad que cree UMF.

Procedimiento

1. Cree un nuevo documento de entrada UMF_QUERY.
2. En el segmento ROOT, especifique los códigos y valores UMF necesarios:
   a. Especifique el código de fuente de datos en el código DSRC_CODE. El código de fuente de datos por omisión para las búsquedas de interconexión de servicios Web es 1589. Si no utiliza el código de fuente de datos de búsqueda de interconexión de servicios Web por omisión como código de fuente de datos, asegúrese de que está configurado para no resolver entidades.
   b. Especifique el código de referencia de fuente de datos que hace referencia a la transacción de mensajes que realiza la solicitud en el código DSRC_REF. El código de referencia de fuente de datos debe tener significado, porque se devuelve a la aplicación de llamada.
   c. Especifique el código de formato para indicar el formato de salida de los resultados utilizando el código FORMAT_CODE. Las interconexions se suministran con tres códigos de formato incorporados para una búsqueda de interconexión de servicios Web que utilizan UMF_QUERY:
      - WS_DETAIL, que devuelve todos los datos de entidad disponibles para el ID de entidad de entrada
      - WS_RELATION, que devuelve una lista de todas las entidades relacionadas con el ID de entidad de entrada en una relación de 1 grado
      - La consulta WS_ALERT, que devuelve todas las alertas de rol del sistema que implican el ID de entidad de entrada

Si utiliza un código de formato diferente, debe configurarse en la tabla UMF_OUTPUT_FORMAT.

d. En el código ENTITY_ID, especifique el ID para la entidad de la que desea devolver información.

3. Especifique cualquier otro criterio de búsqueda utilizando los demás segmentos UMF opcionales <NAME>, <ADDRESS>, <EMAIL>, <ATTRIBUTE> y <NUMBER>.
4. Envíe el documento de entrada UMF_QUERY a una interconexión de servicios Web.

Resultados

Una interconexión de servicios Web toma el documento UMF_QUERY, utilizando los criterios especificados para buscar entidades en la base de datos que coinciden con la consulta. A continuación, la interconexión procesa la consulta, crea archivos de registro normales y devuelve los resultados en un documento de salida UMF_QUERY_RESULT mediante los servicios Web a la aplicación de llamada.

Ejemplo de búsqueda UMF_QUERY

En este ejemplo, UMF_QUERY busca toda la información acerca del ID de entidad 1223:

Nota: Este ejemplo está formateado para la lectura y no sigue el formato necesario de una línea por registro UMF.

```
<UMF_QUERY>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>546</DSRC_REF>
  <FORMAT_CODE>WS_DETAIL</FORMAT_CODE>
  <ENTITY_ID>1223</ENTITY_ID>
</UMF_QUERY>
```

Documento de entrada UMF_QUERY

El documento de entrada UMF QUERY contiene la colección de segmentos UMF que estructuran los datos de entrada para consultar la base de datos de entidades y, después, buscar y devolver la información acerca de una entidad específica a la aplicación de llamada. Contiene la solicitud de los criterios de búsqueda para una consulta de interconexión de servicios web.

La información de un documento de entrada UMF_QUERY se basa en sentencias SQL. Los resultados de esta búsqueda de interconexión de servicios Web se devuelven a la aplicación de llamada en un documento de salida UMF_QUERY_RESULT. UMF_QUERY realiza una consulta "Consulta mejorada / Buscar por atributo".

Estos elementos y segmentos UMF necesarios forman el documento de entrada UMF_QUERY

DSRC_CODE

Código UMF del código de fuente de datos que es necesario ya que hace referencia e identifica la aplicación de llamada. Como parte del registro de interconexiones normal, este código de fuente de datos se registra en la tabla UMF_LOG para cada UMF_QUERY procesado.

El sistema ya está configurado con un código de fuente de datos, 1589, que se puede utilizar para todas las búsquedas de interconexión de servicios Web. Este código de fuente de datos realiza el proceso de resolución de entidades sin resolver los criterios de búsqueda de entrada con la entidad

en la base de datos de entidades que coincide con la búsqueda. Puede crear su propio código de fuente de datos para una aplicación de llamada en particular, tan sólo debe asegurarse de que el código de fuente de datos se establezca en no resolver las entidades.

DSRC_REF
Código UMF de referencia de fuente de datos que es necesario ya que hace referencia a la transacción del mensaje de solicitud y se devuelve a la aplicación de llamada.

FORMAT_CODE
Código UMF que se correlaciona con un formato de documento de salida UMF que se especifica en la tabla UMF_OUTPUT_FORMAT. IBM InfoSphere Identity Insight se suministra con tres códigos de formato incorporados para una búsqueda de interconexión de servicios Web que utilizan UMF_QUERY:

- WS_DETAIL, que devuelve todos los datos de entidad disponibles para el ID de entidad solicitado
- WS_RELATION, que devuelve una lista de todas las entidades relacionadas con la entidad de entrada en el grado 1
- La consulta WS_ALERT, que devuelve todas las alertas del sistema que implican el ID de entidad de entrada

Para realizar EQ (Consulta mejorada / Buscar por atributo) a través de este documento de entrada, se debe especificar el siguiente FORMAT_CODE.

Ejemplo de ENHANCED_QUERY_RESULT:

```
<UMF_QUERY>
<FORMAT_CODE>ENHANCED_QUERY_RESULT</FORMAT_CODE>
 <ATTRIBUTE>
  <ATTR_TYPE>CIT</ATTR_TYPE>
  <ATTR_VALUE>CANADA</ATTR_VALUE>
 </ATTRIBUTE>
</UMF_QUERY>
```

ENTITY_ID
Este código UMF necesario especifica el ID de entidad para la entidad de la búsqueda. El sistema devuelve una respuesta con detalles de los datos conocidos acerca de esta entidad de la base de datos de entidades, basándose en los demás criterios de consulta.

Después se especifican los criterios de búsqueda opcionales utilizando los otros segmentos UMF disponibles y sus códigos validos para nombres, direcciones, números, caracteristicas y direcciones de correo electrónico.

NAME
Consulta los atributos de nombre que definen el nombre de una persona, organización, lugar o elemento, tal como se define en el model de identidad y la identidad entrante.

NUMBER
Consulta atributos de nombre que constan de datos normalmente descritos como un número, por ejemplo números de tarjetas de crédito, números de telefono y números de pasaporte.

ADDRESS
Consulta atributos de direcciones que definen una ubicación de la

identidad y que normalmente contienen información de una dirección estándard: nombre de la calle y número; número de edificio, ciudad, estado, país y código postal.

ATTRIBUTE
Consulta características de atributos que definen otros rasgo de identidad o otro tipo de información que no está expresada con otros tipos de atributos.

EMAIL
Consulta atributos de correo electrónico que definen direcciones de correo electrónico de internet.

Ejemplo de búsqueda UMF_QUERY

Este ejemplo de UMF_QUERY utiliza el código de formato WS_DETAIL de ejemplo para consultar la base de datos de entidades y devolver toda la información conocida acerca del ID de entidad 1223:

Nota: Este ejemplo está formateado para la lectura y no sigue el formato necesario de una línea por registro UMF.

```
<UMF_QUERY>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>546</DSRC_REF>
  <FORMAT_CODE>WS_DETAIL</FORMAT_CODE>
   <ENTITY_ID>1223</ENTITY_ID>
</UMF_QUERY>
```

Código de formato de WS_DETAIL:

Cuando construya una búsqueda de interconexión de servicios Web para que devuelva los detalles acerca de una entidad específica de la base de datos de entidades, utilice el código de formato incorporado WS_DETAIL. Este código de formato se especifica en el documento de entrada UMF_QUERY que contiene los criterios para la consulta.

Ejemplo de búsqueda de interconexión de servicios Web utilizando el código de formato WS_DETAIL

Este ejemplo de búsqueda de interconexión de servicios Web devuelve toda la información de la base de datos de entidades para Joe Franklin, ID de entidad 87.

Nota: Este ejemplo está formateado para la lectura y no sigue el formato necesario de una línea por registro UMF.

Para solicitar los detalles del ID de entidad 87 (Joe Franklin), cree un nuevo documento de entrada UMF_QUERY con la solicitud:

```
<UMF_QUERY>
  <FORMAT_CODE>WS_DETAIL</FORMAT_CODE>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>ABC-003</DSRC_REF>
    <ENTITY_ID>87</ENTITY_ID>
</UMF_QUERY>
```

Tras enviar este documento UMF_QUERY a través de los servicios Web para que una interconexión de servicios Web lo procese, la aplicación de llamada recibe una respuesta en el documento UMF_QUERY_RESULT siguiente:

```
<UMF_QUERY_RESULT>
  <DSRC_CODE>1589</DSRC_CODE>
 <ENTITY>
     <ENTITY_ID>87</ENTITY_ID>
  <SOURCE>
    <ACCT>OFAC</ACCT>
  <NAME>
       <NAME_TYPE>MAIN</NAME_TYPE>
      <FIRST_NAME>JOSEPH</FIRST_NAME>
       <LAST_NAME>FRANKLIN</LAST_NAME>
   </NAME>
  <ADDRESS>
      <ADDR_TYPE>H</ADDR_TYPE>
      <ADDR1>5559 W. 4TH ST</ADDR1>
      <CITY>SAN FRANCISCO</CITY>
      <STATE>CA</STATE>
      <POSTAL_CODE>94123-4567</POSTAL_CODE>
      <COUNTRY>USA</COUNTRY>
  </ADDRESS>
  <NUMBER>
      <NUM_TYPE>PHONE</NUM_TYPE>
      <NUM_VALUE>415-555-3325</NUM_VALUE>
  </NUMBER>
  </SOURCE>
  <SOURCE>
    <ACCT>FBI</ACCT>
   <NAME>
        <NAME_TYPE>MAIN</NAME_TYPE>
        <FIRST_NAME>JOEY</FIRST_NAME>
        <LAST_NAME>FRANKLIN</LAST_NAME>
    </NAME>
  <ADDRESS>
      <ADDR_TYPE>H</ADDR_TYPE>
      <ADDR1>392 S.E. MULLENS AVE</ADDR1>
      <CITY>OAKLAND</CITY>
      <STATE>CA</STATE>
      <POSTAL_CODE>94126-1566</POSTAL_CODE>
      <COUNTRY>USA</COUNTRY>
  </ADDRESS>
  <NUMBER>
      <NUM_TYPE>PHONE</NUM_TYPE>
      <NUM_VALUE>415-555-3325</NUM_VALUE>
  </NUMBER>
  <NUMBER>
      <NUM_TYPE>CC</NUM_TYPE>
      <NUM_VALUE>1111-22-3333</NUM_VALUE>
  </NUMBER>
  </SOURCE>
  <SOURCE>
    <ACCT>A9</ACCT>
  <NAME>
       <NAME_TYPE>MAIN</NAME_TYPE>
      <FIRST_NAME>JOE</FIRST_NAME>
       <LAST_NAME>FRANKLIN</LAST_NAME>
   </NAME>
  <ADDRESS>
      <ADDR_TYPE>B</ADDR_TYPE>
      <ADDR1>392 S.E. MULLENS AVE</ADDR1>
      <CITY>OAKLAND</CITY>
      <STATE>CA</STATE>
      <POSTAL_CODE>94126-1566</POSTAL_CODE>
      <COUNTRY>USA</COUNTRY>
  </ADDRESS>
  <NUMBER>
      <NUM_TYPE>PHONE</NUM_TYPE>
      <NUM_VALUE>415-555-3325</NUM_VALUE>
  </NUMBER>
```

```
  <NUMBER>
      <NUM_TYPE>CC</NUM_TYPE>
      <NUM_VALUE>1111-22-3333</NUM_VALUE>
  </NUMBER>
  </SOURCE>
  </ENTITY>
  <FROM_NODE>ABC-003</FROM_NODE>
  <PAGE_NUM>1</PAGE_NUM>
  <FORMAT_CODE>WS_DETAIL</FORMAT_CODE>
</UMF_QUERY_RESULT>
```

En esta respuesta, puede ver que hay tres fuentes de datos con información sobre Joe Franklin: la lista de OFAC, una lista de FBI y la lista de A9. Joe utiliza dos direcciones diferentes pero, en cada caso, utiliza el mismo número de teléfono y tarjeta de crédito.

Código de formato de WS_ALERT:

Cuando se construye una búsqueda de interconexión de servicios Web para que devuelva todas las alertas de rol de la base de datos de entidades que implican una entidad específica, utilice el código de formato incorporado WS_ALERT. Este código de formato se especifica en el documento de entrada UMF_QUERY que contiene los criterios para la consulta.

Ejemplo de búsqueda de interconexión de servicios Web utilizando el código de formato WS_ALERT

Este ejemplo de búsqueda de interconexión de servicios Web devuelve una lista de todas las alertas de rol en las que Joe Franklin, ID de entidad 87, está implicado.

Nota: Este ejemplo está formateado para la lectura y no sigue el formato necesario de una línea por registro UMF.

Para solicitar las alertas de rol para el ID de entidad 87 (Joe Franklin), cree un nuevo documento de entrada UMF_QUERY con la solicitud:

```
<UMF_QUERY>
  <FORMAT_CODE>WS_ALERT</FORMAT_CODE>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>BB123-9003</DSRC_REF>
    <ENTITY_ID>87</ENTITY_ID>
</UMF_QUERY>
```

Tras enviar este documento UMF_QUERY a través de los servicios Web para que una interconexión de servicios Web lo procese, la aplicación de llamada recibe una respuesta en el documento UMF_QUERY_RESULT siguiente:

```
<UMF_QUERY_RESULT>
  <ALERT>
    <CONFLICT_ID>2</CONFLICT_ID>
    <CONFLICT_RULES_DESC>Bad Guy Knows Employee</CONFLICT_RULES_DESC>
    <CONF_ENTITY1>87</CONF_ENTITY1>
    <CONF_ENTITY2>376</CONF_ENTITY2>
    <DEGREE_OF_SEP>1</DEGREE_OF_SEP>
    <INBOUND_ENTITY_ID>87</INBOUND_ENTITY_ID>
    <NAME1>FRANKLIN, JOSEPH</NAME1>
    <NAME2>MILLER, SUSAN</NAME2>
    <PATH_STRENGTH>80</PATH_STRENGTH>
 </ALERT>
 <ALERT>
    <CONFLICT_ID>5</CONFLICT_ID>
    <CONFLICT_RULES_DESC>Bad Guy Knows Vendor</CONFLICT_RULES_DESC>
    <CONF_ENTITY1>87</CONF_ENTITY1>
```

```
    <CONF_ENTITY2>10651</CONF_ENTITY2>
    <DEGREE_OF_SEP>1</DEGREE_OF_SEP>
    <INBOUND_ENTITY_ID>87</INBOUND_ENTITY_ID>
    <NAME1>FRANKLIN, JOSEPH</NAME1>
    <NAME2>MARTINEZ, JULIO</NAME2>
    <PATH_STRENGTH>64</PATH_STRENGTH>
 </ALERT>
  <DSRC_CODE>1589</DSRC_CODE>
  <FROMNODE>BB123-9003</FROMNODE>
</UMF_QUERY_RESULT>
```

En esta respuesta, se puede ver que hay dos alertas de rol para Joe Franklin: una alerta de que la empleada Susan Miller conoce a Joe y otra de que Julio Martinez conoce a Joe.

Código de formato WS_RELATION:

Cuando construya una búsqueda de interconexión de servicios Web para que devuelva una lista de todas las entidades relacionadas con una entidad específica en 1 grado, utilice el código de formato incorporado WS_RELATION. Este código de formato se especifica en el documento de entrada UMF_QUERY que contiene los criterios para la consulta.

Ejemplo de búsqueda de interconexión de servicios Web utilizando el código de formato WS_RELATION

Este ejemplo de búsqueda de interconexión de servicios Web devuelve una lista de todas las entidades relacionadas en 1 grado con Joe Franklin, ID de entidad 87.

Nota: Este ejemplo está formateado para la lectura y no sigue el formato necesario de una línea por registro UMF.

```
<UMF_QUERY>
  <FORMAT_CODE>WS_RELATION</FORMAT_CODE>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>ABC-003</DSRC_REF>
    <ENTITY_ID>87</ENTITY_ID>
</UMF_QUERY>
```

Tras enviar este documento UMF_QUERY a través de los servicios Web para que una interconexión de servicios Web lo procese, la aplicación de llamada recibe una respuesta en el documento UMF_QUERY_RESULT siguiente:

```
<UMF_QUERY_RESULT>
  <DSRC_CODE>1589</DSRC_CODE>
 <RELATION>
  <DETAIL>
      <ENTITY_ID>87</ENTITY_ID>
      <INBOUND_VALUE_ABST>415-555-3325</INBOUND_VALUE_ABST>
      <MATCHED_CODE>6</MATCHED_CODE>
      <MATCHED_DSRC_ACCT>6</MATCHED_DSRC_CODE>
      <MATCHED_ENTITY_ID>376</MATCHED_ENTITY_ID>
      <MATCHED_KEY_ID>16</MATCHED_KEY_ID>
      <MATCHED_TYPE>NUMBER</MATCHED_TYPE>
      <MATCHED_VALUE_ABST>415-555-3325</MATCHED_VALUE_ABST>
      <MATCH_PRECISION>EXACT MATCH</MATCH_PRECISION>
      <SIMILARITY_ID>1</SIMILARITY_ID>
  </DETAIL>
  <DETAIL>
      <ENTITY_ID>87</ENTITY_ID>
      <LIKE_CONF>40</LIKE_CONF>
      <MATCH_ID>376</MATCH_ID>
      <RELTO_ID>6</RELTO_ID>
```

```
  </DETAIL>
  <DETAIL>
      <ENTITY_ID>87</ENTITY_ID>
      <INBOUND_VALUE_ABST>1111-22-3333</INBOUND_VALUE_ABST>
      <MATCHED_CODE>6</MATCHED_CODE>
      <MATCHED_DSRC_ACCT>6</MATCHED_DSRC_CODE>
   <MATCHED_ENTITY_ID>10651/MATCHED_ENTITY_ID>
      <MATCHED_KEY_ID>16</MATCHED_KEY_ID>
      <MATCHED_TYPE>NUMBER</MATCHED_TYPE>
      <MATCH_PRECISION>EXACT MATCH</MATCH_PRECISION>
      <SIMILARITY_ID>1</SIMILARITY_ID>
  </DETAIL>
  <DETAIL>
      <ENTITY_ID>87</ENTITY_ID>
      <LIKE_CONF>40</LIKE_CONF>
      <MATCH_ID>10651</MATCH_ID>
      <RELTO_ID>6</RELTO_ID>
 </RELATION>
   <FORMAT_CODE>WS_RELATION</FORMAT_CODE>
<UMF_QUERY_RESULT>
```

Creación de consultas de servicios Web para encontrar entidades con atributos similares

Utilice estas instrucciones para crear un documento de entrada UMF_SEARCH a fin de buscar entidades en la base de datos de entidades que coincidan con los valores de datos de los atributos especificados en los criterios de búsqueda. El documento de entrada UMF_SEARCH se envía mediante los servicios Web a una interconexión de servicios Web para proceso. Después de que la interconexión procese la consulta, los servicios Web devuelven un documento de salida UMF_SEARCH_RESULTS que contiene una lista de entidades que han coincidido con los criterios de búsqueda.

Antes de empezar

El servidor WebSphere Application Server incrustado debe estar en ejecución y se debe haber iniciado al menos una interconexión de servicios Web y estar en ejecución para recibir y procesar el documento de entrada UMF_SEARCH.

Acerca de esta tarea

Puesto que la solicitud de búsqueda es un documento de entrada UMF, se deben formatear los criterios utilizando códigos UMF válidos. Puede utilizar cualquier editor de texto o programa de utilidad que cree UMF.

Procedimiento

1. Cree un nuevo documento de entrada UMF_SEARCH.
2. En el segmento ROOT, especifique los códigos y valores UMF necesarios, así como cualquier código y valores UMF opcionales que desee utilizar para especificar los criterios de búsqueda. Como mínimo, especifique valores para estos códigos UMF:
   a. Especifique el código de fuente de datos en el código DSRC_CODE. El código de fuente de datos por omisión para las búsquedas de interconexión de servicios Web es 1589. Si no utiliza el código de fuente de datos de búsqueda de interconexión de servicios Web por omisión como código de fuente de datos, asegúrese de que está configurado para no resolver entidades.

b. Especifique el código de referencia de fuente de datos que hace referencia a la transacción de mensajes que realiza la solicitud en el código DSRC_REF. El código de referencia de fuente de datos debe tener significado, porque se devuelve a la aplicación de llamada.

c. Especifique el código de formato para indicar el formato de salida de los resultados utilizando el código FORMAT_CODE. Las interconexions se suministran con tres códigos de formato incorporados para una búsqueda de interconexión de servicios Web que utilizan UMF_SEARCH:
   - WS_SUMMARY_TOP10, que devuelve las 10 primeras entidades que coinciden con los criterios de búsqueda
   - WS_SUMMARY_TOP100, que devuelve las 100 primeras entidades que coinciden con los criterios de búsqueda
   - La consulta WS_SUMMARY, que devuelve todas las entidades que coinciden con los criterios de búsqueda

   Si utiliza un código de formato diferente, debe configurarse en la tabla UMF_OUTPUT_FORMAT.

d. Especifique la puntuación de resolución mínima en el código MIN_LIKE_SCORE para establecer la puntuación numérica más baja que se considerará una coincidencia entre los valores de atributos de los criterios de búsqueda y las entidades de la base de datos de entidades que contengan los mismos atributos. Cuanto más alta es la puntuación, más exacta debe ser la coincidencia. Una puntuación de 100 indica una coincidencia exacta.

3. Especifique los valores de datos para los atributos que componen los criterios de búsqueda utilizando los demás segmentos de documento de entrada UMF válidos. Estos valores son los atributos que la búsqueda de interconexión de servicios Web busca para crear la lista de entidades con valores coincidentes o similares. El grado de coincidencia dependerá del valor de MIN_LIKE_SCORE.
4. Envíe el documento de entrada UMF_SEARCH mediante los servicios Web.

Resultados

Una interconexión de servicios Web toma el documento UMF_SEARCH, utilizando el proceso de resolución de entidades para buscar entidades en la base de datos con los criterios especificados. A continuación, la interconexión procesa la consulta, crea archivos de registro normales y devuelve los resultados en un documento UMF_SEARCH_RESULTS mediante los servicios Web a la aplicación de llamada utilizando el formato seleccionado.

Ejemplo de consulta de documento UMF_SEARCH

En este ejemplo, el documento de entrada UMF_SEARCH utiliza el código de formato WS_SUMMARY_TOP10 para consultar la base de datos de entidades a fin de buscar las 10 primeras entidades que contengan números de seguridad social en que el valor de datos del número de seguridad social coincida exactamente con el valor de datos 555-09-8761:

Nota: Este ejemplo está formateado para la lectura y no sigue el formato necesario de una línea por registro UMF.

```
<UMF_SEARCH>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>1223</DSRC_REF>
  <MIN_LIKE_SCORE>100</MIN_LIKE_SCORE>
  <FORMAT_CODE>WS_SUMMARY_TOP10</FORMAT_CODE>
```

```
 <NUMBER>
    <NUM_TYPE>SSN</NUM_TYPE>
    <NUM_VALUE>555-09-8761</NUM_VALUE>
 </NUMBER>
</UMF_SEARCH>
```

Documento de entrada UMF_SEARCH

El documento de entrada UMF_SEARCH contiene la solicitud y los criterios de una búsqueda de interconexión de servicios Web. Contiene la colección de segmentos UMF que estructuran los datos de entrada para buscar, en la base de datos de entidades, las entidades que contienen valores de atributo que coinciden con los criterios de búsqueda y, después, devolver la lista de entidades a la aplicación de llamada. Los resultados de la búsqueda de interconexión de servicios Web se devuelven a la aplicación de llamada en un documento de salida UMF_SEARCH_RESULT. UMF_SEARCH empieza un proceso "Buscar por resolución" completo.

Estos elementos y segmentos UMF necesarios comprenden el documento de entrada UMF_SEARCH

DSRC_CODE
: Código UMF del código de fuente de datos que es necesario ya que hace referencia e identifica la aplicación de llamada. Como parte del registro de interconexiones normal, este código de fuente de datos se registra en la tabla UMF_LOG para cada UMF_SEARCH procesado.

  El sistema ya está configurado con un código de fuente de datos, 1589, que se puede utilizar para todas las búsquedas de interconexión de servicios Web. Este código de fuente de datos realiza el proceso de resolución de entidades sin resolver los criterios de búsqueda de entrada con la entidad en la base de datos de entidades que coincide con la búsqueda. Puede crear su propio código de fuente de datos para una aplicación de llamada en particular, tan sólo debe asegurarse de que el código de fuente de datos se establezca en no resolver las entidades.

DSRC_REF
: Código UMF de referencia de fuente de datos que es necesario ya que hace referencia a la transacción del mensaje de solicitud y se devuelve a la aplicación de llamada.

SRC_CREATE_DT
: Código UMF de la fecha de creación del origen, que es opcional. Si este código contiene un valor, se utiliza para registro.

SRC_LSTUPD_DT
: Código UMF de la fecha de la última actualización del origen, que es opcional. Si este código contiene un valor, se utiliza para registro.

SRC_LSTUP_US
: Código UMF del último usuario actualizado del origen, que es opcional. Si este código contiene un valor, se utiliza para registro.

MIN_LIKE_SCORE
: Código UMF de puntuación de resolución (o similitud) mínima que es necesario a fin de establecer el valor de coincidencia más bajo para los demás segmentos y códigos UMF especificados. Esta puntuación numérica determina lo que se considera una coincidencia entre los valores de atributo solicitados y las entidades de la base de datos de entidad que

contienen los mismos atributos. Cuanto más alta es la puntuación, más exacta debe ser la coincidencia. Una puntuación de 100 indica una coincidencia exacta.

Por ejemplo, si la búsqueda es para encontrar todas las entidades con un número de seguridad social específico, MIN_LIKE_SCORE determina el grado de coincidencia que el número de seguridad social debe tener con el valor de datos de seguridad social especificado en la consulta antes de que una entidad de la base de datos se liste como parte del conjunto de resultados para esta consulta.

FORMAT_CODE
Código UMF que se correlaciona con el formato de documento de salida UMF que se especifica en la tabla UMF_FORMAT_CODE. IBM InfoSphere Identity Insight se suministra con tres códigos de formato incorporados para una búsqueda de interconexión de servicios Web que utilizan UMF_SEARCH:

- WS_SUMMARY_TOP10, que devuelve las 10 primeras entidades que coinciden con los criterios de búsqueda
- WS_SUMMARY_TOP100, que devuelve las 100 primeras entidades que coinciden con los criterios de búsqueda
- La consulta WS_SUMMARY, que devuelve todas las entidades que coinciden con los criterios de búsqueda

La única diferencia entre estas consultas es el número de registros devueltos, que se especifica en el nombre de la consulta.

Después se especifican los criterios de búsqueda opcionales utilizando los otros segmentos UMF disponibles y sus códigos validos para nombres, direcciones, números, caracteristicas y direcciones de correo electrónico.

NAME
Busca los atributos de nombre que definen el nombre de una persona, organización, lugar o elemento, tal como se define en el model de identidad y la identidad entrante.

NUMBER
Busca atributos de nombre que constan de datos normalmente descritos como un número, por ejemplo números de tarjetas de crédito, números de telefono y números de pasaporte.

ADDRESS
Busca atributos de direcciones que definen una ubicación de la identidad y que normalmente contienen información de una dirección estándard: nombre de la calle y número; número de edificio, ciudad, estado, país y código postal.

ATTRIBUTE
Busca características de atributos que definen otros rasgo de identidad o otro tipo de información que no está expresada con otros tipos de atributos.

EMAIL
Busca atributos de correo electrónico que definen direcciones de correo electrónico de internet.

Ejemplo de consulta UMF_SEARCH

Este ejemplo de consulta UMF_SEARCH devuelve las 5 primeras entidades de la base de datos de entidades que tienen un número de seguridad social que coincide exactamente con el número de seguridad social de 555-09-8761. Aunque se encontrasen más entidades, sólo se devuelven las 5 primeras entidades de la lista.

Nota: Este ejemplo está formateado para la lectura y no sigue el formato necesario de una línea por registro UMF.

```
<UMF_SEARCH>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>1223</DSRC_REF>
  <MIN_LIKE_SCORE>100</MIN_LIKE_SCORE>
  <MAX_RETURN_CNT>5</MAX_RETURN_CNT>
  <FORMAT_CODE>WS_SUMMARY</FORMAT_CODE>
 <NUMBER>
    <NUM_TYPE>SSN</NUM_TYPE>
    <NUM_VALUE>555-09-8761</NUM_VALUE>
 </NUMBER>
</UMF_SEARCH>
```

Códigos de formato de WS_SUMMARY:

IBM InfoSphere Identity Insight se suministra junto con tres códigos de formato previamente incorporados para utilizarlos con el documento de entrada UMF_SUMMARY: WS_SUMMARY, WS_SUMMARY_TOP10 y WS_SUMMARY_TOP100. Estos códigos de formato devuelven una lista de entidades que coinciden con los criterios especificados en el documento de entrada UMF_SUMMARY. La única diferencia entre estos códigos de formato es el número máximo de registros devueltos, que se especifica en el nombre de código de formato.

Ejemplo de búsqueda de interconexión de servicios Web utilizando el código de formato WS_SUMMARY_TOP10

Este ejemplo de búsqueda de interconexión de servicios Web devuelve las 10 primeras entidades de la base de datos de entidades que coinciden mejor con los siguientes criterios de búsqueda:

- Nombre: Joe Franklin
- Número de teléfono: 415-555-3325
- Fecha de nacimiento: 2 de enero de 1956

Utiliza el documento de entrada UMF_SEARCH para especificar estos criterios, que también especifica el código de formato `WS_SUMMARY_TOP10`.

Nota: Este ejemplo está formateado para la lectura y no sigue el formato necesario de una línea por registro UMF.

```
<UMF_SEARCH>
  <FORMAT_CODE>WS_SUMMARY_TOP10</FORMAT_CODE>
  <DSRC_CODE>1589</DSRC_CODE>
  <DSRC_REF>556</DSRC_REF>
  <MIN_LIKE_SCORE>80</MIN_LIKE_SCORE>
 <NAME>
    <NAME_TYPE>M</NAME_TYPE>
      <LAST_NAME>FRANKLIN</LAST_NAME>
     <FIRST_NAME>JOE</FIRST_NAME>
  </NAME>
 <NUMBER>
     <NUM_TYPE>PHONE</NUM_TYPE>
```

```
    <NUM_VALUE>415-555-3325</NUM_VALUE>
 </NUMBER>
 <ATTRIBUTE>
    <ATTR_TYPE>DOB</ATTR_TYPE>
    <ATTR_VALUE>01/02/1956</ATTR_VALUE>
 </ATTRIBUTE>
</UMF_SEARCH>
```

Tras enviar este documento UMF_SEARCH a través de los servicios Web para que una interconexión de servicios Web lo procese, la aplicación de llamada recibe una respuesta en el documento UMF_SEARCH_RESULT siguiente:

```
<UMF_SEARCH_RESULT>
  <DSRC_CODE>1589</DSRC_CODE>
 <ENTITY>
    <MATCHED_ENTITY_ID>38763</MATCHED_ENTITY_ID>
    <ENT_NAME>FRANKLIN, JOEY</ENT_NAME>
    <ENT_PHONE>415-555-3325</ENT_PHONE>
    <ENT_DOB>01/02/1956</ENT_DOB>
    <LIKE_SCORE>90</LIKE_SCORE>
  </ENTITY>
 <ENTITY>
    <MATCHED_ENTITY_ID>87</MATCHED_ENTITY_ID>
    <ENT_NAME>FRANKLIN, JOSEPH</ENT_NAME>
    <ENT_PHONE>415-555-3325</ENT_PHONE>
    <ENT_DOB>02/01/1956</ENT_DOB>
    <LIKE_SCORE>80</LIKE_SCORE>
  </ENTITY>
 <ENTITY>
    <MATCHED_ENTITY_ID>330</MATCHED_ENTITY_ID>
    <ENT_NAME>FRANKLIN, J</ENT_NAME>
    <ENT_PHONE>451-555-3325</ENT_PHONE>
    <ENT_DOB>01/02/1956</ENT_DOB>
    <LIKE_SCORE>80</LIKE_SCORE>
  </ENTITY>
  <FROM_NODE>556</FROM_NODE>
  <FORMAT_CODE>WS_SUMMARY_TOP10</FORMAT_CODE>
  <MIN_LIKE_SCORE>80</MIN_LIKE_SCORE>
  <PAGE_NUM>1</PAGE_NUM>
  <RETURN_CNT>3</RETURN_CNT>
</UMF_SEARCH_RESULT>
```

En este caso, sólo hay 3 entidades en la base de datos de entidades que coincidan con los criterios de búsqueda con una puntuación de similitud mínima de 80.

Capítulo 10. Resolución de problemas y soporte

Esta sección contiene información sobre cómo solucionar un problema con el software IBM InfoSphere Identity Insight, incluidas instrucciones para buscar en bases de conocimientos, para descargar arreglos y para ponerse en contacto con el equipo de soporte.

Visión general de la resolución de problemas

La resolución de problemas es un enfoque sistemático a la búsqueda de la solución de un problema. El objetivo es determinar por qué algo no funciona según lo esperado y cómo resolver el problema.

El primer paso del proceso de resolución de problemas consiste en describir el problema por completo. Sin una descripción del problema, ni el usuario ni IBM pueden saber por dónde empezar para encontrar la causa del problema. Este paso incluye realizarse preguntas básicas, cómo las siguientes:

- ¿Cuáles son los síntomas del problema?
- ¿Dónde se produce el problema?
- ¿Cuándo se produce el problema?
- ¿Bajo qué condiciones se produce el problema?
- ¿Se puede reproducir el problema?

Las respuestas a estas preguntas suelen dar lugar a una buena descripción del problema, y esta es la mejor manera de comenzar a solucionarlo.

¿Cuáles son los síntomas del problema?

Cuando se empieza a describir un problema, la pregunta más obvia es "¿Cuál es el problema?". Esta parece una pregunta directa; sin embargo, puede descomponerla en varias preguntas más detalladas que creen una imagen más descriptiva del problema. Estas preguntas pueden incluir:

- ¿Quién o qué ha notificado el problema?
- ¿Cuáles son los códigos y los mensajes de error?
- ¿Cómo falla el sistema? Por ejemplo, ¿se trata de un bucle, el sistema se cuelga, se desactiva, baja su rendimiento o se genera un resultado incorrecto?
- ¿Cuál es el impacto empresarial del problema?

¿Dónde se produce el problema?

El hecho de determinar dónde se origina el problema no siempre es fácil, pero es uno de los pasos más importantes para solucionarlo. Puede haber muchas capas de tecnología entre el componente de notificación y el componente anómalo. Redes, discos y controladores son sólo unos de los componentes que hay que tener en cuenta cuando se investigan problemas.

Las siguientes preguntas pueden ayudarle a centrarse en dónde se produce el problema a fin de identificar la capa del mismo.

- ¿El problema es específico de una plataforma o sistema operativo?
- ¿El problema es común entre varios servidores?

- ¿Se da soporte al entorno y a la configuración actuales?

Recuerde que, aunque una capa notifique el problema, no significa que el problema se origine en dicha capa. Parte de la identificación del lugar donde se origina un problema consiste en comprender el entorno en el que existe. Dedique un tiempo a describir por completo el entorno del problema, incluido el sistema operativo, su versión, todo el software y las versiones correspondientes e información sobre el hardware. Confirme que está ejecutando el programa en un entorno que constituye una configuración soportada; muchos problemas se deben a niveles de software que no están diseñados para que se ejecuten juntos o que no se han probado juntos por completo.

¿Cuándo se produce el problema?

Desarrolle un plan detallado de sucesos que dan lugar a un error, especialmente en los casos en los que el problema sólo se produce una vez. Puede hacerlo más fácilmente trabajando hacia atrás; comience en el momento en que se ha notificado el error (de la forma más precisa posible, incluso al nivel de milisegundos) y trabaje hacia atrás pasando por los registros y la información disponibles. Generalmente, tiene que observar hasta el primer suceso sospechoso que encuentre en el registro de diagnóstico; sin embargo, no siempre es fácil hacerlo y requiere práctica. Saber cuándo hay que dejar de observar resulta especialmente difícil cuando intervienen varias capas de tecnología y cuando cada una tiene su propia información de diagnóstico.

Para desarrollar un plan detallado de sucesos, intente responder las siguientes preguntas:

- ¿El problema sólo se produce a una determinada hora del día o de la noche?
- ¿Con qué frecuencia se produce el problema?
- ¿Qué secuencia de sucesos se han producido hasta la hora en que se ha notificado el problema?
- ¿Se produce el problema tras un cambio en el entorno, como por ejemplo una actualización o una instalación de software o de hardware?

Responder a preguntas como estas puede ayudarle a ofrecer un marco de referencia en el que investigar el problema.

¿Bajo qué condiciones se produce el problema?

Saber qué otros sistemas y aplicaciones se estaban ejecutando cuando se produjo el problema es una parte importante de la resolución de problemas. Estas y otras preguntas sobre el entorno le pueden ayudar a identificar la causa raíz del problema:

- ¿El problema siempre se produce cuando se realiza la misma tarea?
- ¿Se tiene que producir una determinada secuencia de sucesos para que aflore el problema?
- ¿Falla alguna otra aplicación a la vez?

Responder a este tipo de preguntas le puede ayudar a explicar el entorno en el que se produce el problema y a correlacionar dependencias. Recuerde que, aunque pueden haberse producido varios problemas a la misma hora, esto no necesariamente significa que los problemas estén relacionados.

¿Se puede reproducir el problema?

Desde el punto de vista de la resolución de problemas, el problema "ideal" es uno que se pueda reproducir. Generalmente, en el caso de problemas que se pueden reproducir, dispone de un gran número de herramientas o procedimientos que le ayuden a investigar. Por lo tanto, los problemas que puede reproducir suelen ser más fáciles de depurar y de solucionar. Sin embargo, los problemas que se pueden reproducir tienen una desventaja; si el problema tiene un impacto empresarial significativo, no desea que se reproduzca. Si es posible, vuelva a crear el problema en un entorno de prueba o de desarrollo, lo que suele ofrecerle más flexibilidad y control durante la investigación.

- ¿Se puede reproducir el problema en una máquina de prueba?
- ¿Varios usuarios o aplicaciones encuentran el mismo tipo de problema?
- ¿Se puede reproducir el problema ejecutando un solo mandato, un conjunto de mandatos o una determinada aplicación, o bien una aplicación autónoma?

Resolución de problemas de IBM InfoSphere Identity Insight

Utilice las siguientes preguntas como ayuda para identificar los problemas que se producen con IBM InfoSphere Identity Insight y buscar soluciones.

1. Durante la instalación, ¿ha informado el programa de instalación que uno o varios componentes no se han instalado satisfactoriamente? Si es así, revise los archivos de registro de instalación para determinar y solucionar el problema.
2. ¿Están las actualizaciones de servicio en el nivel más reciente?
3. ¿Recibe un mensaje de error?
4. ¿Ha comprobado los archivos de registro para ver si contienen algún mensaje acerca del problema?
5. ¿Se produce el problema cuando se utiliza uno de los siguientes componentes?
   - las aplicaciones web del kit de herramientas de Analista - revise la “Lista de comprobación de resolución de problemas de aplicaciones web de kit de herramientas de analista” en la página 393
   - las interconexiones - consulte lista de comprobación de resolución de problemas de interconexión
6. ¿Ha consultado las bases de información del producto para obtener información que pueda resolver el problema?
7. Si ha intentado todas estas opciones aplicables y sigue sin resolver el problema, póngase en contacto con el Centro de soporte de software de IBM.

Lista de comprobación para la resolución de problemas de interconexiones

Si tiene problemas con las interconexiones, antes de llamar al Centro de soporte de software de IBM, revise esta lista de problemas de interconexión que se producen más habitualmente.

1. La interconexión informa de un estado inactivo o no informa de ningún estado
2. La interconexión concluye
3. Las interconexiones no respetan los cambios en la configuración realizados en la Consola de configuración
4. Las interconexiones no se inician en AIX
5. La interconexión sólo procesa parte de un registro de entrada
6. El transporte no funciona

7. La interconexión no carga las notaciones científicas o los números de coma decimal flotante
8. Después de iniciar una interconexión, recibo un mensaje de aviso que indica que no existe ninguna ruta definida

1. **La interconexión notifica un estado de "Inactivo" o no notifica ningún estado**
   - ¿Contiene un error el nodo de interconexión o no está en ejecución?
   - ¿Ha utilizado el transporte especificado en el mandato de interconexión la sintaxis correcta?
   - ¿Ha concluido la interconexión?
2. **La interconexión concluye o se detiene de forma anómala**
   - ¿Ha encontrado la interconexión demasiados errores al procesar archivos de datos de entrada?
     - Examine los archivos de registro para obtener más información sobre los errores. Utilice esa información para resolver el problema.
     - Examine el valor *ErrorLimit* en el archivo de configuración de la interconexión. Podría ser necesario aumentar este valor.
   - ¿Se ha quedado la interconexión sin recursos de memoria?
   - Es la base de datos la causa del problema debido a una de estas razones:
     - ¿No hay suficiente espacio de disco?
     - ¿Se ha perdido la conectividad con la interconexión?
     - ¿Se ha cambiado el nombre y la contraseña de usuario para esta base de datos?
3. **Las interconexiones no respetan los cambios en la configuración realizados en la Consola de configuración**
   - Para que las interconexiones apliquen los cambios de configuración, deben detenerse y reiniciarse. Cuando se reinicien las interconexiones, se aplicarán los cambios de configuración como parte del proceso de inicialización de la interconexión.
   - Para conservar la integridad de los datos, detenga y reinicie todas las interconexiones en ejecución después de un cambio en la configuración.
4. **La interconexión no se inicia en AIX**
   - ¿Ha recibido un mensaje de error que indica que "no se pudo encontrar el módulo dependiente libicuio.a"?
     - Si la respuesta es positiva, compruebe que la biblioteca esté situada en uno de estos directorios: `/usr/lib`, `/lib`, `$DB2INSTHOM/sqllib/lib`. O bien defina la variable de entorno `LIBPATH` de forma que incluya el directorio *`directorio_inicial_instalación`*`/lib` del producto.
   - Compruebe la versión y ubicación de las bibliotecas de ejecución de C++. El problema puede ser debido a la presencia de valores incorrectos en `RunTime Update` y el entorno `LIBPATH`. Consulte la publicación “IBM InfoSphere Identity Insight Installation and Configuration Guide” para la información de soporte más reciente.
5. **La interconexión sólo procesa parte de un registro de entrada y no el registro completo**
   - Compruebe si el archivo de registro *.BAD contiene mensajes no válidos de UMF. Este archivo de registro indica el nombre del archivo origen de datos de entrada que se estaba procesando.
   - Examine el panel **Excepciones de UMF** en la Consola de configuración.
6. **El transporte de la interconexión no funciona**

- Compruebe que sea correcta la sintaxis utilizada para el transporte. Por ejemplo, si está especificando un transporte de base de datos, ¿incluyó comillas en el lugar apropiado?
- Si el transporte es un transporte de cola, ¿existe la cola de mensajes?
- Si el transporte es un archivo, ¿existe el archivo? ¿Está el archivo ubicado en el directorio especificado en el transporte?

7. **La interconexión no carga la notación científica ni un número de coma flotante**
   - Esto es una limitación conocida de la interconexión. Revise las notaciones científicas o los números de coma flotante en UMF para multiplicar el exponente, de modo que el número esté en una notación numérica estándar. Por ejemplo, la multiplicación de `-1.267E-05` es `-0.00001267`.
8. **Después de iniciar una interconexión, recibo un mensaje de aviso que indica que no existe ninguna ruta definida**
   - Este mensaje es solamente un mensaje de aviso informativo. Puede pasarlo por alto sin riesgo. (El mensaje simplemente le informa de que no existen rutas definidas para la interconexión. No son necesarias rutas para ejecutar una interconexión.)

Lista de comprobación de resolución de problemas de aplicaciones web de kit de herramientas de analista

Si experimenta problemas con las aplicaciones web, antes de llamar al soporte de software de IBM, revise esta lista de los problemas más comunes encontrados:

1. No puedo ver la pantalla de inicio de sesión de la Consola de configuración
2. No puedo iniciar la sesión en la Consola de configuración
3. Se abre un informe en el navegador web, pero no se visualiza nada en el informe
4. No puedo ver el estado de una interconexión en el panel Estado de interconexión
5. Los cambios de configuración realizados en la Consola de configuración no se respetan en las interconexiones.

1. **No puedo ver la pantalla Inicio de sesión.**
   - ¿Ve el mensaje "No se puede visualizar la página"?
     - El URL de aplicación web es probablemente incorrecto. Vuelva a escribir el URL. Si no está seguro del URL correcto, póngase en contacto con el administrador del sistema o con el soporte técnico interno para obtener ayuda.
     - Otras razones posibles: el puerto que conecta la máquina al servidor de WebSphere Liberty puede estar bloqueado o el servidor WebSphere Liberty puede no estar iniciado. Póngase en contacto con el administrador del sistema o con el soporte técnico interno para obtener ayuda.
   - ¿Está la pantalla en blanco?
     - Póngase en contacto con el administrador del sistema o con el soporte técnico interno. Es posible que el puerto que conecta la máquina al servidor de WebSphere Liberty no se haya iniciado o que la contraseña de base de datos de Identity Insight puede haber cambiado.
   - Si ninguna de estas soluciones resuelve el problema, póngase en contacto con el administrador del sistema o con el soporte técnico interno para obtener ayuda.
2. **No puedo iniciar la sesión en la aplicación web.**

- Asegúrese de que especifica el nombre de usuario y contraseña correctos. Las aplicaciones de kit de herramientas de analista no bloquean las cuentas de usuario, independientemente del número de intentos de inicio de sesión incorrectos, por lo tanto intente entrar el nombre de usuario y la contraseña de nuevo.
- Si ha olvidado el nombre de usuario y contraseña, póngase en contacto con el administrador del sistema o con el soporte técnico interno para obtener ayuda. Es posible que deba restablecer la contraseña.

3. **Los cambios de configuración realizados en la Consola de configuración no se respetan en la interconexión.**
   - Para que las interconexiones apliquen los cambios de configuración, deben detenerse y reiniciarse. Cuando se reinicien las interconexiones, se aplicarán los cambios de configuración como parte del proceso de inicialización de la interconexión.
   - Para conservar la integridad de los datos, detenga y reinicie todas las interconexiones en ejecución después de un cambio en la configuración.

Lista de comprobación de resolución de problemas del Visualizador

Si experimenta problemas con el Visualizador, antes de llamar al Centro de soporte de IBM, compruebe esta lista de los problemas más comunes que se encuentran al utilizar el Visualizador. Es posible que usted mismo pueda resolver el problema del Visualizador.

1. No puede iniciar el Visualizador
2. No puedo iniciar la sesión en el Visualizador
3. He generado un informe del Visualizador. El informe se abre en el navegador web, pero no se visualiza nada en el informe
4. Estoy recibiendo mensajes de error acerca de la interconexión
5. El Visualizador se 'cuelga' o queda 'bloqueado'
6. La función Buscar por atributo no devuelve los resultados esperados
7. Estoy recibiendo un mensaje de error sobre "índices insuficientes" al utilizar la ventana Buscar por atributo
8. Los iconos personalizados para gráficos del Visualizador no se visualizan o se visualizan incorrectamente
9. Los enlaces (o hiperenlaces) no funcionan en el Visualizador

1. **No puede iniciar el Visualizador**
   - En primer lugar, asegúrese de que el cliente de la estación de trabajo tiene la versión de cliente necesaria de Java instalada.
   - Si tiene varias versiones de Java instaladas en la máquina de cliente, es posible que la versión predeterminada del sistema de Java Web Start no sea la versión necesaria para ejecutar el Visualizador. Tenga también en cuenta que la versión de Java de cliente necesaria para abrir y ejecutar el Visualizador puede no ser la versión más reciente de Java instalada en su máquina. Hay dos maneras de resolver este problema: Asocie la versión de cliente necesaria de Java Web Start en su navegador web o utilice un método de lanzamiento directo.
     – ¿El Visualizador es la única aplicación Web Start que utiliza en este cliente de estación de trabajo? Si la respuesta es afirmativa, establezca el navegador web para asociar el tipo de archivo *.JNLP para utilizar la versión de cliente necesaria de Java Web Start.

  - ¿Ejecuta aplicaciones Web Start adicionales además del Visualizador en este estación de trabajo o desea evitar cambiar valores del sistema y de Java? Si la respuesta es afirmativa, lance directamente el Visualizador desde el archivo Java Web Start.
- ¿Está recibiendo un mensaje de error que indica que la aplicación ha solicitado una versión de JRE que no está instalada? Si la respuesta es afirmativa, configure Java versión 1.6 para aceptar descargas automáticas.
- ¿Puede ver la página de inicio web del Visualizador?
  - Sí, veo la página de inicio web del Visualizador, pero veo un mensaje que indica que "Es necesario Java Web Start para lanzar el Visualizador." No veo un enlace **"Pulse aquí para iniciar el Visualizador de IBM InfoSphere Identity Insight"**.
    - ¿Sólo utiliza este cliente de estación de trabajo para el Visualizador? Si la respuesta es afirmativa, establezca el navegador web para asociar el tipo de archivo JNLP para utilizar la versión de cliente necesaria de Java Web Start.
    - ¿Utiliza este cliente de estación de trabajo para abrir otras aplicaciones Web Start o desea evitar cambiar valores del sistema y de Java? Si la respuesta es afirmativa, inicie directamente el Visualizador desde el archivo Java Web Start
  - Sí, he visto la página de inicio web del Visualizador y una pantalla inicial del Visualizador, pero no veo una ventana de **Inicio de sesión** del Visualizador.
    - ¿Ha pulsado el enlace **"Pulse aquí para iniciar el Visualizador de IBM InfoSphere Identity Insight"**?
      - Si la respuesta es afirmativa, Java podría estar en proceso de abrir el Visualizador, lo que puede tardar varios minutos. Si el Visualizador está en proceso de abrirse, normalmente verá una pantalla inicial de Java o una ventana de Java Web Start.
      - Si la respuesta es negativa, pulse el enlace para iniciar el Visualizador.
    - Probablemente el problema se produce en el servidor WebSphere Application Server incrustado. El servidor de aplicaciones está sufriendo un error o problema y podría ser necesario reiniciarlo, o bien el servidor de aplicaciones no puede conectarse a la base de datos del producto correcta. Póngase en contacto con el administrador del sistema o con el soporte técnico interno.
  - No, no veo la página de inicio web del Visualizador.
    - Si ve el mensaje "No se puede visualizar la página", compruebe el URL del Visualizador. El URL podría contener una errata o podría ser un URL incorrecto para el Visualizador. Vuelva a escribir el URL. Si no conoce el URL del Visualizador, póngase en contacto con el administrador del sistema o con el soporte técnico interno.
    - Si el URL es correcto, estas son otras posibles razones por las que la página de inicio web del Visualizador no aparece:
      - WebSphere Application Server está sufriendo un error o problema y podría ser necesario reiniciarlo.
      - El puerto que conecta el cliente de estación de trabajo a WebSphere Application Server podría estar bloqueado o podría estar utilizándolo otra aplicación.

- Si ninguna de estas acciones resuelve el problema, solicite al administrador del sistema o al soporte técnico interno que se ponga en contacto con el Centro de soporte de software de IBM.

2. **No puedo iniciar la sesión en el Visualizador.**
   - ¿Puede ver la pantalla **Inicio de sesión** del Visualizador?
     – No, no puedo ver la pantalla **Inicio de sesión** del Visualizador.
       - Probablemente el problema se produce en el servidor WebSphere Application Server incrustado. El servidor de aplicaciones está sufriendo un error o problema (no conectado, o bien el servidor de aplicaciones no puede conectarse a la base de datos del producto correcta. Póngase en contacto con el administrador del sistema o con el soporte técnico interno para obtener ayuda.

     – Si, puedo ver la pantalla **Inicio de sesión** del Visualizador, pero no puedo iniciar la sesión.
       - Asegúrese de que especifica el nombre de usuario y contraseña correctos para su cuenta de usuario del Visualizador. El Visualizador no bloquea las cuentas de usuario, independientemente del número de intentos de inicio de sesión incorrectos. Así que puede volver a intentar entrar su nombre de usuario y contraseña. El acceso a su cuenta no puede quedar bloqueado.
       - Asegúrese de pulsar **Inicio de sesión**. El botón **Inicio de sesión** no se selecciona automáticamente, por lo que si especifica un nombre de usuario y contraseña y pulsa **Intro**, no sucede nada. Debe utilizar el ratón para pulsar en **Inicio de sesión** o seleccionar **Inicio de sesión** mediante el teclado.

   - ¿Ha olvidado el nombre de usuario y contraseña?
     – Sí. Póngase en contacto con el administrador del sistema o con el soporte técnico interno para buscar su nombre de usuario o restablecer su contraseña de la cuenta del Visualizador en la Consola de configuración.

3. **He generado un informe del Visualizador. El informe se abre en el navegador web, pero no se visualiza nada en el informe.**
   - Espere un minuto o dos más, porque es posible que el informe todavía se esté generando. Cuando el sistema genera un informe, se inicia con una pantalla en blanco en el navegador. Una vez se ha generado completamente el informe y está preparado para visualizarse, el sistema lo visualiza.
   - Asegúrese de que Adobe Acrobat Reader versión 7.0 o posterior está instalado en la máquina local. Si no, puede descargar gratis la aplicación Adobe Acrobat Reader más recientes del sitio web de Adobe.
   - ¿Existe un cortafuegos en el sistema? Si es así, examine el cortafuegos para comprobar que el sistema principal local y el servidor de aplicaciones tengan acceso a través del cortafuegos.

4. **Estoy recibiendo mensajes de error acerca de la interconexión.**
   - Repase el mensaje de error detenidamente para obtener más información acerca de la causa del problema.
   - Compruebe que la interconexión del Visualizador sea una interconexión HTTP.
   - ¿Su estación de trabajo tiene activado el registro de clientes del Visualizador?
     – No.
       - "Activación del registro cronológico del cliente del Visualizador" en la página 415 en la máquina. Establezca el nivel de registro en Depuración. A continuación póngase en contacto con el administrador

del sistema o el soporte técnico interno, proporcionando el texto del mensaje de error y notificando a esa persona que ha activado el registro del cliente del Visualizador. Puede que el administrador del sistema o el soporte técnico interno desee intentar conectar con la interconexión de nuevo, y después examinar el archivo de registro.
    - Cuando haya resuelto el problema, desactive el registro cronológico del cliente del Visualizador.
  – Sí.
    - Examine los archivos de registro del cliente del Visualizador situados en *directorio_instalación*/logs/ewas.
    - Póngase en contacto con el administrador del sistema o con el soporte técnico interno. Es posible que el administrador del sistema o el soporte técnico interno desee revisar el archivo de registro de cliente del Visualizador.

5. **El Visualizador se 'cuelga' o queda 'bloqueado'.**
   - El puerto que conecta la máquina al servidor WebSphere Application Server incrustado puede estar bloqueado, o puede que el servidor WebSphere Application Server incrustado no se haya iniciado. Póngase en contacto con el administrador del sistema o con el soporte técnico interno
   - Información para administradores de bases de datos, administradores del sistema o soporte técnico interno:
     – Tenga en cuenta la posibilidad de ejecutar estadísticas sobre las tablas de base de datos de entidad que afectan al Visualizador.
     – Si todos los usuarios del Visualizador tienen problemas debidos a que el Visualizador queda bloqueado, compruebe que los índices de tabla de la base de datos no se hayan modificado. El modificar los índices en las tablas de base de datos puede producir resultados imprevisibles y no deseables. Si detecta que los índices se han modificado, consulte al Centro de soporte de software de IBM.
6. **Buscar por atributo no devuelve los resultados esperados.**
   - Repase los criterios de búsqueda.
     – Si obtiene menos resultados que los esperados, podría ser necesario ampliar los criterios de búsqueda.
     – Si obtiene más resultados que los esperados, podría ser necesario restringir los criterios de búsqueda.
     – De forma predeterminada, el sistema solamente devuelve un máximo de 1000 registros en cada búsqueda. (No obstante, el valor puede configurarse. Este valor está controlado por el parámetro MAX_ENTITIES_RETURNED en el panel **Parámetros del sistema** de la Consola de configuración. Puede interesarle ponerse en contacto con el administrador del sistema o con el soporte técnico interno para verificar o modificar este valor.)
   - El problema puede estar relacionado con la forma en que está configurado el reconocimiento de letras mayúsculas y minúsculas en la base de datos. Póngase en contacto con el administrador del sistema o con el soporte técnico interno para comprobar si en la configuración de la base de datos hay valores sensibles a mayúsculas y minúsculas.
     – Para bases de datos DB2: Puede ser necesario que el administrador de bases de datos, el administrador del sistema o el soporte técnico interno tenga que aplicar un script para permitir las búsquedas de base de datos

sin distinción de mayúsculas y minúsculas. Pida al administrador del sistema que solicite el script y sus instrucciones de manejo al Centro de soporte de software de IBM.

- Para bases de datos Microsoft SQL Server: puede ser necesario configurar la base de datos para realice la distinción entre mayúsculas y minúsculas. Puede ser necesario que el administrador de bases de datos, el administrador del sistema o el soporte técnico interno tenga que cambiar el valor de distinción de mayúsculas y minúsculas para la base de datos.
- Para bases de datos Oracle: Puede ser necesario que el administrador de bases de datos, el administrador del sistema o el soporte técnico interno tenga que crear índices basados en funciones con UPPER para permitir las búsquedas de base de datos sin distinción de mayúsculas y minúsculas.

7. **Estoy recibiendo un mensaje de error sobre "índices insuficientes" al utilizar la ventana Buscar por atributo.**
   - El usuario está intentando buscar para un campo que no está indexado.
     - Restrinja la búsqueda añadiendo más criterios de búsqueda.
     - O bien póngase en contacto con el administrador del sistema o con el soporte técnico interno. Dependiendo del efecto sobre el rendimiento del sistema, el administrador del sistema puede crear un nuevo índice para este campo. (El administrador del sistema o el soporte técnico interno también podrían comprobar el parámetro `ENABLE_SEARCH_INDEX_CHECK` en el panel **Parámetros del sistema** en la Consola de configuración. Si este valor no está establecido en 1, el rendimiento del sistema puede resultar afectado.)
8. **Los iconos personalizados para gráficos del Visualizador no se visualizan o se visualizan incorrectamente.**
   - Es posible que los iconos no estén ubicados en el directorio correcto en el servidor de aplicaciones. Póngase en contacto con el administrador del sistema o con el soporte técnico interno para verificar la ubicación de vía de acceso de los iconos gráficos personalizados.
   - Los nombres de icono podrían tener una combinación de mayúsculas y minúsculas en lugar de todo en minúsculas, o podrían no coincidir con el tipo de atributo correspondiente. Por ejemplo, si **`Foto prueba`** es el nombre del tipo de atributo, el nombre del archivo de imagen deberá constar solo de minúsculas e incluir el espacio entre las palabras `foto` y `prueba`. El nombre de archivo debe tener este aspecto:**`foto prueba.gif`**. Póngase en contacto con el administrador del sistema o con el soporte técnico interno para asegurarse de que el nombre de archivo del icono es correcto.
   - Es posible que los iconos no tengan el formato de archivo .GIF recomendado. O bien, es posible que los iconos no tengan el tamaño recomendado, que es de 24 por 24 píxeles. Póngase en contacto con el administrador del sistema o con el soporte técnico interno para asegurarse de que el icono tiene el formato de archivo correcto y que utiliza el tamaño de imagen recomendado.
9. **Los enlaces (o hiperenlaces) del Visualizador no funcionan. Veo un mensaje de error cuando pulso en un enlace de atributo.**
   - Configure los valores de hiperenlace para la estación de trabajo. En las preferencias del sistema del Visualizador, puede elegir el navegador web o el programa que se utilizará para abrir archivos asociados con atributos de registro de identidad. Este valor debe configurarse en cada estación de trabajo que ejecute el Visualizador.
   - Después de configurar los valores de hiperenlace, asegúrese de cerrar el Visualizador y vuelva a iniciarlo.

Salud del sistema

Aquí encontrará algunas sugerencias para los administradores de bases de datos y administradores del sistema para mantener saludable el sistema IBM InfoSphere Identity Insight.

Sugerencias de rendimiento

Si observa una degradación en el rendimiento global del sistema, revise esta lista para obtener ideas sobre las causas posibles:

- Ajuste de la base de datos: ¿Cuándo fue la última vez que alguien ejecutó estadísticas de base de datos sobre las tablas de IBM InfoSphere Identity Insight?
- Entidades muy grandes: ¿La base de datos de entidades contiene entidades muy grandes- entidades con numerosas identidades?

Aunque en esta lista no está incluido todo, proporciona un punto de partida para validar que el sistema está en su máximo rendimiento.

Sugerencias para supervisar la base de datos de entidades

Estos son algunos elementos específicos que deben comprobarse como ayuda para supervisar la salud de la base de datos de entidades:

- Ajuste de la base de datos: ¿Cuál es la planificación para ejecutar estadísticas de base de datos sobre las tablas de IBM InfoSphere Identity Insight?
- Números exclusivos: ¿La base de datos de entidades contiene varias entidades que comparten el mismo número exclusivo?
- Entidades: ¿La base de datos de entidades contiene entidades con muchos números exclusivos?
- Resolución excesiva: ¿La base de datos de entidades contiene entidades muy grandes– entidades con numerosas identidades?

Aunque en esta lista no está incluido todo, proporciona algunas sugerencias rápidas para supervisar la salud global del sistema.

Tablas de base de datos que afectan al rendimiento del sistema

Si el rendimiento del sistema parece lento, los Administradores de bases de datos pueden ejecutar estadísticas de base de datos sobre varias tablas de bases de datos de entidades para mejorar el rendimiento de la interconexión y la experiencia del usuario en el Visualizador.

Tablas de la interconexión

Si el rendimiento de la interconexión parece lento, intente ejecutar estadísticas de bases de datos sobre las siguientes tablas de bases de datos de entidades:

- DQM_NAME_DICT
- NAME
- ADDRESS
- NUMS
- ATTRIBUTES
- EMAIL_ADDR
- DSRC_ACCT
- SEP_RELATIONS

- SEP_ROLES
- ENTITY
- DISCLOSED_RELATIONS
- UMF_LOG
- UMF_EXCEPT

Tablas del Visualizador

Si los usuarios del Visualizador se quejan de que el rendimiento del Visualizador parece lento, intente ejecutar estadísticas de bases de datos sobre las siguientes tablas de bases de datos de entidades:

- ER_ENTITY_SCORE
- ER_HISTORY
- ER_RELOCATION
- ER_DETAIL
- ER_ACCT_SCORE
- ER_ENTITY_STATE
- ER_FORCED_LOG
- SEP_CONFLICT
- SEP_CONFLICT_REL
- SEARCH
- APP_ACTIVITY_CODES
- APP_ACTIVITY_HISTORY
- APP_CONFLICT_GROUP
- APP_INBOX
- APP_ROLE
- APP_SEND
- MATCH_MERGE_RULES
- CONFLICT_RULES

Además, debido a que el Visualizador también utiliza una interconexión en segundo plano para realizar varias tareas del Visualizador (por ejemplo añadir entidades, buscar entidades por resolución de entidad, y divulgar relaciones), los Administradores de bases de datos también deberán ejecutar estadísticas de bases de datos sobre las tablas de bases de datos listadas en la sección Tablas de la interconexión.

Consulta de Grandes entidades

Esta consulta SQL busca grandes entidades. Cuantos más registros de identidad tenga una entidad, más grande se hará. A veces, los resultados de procesar datos de identidad de entrada pueden provocar que el sistema resuelva excesivamente registros de identidad durante la resolución de entidades y relaciones. Las grandes entidades pueden provocar que el rendimiento del sistema sea notablemente más lento.

Sentencia de consulta SQL de Grandes entidades

```
select entity_id
  count(dsrc_acct) as IDENTITY_CNT
from
 DSRC_ACCTwhere
  sys_delete_dt is null
```

```
group by
 entity_id
count(dsrc_acct) > 100
order by count(dsrc_acct)desc;
```

¿Qué hay que hacer a continuación?

En el plug-in de Identity Insight para i2 o la aplicación Explorer, utilice la pantalla **Buscar por ID de entidad** para buscar los ID de entidad devueltos por los resultados de consulta de Grandes entidades. Verifique que las identidades asociadas con esta entidad están asociadas correctamente. Para las entidades construidas correctamente, la entidad tiene muchas cuentas de orígenes de datos distintos, mientras que la mayoría de los datos para nombres, direcciones y números asociados son muy similares. Si tiene preguntas sobre si la entidad está construida correctamente, póngase en contacto con los servicios o el soporte de IBM para obtener ayuda.

Resultados de ejemplo de la consulta de Grandes entidades

Este es un ejemplo del aspecto que podrían tener los resultados de ejecutar la consulta de Grandes entidades:

ENTITY_ID	IDENTITY_CNT
3015	22
5241	41
7854	36

Consulta Números totales exclusivos por entidad

Esta consulta devuelve información sobre cuántos números exclusivos distintos están asociados con una entidad concreta, por ID de entidad. Esta consulta puede resultar de utilidad si cada entidad suele tener solamente un número exclusivo. Comprobar si las entidades contienen muchos tipos distintos de números exclusivos es una manera excelente de buscar anomalías en los datos y verificar que las normas de resolución están funcionando como está previsto.

Sentencia de Consulta SQL Número total de números exclusivos asociados con una sola entidad

```
select distinct *
from
  (select entity_id,
    (select count(distinct num_value)
  from
   nums,
   num_type
  Where
   nums.num_type_id=num.type.num_type_id
   and num_type.unique_FLAG='Y'
   and nums.entity_id=dsrc_acct.entity_id
    ) as UNIQUE_NUMBER_CNT
 from dscr_acct
  )as tab1
where
 UNIQUE_NUMBER_CNT>1
order by
  UNIQUE_NUMBER_CNT DESC;
```

¿Qué hay que hacer a continuación?

En el plug-in de Identity Insight para i2 o la aplicación Explorer, utilice la pantalla **Buscar por ID de entidad** para buscar los ID de entidad devueltos de los resultados de consulta Número total de números exclusivos por ID de entidad. Revisando el resumen de cada entidad, puede determinar si la entidad debería tener más de un número exclusivo. En algunos casos, esta situación podría ser un indicativo de fraude. Por ejemplo, en los EE.UU., los números de la Seguridad Social (SSN) son números exclusivos. Normalmente, cada entidad de los EE.UU. tiene solo un SSN. Si esta consulta descubre una entidad que tiene varios SSN, el paso siguiente probablemente será investigar más a fondo y analizar por qué la entidad tiene varios SSN.

Resultados de ejemplo de la consulta Número total de números exclusivos por entidad

Este es un ejemplo del aspecto que podrían tener los resultados de ejecutar la consulta Número total de números exclusivos por entidad:

ENTITY_ID	UNIQUE_NUMBER_CNT
3003	2
3030	2
3039	2

Consulta Número exclusivo compartido por varias entidades

Los números exclusivos son números que, normalmente, solo pertenecen a una entidad y no son compartidos por varias entidades. Comprobar si varias entidades comparten los mismos números exclusivos es una manera excelente de probar si hay anomalías en los datos y verificar que las normas de resolución están funcionando como está previsto. Puede utilizar la consulta Número exclusivo compartido por varias entidades para descubrir entidades que comparten el mismo número exclusivo. La consulta cuenta un número exclusivo para una sola entidad solamente una vez, independientemente de cuántos registros de identidad de esa entidad contengan el mismo número exclusivo.

Sentencia de consulta SQL Números exclusivos compartidos por varias entidades

```
select num_type,
 num_value,
  count(distinct ENTITY_ID) as cnt
from nums,
 num_type
Where   nums.num_type_id=num_type.num_type_id
 and num_type.unique_FLAG='Y'
Group by
 num_type
 num_value
Having
  count(distinct ENTITY_ID)>1
Order by
  count(distinct ENTITY_ID)desc;
```

¿Qué hay que hacer a continuación?

En el plug-in de Identity Insight para i2 o la aplicación Explorer, utilice la pantalla **Buscar por atributo** para buscar cada número devuelto por la consulta SQL

Números exclusivos compartidos por varias entidades. En el panel **Resultados**, revise la información de cada entidad que comparta el número exclusivo. También puede revisar los resúmenes de entidad de estas entidades para poder determinar por qué las entidades comparten el mismo número exclusivo.

Podría descubrir relaciones interesantes entre las entidades, basándose en el número exclusivo. Por ejemplo, podría descubrir que dos entidades distintas está utilizando el mismo número de la Seguridad Social.

O bien podría detectar un problema en la codificación de UMF para números exclusivos. Por ejemplo, podría descubrir que dos entidades comparten el mismo número de pasaporte, debido a que el registro de identidad de UMF entrante no ha utilizado NUM_LOC para indicar el país (ubicación) que emite el número de pasaporte. Los números como los pasaportes o los carnets de conducir solamente son exclusivos de una ubicación concreta, por ejemplo un país o estado/provincia. Por sí mismos, estos números podrían no ser tan exclusivos como piensa.

Resultados de ejemplo de la consulta Número exclusivo compartido por varias entidades

Este es un ejemplo del aspecto que podrían tener los resultados de ejecutar la consulta Número exclusivo compartido por varias entidades:

NUM_TYPE	NUM_VALUE	cnt
SSN	000-00-0000	9
SSN	111-11-1111	9
SSN	555-55-5555	5
SSN	611-00-6666	2
SSN	999-99-9999	3

Búsqueda en bases de conocimientos

En muchas ocasiones puede encontrar soluciones a problemas buscando en las bases de conocimientos de IBM. En este tema se describe cómo optimizar los resultados utilizando los recursos disponibles, las herramientas de soporte y los métodos de búsqueda.

Recursos técnicos disponibles

Además de este centro de información, dispone de los siguientes recursos técnicos para ayudarle a contestar preguntas y a resolver problemas:

Notas técnicas de IBM InfoSphere Identity Insight en www.ibm.com/software/support/isa/

Búsqueda con herramientas de soporte

Dispone de las siguientes herramientas de escritorio para ayudarle a realizar búsquedas en bases de conocimientos de IBM:

- **IBM Support Assistant (ISA)** es un entorno de trabajo de servicio de software gratuito que le ayuda a resolver preguntas y problemas con productos de software de IBM. Encontrará instrucciones para descargar e instalar ISA en el sitio Web de ISA en www.ibm.com/software/support/isa/

- **Barra de herramientas de soporte de software de IBM** es un plug-in de navegador que le proporciona un mecanismo para realizar búsquedas fácilmente en sitios de soporte de IBM. Puede descargar la barra de herramientas en www.ibm.com/software/support/toolbar/.

Consejos para la búsqueda

Los siguientes recursos describen cómo optimizar los resultados de la búsqueda:

- Búsqueda del sitio Web de soporte de IBM
- Utilización del motor de búsqueda de Google

Recepción de actualizaciones automáticas

- **Mi soporte**. Para recibir notificaciones semanales por correo electrónico sobre arreglos y otras noticias de soporte, siga estos pasos:
  1. Vaya al sitio Web de soporte de software de IBM en www.ibm.com/software/support/.
  2. Pulse **Mi soporte** en la esquina superior derecha del panel bajo **Soporte personalizado**.
  3. Si ya se ha registrado para Mi soporte, inicie la sesión y salte al paso siguiente. Si aún no se ha registrado, pulse **registrar ahora**. Complete el formulario de registro utilizando su dirección de correo electrónico y su ID de IBM y pulse **Enviar**.
  4. Pulse **Editar perfil**.
  5. En la **Lista de productos**, seleccione **Software** . Se muestra una segunda lista.
  6. En la segunda lista, seleccione un segmento del producto, por ejemplo **Gestión de sistemas**. Se muestra una tercera lista.
  7. En la tercera lista, seleccione un subsegmento del producto, por ejemplo **Rendimiento y disponibilidad de aplicaciones**. Se muestra una lista de productos aplicables.
  8. Seleccione los productos para los que desea recibir actualizaciones.
  9. Pulse **Añadir productos**.
  10. Después de seleccionar todos los productos que le interesan, pulse **Suscribir a correo electrónico** en el panel **Editar perfil**.
  11. Seleccione **Enviar estos documentos por correo electrónico semanal**.
  12. Actualice su dirección de correo electrónico si es necesario.
  13. En la **Lista de documentos**, seleccione **Software**.
  14. Seleccione los tipos de documentos sobre los que desea recibir información.
  15. Pulse **Actualizar**.

Visión general de los mensajes

Cuando recibe un mensaje de un componente del sistema, muchas veces puede resolver el problema leyendo el texto completo del mensaje y las acciones de recuperación asociadas al mismo.

Los identificadores de mensajes tienen 10 caracteres de longitud y los caracteres del identificador del mensaje ofrecen más información sobre el mismo.

- Los tres primeros caracteres identifican el producto.
  - **CWU** es el identificador de producto correspondiente a IBM InfoSphere Identity Insight.

- Los dos siguientes caracteres identifican el componente específico del producto que ha generado el mensaje.
  - **AE** es el identificador de componente correspondiente a la interconexión.
  - **AI** es el identificador de componente para la Consola de configuración.
  - **AK** es el identificador de componente correspondiente al Event Manager.
  - **AL** es el identificador de componente para los servicios web.
- Los cuatro siguientes caracteres son el número de mensaje.
- El último carácter es el código de tipo de mensaje, que describe la gravedad del mismo:
  - **E** indica un mensaje de error. Este tipo de mensaje indica un problema con un componente específico del producto que requiere una acción inmediata. Revise los archivos de registro del componente para obtener información que le ayudará a solucionar el problema.
  - **I** indica un mensaje informativo. Este tipo de mensaje no requiere una acción inmediata, pero es posible que desee revisar los archivos de registro del componente para obtener más información.
  - **W** indica un mensaje de aviso. Este tipo de mensaje indica que se ha producido una condición que puede requerir atención. Revise los archivos de registro del componente para obtener más información sobre el significado de la condición de aviso y sobre cómo puede resolver la condición.

Ejemplos de mensajes

Si recibe un mensaje con el identificador CWUAE0001E, se trata de un mensaje de error procedente de una interconexión que probablemente ha hecho que la interconexión se cerrara y se detuviera el proceso. Debe revisar los archivos de registro de la interconexión para solucionar el problema y poder reiniciar la interconexión.

Si recibe un mensaje con el identificador CWUAE325W, se trata de un mensaje de aviso que se ha producido en la interconexión, pero el aviso no ha hecho que la interconexión dejara de procesar registros de entrada. Puede consultar los archivos de registro de la interconexión para obtener más información sobre el aviso, para ver las acciones que puede emprender para corregir el problema o el registro de datos de entrada. Si esta interconexión en particular está supervisada por el supervisor de aplicaciones, también puede comprobar las ventanas del supervisor de aplicaciones de la Consola de configuración para obtener más información.

Errores de análisis de UMF

Los errores de análisis de UMF se producen cuando se formatean incorrectamente registros de identidad de UMF, tales como la falta de un código final o la presencia de caracteres no válidos en UMF.

Tabla 37. Errores de análisis de UMF

Código de error de UMF	Descripción de código	Gravedad
005	Los espacios en blanco iniciales no están permitidos en la *serie* de nombre de código	Grave
010	En el código de inicio de nivel raíz falta <*serie*>	Grave
015	Se ha encontrado un código final inesperado </*serie_caracteres*>	Grave

Tabla 37. Errores de análisis de UMF (continuación)

020	Se ha encontrado un código final incorrecto </*serie_caracteres*>, se esperaba </*serie_caracteres*>	Grave
025	El documento está incompleto, no hay suficientes códigos finales...Último segmento: <*serie_caracteres*>	Grave
030	El documento está vacío	Aviso
035	Los segmentos no pueden contener datos de código '*serie_caracteres*' cuando tienen segmentos hijos	Grave

Registros

IBM InfoSphere Identity Insight contiene mecanismos de registro que graban información en una serie de archivos de registro. Generalmente, el sistema empieza grabando información en los archivos de registro cuando se produce una condición cualificada en un componente específico del sistema, como por ejemplo que se instala o se inicia el componente, un usuario inicia una sesión en el componente o se produce un error durante el proceso.

Los siguientes componentes del sistema crean archivos de registro:

- Interconexiones
- Aplicaciones web de kit de herramientas de analista
- Servicios web
- Event Manager

Archivos de registro de interconexión

Cuando se inicia una interconexión, el sistema inicia automáticamente el registro, basándose en la configuración del registro de interconexiones actual en el archivo de configuración de interconexiones. Se crean archivos de registro para cada interconexión, por nombre de interconexión, aunque haya iniciado varias interconexiones utilizando el mismo archivo de configuración.

Tipos de archivos de registro de interconexiones

Por omisión, todos los archivos de registro de interconexiones se graban en el directorio del nodo de interconexión donde se ha iniciado la interconexión. Existen varios tipos diferentes de archivos de registro de interconexiones. El mensaje que se registra y el archivo en el que se registra dependen de la modalidad en la que se ha iniciado la interconexión (modalidad de depuración `-d` o modalidad de daemon/servicio `-s`), el tipo de mensaje que se registra y la configuración de registro actual.

Tabla 38. Archivos de registro de interconexiones por tipo de mensaje, nombre de archivo de registro y modalidades de registro

Tipo de mensaje	**Nombre de archivo de registro**	**Acción**	**Modalidad o modalidades de registro**
Mensajes de error	*nombre_interconexión*.err Registra los errores críticos que se han producido en la interconexión.	Después de revisar los archivos de registro, arregle los errores o problemas indicados de la interconexión.	Servicio Depuración

Tabla 38. Archivos de registro de interconexiones por tipo de mensaje, nombre de archivo de registro y modalidades de registro (continuación)

Tipo de mensaje	**Nombre de archivo de registro**	**Acción**	**Modalidad o modalidades de registro**
Mensajes de error de SQL	*nombre_interconexión*.SqlErr.log Registra los errores SQL que se han producido en la interconexión. Este archivo tiene un límite de tamaño de 1 megabyte. Cuando el archivo alcanza ese límite de tamaño, el sistema archiva automáticamente el archivo de registro actual y crea uno nuevo.	Después de revisar este archivo de registro, arregle los errores o problemas de SQL indicados.	Servicio Depuración
Errores de cola	*nombre_interconexión*.MQErr.log Registra errores de cola.	Después de revisar este archivo de registro, arregle los errores o problemas de MQ indicados.	
Visor de sucesos de Windows	(Sólo en plataformas Microsoft Windows) Si la interconexión tiene servicios instalados y se ha iniciado utilizando la modalidad de servicio (opción de interconexión `-s`), la interconexión también envía errores y mensajes importantes al Visor de sucesos de Windows.	Supervise los mensajes de la vista de Sucesos de Windows y arregle los errores o problemas indicados.	Servicio (sólo en plataformas Microsoft Windows)
Mensajes UMF incorrectos/ no válidos que no se han podido procesar	*nombre_interconexión*.bad Registra información acerca de los registros del archivo de origen de datos de entrada que contenían un UMF incorrectamente formado o no válido. La interconexión no ha podido procesar la parte del registro que contenía este UMF incorrecto o no válido, lo que a veces significa que la interconexión procesa registros parciales.	Tras consultar este archivo de registro, arregle los registros del archivo de origen de datos de entrada con un UMF incorrecto o no válido. Después devuelva los registros corregidos a través de una interconexión para proceso.	Servicio Depuración

Tabla 38. Archivos de registro de interconexiones por tipo de mensaje, nombre de archivo de registro y modalidades de registro (continuación)

Tipo de mensaje	Nombre de archivo de registro	Acción	Modalidad o modalidades de registro
Mensajes UMF que han generado excepciones	*nombre_interconexión*.msg Registra información acerca de registros del archivo de origen de datos de entrada que contienen excepciones generadas durante el proceso. La interconexión no ha procesado el registro. Este tipo de mensaje puede indicar un problema con la calidad de los datos para este archivo de origen de datos.	Después de revisar este archivo de registro, es posible que aún deba arreglar registros del archivo de origen de datos de entrada que ha generado la excepción UMF. Después devuelva los registros corregidos a través de una interconexión para proceso. También puede consultar el Informe de resumen de carga o el Informe de resumen de origen de datos para obtener más información.	Servicio Depuración
Rastreo de depuración	Registra la información de rastreo de depuración cuando la interconexión se ha iniciado utilizando la modalidad de depuración (opción de interconexión `-d`). No hay archivo de registro. La interconexión se ejecuta en primer plano con mensajes de salida que se envían directamente al shell de mandatos. Puede usar la característica de redirección para crear un archivo a partir de la salida del mandato de interconexión. `pipeline -d -f my_umf.xml > my_log_file.log`		Depuración
Sentencias SQL y estadísticas de rendimiento	*nombre_interconexión*.SqlDebug.log Registra sentencias SQL y estadísticas de rendimiento que pueden ayudarle a solucionar problemas y supervisar el rendimiento. Este archivo tiene un límite de tamaño de 48 megabytes. Cuando un archivo alcanza el límite de tamaño, el sistema archiva automáticamente el archivo de registro actual y crea un nuevo archivo de registro.		Depuración

Tabla 38. Archivos de registro de interconexiones por tipo de mensaje, nombre de archivo de registro y modalidades de registro (continuación)

Tipo de mensaje	Nombre de archivo de registro	Acción	Modalidad o modalidades de registro
La interconexión concluye mientras se procesa un archivo	*nombre_interconexión*.cnt A medida que la interconexión procesa registros de entrada, registra el nombre del archivo de origen de datos que se está procesando, así como un recuento de registros para cada 100 registros del archivo procesados satisfactoriamente. Si una interconexión concluye mientras se procesa un archivo de origen de datos de entrada, este archivo puede ayudarle a determinar los registros del archivo de origen de datos que se deben volver a cargar en la interconexión para proceso.	Tras revisar este archivo de registro y arreglar el problema que ha concluido la interconexión, vuelva a cargar los registros no procesados en la interconexión para proceso.	Archivo

Configuraciones del registro de interconexiones

IBM InfoSphere Identity Insight proporciona una configuración de registro por omisión que registra los sucesos y errores de las interconexiones. Esta configuración de registro por omisión se utiliza automáticamente, a menos que se especifique una configuración de registro de interconexiones personalizada en el archivo de configuración de interconexiones.

Hay dos maneras principales de iniciar las interconexiones: la modalidad de depuración (opción de interconexión `-d`) o la modalidad de servicio/daemon (opción de interconexión `-s`).

- La modalidad de depuración es útil para probar y solucionar problemas del sistema. Normalmente no se utiliza en entornos de producción. El registro para la modalidad de depuración incluye más información de rastreo y de funcionamiento de la interconexión.
- La modalidad de servicio/daemon es la modalidad típica del entorno de producción. El registro para la modalidad de servicio/daemon se limita normalmente a errores y problemas que requieren acción.

Todas las configuraciones de registro de interconexiones (por omisión y personalizada) deben especificar cómo registrar los sucesos de interconexión en modalidad de depuración y en modalidad de servicio/daemon. Si la configuración de registro por omisión no satisface sus necesidades, puede crear una configuración de registro personalizada añadiendo una sección de registro al archivo de configuración de interconexiones y utilizando los componentes de configuración de interconexiones para especificar la forma en que el sistema debe registrar los sucesos y los errores de interconexión para la modalidad de interconexión de depuración y la modalidad de interconexión de servicio/daemon.

Configuración de registro de modalidad de depuración por omisión

```
console://stdout $NODE_NAME.*;*.CRIT;*.ERR;*.NOTE
 cmeadmin:/// *.CRIT;*.ERR file://./$NODE_NAME.err *.CRIT
 file://./$NODE_NAME.SqlDebug.log?rotateSize=49152 sql.DBUG;sql.PERF
```

```
 file://./$NODE_NAME.SqlErr.log?rotateSize=1024 sql.ERR;sql.CRIT
 file://./$NODE_NAME.MQErr.log mq.!DBUG
 file://./$NODE_NAME.bad?style=bare bad_xml.*
 file://./$NODE_NAME.msg?style=bare msg.*
```

Configuración de registro de modalidad de servicio de Microsoft Windows por omisión

```
eventlog://./ *.NOTE;*.CRIT;*.ERR
 cmeadmin:/// *.CRIT;*.ERR file://./$NODE_NAME.err *.CRIT
 file://./$NODE_NAME.SqlDebug.log?rotateSize=49152 sql.DBUG;sql.PERF
 file://./$NODE_NAME.SqlErr.log?rotateSize=1024 sql.ERR;sql.CRIT
 file://./$NODE_NAME.MQErr.log mq.!DBUG
 file://./$NODE_NAME.bad?style=bare bad_xml.*
 file://./$NODE_NAME.msg?style=bare msg.*
```

Configuración de registro de modalidad de daemon de UNIX por omisión

```
file://./$NODE_NAME.log *.CRIT;*.ERR;*.NOTE;*.INFO;logger.!DBUG
 cmeadmin:/// *.CRIT;*.ERR file://./$NODE_NAME.err *.CRIT
 file://./$NODE_NAME.SqlDebug.log?rotateSize=49152 sql.DBUG;sql.PERF
 file://./$NODE_NAME.SqlErr.log?rotateSize=1024 sql.ERR;sql.CRIT
 file://./$NODE_NAME.MQErr.log mq.!DBUG
 file://./$NODE_NAME.bad?style=bare bad_xml.*
 file://./$NODE_NAME.msg?style=bare msg.*
```

Componentes del registro de interconexiones

Los componentes del registro de interconexiones ayudan a crear configuraciones de registro de interconexiones personalizadas. Proporcionan al sistema las instrucciones sobre cómo registrar sucesos y mensajes de interconexión.

Log writer

Especifica el transcriptor de registro que se debe utilizar para grabar o visualizar el archivo de registro:

file Graba los sucesos y mensajes de registro en un nombre de archivo especificado.

El transcriptor de registro de archivos utiliza los componentes de registro Vía de acceso, Parámetro, Espacio en blanco y Filtro. Por ejemplo:

`file://`*`vía acceso absoluta`*`?`*`parámetros`* `[espacio en blanco]` *`filtro`*

cmeadmin

Graba los sucesos y mensajes de registro en el registro cmeadmin.

El transcriptor de registro cmeadmin utiliza los componentes de registro Espacio en blanco y Filtro. Por ejemplo:

`cmeadmin://[espacio en blanco]` *`filtro`*

console

Escribe los sucesos y mensajes de registro en la consola de la línea de mandatos.

El transcriptor de registro de la consola utiliza los componentes de registro Ubicación, Parámetros y Filtro. Por ejemplo:

`console://`*`ubicación de archivo`*`?`*`parámetros filtro`*

eventlog

(Sólo plataformas Microsoft Windows) Graba los sucesos y mensajes de registro en el visor de sucesos de Microsoft Windows.

El transcriptor de sucesos eventlog utiliza el componente de registro Filtro. Por ejemplo:

`eventlog://./filtro`

Path Especifica la ubicación y el nombre del archivo en el que se debe grabar la información de registro:

File location
Los valores válidos son:

- stdout - se utiliza con el transcriptor de registro de la consola
- stderr - se utiliza con el transcriptor de registro de la consola
- *vía de acceso absoluta* - se utiliza con el transcriptor de registro de archivo

file name
Indica en qué archivo de registro de producto estándar se debe grabar la información. La extensión de nombre de archivo determina el tipo de archivo de registro. Entre los valores válidos de archivo de registro se incluyen los siguientes:

- .err
- .bad
- .msg
- .SqlDebug.log
- .SqlErr.log
- .MQErr.log

Parameter
Especifica los parámetros de registro opcionales. Los valores válidos son:

style=bare
Indica que el registro no incluye indicaciones de fecha y hora ni otra información de cabecera. Normalmente, este parámetro se incluye en archivos que registran mensajes UMF.

rotateSize=*número máximo tamaño archivo*
Indica el tamaño máximo de archivo en kilobytes para el archivo de registro. Cuando el archivo excede del tamaño máximo de archivo, el sistema archiva automáticamente el archivo de registro y crea un nuevo archivo que se debe utilizar para el registro. El sistema añade un 0 al nombre del archivo de archivado y el nuevo archivo toma el nombre del archivo original. Este proceso continúa hasta que el sistema alcanza el número máximo de archivos de archivado indicado en el parámetro `keep`.

keep=*número máximo de archivos de archivado*
Indica el número máximo de archivos de archivado que se deben conservar durante la rotación automática de archivos, basándose en el parámetro `rotateSize`. Cuando se excede el número máximo de archivos, el sistema graba sobre el archivo de registro de archivado más antiguo la nueva información de registro.

White Space
Indica qué tipo de espacio en blanco se debe colocar en el archivo de registro. Los valores válidos son:

- Space
- Tab

Filter Indica la información de registro que se debe grabar. Los valores válidos son:

Módulo
Indica el tipo de mensajes que se deben registrar. Los valores válidos son:

- $NODE_NAME - mensajes genéricos
- sql - mensajes SQL
- mq - mensajes de cola de mensajes
- bad_xml - mensajes UMF no válidos o incorrectamente formados
- msg - excepciones UMF
- logger - mensajes del registrador

Si desea incluir todos los tipos de módulo, utilice un carácter comodín de asterisco. Por ejemplo:

```
console://stdout *.ERR
```

Gravedad
Indica el nivel de gravedad del mensaje de registro. Los valores válidos son:

- CRIT - mensajes críticos
- ERR - mensajes de error
- WARN - mensajes de aviso
- NOTE - avisos
- INFO - mensajes informativos
- PERF - mensajes de rendimiento
- DBUG - mensajes de depuración

Si desea incluir todos los tipos de gravedad, utilice el carácter comodín de asterisco. Por ejemplo:

```
console://stdout *.*
```

Si desea excluir una gravedad del informe, utilice el signo de admiración. Por ejemplo:

```
console://stdout mq.!DBUG
```

Configuración del registro de interconexiones personalizado

IBM InfoSphere Identity Insight proporciona configuraciones de registro de interconexiones por omisión que determinan la forma en que las interconexiones registran los errores y mensajes en modalidad de depuración y en modalidad de servicio/daemon. Pero puede modificar la configuración de registro de interconexiones por omisión o crear una configuración de registro personalizada para satisfacer las necesidades de la organización. Para ello, debe crear dos archivos de registro que especifiquen la configuración de registro personalizada y después modificar el archivo de configuración de interconexiones para que utilice esos archivos de registro personalizados.

Acerca de esta tarea

El registro de interconexiones se efectúa por nodo de interconexión, por lo que deberá realizar estos cambios en cada nodo de interconexión. Después de crearlos, puede copiar los archivos de depuración y de configuración estándar en cada nodo de interconexión. También puede copiar y pegar el texto de la sección [logging] de un archivo de configuración de interconexiones en otro, o puede copiar todo el archivo de configuración de interconexiones de un nodo de interconexión a otro. Tan solo debe recordar que debe ajustar los valores de conexión, según sea adecuado.

Procedimiento

1. Con cualquier editor de texto, cree dos archivos:
   a. Un archivo de configuración de depuración, que se utiliza para especificar el registro para las interconexiones que funcionan en modalidad de depuración
   b. Un archivo de configuración estándar, que se utiliza para especificar el registro para las interconexiones que funcionan en modalidad de servicio/daemon
2. En cada archivo, utilice los componentes de registro de interconexión adecuados para dar instrucciones al sistema de cómo registrar en esa modalidad.
3. Guarde cada archivo. Es un buena idea guardar estos archivos en el mismo directorio en el que está ubicado el archivo de configuración de interconexiones.
4. En el archivo de configuración de interconexiones, añada una nueva sección denominada `[logging]`. Se trata de la sección donde especificará los nombres de los dos archivos de configuración que ha creado.
5. Bajo la cabecera de sección `[logging]`, añada los dos valores siguientes:
   a. `DebugConfigFile=`*`nombre de archivo de configuración de registro de depuración`*
   b. `ConfigFile=`*`nombre de archivo de configuración de registro de servicio/daemon`*

      Nota: Si no ha guardado los archivos de configuración de registro en el directorio donde está ubicado el archivo de configuración de interconexiones, asegúrese de indicar la vía de acceso completa para el archivo.
6. Guarde los cambios en el archivo de configuración de interconexiones.

Qué hacer a continuación

Antes de que surtan efecto estos cambios de registro, deberá detener y reiniciar todas las interconexiones que se ejecutan en cada nodo de interconexión afectado.

Archivos de registro de aplicación web de kit de herramientas de analista

Las aplicaciones web se basan en IBM WebSphere Liberty para comunicarse y conectar con IBM InfoSphere Identity Insight. Los archivos de registro de WebSphere Liberty incluyen información sobre los servicios web y las aplicaciones de kit de herramientas de analista, así como los errores de WebSphere Liberty. Si el sistema está habilitado para procesar sucesos (utilizando Event Manader), los errores de suceso también se registran en los archivos de registro de errores web.

El servidor de aplicaciones contiene dos archivos de registro primarios que se pueden utilizar para resolver problemas:

- Corrientes de errores y salida estándar, que se registran en el archivo denominado `console.log`
- Mensajes capturados por los componentes de registro, que se registran en el archivo denominado `messages.log`. Los mensajes grabados en este archivo contienen información adicional como indicación de fecha y hora de mensaje e ID de la hebra que ha grabado el mensaje.

Estos archivos de registro están ubicados en el siguiente directorio:

directorio_instalación`/wlp/usr/servers/iiServer/logs`

Los archivos de registro de WebSphere Liberty los configura un administrador del sistema o el servidor de aplicaciones.

Archivos de registro del Visualizador

El Visualizador tiene dos tipos de archivos de registro para ayudar a los usuarios a resolver problemas o mensajes del Visualizador: un archivo de registro local para cada cliente del Visualizador y archivos de registro para el servidor IBM WebSphere Application Server donde reside el Visualizador.

Registro de cliente del Visualizador

Puede configurar el Visualizador para que registre los errores, avisos y mensajes informativos que se producen en el cliente del Visualizador local. Cada estación de trabajo contiene un cliente de Visualizador, por lo que puede determinar si la estación de trabajo debe registrar o no los mensajes del Visualizador.

Por omisión, el registro del cliente de Visualizador está desactivado. El registro del Visualizador se activa o desactiva y se seleccionan los valores de registro en la ventana **Configurar preferencias de pantalla** del panel **Valores de registro**.

La ubicación del directorio del archivo de registro del cliente del Visualizador se determina cuando se activa el registro del cliente del Visualizador, especificando el nombre del directorio o navegando a un directorio existente. El nombre por omisión de los archivos de registro del cliente del Visualizador es visualizer.log. Se trata de un archivo de texto, que se puede visualizar utilizando cualquier editor de texto.

Los mensajes se añaden al archivo de registro existente, hasta que se alcanza el tamaño máximo de archivo. El tamaño máximo para un registro de cliente del Visualizador es 1 megabyte.

- Si el archivo de registro alcanza el tamaño máximo de archivo, el sistema crea otro archivo de registro de cliente del Visualizador en la ubicación del directorio configurado y empieza a registrar mensajes en ese archivo de registro.
- Una vez el segundo archivo de registro alcanza el límite de tamaño máximo, el sistema hace girar automáticamente el registro de mensajes al primer archivo de registro, hasta que está lleno.

Esta rotación automática de archivo de registro continúa cada vez que el archivo de registro actual alcanza el límite de tamaño de archivo. Cuando el sistema hace girar los archivos de registro, graba encima de los mensajes anteriores de ese archivo de registro.

Registro cronológico de WebSphere Application Server

El Visualizador depende de WebSphere Application Server para establecer comunicación y conectar con IBM InfoSphere Identity Insight. Los sucesos de los servicios Web se registran en los archivos de registro del servidor de aplicaciones, junto con los sucesos de la Consola de configuración y de los servicios Web, que también dependen de WebSphere Application Server.

El servidor de aplicaciones contiene dos archivos de registro primarios que se pueden utilizar para resolver problemas:

- Mensajes del sistema, que se registran en el archivo denominado `SystemOut.log`
- Mensajes de error del sistema, que se registran en el archivo denomiado `SystemErr.log`

Estos archivos de registro están ubicados en el siguiente directorio:

directorio_instalación`/logs/ewas`

Los archivos de registro de WebSphere Application Server son configurados por un administrador del sistema en el servidor de aplicaciones o mediante el programa de utilidad de configuración de IBM InfoSphere Identity Insight.

Activación del registro cronológico del cliente del Visualizador

Siga estas instrucciones para activar el registro cronológico del cliente del Visualizador y configurar los valores para el registro cronológico del cliente del Visualizador. Si realiza cambios en el registro cronológico o los valores del cliente del Visualizador, deberá reiniciar el Visualizador antes de que los cambios surtan efecto.

Acerca de esta tarea

Los valores de registro cronológico del cliente del Visualizador se configuran para cada cliente del Visualizador local. Si sigue estas instrucciones para activar el registro cronológico, sólo afectará a los valores para el cliente del Visualizador de esta máquina local.

Procedimiento

1. En el menú **Archivo**, seleccione **Preferencias**.
2. Seleccione el panel **Valores de registro**.
3. En el recuadro de selección **Activar registro cronológico** bajo **Valores de registro**, pulse el recuadro de selección para que aparezca una marca de selección en el recuadro. (El recuadro de selección debe contener una marca de selección cuando el registro cronológico está activado.)
4. Seleccione el nivel de detalle del registro cronológico en el recuadro de selección **Nivel de detalle del registro**:
   a. Seleccione **Errores** para registrar cronológicamente los sucesos del cliente del Visualizador que han causado mensajes de error. Este nivel de registro cronológico es el nivel de registro cronológico por omisión cuando se activa el registro cronológico. Este nivel de registro proporciona un buen equilibrio de rendimiento e información de registro cronológico.
   b. Seleccione **Avisos** para registrar cronológicamente los sucesos del cliente del Visualizador que han causado avisos o mensajes de error.

c. Seleccione **Informativo** para registrar cronológicamente los sucesos del cliente del Visualizador que han causado mensajes informativos, avisos o mensajes de error.

d. Seleccione **Depuración** para registrar cronológicamente mensajes de rastreo para todos los sucesos del Visualizador. Normalmente, este nivel de registro cronológico sólo se establece cuando se soluciona el problema de un error específico del Visualizador, con frecuencia con ayuda del soporte técnico de IBM. El nivel de registro cronológico de depuración puede generar un gran volumen de mensajes de rastreo, que son útiles para solucionar problemas pero pueden afectar negativamente al rendimiento del Visualizador para operaciones normales.

5. En el campo **Vía de acceso al directorio de archivos de registro**, especifique la vía de acceso completa del directorio y el nombre para el archivo de registro del cliente del Visualizador o navegue hasta un directorio existente.
   - Especifique la vía de acceso completa del directorio para el archivo del registro de cliente del Visualizador
   - O bien, navegue hasta un directorio existente en la máquina local para seleccionarlo como directorio de registro cronológico del cliente del Visualizador.
6. Pulse el botón **Enviar** para guardar los cambios.
7. Reinicie el Visualizador finalizando la sesión del Visualizador y volviéndola a iniciar. Los cambios en los valores de registro cronológico para el cliente del Visualizador no surten efecto hasta que se reinicia el Visualizador.

Desactivación del registro cronológico del cliente del Visualizador

Siga estas instrucciones para desactivar el registro del cliente del Visualizador, especialmente si ha activado el registro cronológico a nivel de depuración para solucionar un problema específico del Visualizador. Aunque los archivos de registro pueden ayudar a resolver problemas, algunos niveles de registro, como el nivel de registro cronológico de depuración, pueden afectar al rendimiento del Visualizador. Si realiza cambios en el registro cronológico o los valores del cliente del Visualizador, deberá reiniciar el Visualizador antes de que los cambios surtan efecto.

Antes de empezar

Asegúrese de que ha iniciado la sesión en una sesión activa del Visualizador.

Acerca de esta tarea

Los valores de registro cronológico del cliente del Visualizador se configuran para cada cliente del Visualizador local. Si sigue estas instrucciones para desactivar el registro cronológico, sólo afectará a los valores para el cliente del Visualizador de esta máquina local.

Procedimiento

1. En el menú **Archivo**, seleccione **Preferencias**.
2. Seleccione el panel **Valores de registro**.
3. En el recuadro de selección **Activar registro cronológico** bajo **Valores de registro**, pulse el recuadro de selección para que no aparezca ninguna marca de selección en el recuadro. (El recuadro de selección debe estar vacío cuando el registro cronológico está desactivado.) Cuando se desactiva el registro cronológico, los valores de configuración del registro cronológico se inhabilitan.

4. Pulse el botón **Enviar** para guardar los cambios.
5. Reinicie el Visualizador finalizando la sesión del Visualizador y volviéndola a iniciar. Los cambios en los valores de registro cronológico para el cliente del Visualizador no surten efecto hasta que se reinicia el Visualizador.

Archivos de registro de Event Manager

Si el sistema está habilitado para procesar sucesos utilizando Event Mananger, el sistema crea un archivo de registro que contiene información del programa sobre sucesos. Los mensajes de error del procesador de sucesos externo se registran en los archivos de registro de errores de WebSphere Liberty. Los errores de interconexion estándares eoncontrados durante el proceso de interconexión se registran en los archivos de registro de interconexión, basados en la configuración de registro de interconexión actual.

El servidor de aplicaciones contiene los archivos de registro primarios que se pueden utilizar para resolver problemas y mensajes de Event Manager:

- Información de programa de Event Manager, que se encuentra en el archivo denominado `gem_prog_`*`date`*`.log`
- Mensajes de error de Event Manager, que se registran en el directorio *`directorio_instalación`*`/logs`.

Los mensajes se añaden a los registros de datos y de programa según la fecha del suceso. Estos archivos de registro se deberían revisar periódicamente, y después archivar o suprimir, de acuerdo con las políticas de su organización.

Estos archivos de registro están ubicados en el siguiente directorio:

`directorio_instalación``/logs`

Rastreo

Los rastreos son registros del proceso de componentes o transacciones. La información recopilada de un rastreo se puede utilizar para evaluar problemas y rendimiento. En IBM InfoSphere Identity Insight, los rastreos forman parte del registro de componentes de depuración.

Obtención de arreglos

Es posible que esté disponible un arreglo del producto para resolver el problema. Puede descargar los arreglos del producto siguiendo estos pasos.

Procedimiento

1. Determine el arreglo que necesita. Vaya al documento *Fixes by version for IBM InfoSphere Identity Insight* ubicado en http://www-1.ibm.com/support/docview.wss?rs=2216&uid=swg27008307 y pulse en uno de los arreglos listados para ver más información acerca de todos los arreglos de esa versión en particular. (Los arreglos se listan en formato de versión, release, modificación.)
2. Descargue el arreglo. En la lista de arreglos, pulse en el enlace Descargar información. En la sección “Descargar paquete” (Download package), pulse en el enlace “Descargar opciones” (Download Options) para el entorno.
   - Si se visualiza la pantalla de acuerdo de licencia de IBM, lea la información y pulse **Acepto** (I Accept) si acepta el acuerdo y desea continuar descargando el arreglo.
   - Si pulsa **No acepto** (I Do Not Accept), el arreglo no se descargará.

En las ventanas **Descarga de archivos** (File Download), pulse **Guardar** (Save) y guarde el archivo del arreglo localmente.

3. Aplique el arreglo. Vaya a la ubicación en la que se ha guardado el archivo del arreglo. Extraiga o desempaquete (unzip) los archivos del archivo empaquetado del arreglo y siga las instrucciones del documento "readme" para instalar el arreglo.

Más información sobre arreglos y actualizaciones de servicio

Si encuentra un problema al utilizar IBM InfoSphere Identity Insight, primero compruebe la lista de actualizaciones recomendadas para verificar que el software tiene el nivel de mantenimiento más reciente. A continuación, compruebe la lista de problemas arreglados para ver si IBM ya ha publicado un arreglo individual para solucionar el problema.

Se publican arreglos individuales con la frecuencia necesaria para solucionar defectos en el producto. Además periódicamente se publican dos tipos de grupos de arreglos acumulativos, denominados fix packs o refresch packs, a fin de mantener a los usuarios al último nivel de mantenimiento.Debe instalar estos paquetes de actualización lo antes posible para evitar problemas.

Para recibir notificaciones semanales sobre arreglos y actualizaciones, suscríbase a las actualizaciones por correo electrónico My Support.

En la tabla siguiente se describen las características de cada vehículo de distribución de mantenimiento.

Tabla 39. Características de un arreglo, de un fix pack y de un refresh pack

Nombre	Características
Arreglo	• Se publica un solo arreglo entre actualizaciones para solucionar un problema específico, por ejemplo PQ79582. • Después de instalar un arreglo, pruebe las funciones a las que afecta el componente arreglado.
Fix pack	• Un fix pack acumulativo contiene todos los arreglos que se han publicado desde el fix pack o refresh pack anterior; un fix pack también puede contener nuevos arreglos. • Los fix packs aumentan el nivel de modificación del producto y se denominan según el mismo, por ejemplo 4.0.2. • Un fix pack puede actualizar componentes específicos o puede actualizar toda la imagen del producto. • Durante la instalación de fix pack, todos los arreglos aplicados anteriormente se desinstalan automáticamente. • Después de instalar un refresh pack, debe realizar una prueba de regresión de todas las funciones críticas. • Los dos fix packs más recientes están disponibles para su descarga (por ejemplo, 4.0.2 y 4.0.1). Los fix packs anteriores no están disponibles.

Tabla 39. Características de un arreglo, de un fix pack y de un refresh pack (continuación)

Nombre	Características
Refresh pack	• Un fix pack acumulativo contiene todos los arreglos que se han publicado desde el fix pack o refresh pack anterior, así como los nuevos arreglos. • Un refresh pack suele contener una nueva función, además de arreglos, y actualiza la imagen entera del producto. • Los refresh packs aumentan el nivel de modificación del producto y se denominan según el mismo, por ejemplo 4.0.2. • Durante la instalación de fix pack, todos los arreglos aplicados anteriormente se desinstalan automáticamente. • Después de instalar un refresh pack, debe realizar una prueba de regresión de todas las funciones críticas.

Actualizaciones de servicio

Las actualizaciones de servicio ayudan a conservar el sistema en el nivel de mantenimiento de software más reciente.

Puede acceder a las últimas actualizaciones de servicio en la página del centro de soporte del producto IBM InfoSphere Identity Insight. El URL es

```
https://www-947.ibm.com/support/entry/portal/Overview/Software/
Information_Management/InfoSphere_Identity_Insight
```

Para determinar el nivel de servicio de interconexión del sistema:

1. En una línea de mandatos del nodo de interconexión, emita el mandato siguiente:

   ```
   pipeline
   ```

2. La versión de la interconexión aparece en la primera línea. El número determina el nivel de servicio.

Para determinar el nivel de servicio de la Consola de configuración en el sistema:

1. Inicie la Consola de configuración.
2. Inicie la sesión en la Consola de configuración.
3. Seleccione **Acerca de** en el menú superior.
4. Observe el número de versión que se muestra en la ventana Acerca de. El número determina el nivel de servicio.

Cómo ponerse en contacto con el centro de soporte de software de IBM

El centro de soporte de software de IBM proporciona ayuda para los defectos del producto.

Antes de empezar

Antes de ponerse en contacto con el centro de soporte de software de IBM, la compañía debe disponer de un contrato de mantenimiento de software de IBM activo y el usuario debe estar autorizado para enviar problemas a IBM. Para obtener información acerca de los tipos de contratos de mantenimiento disponibles, consulte "Enhanced Support" en la publicación *Software Support Handbook* en

techsupport.services.ibm.com/guides/services.html

Acerca de esta tarea

Complete los pasos siguientes para ponerse en contacto con el centro de soporte de software de IBM con un problema:

Procedimiento

1. Defina el problema, reúna la información de fondo, y determine la gravedad del problema. Para obtener ayuda, consulte "Contacting IBM" en la publicación *Software Support Handbook* en techsupport.services.ibm.com/guides/beforecontacting.html
2. Reúna la información de diagnóstico.
3. Cuando vaya a notificar el problema, tenga preparada la información siguiente para ayudar al centro de soporte de software de IBM:
   - Nombre y versión del producto
   - Tipo y versión de la base de datos
   - Nombre y versión del sistema operativo
4. Envíe el problema al centro de soporte de software de IBM de una de las maneras siguientes:
   - De forma electrónica: pulse **Enviar y hacer seguimiento de problemas** (Submit and track problems) en el sitio Web del centro soporte de software de IBM, situado en http://www.ibm.com/software/support/probsub.html
   - Por teléfono: para obtener el número de teléfono al que debe llamar en su país, vaya a la página Contacts de la publicación IBM Software Support Handbook en techsupport.services.ibm.com/guides/contacts.html

Qué hacer a continuación

Si envía un problema por un defecto de software o porque falta documentación, o ésta no es exacta, el centro de soporte de software de IBM crea un APAR (informe autorizado de análisis de programa). El APAR describe del problema con detalle. Siempre que es posible, el centro de soporte de software de IBM proporciona un método alternativo que se puede implementar hasta que se resuelve el APAR y se entrega un arreglo. IBM publica los APAR resueltos en el sitio web del centro de soporte diariamente, por lo que otros usuarios que experimenten el mismo problema pueden beneficiarse de la misma resolución.

Avisos

Esta información se ha desarrollado para productos y servicios que se comercializan en los EE.UU. IBM InfoSphere Identity Insight Versión 9.0.

Es posible que IBM no comercialice en todos los países algunos productos, servicios o características descritos en este manual. Consulte al representante local de IBM para obtener información sobre los productos y servicios que actualmente pueden adquirirse en su zona. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar ni implicar que sólo pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes en tramitación que afecten al tema tratado en este documento. La posesión de este documento no otorga ninguna licencia sobre dichas patentes. Puede realizar consultas sobre licencias escribiendo a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE.UU.

Para realizar consultas sobre licencias relativas a información de doble byte (DBCS), póngase en contacto con el Departamento de la propiedad intelectual de IBM de su país o envíe las consultas por escrito a:

IBM World Trade Asia Corporation
Licensing 2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japón

El párrafo siguiente no es aplicable al Reino Unido ni a ningún país en donde tales disposiciones sean incompatibles con la legislación local:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍA DE NINGUNA CLASE, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN DETERMINADO. Algunos estados no permiten la exclusión de garantías expresas o implícitas en determinadas transacciones, por lo que es posible que esta declaración no sea aplicable en su caso.

Esta publicación puede contener inexactitudes técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; dichos cambios se incorporarán a las nuevas ediciones de la publicación. IBM puede efectuar, en cualquier momento y sin previo aviso, mejoras y cambios en los productos y programas descritos en esta publicación.

Las referencias hechas en esta publicación a sitios Web que no son de IBM se proporcionan sólo para la comodidad del usuario y no constituyen un aval de esos sitios Web. La información contenida en esos sitios Web no forma parte de la información del presente producto IBM y el usuario es responsable de la utilización de dichos sitios Web.

IBM puede utilizar o distribuir cualquier información que se le facilite de la manera que considere adecuada, sin contraer por ello ninguna obligación con el remitente.

Los licenciatarios de este programa que deseen obtener información sobre él con el fin de habilitar: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) el uso mutuo de la información intercambiada, deben ponerse en contacto con:

IBM Corporation
J46A/G4
555 Bailey Avenue
San José, CA 95141-1003
EE.UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones apropiados, incluido en algunos casos el pago de una tarifa.

El programa bajo licencia descrito en este documento y todo el material bajo licencia asociado a él, los proporciona IBM según los términos del Acuerdo de Cliente de IBM, el Acuerdo Internacional de Programas Bajo Licencia de IBM o cualquier acuerdo equivalente entre el usuario e IBM.

Los datos de rendimiento contenidos en este documento se obtuvieron en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Algunas mediciones pueden haberse realizado en sistemas experimentales y no es seguro que estas mediciones sean las mismas en los sistemas disponibles comercialmente. Además, algunas mediciones pueden haberse calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios del presente manual deben verificar los datos aplicables para su entorno específico.

La información referente a productos que no son de IBM se ha obtenido de los proveedores de esos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la exactitud del rendimiento, la compatibilidad ni ninguna otra afirmación referente a productos que no son de IBM. Las preguntas sobre las prestaciones de productos que no son de IBM deben dirigirse a los proveedores de esos productos.

Todas las declaraciones relativas a la dirección o a la intención futura de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente metas y objetivos. Esta información está destinada solamente a la planificación. La información aquí contenida está sujeta a cambios antes de que los productos descritos estén disponibles.

Este manual contiene ejemplos de datos e informes que se utilizan en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos

incluyen nombres personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con nombres y direcciones utilizados por una empresa real es totalmente fortuita.

LICENCIA DE COPYRIGHT:

Este manual contiene programas de aplicaciones de ejemplo escritos en lenguaje fuente, que muestran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo como desee, sin pago alguno a IBM, con la intención de desarrollar, utilizar, comercializar o distribuir programas de aplicaciones de acuerdo con la interfaz de programación de aplicaciones correspondiente a la plataforma operativa para la que están escritos los programas de ejemplo. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por lo tanto, IBM no puede asegurar ni implicar la fiabilidad, utilidad o función de estos programas.

Si visualiza la copia software de esta información, puede que no aparezcan fotografías e ilustraciones en color.

Marcas registradas

Las marcas registradas de IBM y determinadas marcas registradas no de IBM están marcadas en su primera aparición en esta información con el símbolo correspondiente.

IBM, el logotipo de IBM e ibm.com son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países. Si estos y otros términos registrados de IBM están marcados en su primera aparición en esta información con un símbolo de marca registrada (® o ™), estos símbolos indican las marcas registradas de derecho consuetudinario o registradas en los EE.UU., propiedad de IBM en el momento en que se publicó esta información. Tales marcas registradas también pueden ser de derecho consuetudinario o registradas en otros países. Hay una lista actual de marcas registradas de IBM disponible en la web en "Copyright and trademark information" en www.ibm.com/legal/copytrade.shtml.

Los siguientes términos son marcas registradas de otras empresas:

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en Estados Unidos y/o en otros países.

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, y Pentium son marcas registradas de Intel Corporation o sus empresas subsidiarias en Estados Unidos y en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en los EE.UU. y/o en otros países.

Java y todas las marcas registradas basadas en Java son marcas registradas de Oracle Corporation en EE.UU. y/o en otros países.

Otros nombres de empresas, productos o servicios, pueden ser marcas registradas o marcas de servicio de otras empresas.

Índice

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Impreso en España

SC19-2870-01